169960/EU XXVII. GP
Eingelangt am 22/01/24

Council of the
European Union

Brussels, 22 January 2024
(OR. en)

5454/24
ADD 1

DATAPROTECT 23
JAI 62
RELEX 42

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	15 January 2024
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	SWD(2024) 3 final
Subject:	COMMISSION STAFF WORKING DOCUMENT Country reports on the functioning of the adequacy decisions adopted under Directive 95/46/EC Accompanying the document Report from the Commission to the European Parliament and the Council on the first review of the functioning of the adequacy decisions adopted pursuant to Article 25(6) of Directive 95/46/EC

Delegations will find attached document SWD(2024) 3 final.

Encl.: SWD(2024) 3 final

www.parlament.gv.at

EUROPEAN
COMMISSION

Brussels, 15.1.2024
SWD(2024) 3 final

COMMISSION STAFF WORKING DOCUMENT

Country reports on the functioning of the adequacy decisions adopted under Directive 95/46/EC

Accompanying the document

Report from the Commission to the European Parliament and the Council

on the first review of the functioning of the adequacy decisions adopted pursuant to Article 25(6) of Directive 95/46/EC

{COM(2024) 7 final}

www.parlament.gv.at

TABLE OF CONTENTS

I. ANDORRA **2**

II. REPUBLIC OF ARGENTINA **22**

III. CANADA **56**

IV. FAROE ISLANDS **96**

V. BAILIWICK OF GUERNSEY **123**

VI. ISLE OF MAN **155**

VII. STATE OF ISRAEL **182**

VIII. JERSEY **215**

IX. NEW ZEALAND **246**

X. SWITZERLAND **279**

XI. EASTERN REPUBLIC OF URUGUAY **314**

I. ANDORRA

1. RULES APPLYING TO THE PROCESSING OF PERSONAL DATA

1.1. Relevant developments in the data protection framework of Andorra

The Commission adopted the adequacy decision for Andorra on 19 October 2010[1], after having received the opinion of the Article 29 Working Party on 1 December 2009[2]. The decision found that, for the purposes of Article 25(2) of Directive 95/46/EC (Data Protection Directive)[3], Andorra provided an adequate level of protection for personal data transferred from the EU.

At the time of the adoption of the adequacy decision, the legislative framework for the protection of personal data in Andorra consisted of the Qualified Law 15/2003 of 18 December 2003 on the protection of personal data[4] (LQPDP), as further implemented through two Decrees of 1 July 2004[5]. The LQPDP and its implementing regulations were largely based on the standards of the former Data Protection Directive of the EU.

In November 2020, Andorra initiated a process to modernise the LQPDP, which led to the adoption of the new Qualified Law 29/2021 on the protection of personal data (Data Protection Act)[6] that entered into force in May 2022[7]. As explained in more detail below, the Data Protection Act is closely aligned with Regulation (EU) 2016/679 (GDPR)[8] in its structure and main components, and significantly strengthens the Andorran data protection framework.

As regards the scope of application, the LQPDP already followed the same approach as the Data Protection Directive, while the new Data Protection Act brings the Andorran data protection framework even closer to the GDPR. It not only defines the key notions of 'personal data'[9], 'data subject'[10] and 'processing'[11] in the same way as the GDPR, but also

---

[1] Commission Decision 2010/625/EU of 19 October 2010 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Andorra, OJ L 277, 21.10.2010, page 27.

[2] Opinion 7/2009 of 1 December 2009, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp166_en.pdf.

[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[4] Available at: https://apda.ad/sites/default/files/2018-10/llei_qualificada_de_proteccio_de_dades_personals_-_en.pdf - English version. All the references to the LQPDP have as a source the translation available on the website of the Andorran Data Protection Authority.

[5] The first Decree approving the Regulations of the Andorran Data Protection Agency, and the second Decree the Regulations of the Public Register for the Inscription of Personal Data Files. Both decrees were significantly updated through the decree of 9 June 2010 approving the Regulations of the Andorran Data Protection Agency (DPD), available at: https://www.apda.ad/sites/default/files/2018-10/decret_reglament_agencia_andorrana_proteccio_dades_-_en.pdf - English version.

[6] Act No. 80 of 7 June 2020 on the protection of personal data (Data Protection Act).

[7] According to its final provision, the Act entered into force six months after its publication in the official gazette, which was on 17 November 2021. The Data Protection Act, as published in the official gazette, is available at: https://www.bopa.ad/bopa/033119/Pagines/CGL20211115_08_58_32.aspx.

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[9] Article 4(1) Data Protection Act.

[10] Article 4(1) Data Protection Act.

[11] Article 4(3) Data Protection Act.

introduces definitions for the notions of 'profiling'[12] and 'pseudonymization'[13] that are identical to the ones used in the GDPR. The Data Protection Act also provides for a more comprehensive protection of personal data by no longer allowing certain specific data protection regulations to prevail over its general rules in case of conflict[14] and by removing certain partial exclusions that existed under the LQPDP[15].

At the time of the adoption of the Commission adequacy decision, the Andorran data protection framework already contained all the basic data protection principles (i.e., the principles of purpose limitation, data quality and proportionality, transparency, fairness, data minimisation, accuracy, storage limitation, and integrity and confidentiality). Building on that foundation, the Data Protection Act reinforces some of the existing principles, better aligning them with the GDPR.

In particular, as regards the principle of lawfulness, the Data Protection Act specifies and strengthens the notion of consent by adding a definition of this term in its Article 4(2) that is identical to the one used in the GDPR, i.e., requiring that, in addition to being freely given, specific and informed, consent must be unambiguous and expressed by a clear affirmative action[16]. Moreover, the Data Protection Act fully aligns the grounds that are available for processing with those listed in Article 6(1) GDPR[17]. Similarly, the Data Protection Act reinforces the existing transparency requirements by requiring the information of the data subject also in situations where data is not collected directly from the data subject[18].

The principle of data security has been strengthened in the Data Protection Act with respect to the handling of data breaches. Under the LQPD and its implementing regulations, there was no obligation to notify data breaches affecting personal data. The Data Protection Act establishes a duty for data controllers to notify the supervisory authority (*l'Agencia Andorrana de Protecció de Dades*, APDA) without undue delay and, if possible, within a maximum period of 72 hours, after becoming aware of a data breach, unless it is unlikely that the data breach constitutes a risk to the rights and freedoms of individuals[19].

Finally, the Data Protection Act includes several provisions that give effect to the principle of accountability. Under the LQPDP, the APDA had already introduced some aspects of this principle through a guideline, including the need to carry out impact assessments, keep

[12] Article 4(5) Data Protection Act.
[13] Article 4(8) Data Protection Act.
[14] The LQPDP contained a provision from which it followed that specific regulations covering public registries were to be treated as lex specialis and that, in case of contradiction with the general rules of the LQPDP, such specific regulations prevailed over those rules, see Article 8 LQPDP. The Data Protection Act does not contain such a provision.
[15] Contrary to the current LQPDP, the Data Protection Act does not contain a partial exclusion from its scope of application for data of natural persons linked to their business, professional or commercial activity, see Article 2(2) of the Data Protection Act.
[16] Article 17 LQPDP provided that the processing of personal data may only be carried out with the unequivocal consent of the data subject. Consent is defined in Article 5(2) DPD as "any free, specific, clear, certain and informed declaration of will, through which the person concerned consents to the processing of his/her personal data".
[17] Article 6 Data Protection Act.
[18] Article 17 Data Protection Act. Where personal data have not been obtained from the data subject, Article 17(5) of the Data Protection Act lists some exceptions to the transparency requirements. These exceptions are similar to the ones listed in Article 14(5) GDPR.
[19] Article 36 Data Protection Act.

records of processing activities and appoint a data protection officer in certain cases[20]. Chapter IV of the Data Protection Act anchors these and other accountability requirements more firmly into legislation, in particular by imposing an obligation to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the law[21], to implement the principles of data protection by design and default[22], to carry out data protection impact assessments[23], to keep records of processing and make them available to the APDA upon request[24], and to appoint a data protection officer in certain situations[25].

Importantly, special categories of personal data (or sensitive data) benefit from enhanced protection under the Data Protection Act. The Act expands the current notion of sensitive data to cover all the categories of personal data that are considered 'sensitive' under the GDPR[26]. In particular, the categories of genetic and biometric data, data revealing racial origin or philosophical beliefs and data concerning sexual life have been added to the list of special categories[27]. Moreover, the Data Protection Act imposes a general prohibition to process sensitive data and the processing of sensitive data is only allowed in a limited number of situations, corresponding to the situations in which the processing of sensitive data is allowed under the GDPR[28].

The Data Protection Act also modernises and strengthens the existing provisions on data protection rights. In particular, the provisions on the right to rectification[29], the right to erasure[30] and the right to object[31] have been fully aligned with the GDPR. For example, the right to erasure now includes an obligation for the controller to take reasonable steps to inform other controllers that are processing the relevant information that the data subject has requested the erasure of his data[32]. The right to object is no longer limited to personal data not collected directly from the data subject, and a specific right to object to direct marketing has been introduced[33]. Moreover, the right of access not only requires the controller to confirm,

---

[20] Available at: https://www.apda.ad/sites/default/files/2018-11/Gu%C3%ADa%20adaptaci%C3%B3%20al%20RGPD%20a%20Andorra.pdf.
[21] Article 27 Data Protection Act.
[22] Article 28 Data Protection Act.
[23] Article 32 Data Protection Act.
[24] Article 34 Data Protection Act.
[25] Article 38 Data Protection Act.
[26] The LQPDP already offered additional protection to sensitive data, which it defined as 'data referring to political opinions, religious beliefs, membership of political or trade union organisations, health, sex life or ethnic origin of the interested parties' (Article 3(11) LQPDP).
[27] Article 9(1) Data Protection Act.
[28] The processing of special categories of personal data is allowed for instance with the data subject's explicit consent, where processing is necessary to fulfil a legal obligation of the controller in the field of social security law, where processing is necessary to protect the vital interest of the data subject, or where processing is necessary for reasons of substantial public interest, see Article 9 Data Protection Act.
[29] Article 19 Data Protection Act.
[30] Article 20 Data Protection Act.
[31] Article 24 Data Protection Act.
[32] Article 20(3) Data Protection Act. Article 20(4) contains exceptions to the right of erasure, i.e. to the extent that processing is necessary for exercising the right of freedom of expression and information; for compliance with a legal obligation; for the establishment, exercise or defence of legal claims; or for archiving purposes, historical, statistical or scientific purposes (in so far as erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing). These exceptions are similar to the ones listed in Article 17(3) GDPR.
[33] Article 24(2) Data Protection Act.

upon request of an individual, whether or not personal data concerning him/her is being processed, and, where that is the case, give access to that data (as was already the case under the LQPDP), but also requires the controller to provide further information, e.g., the purpose of processing, the categories of personal data that is being processed, the source of personal data, information on the retention period, the right to lodge a complaint with the APDA, the existence of other rights, the fact that the controller intends to transfer the data to third countries, and the existence of automated decision-making[34].

In addition to the strengthening of existing rights, new rights have been introduced in the Data Protection Act, again mirroring the corresponding rights under the GDPR. In particular, the Data Protection Act provides for specific safeguards and rights for individuals in the context of automated decision-making. First, it requires controllers to provide individuals with information on the existence of automated decision-making when collecting their personal data[35]. Second, when responding to an individual's exercise of the right of access, controllers are required to provide information on the existence of automated decision-making, as well as meaningful information about the logic involved and the envisaged consequences of such processing for the data subject[36]. Third, the Data Protection Act introduces the right not to be subject to a decision based solely on automated processing. Automated decision-making may only take place under certain conditions, e.g., only where authorised by law or based on the data subject's explicit consent, and subject to specific safeguards, e.g., informing the individual about the processing, the logic involved and the envisaged consequences[37]. In case of data processing intended for profiling, the controller must implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision. The Data Protection Act also introduces a right to the restriction of processing[38] and a right to data portability[39], which each correspond to the relevant right in the GDPR.

In terms of restrictions to the exercise of data subject rights, the Data Protection Act clarifies, in identical terms as the GDPR, the conditions for the application of such restrictions by introducing a provision which explicitly sets out that restrictions to data subject rights are only allowed when they respect the essence of the fundamental rights and freedoms and are a necessary and proportionate measure in a democratic society to safeguard certain important objectives of general public interest such as national security, public security and the prevention, investigation, detection or prosecution of criminal offences[40].

As regards the international transfer of personal data, the Data Protection Act introduces several changes to the existing transfer regime, putting in place a system that is very similar to the rules on international transfers set out in Chapter V of the GDPR in terms of structure and requirements.

[34] Article 18 Data Protection Act.
[35] Articles 16(j) and 17(2) (e) Data Protection Act.
[36] Article 18(1) (h) Data Protection Act.
[37] Article 25 Data Protection Act.
[38] Article 22 Data Protection Act.
[39] Article 23 Data Protection Act.
[40] Article 26 Data Protection Act.

As a general principle, international transfers may not be carried out when the third country does not establish, in its current regulations, a level of protection for personal data at least equivalent to that established under the Data Protection Act[41]. Furthermore, when transferring data to a third country, it must be ensured that the level of protection of natural persons established by the Act is not diminished[42]. The Data Protection Act stipulates that whether a third country offers an equivalent level of protection will be determined on the basis of three (alternative) criteria: whether the third country benefits from an adequacy decision from the European Commission, whether the third country has effectively submitted itself to the provisions of the modernised Convention 108 (Convention 108+) and whether the third country is an EU Member State[43].

International transfers to third countries that do not offer an equivalent level of protection are allowed where the controller or processor has provided appropriate safeguards, and on the condition that enforceable data subject rights and effective legal remedies are available to the data subject[44]. The existence of such appropriate safeguards, enforceable rights and effective remedies will be evaluated by the APDA taking into account a set of factors that are identical to the factors listed in Article 45(2) GDPR. The instruments that can be used to provide for appropriate safeguards are legally binding arrangements, binding corporate rules, standard contractual clauses, whether adopted by the European Commission or the APDA, codes of conduct and certification mechanisms in conformity with EU data protection rules[45].

Finally, the Data Protection Act reduces and clarifies the derogations for specific situations, i.e., the situations in which transfers can take place to non-adequate third countries and without the existence of appropriate safeguards. The new derogations are laid down in Article 45 of the Data Protection Act and closely resemble the derogations listed in Article 49 GDPR[46]. The Data Protection Act stipulates that they must be interpreted restrictively[47].

Finally, the Andorran transfer regime has also been amended so that the above-mentioned requirements cover not only transfers of personal data to third countries, but also to international organisations[48].

1.2. Oversight, enforcement and redress

The independent authority that is charged with oversight and enforcement under the Data Protection Act is the APDA[49]. The Agency oversees compliance with the Data Protection Act by both private entities and by Andorran public authorities[50]. It has the power to carry out

[41] Article 42(1) Data Protection Act.
[42] Article 42(2) Data Protection Act.
[43] Article 43 Data Protection Act.
[44] Article 44 Data Protection Act.
[45] Article 44(3) Data Protection Act. So far, the APDA has not adapted a set of standard contractual clauses.
[46] For instance, transfers to third countries or international organisations can take place when the data subject has explicitly consented to the proposed transfer, when the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request, or when the transfer is necessary for important reasons of public interest.
[47] Article 45(4) Data Protection Act.
[48] Article 42(1) Data Protection Act.
[49] Article 46 Data Protection Act.
[50] Article 48 Data Protection Act.

inspections and impose sanctions for infringements of the Act[51]. In addition, it carries out a number of additional tasks, such as answering questions from public authorities and private individuals or entities about the application of the data protection legislation, giving its opinion on current and future data protection legislation, raising public awareness about data protection, dealing with complaints it receives, and preparing annual reports on its activities[52]. In carrying out its investigations, the Agency has access to any relevant information, as well as to the premises where processing operations are carried out, including computer systems or other resources used in data processing[53]. It may also compel the production of evidence[54].

The Data Protection Act integrates in its Chapter VII the provisions of the DPD concerning the APDA without significantly changing the composition, tasks and powers of the agency and the statutory safeguards for its independence[55]. It clarifies some aspects, including the regime on incompatible activities applicable to the Head of the Agency and the inspectors as well as on international cooperation. Furthermore, the Data Protection Act establishes a specific sanctioning regime for public authorities, including reprimands and disciplinary procedures to deal with staff liability[56]. In addition, the decisions concerning public authorities and bodies are made public through publication on the APDA's website[57].

As regards possibilities for individuals to obtain redress, the Andorran system continues to offer various avenues, including the possibility to lodge a complaint with the APDA[58], obtain judicial redress directly against controllers and processors (both private operators and public controllers)[59] and obtain compensation for damages[60].

---

[51] Article 67 Data Protection Act.
[52] Article 50 Data Protection Act.
[53] Article 62 Data Protection Act. During an inspection, the APDA's inspectors may also carry out audits of the computer systems of the controller or processor to verify that they comply with the requirements of the LQPDP.
[54] Article 62 Data Protection Act.
[55] The APDA is formed as a public authority with its own legal personality, independent of other public authorities, and with full capacity to operate (Article 46 Data Protection Act). It is composed of the Head of the APDA and two inspectors. Both the Head and the inspectors are appointed by the Parliament by a qualified (2/3) majority for a term of four years. The appointment may be renewed at the end of each period. The APDA is financed exclusively from the budget appropriations established each year for its functioning in the general budget of the Parliament (Article 47 Data Protection Act). Regarding private entities, the APDA has the power to impose fines, issue binding orders as well as non-binding instructions and recommendations (Article 67 Data Protection Act). Furthermore, the APDA may bring and decide disciplinary proceedings against public entities, including state-owned companies (Article 74(3) Data Protection Act). Under the Data Protection Act, the amount of the maximum fine will depend on whether the violation is designated as a 'very serious', 'serious' or 'minor' offence, with fines ranging from € 500 minimum for a minor offence to € 100 000 maximum for a very serious offence (see Article 73 Data Protection Act). Although public authorities cannot be sanctioned with a fine, the APDA can issue instructions, recommendations and binding orders against those authorities. In addition, it can urge the initiation of disciplinary proceedings against them and verify the effectiveness of such proceedings (Article 74 Data Protection Act).
[56] Article 74 Data Protection Act.
[57] Article 74(5) Data Protection Act.
[58] Article 61 Data Protection Act.
[59] Article 41 of the Andorran Constitution stipulates that fundamental rights, including the right to privacy, are protected by regular courts through urgent and preferential proceedings established by law that, in all cases, involve court hearings at two levels. Moreover, the Andorran legal system provides for an extraordinary procedure of appeal (empara) before the Constitutional Court (Article 42 and 102 of the Andorran Constitution), which becomes available after the applicant has exhausted the previously mentioned urgent and preferential procedure before the regular courts. The remedies that can be obtained through empara are the establishment of the violation and its cessation.

Despite its relatively small office, the APDA plays an active role, both when it comes to its engagement with stakeholders and exercising its oversight role.

Since the adoption of the adequacy decision, the APDA has issued several general and specific guidance documents, which cover topics such as the application of the GDPR in Andorra, data processing in the context of COVID-19, the processing of biometric data, international transfers after Brexit, the principle of proportionality, transparency obligations, cookies and obligations of the processor[61]. Furthermore, the APDA has published several guidance documents that aim to inform the general public about data protection, covering topics such as teleworking, smart devices, data subject rights, collection of COVID-19 data in restaurants and instant messaging apps[62]. In addition, the APDA has created several templates and standard forms to support compliance with data protection rules and the exercise of individual rights, including a consent form, templates for the exercise of data subject rights, a model complaint form and an international data transfer form[63].

Its annual reports show that the APDA handles a number of individual complaints every year. For example, in 2020 it received nineteen complaints for alleged infringements of the LQPDP, in 2019 it received thirteen such complaints, while in 2018 it received sixteen such complaints. These complaints have on various occasions led to enforcement actions. For example, during the period 2019-2020, in thirteen cases the APDA's inspection service decided to carry out an inspection to establish whether a violation of the rights enshrined in the LQPDP and the DPD had taken place. In all of these thirteen cases a violation was detected and based on the severity of the violation and the number of affected data subjects, the APDA issued binding orders to remedy that violation. According to information received, in one case, a fine was imposed, due to the seriousness of the detected violation and the fact that the violation was a repeated offence[64].

Finally, the APDA fulfils an important consultative function. Every year it responds to numerous queries made by natural or legal persons, as well as public authorities, with regard to issues that have arisen in the context of their processing activities. For example, in 2020 a total of 2116 of queries were submitted to the ADPA, in 2019 it received 1763 queries, while in 2018 it received 1747 queries. The APDA also actively engages with the general public and stakeholders. For example, in 2020, the APDA engaged in outreach activities to disseminate information about the processing of personal data in the context of the COVID-19 pandemic, aimed both at citizens and those responsible for such processing activities[65]. In the same year, the APDA participated in four television and three radio broadcasts[66]. The APDA also

[60] They can also do so based on the causes for action, set out in in Law 30/2014 on civil protection of the rights to privacy, honour and self-image. This law offers remedies to "illegitimate interference" with the constitutionally protected rights to privacy, honour and self-image. An "illegitimate interference" is defined as an act that breaches the core of these rights and which cannot be justified on one of the grounds specified in the Act (see Article 4 of the Act). The Andorran authorities have explained that the available remedies are, after the declaration, cessation and compensation for the damage caused.
[61] Available at: https://www.apda.ad/ca/guies-i-publicacions.
[62] Available at: https://www.apda.ad/ca/guies-i-publicacions.
[63] Available at: https://www.apda.ad/ca/models.
[64] Case No. 280-18 (unpublished).
[65] 2020 Annual Report, p. 4, available at: https://www.apda.ad/ca/memories-de-lapda. The APDA has also created a special website with information about data processing in the context of the COVID-19 pandemic:
[66] 2020 Annual Report, p. 20. Available at: https://www.apda.ad/ca/memories-de-lapda.

regularly provides training in data protection to professionals. In 2019, for instance, the APDA provided data protection training to the Andorran fiscal intelligence unit (UIFAND) and the Federation of people with disabilities (FAAD)[67]. In 2020, the APDA also analysed a privacy impact assessment concerning the development of a COVID-19 contact tracing app, focusing on the proportionality with respect to the purpose pursued[68].

2. ACCESS TO AND USE OF PERSONAL DATA TRANSFERRED FROM THE EUROPEAN UNION BY PUBLIC AUTHORITIES IN ANDORRA

In Andorra, the personal data of EU individuals transferred under the adequacy decision can only be accessed by Andorran public authorities for purposes of criminal law enforcement. In connection with the size of its territory (~464km2) and population (which does not exceed 80 000 inhabitants), there is no specific authority in Andorra engaged in the collection of personal data for national security purposes, nor is there any specific legislation that allows access to personal data for national security purposes[69]. While the Andorran Police may be entrusted with certain tasks in the area of national security[70], any data collection in that context only takes place to prevent, investigate, detect or prosecute offences under the Criminal Code and under the conditions and limitations set out in the Code of Criminal Procedure[71].

2.1 General legal framework

When collecting and (further) processing personal data for criminal law enforcement purposes in Andorra, public authorities are subject to clear, precise and accessible rules governing the scope and application of a measure and imposing minimum safeguards. These limitations and safeguards follow from the overarching constitutional framework and specific laws that regulate activities in the areas of criminal law enforcement.

First, as an exercise of power by a public authority, government access in Andorra must be carried out in full respect of the law[72]. In particular, fundamental rights and freedoms recognised by the Constitution – which include the right to privacy, honour and reputation[73] and the inviolability of the home and the confidentiality of communications[74] – may only be

[67] 2019 Annual Report, p. 19. Available at: https://www.apda.ad/ca/memories-de-lapda.
[68] 2020 Annual Report, p. 11. Available at: https://www.apda.ad/ca/memories-de-lapda.
[69] In addition, Andorra has no army, nor military forces.
[70] In accordance with Article 10 Qualified Law 8/2004 the Police Corps may be entrusted with tasks in the field of national security. According to explanations received, national security within the meaning of Law 8/2004 covers the maintenance of public security (such as guaranteeing citizen coexistence and public tranquillity, fighting violence, ensuring the peaceful use of public spaces and preventing criminal acts).
[71] The Andorran authorities have explicitly confirmed that "personal data of EU individuals, transferred to Andorra under the adequacy decision can only be accessed by Andorran public authorities for criminal law enforcement purposes".
[72] See Article 1 of the Constitution: "Andorra is a Democratic and Social independent State abiding by the Rule of Law". See also Article 3(2) of the Constitution, which guarantees the principles of equality, hierarchy, publicity of the judicial rules, non-retroactivity of the rules restricting individual rights or those that are unfavourable in their effect or sanction, legal certainty, accountability of public institutions and prohibition of any kind of arbitrariness.
[73] Article 14 of the Constitution. According to the judgement of the High Court of Justice of 21 February 2019, this right "must be interpreted in light of the European Convention on Human Rights, as the Constitutional Court has been doing repeatedly (judgment of 11-14-2016, issued in case 2016-7-RE, and order of 6-4-2018, issued in case 2018-15 -RE, among others)".
[74] Article 15 of the Constitution.

www.parlament.gv.at

restricted by means of a so-called qualified law (a law that can only be enacted by qualified majority of the Parliament)[75]. With respect to the inviolability of the home and the confidentiality of communications specifically, the Constitution provides that interferences with these rights are only allowed when a reasoned judicial warrant is issued[76].

Second, the right to the protection of personal data is also guaranteed through Andorra's adherence to the European Convention on Human Rights and the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108). In addition, in October 2022, Andorra ratified the amending Protocol creating the modernised Convention 108+[77].

The European Convention on Human Rights protects the right to respect for private and family life (and the right to the protection of personal data as part of it). In particular, pursuant to Article 8 of that Convention, a public authority may only interfere with the right to privacy in accordance with the law, in the interests of one of the aims set out in Article 8(2), and if proportionate in light of that aim. Article 8 also requires that the interference is foreseeable, i.e., has a clear, accessible basis in law, and that the law contains appropriate safeguards to prevent abuse.

In addition, in its case law, the European Court of Human Rights has specified that any interference with the right to privacy and data protection should be subject to an effective, independent and impartial oversight system that must be provided for either by a judge or by another independent body (e.g., an administrative authority or a parliamentary body)[78]. Moreover, individuals must be provided with an effective remedy, and the European Court of Human Rights has clarified that the remedy must be offered by an independent and impartial body which has adopted its own rules of procedure, consisting of members that must hold or have held high judicial office or be experienced lawyers, and that there must be no evidential burden to be overcome in order to lodge an application with it. In undertaking its examination of complaints by individuals, the independent and impartial body should have access to all relevant information, including closed materials. Finally, it should have the powers to remedy non-compliance[79].

Convention 108 protects the individual's right to privacy with regard to automatic processing of personal data relating to him (data protection)[80]. Article 9 of Convention 108 provides that derogations from the general data protection principles (Article 5 Quality of data), the rules governing special categories of data (Article 6 Special categories of data) and data subject rights (Article 8 Additional safeguards to the data subject) are only permissible when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of protecting State security, public safety, the monetary

[75] Article 40, read in conjunction with Article 57(3) of the Constitution.
[76] Article 15 of the Constitution. The provision furthermore sets out the only exceptional circumstance in which a dwelling may be entered against the will of the owner or without a court warrant, namely in case of flagrante delicto (when an individual is caught while committing the offence).
[77] See the current chart of signatures and ratifications, available at: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=223
[78] European Court of Human Rights, Klass and others v. Germany, Application no. 5029/71, paragraphs 17-51.
[79] European Court of Human Rights, Kennedy v. the United Kingdom, Application no. 26839/05, (Kennedy), paragraphs 167 and 190.
[80] Article 1 of Convention 108.

interests of the State or the suppression of criminal offences, or for protecting the data subject or the rights and freedoms of others.

Therefore, through adherence to the European Convention on Human Rights and Convention 108, as well as its submission to the jurisdiction of the European Court of Human Rights, Andorra is subject to a number of obligations, enshrined in international law, that frame its system of government access on the basis of principles, safeguards and individual rights similar to those guaranteed under EU law and applicable to the Member States.

These international obligations are anchored in the Andorran legal framework through the Constitution, which provides that international agreements such as the European Convention on Human Rights and Convention 108, from the moment of their publication in the official state gazette, form part of Andorran law and may not be amended or overridden by domestic laws[81]. They are thus of direct application in Andorra and can be directly invoked before the Andorran courts[82].

Third, the processing of personal data by Andorran public authorities for law enforcement purposes is subject to specific data protection rules under the new Data Protection Act. These specific rules are set out in the Data Protection Act's third final provision and essentially replicate the core elements of the Law Enforcement Directive. The material scope of these rules is identical to the one of the Law Enforcement Directive. They apply to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security[83]. Furthermore, the data protection principles of lawfulness and fairness, purpose limitation, data minimisation, accuracy, storage limitation and security are formulated using almost the exact same terms as Article 4(1) Law Enforcement Directive. In addition, these rules impose transparency obligations and, like the Law Enforcement Directive, establish the data subject rights of access, correction and deletion[84]. For the same purposes as those recognised in the Law Enforcement Directive [85] controllers are allowed to deny, in whole or in part, requests to exercise the rights of access, correction and deletion. Controllers may only restrict those rights having due regard to the fundamental rights and interest of the concerned individual[86]. Finally, the Andorran Data Protection Authority (ADPA) is charged with monitoring and enforcing these specific rules[87].

The specific rules set out in the Data Protection's Act third final provision anticipate on planned future legislation in this area. In particular, the third final provision instructs the

[81] Article 3(4) of the Constitution.
[82] See Human Rights Council, National report submitted by Andorra to the United Nations Human Rights Council in accordance with paragraph 15(a) of the annex to Human Rights Council resolution 5/1, A/HRC/WG.6/AND/1, p. 4.
[83] Third final provision of the Data Protection Act, paragraph 1.
[84] Third final provision of the Data Protection Act, paragraph 3.
[85] See Articles 15(1) and 16(4), i.e., to avoid obstructing official or legal inquiries, investigations or procedures, prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, protect public security, protect national security or to protect the rights and freedoms of others.
[86] See previous footnote.
[87] Third final provision of the Data Protection Act, paragraph 4.

Andorran government to present in Parliament, within two years from the entry into force of the Act (thus in May 2024 at the latest), a bill that regulates in more detail and following the model set out in the Law Enforcement Directive the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. The specific rules contained in the third final provision apply until the entry into force of this future legislation. A draft Bill on the processing of personal data by public authorities for law enforcement purposes is currently being prepared.

The Commission services welcome the Andorran legislator's intention to replace the specific rules by a more permanent and detailed regime that is even further aligned with the rules that apply in the EU. They will closely monitor future developments in this area.

The general limitations and safeguards mentioned above can be invoked by individuals before independent oversight bodies (e.g., the APDA, see section 2.2.3) and courts (see section 2.2.4) to obtain redress.

2.2. Access and use by Andorran public authorities for criminal law enforcement purposes

In Andorra, criminal law enforcement functions are carried out by the police force, officially called the Police Force of the Principality of Andorra (*Cos de Policia del Principat d'Andorra*), which is headed by the Director. In the specific case of financial crime, the responsible authority is the Andorran financial intelligence unit (UIFAND)[88]. Andorran law imposes a number of limitations on the access to and use of personal data for criminal law enforcement purposes, and it provides oversight and redress mechanisms in this area. The conditions under which access to personal data can take place and the safeguards applicable to the use of these powers are assessed in the following sections.

2.2.1. Legal bases and applicable limitations/safeguards

Personal data transferred under the adequacy decision and processed by organisations in Andorra may be obtained by Andorran law enforcement authorities by means of investigative measures or interception measures under the Code of Criminal Procedure. The Code of Criminal Procedure lays down clear and precise rules on the scope and application of these measures, thereby ensuring that the interference with the rights of individuals will be limited

[88] The UIFAND operates on the basis of Law 14/2017 on the prevention and fight against money laundering and terrorist financing. In short, the relevant parts of this law require undertakings and persons covered by this Act (so-called "reporting entities" such as financial institutions or members of independent legal professions such as lawyers and notaries, among others) to inform UIFAND, on their own initiative, when they suspect, or have reasonable grounds to presume, that a transaction or attempted transaction is or has been connected to money laundering or financing of terrorism (Article 20 of Law 14/2017). Prior to such a notification, the Act requires undertakings and persons covered by the Act to investigate certain suspicious transactions (e.g.,complex or unusual transactions whose economic or lawful purpose is not apparent) and store, for a period of 5 years (extendable by UIFAND once for five years) documents, as well as transactions' proofs and records, information on the accounts, business correspondence and the results of all the analyses performed (Article 37 of Law 14/2017). The reporting entities are exempt from the Data Protection Act when performing these processing operations (Article 38(3) of Law 14/2017). In case the UIFAND finds indications for or the existence of money laundering or terrorist financing suspicions, it reports to the Public Prosecutor's Office (Article 55(2)(m) of Law 14/2017).

www.parlament.gv.at

to what is necessary for a specific criminal investigation and proportionate to the pursued purpose[89]. Moreover, to exercise any of these powers, prior judicial authorisation is in principle required[90]. The police only have warrantless powers in exceptional cases, which are specifically listed in the Code of Criminal Procedure[91].

To gather evidence, the police may conduct searches of homes or other premises where an offence presumably has taken place. Unless the affected person has given prior and written consent, subject to prior notice that (s)he has the right to refuse, searches may only take place based on a court-issued search warrant[92]. The search warrant must specify the address where the search is to be carried out, the grounds on which it is based and the reasons for conducting it[93]. Moreover, according to established case law of the Constitutional Court interpreting these requirements, the judge issuing the warrant must give a reasoned decision explaining the necessity and proportionality of the measure[94].

As regards the execution of the search warrant, the Code of Criminal Procedure provides that the search warrant must be presented to any person occupying the home or other premise. In case of the absence of the occupant, the search must be carried out in the presence of a court clerk who must draw up a detailed record[95].

When conducting a search, the police may seize all assets relating to the offense[96]. Any kind of object may be seized, including computer discs or other data storage devices. The seize power cannot be used, however, to gain access to the content of such devices. If the data stored on the seized device is not accessible without the consent of the owner/holder, a prior judicial authorisation specifically issued to have access to this content is required[97]. According to information received, such authorisation may only be granted under the stricter

[89] This has been specifically recognised, regarding access to communications, by the European Court of Human Rights. See European Court of Human Rights 8 November 2016, Figueiredo Teixeira v. Andorra, Application no. 72384/14, paragraph 42: "In the present case, the Court finds that Article 87 of the Code of Criminal Procedure in force at the material time set out in detail the conditions under which interference with the right to privacy was permitted (…)".

[90] Article 26(2) Code of Criminal Procedure, which provides that obtaining any evidence that may affect the integrity or privacy of the person under investigation requires prior judicial authorization in case of refusal or lack of express consent.

[91] Article 26(2) Code of Criminal Procedure. The following activities are exempted from the requirement of prior judicial authorisation, provided there is no risk to the person's health nor for cruel, inhuman or degrading treatment: identification; fingerprinting or anthropomorphic examinations; information and search on personal records, property, or vehicle registers, provided that they do not constitute the person's registered address; and physical inspection and examination (not) affecting intimate parts of the body.

[92] Article 26(1)(a) Code of Criminal Procedure.

[93] Article 26(1)(a) Code of Criminal Procedure.

[94] See the judgments of the Constitutional Court of 20 April 2015, Janer Rossell v. Andorra, Application no. 2014-44-RE and 3 February 2014, Puig Ariet v. Andorra, Application no. 2013-32-RE. According to this case law, measures resulting in the restriction of liberty, including their nature, manner and timing of execution, duration and intensity must be the result of a weighted jurisdictional consideration. This involves examining all the circumstances present together, weighing the seriousness of the crime attributable to the subject, measuring the notoriety of the evidence or evidence existing against him and also the undesirable effects that could result from not adopting the measures of arrest, surveillance, search, etc., including the possible escape of the suspect or the destruction of evidence.

[95] Article 26(1)(a) Code of Criminal Procedure. Exceptionally, for reasons of urgency, the search may be carried out without the presence of a court clerk, with the prior verbal authorization of the judge, who must give reasons for the authorization afterwards.

[96] Article 26(1)(b) Code of Criminal Procedure.

[97] Article 26(2) Code of Criminal Procedure.

conditions for the accessing of communications, set out in the Code of Criminal Procedure[98] (see below).

Illegal searches and seizures are subject to criminal sanctions[99] and any evidence that is obtained directly or indirectly through a violation of the fundamental rights and freedoms of individuals is considered inadmissible[100].

The police may furthermore collect evidentiary material through the interception of communications**.** The Code of Criminal Procedure recognises three types of communications (telephone, telegraphic and postal) and stipulates that such communications may only be intercepted in the context of a criminal investigation involving a major offence (e.g., drug trafficking) or a minor offence in the area of corruption or influence peddling[101]. In addition, the measure must be necessary for the purpose of seeking the truth[102].

Interceptions may only take place based on a prior court authorisation[103]. The court order must specify the (major) offence in question, the suspects, the reasons why it is necessary to use this procedure, and all the identifying elements of the communication to be intercepted[104]. Furthermore, it must state the period within which the measure may be carried out. This period may not exceed two months and may be extended twice, by reasoned court order, under the same conditions[105]. In addition, the Code of Criminal Procedure provides that the court must give a reasoned decision explaining the necessity and proportionality of the measure and mentioning the evidence obtained, the seriousness of the offence under investigation and the impact on the fundamental right at stake, which must always be guaranteed in its essence[106].

As regards the execution of the court order, the Code of Criminal Procedure stipulates that the interception shall be carried out by a person or department designated by the judge, who is bound by professional secrecy and must keep records, under the supervision of the investigating judge[107]. After the interception has been concluded, the individual whose communication has been intercepted must be notified by the court in case the measure did not

[98] Article 87 Code of Criminal Procedure.
[99] Articles 194-196 Criminal Code.
[100] Article 9(3) Qualified Law on Justice.
[101] Article 87(2) Code of Criminal Procedure. An offence is considered a major offence if it has at least one penalty whose maximum limit exceeds those described in Article 36 of the Criminal Code on sanctions for minor offences, see Article 12 of the Criminal Code. Penalties listed in Article 36 include imprisonment for up to two years or a fine of up to 60 000 euros. Minor offences are those that have at least one penalty whose maximum limit exceeds those described in Article 37 on sanctions for criminal contraventions. Penalties listed in Article 37 include house arrest for up to a month or a fine of up to 6 000 euros.
[102] Article 87(2) Code of Criminal Procedure. Even though the wording of the provision states that interception of communications is allowed if this can be considered 'useful' for the purpose of finding the truth, in practice the courts interpret it as a condition of necessity. See for example, the ruling of the Constitutional Court of 15 March 2019, Campos Tomás vs. Andorra, Application no. 514-2018 and the ruling of the Constitutional Court of 19 April 2021, Miquel Prats and others vs. Andorra, Application no. 25-2021.
[103] Article 87(2) Code of Criminal Procedure.
[104] Article 87(2)(b) Code of Criminal Procedure.
[105] Article 87(2)(b) Code of Criminal Procedure.
[106] Article 87(5) Code of Criminal Procedure.
[107] Article 87(2)(c) Code of Criminal Procedure.

produce evidence of a crime or in case the court has decreed the total or partial secrecy of the measure[108], if the confidentiality of the measure is lifted[109].

Illegal wiretapping and related conduct are subject to criminal sanctions[110] and any evidence that is obtained directly or indirectly through a violation of the fundamental rights and freedoms of individuals is considered inadmissible[111].

Finally, the UIFAND may obtain personal data through disclosure by private individuals, business organisations or public authorities.

Law 14/2017[112] on the prevention and fight against money laundering and terrorist financing imposes an obligation on persons and undertakings subject to the law, such as financial institutions (so-called 'parties under obligation'),[113] to report to the UIFAND, on their own initiative, any transaction or attempted transaction related to funds where the party is aware of, knows, suspects or has reasonable grounds to suspect that are the proceeds of criminal activity or are related to terrorist financing, and to promptly respond to requests made by the UIFAND for additional information in such cases[114]. A similar reporting duty applies to Andorran public authorities, including judicial authorities, who discover facts that could constitute indicia or proof of money laundering or terrorist financing. In those cases, they shall inform the UIFAND in writing and make available to it the information that the UIFAND requests in the exercise of its duties[115].

Prior to notifying the UIFAND, parties under obligation are required by the Act to investigate certain suspicious transactions (e.g., complex or unusually large transactions whose economic or lawful purpose is not apparent) and store, for a period of five years (extendable by UIFAND once for five years) all documents, data and information obtained under the application of the Act, receipts and registers of operations and transactions, account files and business correspondence, and the results of any analysis undertaken, including, where

---

[108] Article 46 Code of Criminal Procedure provides that "during the investigation of the summary for major crimes, the judge, ex officio, at the proposal of the Public Prosecutor or any of the parties, by means of a reasoned order, can decree the secrecy of the whole or a part, making a separate piece in the latter case, up to a maximum non-extendable period of six months, and with the obligation to lift the secrecy at least one month before the conclusion of the judicial investigations".

[109] Article 87(3) Code of Criminal Procedure.

[110] Article 183 and 189 Criminal Code.

[111] Article 9(3) Qualified Law on Justice.

[112] Article 20 of Law 14/2017. An unofficial English translation of this law is available at: https://www.uifand.ad/images/stories/Docs/VF_Text_refos_ANG.pdf

[113] The "parties under obligation" are defined in Article 2 Law 14/2017 and include financial parties under obligation (i.e. operative entities of the financial system, insurance and reinsurance undertakings, authorized payment service providers), natural persons or legal entities, in the exercise of their professional activity (i.e. tax advisers, notaries, lawyers and other independent legal professionals) and non-resident natural and legal persons which carry out in Andorra any activity of the same nature as those listed in Article 2.

[114] Parties under obligation furthermore must provide the UIFAND, at its request, with all the information necessary for the exercise of its functions. All suspicious transactions, including attempted transactions, must be reported. Once the report has been made or after an information request, the parties under obligation must submit to the UIFAND any new element concerning the report of which they are aware.

[115] Article 66(1) and (2) Law 14/2017. Likewise, civil servants and other personnel in the service of the Andorran public administration that discover these facts must make them known immediately to the body in which they work. Article 23 Law 14/2017 furthermore stipulates that if, in the course of checks carried out on the parties under obligation by the competent authorities for prudential supervision, or in any other way, those authorities discover facts that could be related to money laundering or to terrorist financing, they shall promptly inform the UIFAND.

available, information obtained through electronic identification means as set out in the Law on electronic trust services[116]. Any such processing operations performed under the Act by the parties under obligation may only be performed for the purposes of the Act and the concerned data may not be processed in a way that is incompatible with those purposes. Processing of personal data based on the Act for any other purposes, such as commercial purposes, is prohibited[117].

2.2.2. Further use of the information collected

The further use of data collected by Andorran criminal law enforcement authorities on one of the grounds referred to in Section 2.2.1, as well as the sharing of such data with a different authority for purposes other than the ones for which it was originally collected is subject to safeguards and limitations.

First, the processing of personal data by law enforcement authorities in Andorra is governed by the specific rules set out in the Data Protection Act as described in section 2.1[118]. With respect to onward sharing, it follows from the Data Protection Act that personal data collected for law enforcement purposes may be further processed (whether by the original controller or by another controller) for any other law enforcement purpose, provided that the controller is authorised by law to process data for the other purpose[119]. In this case, all the safeguards provided by the Data Protection Act and, where applicable, the specific rules referred to in section 2.1 apply to the processing carried out by the receiving authority.

Second, the different laws that allow for data collection by criminal law enforcement authorities in Andorra impose specific limitations and safeguards as to the use and further dissemination of the information obtained in exercising the powers they grant.

As regards the powers of search and seizure, the Code of Criminal Procedure provides that a detailed record must be made of all the assets seized[120]. The seized objects must be sealed and added to the investigation file, together with the inventory[121]. The seal on all the seized goods

[116] Article 37 Law 14/2017.

[117] Article 38(1) Law 14/2017 states that personal data shall be processed by the parties under obligation on the basis of the Act only for its purposes and shall not be further processed in a way that is incompatible with those purposes. Based on Article 38(3) Law 14/2017, processing of personal data obtained under this Law is not subject to the provisions of the Data Protection Act. However, according to explanations received, this exception applies solely to the parties under obligation (e.g., financial institutions), and only for personal data obtained in the application of Law 14/2017.

[118] As explained in section 2.1 above, the specific rules provide that the processing of personal data collected by Andorran criminal law enforcement authorities, including the further sharing of such data with other authorities in Andorra or in a third country, is subject to all basic data protection principles, including lawfulness and fairness, purpose limitation, data minimisation, data accuracy, storage limitation and data security. See the Third final provision, paragraph 2, of the Data Protection Act. Once Andorra has adopted the Bill on the processing of personal data for law enforcement purposes, referred to section 2.1 above, the rules applying to the processing of personal data by Andorran law enforcement authorities will be become more detailed.

[119] Article 5(4) Data Protection Act stipulates that the processing of personal data for the purposes of prevention, investigation, detection or prosecution of criminal offenses, or enforcement of criminal sanctions, including protection against threats to public safety and prevention can only be carried out if the person responsible for the treatment is authorized by law to process such data.

[120] Article 26(1)(b) and 78 Code of Criminal Procedure.

[121] When because of its volume or other characteristics, the seized goods cannot be attached to the file, an inventory must be made indicating the place where each good is located and the person who takes charge of it, and the goods must remain at the judge's disposal. See Article 26(1)(b) Code of Criminal Procedure.

can only be lifted by the trial judge (*batlle*) or the court[122]. Importantly, the trial judge must adopt the resolutions it deems appropriate to guarantee the restitution of the seized objects if they are not of interest to the case[123].

With respect to the interception of communications, Article 87 of the Code of Criminal Procedure sets out the safeguards that need to be applied to the intercepted material. Notably, recorded tapes, or the (computer) medium on which the communications are stored, must be fully sealed, and attached to the investigation file. The trial judge chooses the texts or documents to be used in the case. Unused recordings are to be kept as an annex to the file and must be destroyed, along with the used recordings, under the supervision of the judicial authority as soon as the case is closed.

In terms of investigative measures carried out in the context of the fight against money laundering and terrorism financing, Law 14/2017 requires the UIFAND to submit to the Public Prosecutor's Office the cases in which there is reasonable suspicion of the commission of a criminal offence[124]. It furthermore requires the UIFAND to share with other public authorities in Andorra (e.g., the Police Force, the Customs Service) any information that is essential for the exercise of their functions[125]. The UIFAND may only respond to requests for information from other competent authorities in Andorra when these requests are motivated by concerns relating to money laundering, associated predicate offences or terrorist financing[126]. In exceptional circumstances, where disclosure of the requested information would be clearly disproportionate to the legitimate interests of a natural or legal person or irrelevant with regard to the purposes for which it has been requested, the UIFAND is under no obligation to comply with the request for information[127].

In addition, the UIFAND is required to share, spontaneously or upon request, any information that may be relevant for the processing or analysis of information by other (foreign) financial intelligence units or equivalent bodies related to money laundering, its predicate offences, or terrorist financing and the natural or legal person involved[128]. The exchange of information requires prior approval from the head of the UIFAND. The party receiving the information must furthermore prove, prior to receiving the information, that certain conditions are met, including that the receiving state shall not use the information for any other purpose than that sought by the Act and that the foreign services receiving the information are bound, under

[122] Article 26(1)(b) Code of Criminal Procedure.
[123] Article 79 Code of Criminal Procedure.
[124] Article 55(2)(m) Law 14/2017. Based on Article 67 Law 14/2017, the UIFAND must inform the Andorran Financial Authority (AFA), in its condition as the body that exercises the disciplinary power of the financial system and the insurance and reinsurance sector, of all transfer of files, whether to the Public Prosecutor's Office, or to the Government, when entities of the financial system or the insurance and reinsurance sector are implicated. This information includes the name of the entity under the supervision of the AFA, a description of the facts observed, and the accounts mentioned in the file.
[125] Article 55(2)(d) and (l) Law 14/2017.
[126] Article 55(6) Law 14/2017.
[127] Article 55(7) Law 14/2017. Based on this provision, the UIFAND is furthermore not obliged to comply with the request, if there are objective grounds for assuming that the provision of such information would have a negative impact on ongoing investigations or analyses.
[128] Article 68(1) Law 14/2017. This duty applies regardless of the type of predicate offences and also if the type of predicate offences is not defined at the time of the exchange.

www.parlament.gv.at

threat of criminal sanction, by a duty of professional secrecy[129]. The UIFAND must use secure channels to exchange information with other financial intelligence units[130].

Law 32/2021 provides the rules on mutual legal assistance in criminal matters. It stipulates that request for legal assistance that refer to bank accounts or the interception of communications, are executed by the trial judge or the competent court, after hearing the Prosecutor's Office and after having verified compliance of the request with Andorran law[131]. The request must contain sufficient elements to allow the legality of the requested measure to be assessed in accordance with Andorran law and must be accompanied by the decision of the judicial authority of the requesting state[132]. In view of the subject-matter and reason of the request, and before communicating the recordings or transcripts to the requesting state, the court must destroy the parts of the recordings or transcripts that are not of interest to the criminal procedure for which the measures have been requested[133]. No information obtained from the Andorran authorities through judicial assistance can be used in the requesting state for purposes other than those specified and, more specifically, for other offenses or facts punishable than those that have been indicated there and of which the Andorran judge has been able to assess of the compatibility with Andorran law[134].

Finally, Andorra has concluded separate international agreements with France and Spain[135] which provide specific safeguards with regard to the sharing of personal data collected for law enforcement purposes. In particular, disclosure can only take place with the express written authorisation of the competent authority of the transferring party, data may only be used for the purposes defined and under the conditions set by the transferring party, and there is a requirement to keep a record of the transferred data[136].

---

[129] Article 68(3) Law 14/2017. Based on this provision, the UIFAND may furthermore refuse to exchange information where there are reasonable grounds to assume that the communication of this information may jeopardise ongoing investigations or analysis.
[130] Article 68(4) Law 14/2017.
[131] Article 32 Law 32/2021.
[132] Article 33 Law 32/2021. Based on Article 4 of 32/201, requests for legal assistance can only be granted if the following conditions are met: (1) the procedure abroad is in accordance with the constitutional principles of the Principality regarding the rights and freedoms guaranteed in the third chapter of Title II of the Constitution, (2) the requested measure is not contrary to the fundamental principles of the Andorran legal system, (3) there are no sufficient reasons to suppose that the procedure has been instigated against a person because of his political opinions, his quality as a member of a certain social group, his race, the their religion or their nationality, (4) all the crimes on which the rogatory commission is based are punishable by Andorran law as a crime, (5) the person subject to the claim has not been convicted by a final sentence in the Principality and has served the sentence or has not been acquitted in Andorra for the same facts, (6) the facts that motivate the request are not of a political nature and the request is not made with a political purpose, (7) the facts that motivate the request, even if they constitute a crime according to Andorran law, are of sufficient importance to justify the intervention of Andorran justice, (8) the communication of the information does not harm the sovereignty, security, public order or other essential interests of the Principality.
[133] Article 34 Law 32/2021.
[134] Article 5 Law 32/2021.
[135] According to information received from the Andorran authorities, sharing of data collected for law enforcement purposes predominantly takes place with Andorra's neighbouring countries, France and Spain.
[136] The agreement with France on cross-border cooperation in police and customs issues was signed on 19 March 2014 and entered into force on 1 April 2018. The agreement is available at: http://www.consellgeneral.ad/fitxers/documents/tractats-i-acords/2014-1/acord-entre-el-govern-del-principat-d2019andorra-i-el-govern-de-la-republica-francesa-relatiu-a-la-cooperacio-transfronterera-en-materia-policial-i-duanera. The provisions in Article 42(1) to (10) of the agreement specify the obligations on the parties regarding data protection. The agreement with Spain concerning the cooperation for fighting against crime and security was signed in 2015 but has not yet entered into force. The agreement is available at:

2.2.3. Oversight

In Andorra, the activities of criminal law enforcement authorities are supervised by different bodies.

First, the APDA is competent to oversee whether the Andorran police complies with the specific data protection rules set out in the Data Protection Act's third final provision (see section 2.1)[137]. The APDA has the power to carry out inspections and impose sanctions for infringements of the Act[138]. In carrying out its investigations, the Agency has access to any relevant information, as well as to the premises where processing operations are carried out, including computer systems or other resources used in data processing[139]. It may also compel the production of evidence[140].

Second, an independent Ombudsman (*Raonador del ciutadá*) is elected by the Andorran Parliament to defend and oversee the fulfillment and application of constitutional rights and liberties and to ensure that the public sector adheres to constitutional principles[141]. It is competent to investigate complaints from individuals who believe their rights have been infringed by the public administration, including the Andorran police[142]. It can also prepare, at its own initiative, reports or recommendations on matters of interest to citizens or society at large, or on matters relating to any of the functions entrusted to him[143]. The independence of the Ombudsman is guaranteed by law[144]. In carrying out its investigations, the Ombudsman has access to all relevant information[145]. Based on the findings of his investigation, the Ombudsman may issue warnings, make recommendations, and otherwise state his views of a case[146]. An annual report is laid before parliament with recommendations based on the Ombudsman's operations throughout the year[147]. In this report he can also recommend the

---

http://www.consellgeneral.ad/ca/arxiu/arxiu-de-lleis-i-textos-aprovats-en-legislatures-anteriors/vii-legislatura-2015-2019/copy_of_tractats-i-acords-internacionals-aprovats/conveni-entre-el-principat-d2019andorra-i-el-regne-d2019espanya-sobre-cooperacio-en-materia-de-lluita-contra-la-delinquencia-i-seguretat. The data protection safeguards are included in its Article 9.

[137] Third final provision, paragraph 4, of the Data Protection Act.

[138] Article 67 Data Protection Act.

[139] Article 62 Data Protection Act. During an inspection, the APDA's inspectors may also carry out audits of the computer systems of the controller or processor to verify that they comply with the requirements of the LQPDP.

[140] Article 62 Data Protection Act.

[141] Article 1 and 8 Law on the creation and functioning of the Ombudsman.

[142] Article 2(3) Law on the creation and functioning of the Ombudsman. According to explanations received, complaints must be made in writing and must contain the contact details of the complainant, and the reasons for the complaint. They can be made in person at the Ombudsman's office, or can be sent by conventional mail, fax, e-mail or by filling out the form available on the website. A personal interview is conducted with the Ombudsman, who decides within a maximum of 13 working days on the acceptance or non-acceptance of the request. If the request is accepted, the Ombudsman initiates the investigation.

[143] Article 5 Law on the creation and functioning of the Ombudsman.

[144] Article 6(1) Law on the creation and functioning of the Ombudsman. The Ombudsman enjoys immunity for the opinions he expresses and acts he performs in the exercise of his functions (Article 6(2) of the Act). S/he is appointed for a (non-renewable) period of six years and can only be dismissed on specific grounds, see Article 9(3) of the Act (e.g., by express resignation, in case of manifest negligence in the exercise of his functions, which may only be declared by an absolute majority of Parliament, or in case of a criminal conviction). The Ombudsman has its own budget, which is approved by the Parliament (Article 18 of the Act).

[145] Article 19(3) Law on the creation and functioning of the Ombudsman.

[146] Article 20 Law on the creation and functioning of the Ombudsman.

[147] Article 21 Law on the creation and functioning of the Ombudsman.

introduction of changes or modifications in the existing legislation in case he observes a possible violation of human rights[148].

2.2.4. Redress

The Andorran system offers different (judicial) avenues to obtain redress, including compensation for damages.

First, the Data Protection Act provides the rights of access, rectification, deletion and restriction with respect to personal data processed for criminal law purposes[149]. In the event a controller refuses or restricts the exercise of these rights, the concerned person may lodge a complaint with the APDA[150]. Decisions of the APDA can be appealed in court, after having exhausted the prior internal administrative review procedure[151]. The subsequent judicial process entails a review of the facts and the decision adopted by the APDA, with the judge being able to revoke or rectify the decision if it violates the appellant's right. The appellant can also claim compensation for damages suffered[152].

Second, individuals may obtain compensation for damages before Andorran courts. This first of all includes the possibility to claim compensation for violations of the Data Protection Act committed by criminal law enforcement authorities[153]. More generally, individuals may apply for compensation of damages caused by an unlawful interference with the right to privacy, honour and reputation, based on Qualified law 30/2014 on the protection of the civil rights to privacy, honour and reputation[154].

Third, it follows from Article 41 of the Andorran Constitution that the protection of fundamental rights and public freedoms of individuals, including data protection and privacy rights, is ensured in ordinary courts through an urgent and preferential procedure established by law which, in all cases, shall include two courts. Any action that has violated an individual right can be challenged through these proceedings, including court orders. Applicants must file a lawsuit in writing, signed by a lawyer duly registered to exercise in Andorra, outlining their request and the alleged damage. The case can be brought before the judge at any time, without mandatory deadlines or other requirements. Possible remedies can be a cessation of

[148] Article 22(2) Law on the creation and functioning of the Ombudsman.
[149] Third final provision, paragraph 3, of the Data Protection Act.
[150] Third final provision, paragraph 4, of the Data Protection Act.
[151] Article 126bis Code of Administration. Any person who considers himself harmed by an act or a resolution of the Administration may file an administrative appeal (Article 124(1) Code of Administration). The deadline for filing an administrative appeal is one month from the date of notification of the act subject to appeal, except when a different deadline is established by law (Article 124(3) Code of Administration). The resolution of the appeal must decide on all the issues raised, even if they have not been alleged by the interested parties; in the latter case, they must be given a preliminary hearing procedure for a period of ten working days. However, the resolution must be consistent with the requests made by the person making the appeal, who cannot see their situation worsen as a result of the appeal. See Article 125 Code of Administration.
[152] Articles 58 and 59 Code of Administration.
[153] Article 71(2) and (7) Data Protection Act. Legal actions in the exercise of the right to compensation must be brought before the courts within a period of one year from the date of the firm declaration of liability of the person responsible or in charge of the processing, see Article 71(6) Data Protection Act.
[154] See Article 20-25 of the Act. An "illegitimate interference" is defined as an act that breaches the core of these rights and which cannot be justified on one of the grounds specified in the Act, see Article 4 of the Act. The Andorran authorities have explained that the available remedies are, after the declaration, cessation and compensation for the damage caused.

the offending action, the annulation of the effects that have occurred, the issuance of a rectification order and/or the fixation of an indemnity.

In addition, sentences and orders that violate constitutional rights, including the right to privacy, honor and reputation and the inviolability of the home and the confidentiality of communication, can be challenged before the Constitutional Court through the exceptional judicial remedy of '*empara*'[155]. An appeal for *empara* can be filed against rulings dismissing claims brought under the urgent and preferential procedure[156]. The empara appeal must be filed within thirteen business days following the day on which the contested ruling is delivered. Through it, the appellant requests the annulment of the ruling, and, if necessary, the suspension of its effects. If the appeal is upheld, the Constitutional Court will annul the contested ruling and all its effects, declare an infringement of a constitutional right, reinstate the appellant in the fulness of his right and adopt the necessary measures to this end, if necessary. If the violation is materially irreparable[157], the Constitutional Court determines the type of liability incurred by the public authority who violated the appellant's right so that compensation can be claimed before the ordinary courts.

Finally, any individual may obtain judicial redress before the European Court of Human Rights against the unlawful collection of his/her data by Andorran criminal law enforcement authorities, provided that all available domestic remedies have been exhausted.

[155] See Articles 85-96 Qualified Law on the Constitutional Court.
[156] It can also be filed against rulings issued by the High Court of Justice.
[157] Meaning that it has caused damage that cannot be quantified in monetary terms.

II. REPUBLIC OF ARGENTINA

1. RULES APPLYING TO THE PROCESSING OF PERSONAL DATA

1.1. Relevant developments in the data protection framework of Argentina

The Commission adopted the adequacy decision for Argentina on 30 June 2003[158], after having received the opinion of the Article 29 Working Party on 3 October 2002[159]. The decision finds that, for the purposes of Article 25(2) of Directive 95/46/EC (Data Protection Directive)[160], Argentina provides an adequate level of protection for personal data transferred from the EU.

In Argentina, core data protection rights are recognised by the so-called 'habeas data action' that was incorporated into the Argentinian Federal Constitution in 1994[161] and that is also part of thirteen provincial constitutions[162]. The recognition of these rights created the basis for the protection of the right to privacy[163], and served as a foundation for Law 25.326 on Personal Data Protection of 4 October 2000 (*Ley de Protección de Datos Personales*, LPDP) and Regulation of Law 25.326 approved by Decree No. 1558/2001 (LPDP Regulation).

The LPDP sets out the general data protection principles, the rights of data subjects, the obligations of data controllers and data users, the set-up, tasks and powers of the supervisory authority, sanctions, and rules of procedure in seeking 'habeas data' as a judicial remedy. The LPDP Regulation introduces implementing provisions and further clarifies specific aspects of the LPDP.

---

[158] Commission Decision 2003/490/EC of 30 June 2003 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina, OJ L 168, 5.7.2003, p. 19, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32003D0490.

[159] Opinion 4/2002 on the level of protection of personal data in Argentina (WP63), available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp63_en.pdf.

[160] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[161] Article 43(3) of the Argentinian Federal Constitution provides that "Any person shall file a prompt and summary proceeding regarding constitutional guarantees, provided there is no other legal remedy, against any act or omission of the public authorities or individuals which currently or imminently may damage, limit, modify or threaten rights and guarantees recognised by this Constitution, treaties or laws, with open arbitrariness or illegality. […] Any person shall file this action to obtain information on the data about himself and their purpose, registered in public records or data bases, or in private ones intended to supply information; and in case of false data or discrimination, this action may be filed to request the suppression, rectification, confidentiality or updating of said data. The secret nature of the sources of journalistic information shall not be impaired".

[162] Constitution of the Ciudad Autónoma de Buenos Aires, Article 16; Constitution of the Provincia de Buenos Aires, Article 20 (3); Constitution of the Provincia del Chaco, Article 19; Constitution of the Provincia del Chubut, Article 56; Constitution of the Provincia de Córdoba, Article 50; Constitution of the Provincia de Entre Ríos, Article 63; Constitution of the Provincia de Jujuy, Article 19 incs. 6 and 8; Constitution of the Provincia de Neuquén, Article 61; Constitution of the Provincia de Santiago del Estero, Article 60; Constitution of the Provincia de La Rioja, Article 30; Constitution of the Provincia de Río Negro, Article 20; Constitution of the Provincia de Salta, Article 89; Constitution of the Provincia de Tierra del Fuego, Antártida e Islas del Atlántico Sur, Article 45. The provincial constitutions and the one of the Ciudad Autónoma de Buenos Aires are available at: https://www.argentina.gob.ar/normativa/constituciones/provinciales-y-caba.

[163] The rights protected by the Constitution apply equally to foreigners (such as EU citizens). Article 20 of the Constitution establishes that "foreigners enjoy in the territory of the Nation all the civil rights of a citizen". Article 16 of the Constitution states that "the Nation of Argentina does not allow prerogatives of blood or birth".

Both the LPDP and the LPDP Regulation were already in place when the adequacy decision was adopted and continue to apply[164]. However, as will be explained in more detail below, several elements of the Argentinian data protection system have been modernised and further reinforced since the adoption of the adequacy decision.

In particular, in a reform that has significantly strengthened the independence of the Argentinian data protection supervisory authority, the *Agencia de Acceso a la Información Pública* (AAIP) has been entrusted with overseeing compliance with the LPDP. Moreover, the AAIP has issued a number of binding regulations and opinions which clarify how the data protection framework is to be interpreted and applied in practice, thus helping to keep the LPDP up to date. Through these regulations/opinions, the AAIP (1) clarified the LPDP's material scope of application by setting out requirements for 'data dissociation' (i.e., anonymisation), (2) expanded the notion of sensitive data, (3) strengthened data protection principles (limited data retention, data security, accountability), rights (right to erasure, right to withdraw data or block data processing) and obligations (additional safeguards required for automated decision-making, restrictions on international transfers). Furthermore, new case law of the Supreme Court has clarified the territorial scope of application of the LPDP.

Since the adoption of the adequacy decision, Argentina also strengthened its international commitments in the field of data protection. In 2019, it joined the Council of Europe Convention for the protection of individuals with regard to the automatic processing of personal data and its additional Protocol (Convention 108)[165]. In 2023, Argentina also ratified the amending Protocol creating the modernised Convention 108+[166].

While the abovementioned developments in terms of guidance, interpretation and case law contribute to an increased level of data protection in Argentina, codifying these developments in legislation would be important to enhance legal certainty and solidify the protection for personal data. The ongoing debate on a reform of the LPDP – in which the AAIP recently concluded a public consultation on a draft Data Protection Bill that is now slated to be submitted to Congress[167] – seems to offer such an opportunity.

As regards the LPDP, it has a broad personal and material scope of application, applying to both private operators and public authorities[168]. While the definitions of 'personal data'[169],

---

[164] Since the adoption of the adequacy decision, the LPDP has been amended by Law 26.343 of 2008, available at: https://www.argentina.gob.ar/normativa/nacional/ley-26343-136483/texto and the LPDP Regulation has been amended by Decree No. 1160/2010, available at the following link: https://www.argentina.gob.ar/normativa/nacional/decreto-1160-2010-170508/texto. These amendments have added new rules to the LPDP on the processing of credit information (Law 26.343) and have clarified and simplified the procedure for the enforcement of the LPDP and the LPDP Regulation (Decree No. 1160/2010).

[165] See the Chart of signatures and ratifications of Treaty 108, available at: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108.

[166] See the Chart of signatures and ratifications of Treaty 223, available at: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=223.

[167] See information about the public consultation available at: https://www.argentina.gob.ar/sites/default/files/informe_consulta_publica_aaip.pdf. The draft Data Protection Bill itself is available at: https://www.argentina.gob.ar/sites/default/files/proyecto_de_ley_de_datos_personales_aaip.pdf

[168] In accordance with Article 1, the LPDP covers the processing of personal data contained in "files, records, databases, databanks or other technical means of data treatment, either public or private for purposes of providing reports, in order to guarantee the right of individuals to their honor and privacy". This provision has a broad interpretation, covering processing by both private entities and public authorities. As explained in Opinion

'controller' and 'processor'[170], 'data owner' (data subject) and 'data treatment' (processing)[171] in the LPDP have not changed since the adoption of the adequacy decision, the AAIP has, through guidance, further clarified the notion of 'data dissociation' in Article 2 LPDP. This notion is akin to the concept of anonymisation used in Regulation (EU) 2016/679 (GDPR)[172] and refers to the processing of personal data in such a way that the information can no longer be associated with a particular person. The AAIP clarified in its Resolution No. 4/2019 that the data is dissociated from the data subject when the process necessary to re-identify the individual would require disproportionate or unviable means. Moreover, the process should be difficult to perform not only for the data controller, but also for third parties[173]. The AAIP thus relies on factors that are similar to those taken into account under the GDPR to assess whether information can be considered anonymous[174].

In addition, the scope of application of the LPDP has been clarified with respect to journalistic information sources and databases[175]. The Argentinian Supreme Court[176] and the AAIP[177] established a distinction between investigative activities and other processing activities of media and journalists. On the one hand, to protect the freedom of the press and the secrecy of sources, personal data used to ensure the truthfulness of investigative information does not fall under the LPDP. On the other hand, when media and journalists act as data controllers, for example when displaying advertising on a website, the LPDP does apply to these specific processing activities.

4/2002 of the Article 29 Working Party, this broad interpretation follows from the wording of Article 43 of the Constitution, Article 24 LPDP, Article 1 of the Regulation and case-law.

[169] Personal data is defined in Article 2 LPDP as any type of information relating to identified or identifiable (determinadas o determinables – translated in English as "certain or ascertainable") physical persons or legal entities.

[170] It follows from Article 25 LPDP and Article 25 of the Regulation that data controllers are those that process data at their own discretion, while data processors are those who process data following the data controller's instructions.

[171] Processing ("data treatment") is defined by Article 2 LPDP as any "systematic operations and procedures, either electronic or otherwise, that enable the collection, preservation, organisation, storage, modification, relation, evaluation, blocking, destruction, and in general, the processing of personal information, as well as its communication to third parties through reports, inquiries, interconnections or transfers".

[172] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[173] Resolution No. 4/2019 (RESOL-2019-4-APN-AAIP) and its annex, available at: https://www.argentina.gob.ar/normativa/nacional/resolucion-4-2019-318874/texto.

[174] See recital 26 of the GDPR.

[175] According to Article 1 LPDP, journalistic information sources and databases are excluded from the scope of application of the LPDP. Law 26.522 on Audio-visual Communication Services specifically regulates the media and journalistic sector.

[176] The Argentinian Supreme Court addressed the relationship between the right to privacy and data protection and the freedom of the press and the right of information in several instances, such as in M., C. S. c/ Editorial Perfil S.A. y otros s/ Daños y Perjuicios (on the right to be forgotten), R., M. B. c/ Google Inc. s/ Daños y Perjuicios (2014 - R.522.XLIX- CSJN) and B., I. c/ Editorial Atlántida S.A. s/ Daños y Perjuicios. In these cases, the Supreme Court established that the right to privacy as a constitutional right is not absolute and must be weighed against other interests, such as the right of information of others and the freedom of the press, on a case-by-case basis.

[177] Resolution No. RESOL-2020-124-APN-AAIP of 2 June 2020, available at: https://www.argentina.gob.ar/sites/default/files/resolucion_redacted.pdf.

As regards its territorial scope of application, the LPDP distinguishes between provisions that are of general application across the country and those that are not[178]. In accordance with Article 44, the provisions of the LPDP included in Chapters I (General Provisions), II (General data protection principles), III (Data subjects rights), IV (Data controllers and processors of files, registers and databanks) and in Article 32 (Criminal sanctions) are of public order and of general application whenever personal data is processed in the territory of Argentina. Furthermore, Articles 36 and 44 LPDP provide that "registers, data files, databases or data banks which are interconnected through networks at inter-jurisdictional (meaning 'interprovincial'), national or international level" fall within federal jurisdiction and are thus subject to the provisions of the law, including those set out in Chapter V, VI and VII on the supervisory authority, the sanctions which may be imposed by the supervisory authority and the specific habeas data procedure that applies to such registers, data files, databases or data banks[179].

Since the adoption of the adequacy decision, several Argentinian courts as well as the Supreme Court have further clarified the interpretation of the notion of "interconnected networks" and thus the scope of application of Chapters V to VII of the LPDP. The judgments clarified in particular that data which is transmitted via the Internet or by any other technical means and can (theoretically) be accessed from all over the country or all over the world is captured by that notion and therefore subject to the provisions of Chapters V to VII of the LPDP, including the competence of the AAIP and the federal judges[180]. On the basis of the case law, data transferred from the EU to Argentina is thus captured by the scope of the entire LPDP, including the provisions regarding the supervisory authority, the applicable sanctions and the habeas data action, as such data is typically transmitted in electronic format via the internet or by other technical means and held in databases that can be accessed via interconnected networks.

The main data protection principles and obligations that were already provided by the LPDP at the time of the adoption of the adequacy decision have remained in place without substantial changes. This is the case for the principles of lawfulness and fairness[181], purpose limitation[182], data accuracy[183], data minimisation[184] and transparency[185]. At the same time, a

[178] Argentina is a Federal State that comprises 23 provinces plus a federal district (Autonomous city of Buenos Aires).
[179] See recital 12 of the adequacy decision.
[180] See for instance Judgement of the Supreme Court of Justice in case Svatzky, Betina Lauras c/ Datos Virtuales S.A (2005); Judgement of the Cámara Nacional de Apelaciones en lo Civil y Comercial Federal in case Scigliano Francisco Vicente c/ Veraz S.A. y otro s/ habeas data (2008); Judgement of the Cámara Nacional de Apelaciones en lo Civil in case Adriao, Alejandro s/ información sumaria s/ competencia (2009) and Judgement of the Supreme Court of Justice in case Ahumada Carlos Agustín C/Google Inc. S/Medidas Precautorias of 27 August 2013. More specifically, the Court in case Svatzky, Betina Lauras c/ Datos Virtuales S.A (2005) noted that in the context of the exercise of the habeas data right to obtain the correction of inaccurate data, both Article 36 and Article 44 of the LPDP subject registers, files, databases or databanks interconnected in inter-jurisdictional, national or international networks to federal jurisdiction. It argued that the Internet was considered an interconnected network within the meaning of these Articles, and that if the information to be deleted was accessible via the Internet, federal judges with civil and commercial jurisdiction should intervene in the dispute. The case is available at: https://sjconsulta.csjn.gov.ar/sjconsulta/documentos/verDocumentoSumario.html?idDocumentoSumario=11617.
[181] Article 5 LPDP.
[182] Article 4(3) LPDP.
[183] Article 4(4) and 4(5) LPDP.
[184] Article 4(1) LPDP.

number of principles and obligations have been further strengthened, in particular through guidance issued by the AAIP. This concerns notably the principles of limited data retention, data security, additional safeguards required for certain types of processing (processing of sensitive data, automated decision-making) and the principle of accountability.

More specifically, the AAIP has further clarified the notion of "suppression" which is relevant in the context of the principle of limited data retention. This principle is enshrined in Article 4(7) of the LPDP, which states that "data shall be destroyed once it has ceased to be necessary or relevant to the purposes for which it has been collected." This provision is supplemented by Article 4 of the LPDP Regulation, stating that if the data is not required anymore for the purposes for which it was obtained or collected, it has to be supressed without a need for the data subject to request such a suppression. According to the AAIP's Resolution No. 47/2018 on Recommended Security Measures, to suppress data means to "eliminate or destroy personal data in a definitive way"[186].

Through the same resolution, the AAIP has also strengthened the principle of data security. First, similarly to the GDPR, the AAIP has reinforced the principles of proactive responsibility and accountability. In particular, it now recommends that organisations are able to demonstrate the appropriateness and effectiveness of the technical and organisational measures used to guarantee the security and confidentiality of the personal data they process. Moreover, the AAIP has issued guidance on how to handle security incidents, recommending that controllers (1) establish internal procedures for dealing with security incidents (2) document security incidents (e.g., the category/ies of affected personal data, the affected users and the measures taken to mitigate the incident and avoid future incidents) and (3) notify the AAIP upon a security incident[187].

The AAIP has not only introduced the concept of accountability, but it has also issued concrete recommendations to operationalise that principle. In Disposition No. 18/2015 it provides privacy best practices for the development of applications, recommending taking into consideration principles like privacy by design and privacy by default[188]. Second, in Resolution No. 40/2018 it approved a model data protection policy for public bodies that recommends the designation of a permanent data protection officer[189]. Finally, Resolution No. 47/2018 recommends security measures for the processing and storage of personal data that include the implementation of review processes to identify, assess and correct possible vulnerabilities in information systems processing personal data[190].

---

[185] Article 6 LPDP.

[186] See Resolution No. 47/2018 (RESOL-2018-47-APN-AAIP), Annex I, paragraph F, available at: https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-47-2018-312662/texto. This part of the resolution at the same time contains important guidance on data retention, as it establishes technical criteria for the implementation of procedures to eliminate data (Annex I, paragraph F).

[187] Resolution No. 47/2018 (RESOL-2018-47-APN-AAIP), available at: https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-47-2018-312662.

[188] Disposition No. 18/2015, available at: https://www.argentina.gob.ar/normativa/nacional/disposici%C3%B3n-18-2015-245973.

[189] Resolution No. 40/2018 (RESOL-2018-40-APN-AAIP), available at: https://www.argentina.gob.ar/normativa/nacional/resolución-40-2018-312130.

[190] Resolution No. 47/2018 (RESOL-2018-47-APN-AAIP), available at: https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-47-2018-312662.

In addition to the strengthening of data protection principles and obligations, the protections for special categories of data have been reinforced since the adoption of the adequacy decision. The LPDP defines special categories of personal data as "revealing racial or ethnic origin, political opinions, religious, philosophical or moral beliefs, labour union membership and information concerning health conditions or sexual habits or behaviours"[191].

Recognising that more modern data protection legislation includes biometric and genetic data in the definition of sensitive data in order to reflect new forms of processing that have emerged in the context of technological transformations, the AAIP has issued guidance on the interpretation of the notion of sensitive data with respect to those categories[192].

In Resolution 4/2019, the AAIP provides guidance on the notion of sensitive data with regard to biometric data[193]. Biometric data is defined by the AAIP in the same way as in the GDPR[194]. Moreover, the AAIP clarifies that it considers biometric data as sensitive data where it can reveal information the use of which could be potentially discriminatory for the data subject (e.g., data revealing ethnic origin or health-related information)[195].

With respect to genetic data, which is again defined in the same way as in the GDPR[196], the AAIP clarifies that genetic data is considered sensitive data when it uniquely identifies a natural person and where it reveals information or information may be deduced from it which is related to the health or physiology of the data subject and the use of which may be potentially discriminatory for the data subject[197].

It is also worth noting that Argentina has ratified Convention 108+ that requires to treat genetic and biometric data uniquely identifying a person as special categories of data[198].

---

[191] Article 2 LPDP.

[192] See the explanatory memorandum to Resolution No. 255/2022 (RESOL-2022-255-APN-AAIP), available at: https://www.boletinoficial.gob.ar/detalleAviso/primera/277889/20221216.

[193] Resolution No. 4/2019 (RESOL-2019-4-APN-AAIP) and its annex, available at: https://www.argentina.gob.ar/normativa/nacional/resolucion-4-2019-318874/texto.

[194] Biometric data are defined as "those personal data obtained from specific technical processing, relating to the physical, physiological or behavioural characteristics of a human person, which allow or confirm his or her unique identification". See the Annex to Resolution 4/2019, under 'Criterion 4. Biometric data'.

[195] See the Annex to Resolution 4/2019, under 'Criterion 4. Biometric data'. The approach adopted by the AAIP in Resolution 4/2019 with regard to biometric data was, prior to the adoption of that resolution, already applied by the Agency in its advisory role. See for example Notice NO-2018-10433281-APN-AAIP of 9 March 2018; Notice NO-2018-38238124-APN-AAIP of 8 August 2018; Notice NO-2017-30610745-APN-AAIP of 30 November 2017. In particular, in Notice NO-2018-38238124-APN-AAIP, the AAIP considered facial recognition data as biometric data the use of which could be potentially discriminatory for the data subject, and which is therefore sensitive.

[196] Pursuant to Article 2 of Resolution 255/202, genetic data is defined as "data relating to the genetic characteristics inherited or acquired from a human person which provides information on their physiology or health".

[197] Resolution No. 255/2022 (RESOL-2022-255-APN-AAIP), available at: https://www.boletinoficial.gob.ar/detalleAviso/primera/277889/20221216. Moreover, the Resolution explicitly states that when genetic data are considered to be sensitive, higher levels of security, confidentiality, restrictions on access, use and circulation of such data must be implemented in accordance with the provisions of Article 9 LPDP and Resolution No. 47/2018. These higher levels of protection apply in addition to the stricter conditions for the processing of sensitive data set out in Article 7 LPDP.

[198] Article 6 of Convention 108+.

Therefore, the same categories of sensitive data that are considered sensitive under the GDPR benefit from additional protections in Argentina[199].

Furthermore, developments in case law, in combination with guidance from the AAIP, have led to a reinforcement and clarification of data subject rights under the LPDP. Importantly, in the case Rodriguez, Maria Belén c/ Google of 2014 the Argentinian Supreme Court created a right to erasure ('right to be forgotten') that is similar to the one provided by the GDPR[200]. The Supreme Court required a search engine provider to de-index certain results, further to a careful balancing of the public interest in the information and the right to data protection in the concrete circumstances of the case. The AAIP recently clarified through guidance how this balancing of rights should be performed[201]. Moreover, in its decision Google Inc. c/ Disposición DNODO No. 3/2011 s/Proceso de Conocimiento, of 2011[202], the AAIP confirmed that not only courts, but also the AAIP itself has the power to enforce the right to be forgotten. Basing itself on the Argentinian Supreme Court's Rodríguez, María Belén c/ Google judgment and taking into consideration the CJEU's judgement in Google Spain (C-131/12), the AAIP ordered the de-indexation of certain search results.

In addition, while the LPDP does not explicitly contain a right to object, the AAIP interpreted Article 27 LPDP – which provides for a "right to withdraw [data] or block [data processing]" – to contain a right to object in relation to data processing for marketing purposes. More specifically, in Disposition No. 4/2009, the AAIP required that all direct marketing messages must contain express information on the possibility of withdrawal and blocking, as well as a mechanism to exercise those rights[203].

Finally, even though the LPDP does not contain a right not to be subjected to automated decision-making for the private sector[204], the AAIP's interpretation of the provisions on access to data has created one in practice[205]. Taking into account the current reality that most data processing is carried out in automated forms, the AAIP considered that on the basis of

[199] According to Article 7 LPDP, no person may be compelled to provide sensitive data. Sensitive data may only be collected and processed when there are reasons of general interest authorized by law. They may also be processed for statistical or scientific purposes when data subjects cannot be identified. The LPDP prohibits the creation of files, databanks or registers storing information that directly or indirectly reveals sensitive data, with the exception of the registers of members of the Catholic Church, religious associations and political and trade union organisations managed by such institutions. Finally, Article 7 LPDP establishes that data relating to criminal records may only be processed by the competent public authorities, within the framework of the respective laws and regulations.

[200] Judgement of the Supreme Court of Justice Rodriguez María Belén c/ Google Inc. s/ daños y perjuicios of 28 October 2014, available at: https://jurisprudencia.mpd.gov.ar/Jurisprudencia/Rodriguez,%20Mar%C3%ADa%20Bel%C3%A9n%20c.%20Google%20Inc.%20s.%20da%C3%B1os%20y%20perjuicios.pdf.

[201] Resolution No. 48/2018, available at: https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-48-2018-312829.

[202] Not published. The Argentinian authorities have provided the Commission services with a redacted copy of the decision.

[203] Disposition No. 4/2009, available at: https://leyesargentinas.com/norma/151221/disposicion-4-proteccion-de-datos-personales-opcion-para-el-ejercicio-del-derecho-de-retiro-o-bloqueo-ley-n-25-326.

[204] Article 20 LPDP sets out a right not to be subject to automated decision-making and profiling. However, the scope of this right is limited to judicial decisions and administrative acts involving an appreciation or assessment of human behaviour. In essence, such decisions and acts may not have as their only basis the result of a computerised processing of personal data defining the profile or personality of the data subject, otherwise they would be void.

[205] Article 15 LPDP.

the transparency principle, which requires controllers to provide clear information about the processing, the controller has to provide an explanation about the logic and specific reasons underlying decisions made exclusively on the basis of automated processing[206]. Furthermore, it is worth noting that Argentina has ratified Convention 108+, which explicitly includes the right not to be subject to decisions based solely on automated processing.

As regards restrictions on international transfers[207], the rules in Argentina have evolved since the adoption of the adequacy decision, increasing the level of protection in case of onward transfers of data originally transferred from the EU. In particular, the AAIP has adopted an approach to international transfers that is similar to the one of the EU.

First, as regards adequacy, the LPDP grants the AAIP the power to adopt adequacy decisions[208]. It currently considers as adequate only countries that have been recognised as providing an adequate level of protection by the European Commission[209], as well as all EU/EEA Member States[210]. Second, in recent years the AAIP has developed several compliance instruments for international transfers to non-adequate countries and organisations. These are essentially the same mechanisms that are recognised by the GDPR: Binding Corporate Rules[211], Standard Contractual Clauses[212] and ad hoc clauses/contracts[213]. Finally, the AAIP has clarified the scope of the exceptions to the general prohibition of transfers to countries or international organisations which do not provide adequate levels of

[206] Resolution No. 4/2019 (RESOL-2019-4-APN-AAIP), available at: http://servicios.infoleg.gob.ar/infolegInterneRijnt/anexos/315000-319999/318874/res4AAIP.pdf.

[207] Article 12 LPDP prohibits transfers of personal data to countries and organisations that do not provide an adequate level of protection. Article 12 of Decree No. 1558/2001 establishes the criteria to be taken into account when assessing the level of protection: "The adequacy of the level of protection afforded by a country or international body shall be assessed in the light of all the circumstances surrounding a transfer or a category of data transfers; in particular, account shall be taken of the nature of the data, the purpose and duration of the processing or the processing envisaged, the place of final destination, the rules of law, general or sectoral, in force in the country concerned, as well as the professional rules, codes of conduct and security measures in force in those places, or which apply to international or supranational bodies. It is understood that a State or international body provides an adequate level of protection where such protection derives directly from the legal system in force, or from self-regulatory systems, or from the protection established by contractual clauses providing for the protection of personal data".

[208] Article 12 of Decree No. 1558/2001 provides that the AAIP has the authority to assess the level of protection in a foreign country or organisation. It can do so ex officio or upon request by an interested party, including the executive.

[209] Argentina considers as adequate the EU/EEA Member States and all countries or territories that benefit from an adequacy finding by the European Commission, except for Japan and South Korea.

[210] Resolution No. 34/2019 (RESOL-2019-34-APN-AAIP), available at: https://www.boletinoficial.gob.ar/detalleAviso/primera/202373/20190226.

[211] Resolution No. 159/2018 (RESOL-2018-159-APN-AAIP), available at: http://servicios.infoleg.gob.ar/infolegInternet/anexos/315000-319999/317228/norma.htm. The Resolution provides guidance on the content of BCRs and stipulates that even if those BCRs do not always need to be pre-approved, they must always follow the principles of the LPDP.

[212] Argentinian standard contractual clauses are largely similar in terms of structure and substance to the standard contractual clauses adopted by the European Commission under the former Data Protection Directive, and are set out by the AAIP in Disposition No. 60 - E/2016, available at: http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/267922/norma.htm. In addition, through Resolution No. 198/2023 published in the Official Gazette on 18 October 2023, the AAIP approved the model contractual clauses for international transfers included in the 'Guide to Implementation of Model Contractual Clauses for the International Transfer of Personal Data (TIDP)' of the Ibero-American Network for Personal Data Protection.

[213] According to Disposition No. 60 - E/2016 (see footnote above), it is possible to create ad hoc clauses but only with regulatory approval requested within 30 calendar days of their execution.

protection, set out in Article 12(2) LPDP[214]. The AAIP now explicitly considers that exceptions to the abovementioned requirements must be interpreted restrictively, and that falling within one of these exceptions is not sufficient to provide a legal basis for transfers; all the data protection principles, obligations and rights of the LPDP must be complied with at all times[215].

1.2. Oversight, enforcement and redress

Since the adoption of the adequacy decision, core elements of the Argentinian system for the monitoring and enforcing of the data protection rules have been strengthened. First, in a reform that has significantly strengthened the independence of the supervisory authority, the AAIP has been charged with monitoring and enforcing the LPDP[216]. Second, the AAIP has adopted two new resolutions that substantially increase the maximum level of fines the Agency may impose. These changes are described in more detail below.

The LPDP provides that 'the controlling Agency' shall ensure compliance with its provisions. At the time of the adoption of the adequacy decision, the *Dirección Nacional de Protección de Datos Personales* (DNPDP) of the Ministry of Human Rights was designated as such. With a view to strengthening the independence of the controlling Agency, the AAIP in 2017 replaced the DNPDP as the supervisory authority for the LPDP. The AAIP was originally created in 2016 as the independent supervisory authority for Law No. 27.275 on Access to Public Information[217]. In 2017, Decree No. 746/2017 expanded its oversight mandate by granting the AAIP additional responsibilities for overseeing compliance with the LPDP[218] and with Law No. 26.951 on the creation of the Do-Not-Call-Register (*Registro Nacional No Llame*)[219].

---

[214] These are: (1) international judicial cooperation; (2) exchange of medical information, when so required for the treatment of the individual affected, or in case of an epidemiological investigation, as long as the data undergoes a "dissociation" procedure, similar to pseudonymisation; (3) stock exchange or banking transfers in pursuance of the applicable laws; (4) transfers arranged within the framework of international treaties to which Argentina is a signatory; (5) transfers made for international cooperation purposes between intelligence agencies in the fight against organised crime, terrorism and drug-trafficking. In any case, in all the instances falling under these exceptions, all the requirements and safeguards of LPDP must be complied with by all the controllers and processors performing the transfer. Specific rules on transfers without consent are contained in Decree No. 1588/01.

[215] For example, the authority considered the legality of an information-sharing agreement relating to foreign trade transactions between the tax authorities of Argentina and Japan. In its Notice IF-2019-04875826-APN-AAIP, the authority established that, although the transfer in question could fall within the exception provided for in Article 12(2)(d), it was also necessary to analyse the content of the agreement in order to determine whether it complied with the principles laid down by Law No 25.326.

[216] See Article 29 LPDP Regulation.

[217] Available at: http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/265949/texact.htm.

[218] Decree No. 746/2017 established in this regard that the agency has the duty of supervising the integral protection of personal data in order to guarantee the rights of individuals to honor and privacy, as well as their right to access their personal data. Decree No. 746/2017 is available at: http://servicios.infoleg.gob.ar/infolegInternet/anexos/275000-279999/279940/norma.htm. Later on, Decree No. 899/2017 modified Decree No. 1558/2001 accordingly and stipulated that the AAIP is the supervisory body for the LPDP, therefore replacing the DNPDP. Decree 899/2017 is available at: https://www.argentina.gob.ar/normativa/nacional/decreto-899-2017-285903/texto

[219] Available at: https://www.argentina.gob.ar/normativa/nacional/ley-26951-233066/actualizacion. This law (also referred to as Do-Not-Call-Law) allows data subjects to block telephone contacts from companies advertising, selling or giving away products and services The law thus implements, within the context of telephony services, the right to block contact from companies advertising, selling or giving away products and services as laid down in Article 27(3) LPDP and Article 27 of the LPDP Regulation.

Other than the former DNPDP, the AAIP benefits from a number of institutional and procedural safeguards for its independence[220]. First, Law No. 27.275 on Access to Public information expressly stipulates that the AAIP is set up as an independent entity with functional autonomy within the President's Chief of Staff Office[221]. Second, as a result of the reform, the system for the designation of the head of the supervisory authority has been reinforced[222]. While the Director of the AAIP is appointed by the Executive (the President of Argentina) for a five-year term that is renewable once[223], (s)he must be selected through an open and transparent public selection process with a public hearing[224]. This new process has led to increased scrutiny of candidates for the function of Director of the AAIP, as illustrated by the procedure that has recently been followed for the selection of a new Director[225]. The law furthermore requires that the Director may not have any interest in, or links to, matters under his or her own right under the conditions laid down in Law No. 25.188 on Ethics in the Exercise of the Civil Service, and (s)he may not have held an elected or advocate position in the last five years prior to the appointment[226]. In addition, the position of Director is deemed incompatible with any other public or private activity other than part-time teaching[227]. Third, the Director may only be removed by the Executive in agreement with Congress, and only for specific reasons that are listed exhaustively in the law, notably misconduct, criminal offences in the performance of their duties or for common crimes[228]. Finally, the AAIP has its own budget granted under the National Budget Law.

In terms of powers, the LPDP continues to provide that the AAIP may impose sanctions consisting of warnings, suspensions, fines ranging between one thousand pesos ($1 000) and one hundred thousand pesos ($100 000), or the closure or cancellation of the file, register or data base[229]. The use of these powers is regulated by resolutions of the AAIP as the controlling Agency that "shall determine the conditions and procedures for the application of the abovementioned sanctions, which shall be graded in proportion to the seriousness and

[220] In its opinion on the draft adequacy decision, the Article 29 Working Party had pointed out that the former DNPDP was part of the Ministry of Justice and Human Rights and that its head was nominated and could be dismissed by the Minister of Justice and Human Rights. It considered that "this situation does not guarantee that the authority may act in complete independence" and urged that "the necessary elements for that purpose be put in place, including changed modalities for appointment and dismissal of the head of the authority". See Opinion 4/2002 on the level of protection of personal data in Argentina, p. 14.
[221] Article 19 Law No. 27.275.
[222] The AAIP is composed of a director, assisted by technical and administrative staff. Decisions of the AAIP are taken by its director. See Articles 20, 22 and 25 of Law No. 27.275.
[223] Article 20 Law No. 27.275.
[224] Article 20 and 21 Law No. 27.225.
[225] As described in the AAIP's annual report of 2020, the now former Director of the AAIP resigned with effect from 1 January 2021 without having yet appointed his replacement. The government subsequently made a proposal for his replacement but had to withdraw its candidate because it faced congressional objections relating to the candidate's qualifications for the position. A second candidate had to be proposed, who was recently appointed. See the press release published on the AAIP's website, available at: https://www.argentina.gob.ar/noticias/beatriz-de-anchorena-asumio-como-nueva-directora-de-la-agencia-de-acceso-la-informacion-0.
[226] Article 23 Law No. 27.225.
[227] Article 23 Law No. 27.225.
[228] Article 27 Law No. 27.225.
[229] Article 31(1) LDPD. The closure or cancellation of databases implies the prohibition to continue the activities of data processing until the AAIP lifts such sanction. Eventually this could require the erasure of the database, as explained by the Argentinian authorities. To enforce the Do-Not-Call-Law, the AAIP may impose the sanctions that are provided for in the LDPD (e.g., fines).

extent of the violation and the damages arising from such violations, guaranteeing the due process of law principle"[230].

Importantly, the AAIP in 2022 adopted two new sanctioning resolutions to ensure that the sanctions provided for in the LPDP maintain an adequate deterrent effect and to further strengthen the effectiveness of the sanctioning regime as a whole[231]. These resolutions, which replace two earlier resolutions adopted by the AAIP's predecessor in 2015/16, increase the level of individual fines that can be imposed for specific categories of infringements and raise the maximum level of fines that the Agency may apply in case of cumulative sanctions.

More specifically, Resolution 240/2022 adjusts the system for the classification and graduation of fines[232]. Like its predecessor, it divides infringements into those of a 'minor', 'serious' and 'very serious nature and provides a non-exhaustive list of examples of each. It furthermore determines the maximum fine to be applied to infringements falling within each category. Compared to the previous resolution, the maximum fines for 'minor' and 'serious' infringements have been raised[233]. The resolution also lists the different factors that the AAIP should take into account when determining the level of the fine to be applied, which are similar to the factors taken account under the GDPR[234]. Resolution 244/2022 then establishes the maximum level of fines to be applied in case of cumulative fines[235].

With respect to the possibilities for individuals to obtain redress, the Argentinian system continues to offer various avenues, including the possibility to lodge a complaint with the

[230] Article 31(2) LPDP.

[231] In addition, Article 77 of the draft National Budget Law for the financial year 2024 that was submitted to the Argentinian Parliament on 15 September 2023 proposes to amend Article 31 of the LDPD on administrative penalties, providing that fines shall be established on the basis of a mobile unit of account which initial value is set at ten million pesos ($10 000). The amount of financial penalties is to be graduated between a minimum of five mobile units and a maximum of one million mobile units. The AAIP shall then, on an annual basis, amend the value of the mobile unit of account in accordance with the change in the Consumer Prices Index. The draft National Budget Law is available at: https://www.hcdn.qob.ai7proYectos/provecto.¡sp?exp=0039-JGM-2023.

[232] Resolution No. 240/2022 (RESOL-2022-240-APN-AAIP), available at: https://www.boletinoficial.gob.ar/detalleAviso/primera/277165/20221205.

[233] The resolution determines that 'minor' infringements (e.g.,charging data subjects a fee for the exercise of their data subject rights) may be sanctioned with a fine up to $80 000 (previously: $25 000), while for serious infringements (e.g.,a violation of basic data protection principles such as data minimisation, data accuracy, storage limitation and data security) a fine up to $90 000 (previously: $80 000) may be imposed. For infringements classified as 'very serious' (e.g., a violation of the rules on cross-border transfers of personal data) a maximum fine of $100 000 applies, in line with the ceiling established in Article 31(1) LPDP.

[234] Factors to be taken into account are for instance the proportionality between the seriousness of the misconduct and the penalty, the nature and extent of the harm or danger to the affected personal rights, and the economic benefit obtained by the infringer or third parties.

[235] Resolution No. 244/2022 (RESOL-2022-244-APN-AAIP), available at: https://www.boletinoficial.gob.ar/detalleAviso/primera/277300/20221206. The resolution raises these maximum levels across the board, taking into account the changes that have taken place since 2015/16 in the consumer price indices published by the National Institute of Statistics and Census of the Argentine Republic. It sets the maximum level of fines to be applied in case of cumulative fines at $3 000 000 (previously: $1 000 000) for infringements classified as 'minor'. For infringements classified as 'serious' the maximum is set at $10 000 000 (previously: $3 000 000), while for infringements classified as 'very serious' a maximum of $15 000 000 (previously: $5 000,000) applies. It follows from Resolution 240/2022 that cumulative fines can be applied when multiple provisions of the LPDP are violated through one action, or when one infringement affects multiple data subjects (e.g., in case of a data breach). In the latter case, the maximum limits laid down in the legislation in force apply. See Annex II to Resolution No. 240/2022, point 7. According to explanations received from the Argentinian authorities, this refers to the LPDP, together with the Resolutions Nos. 240/2022 and 244/2022, which means that the maximum level of fines to be applied in this case is set at a maximum of $15 000 000 for infringements classified as 'very serious'.

AAIP[236], to make use of the special judicial remedy for the protection of personal data known as '*habeas data'*, to obtain judicial redress directly against controllers and processors (both private operators and public authorities)[237] and to obtain compensation for damages[238].

The AAIP plays an active role, both when it comes to its engagement with stakeholders and exercising its oversight role.

In particular, the AAIP each year handles a number of files pertaining to the LDPD, including complaints, consultations and *ex officio* investigations. For example, according to its annual report, in 2021 the AAIP received 386 complaints concerning possible violations of the LDPD and conducted eight *ex officio* investigations[239]. In 2020 the AAIP received 239 complaints, dealt with nine written questions and conducted ten *ex officio* investigations[240]. In 2019, the AAIP handled 214 files, including seven *ex officio* investigations[241].

These supervisory activities have led to enforcement action in multiple cases. In 2021, the AAIP imposed eleven fines[242]. For example, on 31 March 2021 the AAIP fined Rappi Arg S.A.S, an on-demand delivery mobile app for not responding in due time to a request for the suppression of the user's personal data[243]. In 2020, according to its annual report, the AAIP imposed thirteen fines[244]. For instance, on 20 April 2020 the AAIP fined Google Argentina SRL for denying a data subject access to her personal data after her e-mail account was illegally accessed[245]. In 2019, according to its annual report, the Agency imposed eleven fines[246]. For example, on 6 June 2019, Yahoo Argentina SRL was fined in response to a security incident[247].

---

[236] Article 29(b) Decree No. 1558/2001.

[237] Articles 33-43 LPDP. The action of "*habeas data*" can be initiated in case a controller/processor does not respond in time to a data subject's request to have access his/her personal data or to have that data rectified or deleted, see Articles 14(2) and 16(3) LPDP. Article 37 LPDP provides that "the habeas data action shall proceed in accordance with the provisions of this Act and the procedure corresponding to the ordinary action for the protection of constitutional rights (Amparo), and subsidiarily in accordance with the provisions of the National Code of Civil and Commercial Procedure as regards specially expedited summary proceedings". In addition, according to information received from the Argentinian authorities, the data subject can request the judge to make a controller comply with any of the mandatory principles of LPDP, even if he has not filed a complaint with the AAIP. This type of remedy would be available when the habeas data action is not possible, i.e., when the action does not concern the exercise of a right of access, rectification or deletion of personal data. In practice, however, this type of action requesting the enforcement of the law (e.g., the principle of safety) is most often combined with a claim for damages.

[238] Article 31(1) LPDP.

[239] AAIP 2021 annual report, available at: https://www.argentina.gob.ar/sites/default/files/2019/02/informe2021_web.pdf.

[240] AAIP Annual report 2020, available at: https://www.argentina.gob.ar/sites/default/files/informe2020_web.pdf.

[241] AAIP Annual report 2019, available at: https://www.argentina.gob.ar/sites/default/files/informe2019_web.pdf.

[242] AAIP 2021 annual report, available at: https://www.argentina.gob.ar/sites/default/files/2019/02/informe2021_web.pdf.

[243] Resolution 32/2021, available at: https://www.argentina.gob.ar/sites/default/files/2021/04/resol-2021-32-apn-dnpdp-aaip_tachas.pdf

[244] AAIP 2020 annual report, available at: https://www.argentina.gob.ar/sites/default/files/informe2020_web.pdf

[245] Resolution 69/2020, available at: https://www.argentina.gob.ar/sites/default/files/rs-2020-25457045-apn-aaip_google.pdf

[246] AAIP Annual report 2019, available at: https://www.argentina.gob.ar/sites/default/files/informe2019_web.pdf.

[247] File Number EX-2016-04629409 – DNPDP#MJ of 6 June 2019 (unpublished).

Besides fines, the AAIP also applies other sanctions to enforce the LPDP (e.g., warnings, suspension, closure or cancellation of the file, register or database). For example, on 5 February 2020 the Agency issued a warning against the Federal Police in connection with a data breach, a failure to comply with security protocols and a breach of the duty of confidentiality[248]. When investigating private sector controllers, such non-monetary sanctions can also be imposed by the AAIP as a prelude to the imposition of a fine. The AAIP has developed a practice whereby, at the stage of the proceedings where it produces a report on the violations it has found, it simultaneously requires the controller to implement a compliance plan. The extent to which the controller implements this plan is subsequently taken into account when determining the amount of the fine. This approach was for instance followed in a case where a delivery company was found to have breached the security and confidentiality obligations of the LPDP[249].

In addition to the administrative sanctions that can be imposed for violations of the LPDP, the Criminal Code criminalises certain actions involving data processing. Article 117bis of the Criminal Code makes "knowingly providing false information contained in a personal data file to a third party" punishable by a prison sentence of six months up to six years. Article 157bis makes certain forms of 'hacking' (unduly accessing of a database, revealing or supplying confidential information recorded in a file, illegitimately inserting data in a file or database) punishable by a prison sentence of one month up to two years. These crimes are regularly prosecuted. For example, in 2004 an individual was sentenced based on Article 117bis, 156 and 157bis of the Criminal Code for publishing the user database of an internet company on his/her website[250]. In 2007 a public official was prosecuted for unlawfully handing over, transferring, copying, or having intervened in the databases of an agency which contained a list of affiliates of social projects and of unemployed persons[251]

Finally, the AAIP has issued a number of binding resolutions and opinions over the years which have helped to keep the LPDP up to date[252]. These opinions and binding resolutions cover topics ranging from the right of access to personal data collected through closed-circuit television cameras, automated processing of data, dissociation of data, biometric data, and consent, including consent of minors (Resolution No. 4/2019)[253], to the processing of personal data for electoral purposes (Resolution No. 86/2019)[254] and the processing of personal data in the context of the COVID-19 pandemic (Resolution No. 70/2020)[255].

2. ACCESS TO AND USE OF PERSONAL DATA TRANSFERRED FROM THE EUROPEAN UNION BY PUBLIC AUTHORITIES IN ARGENTINA

[248] See Resolution 30/2020, available at: https://www.argentina.gob.ar/sites/default/files/rs-2020-30-apn-aaip.pdf
[249] Resolution 12/2021, available at: https://www.argentina.gob.ar/sites/default/files/resol-2021-12-apn-dnpdpaaip_tachas.pdf
[250] Ruling of 20/10/2004 of the National Criminal and Correctional Appeals Chamber, Chamber VII (Case of Feldman Adrian and other).
[251] Ruling of 11/10/2007 of the National Federal Criminal and Correctional Appeals Chamber, Chamber I (Prieto Manuel E. Case).
[252] See also the Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci, on Argentina, p. 7. The report is available at: https://undocs.org/A/HRC/46/37/Add.5.
[253] Available at: https://www.boletinoficial.gob.ar/detalleAviso/primera/200224/20190116?msclkid=7b14bc8cc18b11eca181e3d7765cd330
[254] Available at: https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-86-2019-323901/texto
[255] Available at: https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-70-2020-336329/texto

2.1. General legal framework

When collecting and (further) processing personal data for criminal law enforcement purposes in Argentina, public authorities are subject to precise and accessible rules governing the scope and application of a measure and imposing minimum safeguards. These limitations and safeguards follow from the overarching constitutional framework and specific laws that regulate the activities of public authorities in the areas of criminal law enforcement and national security.

First, several provisions of the Argentinian Constitution guarantee the rights to privacy and the protection of personal data. Article 18 of the Constitution stipulates that "the domicile may not be violated, as well as the written correspondence and private papers; and a law shall determine in which cases and for what reasons their search and occupation shall be allowed". Importantly, the Supreme Court has ruled that these protections extend to communications via the internet[256]. Article 19 declares that "the private actions of men which in no way offend public order or morality, nor injure a third party, are only reserved to God and are exempted from the authority of judges". The Supreme Court has interpreted this provision as protecting "a sphere of individual autonomy including feelings, practices and customs, family relations, financial situation, religious beliefs, mental and physical health, and, in sum, any actions, events, or information which, considering the lifestyles accepted by the community, are reserved for the individual"[257]. In addition, Article 43 of the Constitution guarantees the right to 'habeas data', a special remedy which any data subject can use to "obtain information on the data about himself and their purpose, registered in public records or data bases, or in private ones intended to supply information" and to achieve "the suppression, rectification, confidentiality or updating of said data" in case of "false data or discrimination".

All laws at both the federal and the provincial levels must conform to the Argentinian Constitution[258]. As described in more detail in sections 2.2.1 and 2.3.1, the general principles following from the Argentinian Constitution are reflected in the specific laws that regulate the powers of law enforcement and national security authorities.

Second, the right to privacy and important aspects of the right to the protection of personal data are also guaranteed through Argentina's adherence to international conventions.

This includes Argentina's adherence to the American Convention on Human Rights and its submission to the jurisdiction of the Inter-American Court of Human Rights[259]. Pursuant to Article 11 of the Convention, everyone has the right to the protection of the law against arbitrary or abusive interference with his private life, his family, his home, or his correspondence. In accordance with Article 30 of the Convention, a public authority may only interfere with the right to privacy in accordance with laws enacted for reasons of general interest and in accordance with the purpose for which such restrictions have been established.

[256] Supreme Court of Justice, Halabi, Ernesto c/PEN ley 25.873 and Decree 1563/04 s/ amparo, case number 332:111, judgment of 24 February 2009.
[257] Supreme Court of Justice, Arriola, Sebastián y otros, case number 332:1963, judgement of 25 August 2009.
[258] Article 5 and 31 of the Argentinian Constitution.
[259] See the list of signatures and ratifications, available at: https://www.cidh.oas.org/basicos/english/Basic4.Amer.Conv.Ratif.htm

These protections apply to all persons falling under the jurisdiction of the state parties to the Convention, irrespective of their nationality[260].

While the Inter-American Court of Human Rights has not yet explicitly recognised the right to the protection of personal data as part of the right to privacy, it has ruled that the protections offered by this right extend to telephone conversations[261]. In addition, the Court has specified that, to determine if an interference with the right to privacy is arbitrary or abusive, three factors must be considered: (1) it must be established by law (2) it must have a legitimate purpose, and (3) it must be appropriate, necessary and proportionate[262]. Regarding the first factor, the Court has clarified that the law on which the interference is based must be clear and precise with detailed rules to establish the boundaries of the restriction. This includes the specific circumstances in which the restriction applies, who can request, order and carry out the restriction, and procedurally how to implement it[263].

Article 75(22) of the Argentinian Constitution stipulates that the American Convention on Human Rights and other human rights treaties specifically mentioned in that provision (e.g., the International Covenant on Civil and Political Rights) enjoy "constitutional rank". As such they have a higher hierarchy than laws and may only be terminated with the approval of two-thirds of all the members of each House of Congress[264].

In 2019, Argentina acceded to the Council of Europe Convention 108 for the protection of individuals with regard to the automatic processing of personal data and its Additional Protocol, regarding supervisory authorities and transnational data flows (Convention 108)[265]. On 17 April 2023 Argentina also ratified the amending Protocol creating the modernised Convention 108 (Convention 108+)[266]. Article 9 of Convention 108 provides that derogations from the general data protection principles (Article 5 Quality of data), the rules governing special categories of data (Article 6 Special categories of data) and data subject rights (Article 8 Additional safeguards to the data subject) are only permissible when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic

[260] Article 1 of the Convention: "The States Parties to this Convention undertake to respect the rights and freedoms recognised herein and to ensure to all persons subject to their jurisdiction the free and full exercise of those rights and freedoms, without any discrimination for reasons of race, color, sex, language, religion, political or other opinion, national or social origin, economic status, birth, or any other social condition".

[261] Inter-American Court of Human Rights, Escher et al. v. Brazil, Series C 200, judgment of 20 November 2009, paragraph 114. This is the case irrespective of the content of these conversations and can even include both the technical operations designed to record this content by taping it and listening to it, or any other element of the communication process (e.g., the destination or origin of the calls that are made, the identity of the speakers, the frequency, time and duration of the calls). See also Inter-American Court of Human Rights, Tristán Donoso v. Panama, Series C 193, judgment of 27 January 2009, paragraph 75-76.

[262] Inter-American Court of Human Rights, Escher et al. v. Brazil, Series C 200, judgment of 20 November 2009, paragraph 129. See also Inter-American Court of Human Rights, Tristán Donoso v. Panama, Series C 193, judgment of 27 January 2009, paragraph 76.

[263] Inter-American Court of Human Rights, Escher et al. v. Brazil, Series C 200, judgement of 20 November 2009, paragraph 130-131.

[264] The Supreme Court has ruled that human rights treaties ratified by Argentina are binding and applicable in the domestic legal order. See Supreme Court of Justice, Ekmekdjian, Miguel Ángel v. Sofovich, Gerardo et al., case number 315:1492, judgment of 7 July 1992. This doctrine was later codified in Article 75(22) of the Argentinian Constitution.

[265] See the Chart of signatures and ratifications, available at: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108.

[266] See the Chart of signatures and ratifications, available at: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=223. Convention 108+ has yet to enter into force.

society in the interests of protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences, or for protecting the data subject or the rights and freedoms of others. The guarantees set out in Convention 108 are extended to every individual regardless of nationality or residence[267].

Therefore, through adherence to the American Convention of Human Rights and Convention 108, as well as its submission to the jurisdiction of the Inter-American Court of Human Rights, Argentina is subject to a number of obligations, enshrined in international law, that frame its system of government access on the basis of principles, safeguards and individual rights similar to those guaranteed under EU law and applicable to the Member States.

Third, the processing of personal data by Argentinian public authorities, including for law enforcement and national security purposes, is subject to the LPDP[268].

The LPDP limits the processing of personal data by law enforcement and national security authorities to what is "necessary for the strict compliance with the duties legally assigned to such bodies for (….) public security or the punishment of crimes"[269]. It contains the principles of lawfulness and fairness, purpose limitation, data minimisation, accuracy, storage limitation and security[270]. Furthermore, the LPDP imposes specific transparency obligations[271] and recognises the data subject rights of access, rectification and erasure ('suppression')[272]. Controllers are allowed to deny, in whole or in part, requests to exercise the rights of access, correction and deletion ('suppression'), but only for specific purposes listed exhaustively in the law and similar to the purposes that allow for a restriction of data subject rights in the EU data protection framework[273]. These exemptions are not absolute but require the relevant authority to decide on a case-by-case basis whether and to what extent to apply them, after balancing the relevant interests at stake, including the privacy interests of the concerned individual[274].

---

[267] See Article 1 of Convention 108, as explained in the Explanatory Report to the Convention, available at: https://rm.coe.int/16800ca434.

[268] See Article 23(1) LPDP. With regard to national security authorities, see also Article 16c of the National Intelligence Act, which stipulates that intelligence agencies "shall unjustifiably frame their activities within the general requirements of the Personal Data Protection Act 25.326".

[269] Article 23(2) LPDP.

[270] See Article 4(3), 4(1), 4(4), 4(5), 5, 9(2) and 23(3) LPDP. As discussed previously (see section 1.1.), the AAIP has issued guidance, clarifying and further developing the basic principles, rights and obligations set out in the LPDP. It is particularly worth recalling here that in Resolution No. 40/2018 the Agency approved a model data protection policy for public bodies that recommends the designation of a permanent data protection officer. Furthermore, Resolution No. 47/2018 provides recommended security measures for the storage and (further) processing of personal data, including a recommendation to notify the AAIP upon a security incident.

[271] Article 6 LPDP.

[272] See Article 14 and 16 LPDP. Regarding the right to suppression, it is important to note that, according to the AAIP's Resolution No. 47/2018 on Recommended Security Measures, to suppress data means to "eliminate or destroy personal data in a definitive way".

[273] See Article 16(5) and 17 LPDP, i.e., to protect public order, to avoid hindering pending judicial or administrative proceedings relating to the compliance with tax or social security obligations or the investigation of crimes and the verification of administrative violations. The decision of the controller to deny the request must be justified and notice thereof must be given to the concerned data subject, see Article 17(2) LPDP.

[274] See for the need to decide on a case-by-case basis the judgement of the Supreme Court of Justice, Ganora, Mario Fernando and Others/hábeas corpus, case number 322: 2139, judgment of 16 September 1999. See for the need to do a balancing exercise the Judgement of the Supreme Court of Justice, Rodriguez María Belén c/ Google Inc. s/ daños y perjuicios, case number 337:1174, judgement of 28 October 2014. See also the AAIP's

The LPDP and LPDP regulation also contain specific provisions on international transfers to a third country or international organisation[275]. As explained previously (section 1.1), these provisions follow an approach similar to the one of the EU data protection framework. Essentially, international transfers are prohibited, unless (1) the AAIP has found that the third country or international organisation provides "adequate levels of protection", (2) such adequate protection is ensured through contractual arrangements between the data exporter and importer or a "self-regulation system", or (3) an exception for a specific situation applies[276].

Finally, the AAIP is charged with monitoring and enforcing these specific rules at the federal level[277]. As regards oversight and enforcement at the provincial level, the LPDP fully applies – including its provisions on supervision by the AAIP – to personal data that is stored in a database that can (theoretically) be accessed from all over the country or all over the world[278].

These abovementioned limitations and safeguards can be invoked by individuals before independent administrative bodies (e.g., the AAIP) and courts to obtain redress, in particular through the habeas data action (see sections 2.2.2, 2.2.3, 2.3.2 and 2.3.3).

2.2. Access and use by Argentinian public authorities for criminal law enforcement purposes

In Argentina, criminal law enforcement functions are carried out by different authorities. At federal level, these include the federal police force, as well as other bodies with specific competences, such as the Gendarmerie and the Prefecture and Airport Police. In the specific case of financial crime, the responsible authority is the Financial Information Unit (UIF)[279]. At the provincial level, criminal law enforcement functions are carried out by the provincial police forces. Argentinian law imposes a number of limitations on the access and use of personal data for criminal law enforcement purposes by each of these authorities and provides oversight and redress mechanisms. The conditions under which such access can take place

---

resolution in the case of Liso Fabbri, RESOL-2020-1-APN-AAIP, available at: https://www.argentina.gob.ar/sites/default/files/rs-2020-1-apn-aaip.pdf.

[275] Article 12 LPDP and Article 12 LPDP regulation.

[276] These exceptions are listed in Article 12(2) LPDP and include cases where "the transfer is arranged within the framework of international treaties which the Argentine Republic is a signatory to", or "the transfer is made for international cooperation purposes between intelligence agencies in the fight against organised crime, terrorism and drug-trafficking". As explained previously (see section 1.1.), the AAIP through its guidance has clarified that exceptions to Article 12 LPDP must be interpreted restrictively, and that falling within one of these exceptions is not sufficient to provide a legal basis for transfers; all the data protection principles, obligations and rights of the LPDP must always be complied with. In addition, Article 12 LPDP Regulation provides that "the prohibition of transferring personal data to countries or international or supranational organisations that do not provide adequate levels of protection, does not apply when the owner of the data has expressly consented to the transfer".

[277] See Article 29 LPDP Regulation, which designates the AAIP as the control body for the LPDP. According to Article 29 LPDP, the Agency must take all necessary actions to ensure compliance with the objectives and other provisions of the LPDP.

[278] Article 36 and 44 LPDP. As explained previously (see section 1.1), data transferred from the EU to Argentina is captured by the scope of the entire LPDP, including the provisions regarding the supervisory authority, the applicable sanctions, and the habeas data action, as such data is typically transmitted in electronic format via the internet or by other technical means and held in databases that can be accessed via interconnected networks.

[279] Article 5 of Law No. 25.246, available at: https://www.argentina.gob.ar/normativa/nacional/ley-25246-62977/actualizacion.

and the safeguards applicable to the use of those powers are described in the following sections.

2.2.1. Legal bases and applicable limitations/safeguards

Personal data transferred from the EU on the basis of the adequacy decision and subsequently processed by Argentinian controllers/processors may be obtained by Argentinian authorities for criminal law enforcement purposes by means of investigative measures under, at federal level, the Federal Code of Criminal Procedure (*Código Procesal Penal Federal*, CPPF)[280]. At the provincial level, access by Argentinian public authorities to personal data transferred under the adequacy decision is governed by the provincial codes of criminal procedure, which provide for conditions, limitations, and safeguards for the access to personal data that are similar to the ones provided by the laws at federal level[281].

The CPPF provides Argentinian criminal law enforcement authorities with a legal basis to access personal data held by controllers/processors through searches and seizures, data seizures, the use of production orders, or the interception of communications. It lays down clear and precise rules on the scope and application of these measures, thereby ensuring that the interference with the rights of individuals will be limited to what is necessary for a

[280] Law 27.063 of 10 December 2014, available at: https://www.argentina.gob.ar/normativa/nacional/ley-27063-239340/actualizacion. The Code replaces Argentina's inquisitive system, laid down in the former Code of Criminal Procedure of the Nation of 1991 (Código Procesal Penal de la Nación, CPPN), with a full accusatory system. It is currently being gradually implemented throughout the country, under the auspices of a special Bicameral Commission established within the scope of Congress by Law 27.063. At present, the CPPN continues to apply at the federal level in the parts of the country where the CPPF is not yet implemented. In 2019, the provinces of Salta and Jujuy became the first provinces to move to the new accusatory system at the federal level (Minutes of the Bicameral Commission No. 15 of 26/3/2019). Next in line to move forward with the reform are the provinces of Mendoza and Rosario (Resolution of the Bicameral Commission CBCPPF-1/2019 (B.O 6/6/2019)). Detailed information about the implementation of the CPPF can be found on the website of the Bicameral Commission, available at: https://www.senado.gob.ar/parlamentario/comisiones/info/379.

[281] Ley 11.922 - Código Procesal Penal de la Provincia de Buenos Aires; Ley 5.097 - Codigo Procesal Penal de Catamarca; Ley 2.945 - Código procesal penal para la Provincia de Corrientes; Ley 8.123 - Codigo Procesal Penal de la Provincia de Cordoba; Ley 4.538 - Código Procesal Penal de la Provincia del Chaco; Ley XV - N° 9 - Código Procesal Penal de Chubut; Ley 9.754 - Código Procesal Penal de Entre Ríos; Ley 696 - Código Procesal Penal de Formosa; Ley 6.259 - Código Procesal Penal de la Provincia de Jujuy; Ley 2.287 - Código Procesal Penal de la provincia de La Pampa; Ley 1.574 - Código Procesal Penal de La Rioja; Ley 6.730 - Código Procesal Penal de Mendoza; Ley XIV – NRO. 13 - Código Procesal Penal de la Provincia Misiones; Ley 1.677 - Código de Procedimiento Penal y Correccional de Neuquén; Ley 5.020 - Código Procesal Penal de Río Negro; Ley 6.345 - Código Procesal Penal de la Provincia de Salta; Ley 7.398 - Código Procesal Penal de la Provincia de San Juan; Ley N. VI-0152-2004 (5724 R) - Código Procesal Criminal de la Provincia de San Luis; Ley 2.424 - Código Procesal Penal de la Provincia de Santa Cruz; Ley 6.740 - Código Procesal Penal de Santa Fe; Ley 1.733 - Código Procesal Criminal y Correccional de Santiago del Estero; Ley 6.203 - Código Procesal Penal de Tucumán; Ley 168 - Código Procesal Penal de la provincia de Tierra del Fuego Antártida e Islas del Atlántico Sur. The following sections focus exclusively on the conditions, limitations and safeguards contained in the CPPF and related laws and regulations, in particular the Criminal Code and Law 27.078 on information technology and communications (Argentina Digital Law). As confirmed by the Argentinian authorities, the CPPN provides for very similar safeguards for the protection of the privacy of individuals as the CPPF, given that the main change brought by the CPPF was to replace the inquisitive by an accusatorial system (see in particular Articles 224-233 on searches and seizures and Articles 234-236 on interception of communications). Furthermore, based on Article 5 of the Argentinian Constitution, the provincial codes of criminal procedure must comply with the privacy safeguards set out in Article 18 and 19 of the Constitution.

specific criminal investigation and proportionate to the purpose pursued. Moreover, to exercise any of these powers, prior judicial authorisation is in principle required[282].

More specifically, searches or seizures may only be carried out if there is a reasonable belief that evidence related to an investigation, or a suspect related to a crime may be found in a home or other place[283]. In terms of procedural safeguards, a search or seizure may only take place on the basis of a court-issued warrant[284]. Warrantless searches or seizures are allowed only in a limited number of exceptional circumstances set out in the CPPF[285]. The person subject to the search is always notified of the search and is in principle present when it is carried out. Where this is not the case, this must be recorded in the minutes of the search[286]. Searches and seizures must be carried out with as little interference as possible with the right to privacy[287]. Moreover, certain communications between the defendant and individuals who must abstain from being a witness (spouse, partner, family member, lawyers, etc.) and objects may not be seized (notes that these individuals might have taken about confidential communications with the defendant or any other circumstances to which the right or duty to abstain from witnessing is extended)[288]. Finally, illegal searches are subject to criminal sanctions[289] and any evidence that is obtained directly or indirectly through a violation of the fundamental rights and freedoms of individuals is considered inadmissible[290].

Specific limitations and safeguards apply to data seizures, defined in the CPPF as the seizure of an entire or partial computer system or data stored on a storage disk or hard drive, with the purpose of seizing the elements of the system, copying the system, or preserving data or information of interest for the investigation[291]. The rules that apply to searches and searches, described above, apply *mutatis mutandis* to data seizures (e.g., data seizures can in principle

[282] See Article 13 CPPF, which stipulates that "the right to privacy, especially freedom of thought, home, correspondence, private documents and any type of communications of the accused and of any other individual must be respected" and that "only with the authorisation of a judge and in accordance with the provisions laid down by this code may these rights be interfered with".

[283] Article 139 and 148 CPPF. Furthermore, the interior of vehicles, aircraft or boats may be searched, if there are sufficient reasons to presume that objects related to the crime that is under investigation are hidden there, see Article 137 CPPF. See also Article 224 CPPN.

[284] Article 143 and 144 CPPF. The application for the search warrant and the warrant itself must contain detailed information. The application must provide, for example, a detailed description of the place(s) to be searched and the reasons that support its necessity. The warrant itself must contain, inter alia, a description of the investigation, the context in which it is being conducted and the day on which it is to be conducted. See also Article 224 CPPN.

[285] In accordance with Article 142 CPPF, a search of a home or other premise may be conducted without a judicial order only in the following cases: a) when there is a fire, explosion or flood, or any other situation that threatens the lives of the residents or the property b) when a complaint has been made on the grounds that one or more individuals were seen entering a house or shop with clear evidence of having committed a crime, whenever it is plausible in relation to the circumstances given c) when a suspect, who is being pursued, enters a house or shop d) when voices coming from a house or shop cry for help or indicate that a crime is being committed therein, and e) when there are well-founded reasons to believe that a person is in danger or is being held hostage in a house or shop, the representative of the Public Prosecutor's Office must authorize the search. The same exceptions apply based on Article 227 CPPN.

[286] 145 CPPF. Only in exceptional circumstances this safeguard does not apply. The CPPF provides that if, due to an obvious risk to the safety of the witnesses to the procedure, it is necessary for the authority to enter the place earlier, it will do so for the time strictly necessary to neutralize the danger. A record of the circumstances will be left in the minutes. See also Article 224 and 228 CPPN.

[287] Article 146 CPPF.

[288] Article 149 CPPF. See also Article 237 CPPN.

[289] Article 151 Criminal Code.

[290] Article 129 CPPF.

[291] Article 151 CPPF.

only take place based on a judicial warrant). Illegal accessing of computer data is subject to criminal sanctions[292] and any evidence that is obtained directly or indirectly through a violation of the fundamental rights and freedoms of individuals is considered inadmissible[293].

Argentinian law enforcement authorities may furthermore obtain personal data through the interception of communications[294]. This power may only be used in the context of a criminal investigation and on the basis of a judicial warrant[295]. An interception of communications may be authorised whenever this is "useful for the investigation of a crime"[296]. Importantly, the Supreme Court, in its capacity as head of the Argentinian judiciary, has introduced additional conditions for the interception of communications by issuing guidelines, addressed to all judicial bodies, which clarify that the interception of communications is "an exceptional measure that may only be authorised with a restrictive approach"[297]. Moreover, based on settled case-law of the Supreme Court and the Inter-American Court of Human Rights, any interference with the inviolability of communications must be provided for by law, pursue a legitimate aim and comply with the requirements of suitability, necessity and proportionality[298].

Procedurally, interception requests must be submitted to federal judges[299], who must approve interception warrants before the interception is conducted by or at the request of the Legal Assistance Directorate for Complex and Organised Crime, a subsidiary body of the Supreme Court[300]. An interception warrant is only valid for a maximum period of 30 days and may be renewed by the court once for the same period, if there are reasons that justify the prolongation of this term given the nature and circumstances of the crime under

[292] Article 153bis and 157bis Criminal Code.
[293] Article 129 CPPF.
[294] Article 150 CPPF. Communications includes postal, telegraphic, electronic correspondence or any other form of communication or of any other effect sent by the accused or intended for this one, albeit under an assumed name (Article 150 CPPF). See also Article 234 and 236 CPPN. Transgressions that are punishable as a crime are defined in Book 2 of the Criminal Code (Law No. 11.179). Outside the Criminal Code, special criminal laws or other laws can also define certain transgressions as a crime.
[295] There are no exceptions to this requirement as Article 5 of the Argentina Digital Act stipulates that the interception of communications, as well as its subsequent registration and analysis, will only proceed at the request of a competent judge.
[296] Article 150 CPPF. See also Article 234 CPPN.
[297] See Agreement ('Acordada') 17/2019 of 19 June 2019, available at: https://www.csjn.gov.ar/documentos/descargar?ID=117364. In this regard, the Agreement notes that the judge examining the request for an interception warrant must have "particular regard to its reasonableness for the purpose of clarifying and resolving the crime". The court order must be "well founded" and may not "be granted on the basis of general terms". It may furthermore "not be intended to obtain indeterminate information with a view to a general and abstract need to prevent or detect criminal offences".
[298] Supreme Court, Halabi, Ernesto c/ PEN law 25,873 and decree 1563/04 on an amparo complaint, case number 332:111, judgment of 24 February 2009, recital 25; Inter-American Court of Human Rights, Escher and Others v. Brazil, Series C 200, judgment of 6 July 2009, paragraph 116, and its citation of the case of Tristan Donoso vs Panama, Series C 193, judgment of 27 January 2009, paragraph 56. See also Article 150 CPPF, which stipulates that when assessing a request for an interception warrant, the court must examine the legality and reasonableness of the request.
[299] Article 150 CPPF. The request for the warrant must indicate the term of duration that it deems necessary according to the circumstances of the case.
[300] The Legal Assistance Directorate for Complex and Organised Crime, which was transferred from the Public Prosecutor's Office to the Supreme Court in December 2015, is the only competent authority for carrying out an interception of communications. See Article 1 of Decree 256/2015, available at: http://servicios.infoleg.gob.ar/infolegInternet/anexos/255000-259999/257346/texact.htm. See also the Agreement ('Acordada') 2/2016 of the Supreme Court of 15 February 2016, available at: https://www.csjn.gov.ar/documentos/descargar?ID=96793.

investigation[301]. The interception must be stopped if the reasons used to authorise the measure disappear, or once the interception warrant has expired or its aim has been achieved[302]. According to explanations received from the AAIP, the defendant will be notified during the criminal proceedings of any interference with his/her privacy, when this no longer endangers the investigation, to enable him/her to contest the legality of that measure and exercise his/her constitutional right of defence in court[303].

Illegal wiretapping and related conduct are subject to criminal sanctions[304] and evidence that is obtained directly or indirectly through a violation of the fundamental rights and freedoms of individuals is considered inadmissible[305].

Under the CPPF, criminal law enforcement authorities may also obtain a production order from a court, ordering a person to hand over objects or documents under his/her power that can serve as evidence[306]. When the production order is not being complied with, the sought-after objects or documents may be seized.

Finally, the UIF may obtain personal data through disclosure by private individuals, business organisations or public authorities.

Law 25.246 imposes an obligation on persons and undertakings subject to the law, such as financial institutions (so-called "parties under obligation")[307], to report to the UIF, on their own initiative, any suspicious fact or transaction, regardless of the amount involved[308]. A suspicious transaction is defined as "those transactions which, in accordance with the customs and practises of the activity in question, as well as the experience and suitability of the persons obliged to report, are unusual, without economic or legal justification or of unusual or unjustified complexity, whether carried out on an isolated or repeated basis"[309]. Prior to notifying the UIF, parties under obligation are required to identify their clients, determine the origin and legality of their funds and to store, in physical or digital form, the information collected on their clients for a minimum period of five years. This information must allow for the reconstruction of transactions carried out, whether domestical or international, and be available for the UIF or the competent authorities when required by them[310].

2.2.2. Further use of the information collected

[301] Article 150 CPPF.
[302] Article 150 CPPF.
[303] Article 18 of the Constitution. Where the existence of an intrusive measure is not notified to the data subject because the procedure has been concluded due to "lack of merit", the AAIP has indicated that there is no obligation in Argentinian criminal procedural law to notify the data subject. However, the AAIP considers that Article 6 PDPL obliges all data controllers to notify data subjects that information related to them is being processed. This would, in its view, include criminal law enforcement authorities and imply an obligation to make a deferred notification, when the risk for the investigation "diminishes".
[304] Article 153 Criminal Code.
[305] Article 129 CPPF.
[306] Article 147 CPPF. Persons who must refrain from testifying as witnesses are exempt from this provision. See also Article 232 CPPN.
[307] The "parties under obligation" are defined in Article 20 Law 25.246 and include financial institutions; individuals or legal persons who, as a regular activity, operate games of chance; insurance companies; public notaries; a number of public authorities including the Central Bank and the Federal Administration of Public Revenues, and registered real estate agents or brokers.
[308] Article 21 Law 25.246.
[309] Article 21(b) Law 25.246.
[310] Article 21bis Law 25.246.

The further use of data collected by Argentinian criminal law enforcement authorities on one of the grounds referred to in Section 2.2.1, as well as the sharing of such data with a different authority for purposes other than the ones for which it was originally collected (so-called 'onward sharing'), is subject to safeguards and limitations.

First, the processing of personal data by law enforcement authorities in Argentina is governed by the LPDP as described in section 2.1. With respect to onward sharing, it follows from the LPDP that personal data collected for law enforcement purposes may be shared with other public authorities for purposes directly related to the legitimate interests of the original controller and the recipient[311]. In this case, the recipient shall be subject to the same regulatory and legal obligations as the controller disclosing the data and the latter shall respond jointly and severally for the observance of such obligations before the AAIP and the data subject[312]. Even though the further processing does not require the consent of the data subject in this case[313], the Argentinian authorities have confirmed that, in accordance with the LPDP[314], the data subject must nevertheless be informed about the purpose of the processing and the identity of the recipient, or other elements that enable the data subject to identify the recipient. Moreover, these requirements are without prejudice to the principles, obligations and rights provided for in the LPDP (e.g., the purpose of the onward sharing has to be compatible with the original purpose of collection). The LPDP and LPDP regulation furthermore contain specific provisions on international transfers to a third country or international organisation. As explained previously (see section 2.1), these provisions follow an approach similar to the one of the EU data protection framework.

Second, the different laws that allow for data collection by criminal law enforcement authorities in Argentina impose specific limitations and safeguards as to the use and further dissemination of the information obtained in exercising the powers they grant.

As regards the powers of search and seizure, the CPPF provides that seized objects must be described, inventoried and placed in safe custody to prevent their modification or substitution[315]. Seized objects that are not subject to confiscation, restitution or embargo must be returned immediately to their owners, after carrying out the procedures for which they were obtained[316]. Regarding data seizures, the CPPF notably provides that any elements that are seized, but are unrelated to the investigation, must be returned to their rightful owner and that any copies that have been made must be destroyed. The data subject may turn to the judge to ensure that the elements are returned and that any copies are destroyed[317].

With respect to the interception of communications, the CPPF sets out the safeguards that need to be applied to the intercepted material. The officials in charge with the execution of the interception warrant and/or those who are responsible for the evidence are bound to a duty of confidentiality with respect to the information obtained. Those who fail to comply with this

[311] Article 11 LPDP.
[312] Article 11(4) LPDP.
[313] Article 11(3)(c) LPDP.
[314] Article 11(1) LPDP.
[315] Article 148 CPPF. The obtaining of copies, reproductions or images of the objects may be arranged when it is more convenient for the investigation. See also Article 233 CPPN.
[316] Article 156 CPPF.
[317] Article 151 CPPF.

duty can be held criminally liable[318]. Once the correspondence or intercepted elements have been obtained, a representative from the Public Prosecutor's Office must open them, examine the elements and read the contents of the correspondence. The representative must subsequently explain to a judge, in a one-party hearing, how and why the seized objects are related and necessary to the investigation. The judge must keep any remaining content confidential and order its return to the defendant, his or her representatives, or close relatives[319]. At the end of the proceedings, the sound records of the communications and transcripts that have been made must be protected from public access. They may not be accessed for any purpose, except by court order, and for justified reasons[320].

In terms of investigative measures carried out in the context of the fight against money laundering and terrorism financing, Law 25.246 requires the UIF to submit to the Public Prosecutor's Office the cases in which there is reasonable suspicion of the commission of a criminal offence[321].

Finally, Law No. 24.767 provides the rules on mutual legal assistance in criminal matters[322]. This law only applies when there is no mutual legal assistance treaty in place between Argentina and the requesting State[323]. In such cases, the law provides that Argentina shall render to any State that so requires the widest assistance in the investigation, prosecution and punishment of offences falling within its jurisdiction[324]. Under this 'principle of broad and prompt cooperation' the granting of assistance (e.g., the provision of evidence, the execution of a search warrant or the interception of communications) is in principle an obligation for the Argentine authorities[325]. However, the request for assistance must be admissible[326] and the

[318] Article 150 CPPF. The Legal Assistance Directorate for Complex and Organised Crime has signed a MoU with the Argentinian Federal Police detailing the rules and security measures concerning access to private communications in the context of a warrant, available at: https://www.csjn.gov.ar/documentos/descargar?ID=106317.

[319] Article 152 CPPF. See also Article 235 CPPN.

[320] Article 153 CPPF.

[321] Article 19 Law 25.246. When the reported transaction is linked to facts under investigation in a criminal case, the UIF may communicate its suspicion directly to the intervening judge.

[322] Law No. 24.767 on International cooperation in criminal matters, available at: https://www.argentina.gob.ar/normativa/nacional/ley-24767-41442/texto.

[323] Article 2 Law No. 24.767.

[324] Article 1 Law No. 24.767.

[325] Article 11 Law No. 24.767 lists the following grounds for refusal of an extradition request, which apply mutatis mutandis to other requests for legal assistance (see Article 70): (a) if the criminal action or the punishment have lapsed according to the law of the requesting State (b) if the person whose extradition is requested has already been tried, in Argentina or in any other country, for the action for which extradition is sought (c) if the person whose extradition is requested would been considered to be below the age of criminal liability pursuant to Argentine law if such person had committed the crime in Argentina (d) if judgment has been rendered in absentia and the requesting State does not provide sufficient assurance that the case would be reopened to hear the convicted person, allow him to assert his rights of defence and render a new judgment accordingly (e) If the requesting State did not provide sufficient assurance that the time during which the person sought is deprived of his liberty during the processing of the extradition shall be considered time served by the extradited person for the proceeding that gave rise to the request.

[326] Article 8 and 10 Law No. 24.767 list the following grounds for in-admissibility for requests for extradition, which apply mutatis mutandis to requests for legal assistance (see Article 70): (1) if the offence for which extradition is requested is regarded as an offence of a political nature (2) if the offence for which extradition is requested is an offence under military criminal law, which is not also an offence under ordinary criminal law (3) if it is sought in the framework of a process pending before one of the ad hoc commissions prohibited under Article 18 of the Argentine Constitution (4) if there are substantial grounds to believe that the request for extradition has been made for the purpose of prosecuting or punishing a person on account of that person's political opinions, nationality, race, religion, or that that person's rights of defence may be prejudiced for any of

obligation to grant assistance does not apply if the assistance sought involves the seizure of property, search of premises, surveillance of persons, postal interception, or phone tapping[327].

2.2.3 Oversight

The activities of Argentinian criminal law enforcement authorities are supervised by different bodies.

First, the AAIP is competent to oversee the processing of personal data by Argentinian criminal law enforcement authorities[328]. The AAIP can, at its own initiative or acting on a complaint by an individual, investigate potential violations of the provisions of the LPDP or its complementary rules[329]. In carrying out its oversight activities, the AAIP has access to all relevant information. In particular, it may request information from public authorities, which are required to provide background, documents, software or any other elements relating to personal data that such entities may be required to process[330]. In addition, it may request a judicial authorisation to access data processing premises, equipment, or software to verify violations of the LPDP[331].

If the AAIP finds a violation of the LPDP, it provides the relevant public authority with a decision stating that the facts investigated constitute an infraction, who is responsible for that infraction, and the sanction to be applied[332]. For example, in 2019 the Agency carried out an *ex officio* investigation into the Argentinian Federal Police over the leaking of information from its databases[333]. This investigation established that the police had not taken the necessary measures to ensure the security and confidentiality of the personal data processed. As a consequence, the AAIP issued three warnings to the Federal Police, two for having breached the duties of data security and confidentiality and one for not having fully cooperated with the AAIP's investigation.

Second, the Argentine Constitution provides for an independent Ombudsman (*Defensor del Pueblo*) to be elected by the Argentine Parliament whose mission is "the defense and protection of human rights and other rights, guarantees and interests protected in this Constitution and the laws, against facts, acts or omissions of the Administration; and control of the exercise of public administrative functions"[334]. It may investigate, *ex officio* or at the

---

those reasons (5) if there are substantial grounds to believe that the person whose extradition is requested could be subjected to torture or cruel, inhuman or degrading treatment or punishment (6) if the offence for which extradition is requested carries the death penalty under the law of the requesting State, and the requesting State does not provide sufficient assurance that the death penalty will not be imposed (7) if Argentina is of the opinion that the request, if granted, would prejudice its sovereignty, security, public order or other essential interests.

[327] Article 5 and 68 of Law No. 24.767. The granting of a request for legal assistance is also subject to the existence or offer of reciprocity, see Article 3 Law No. 24.767.

[328] See Article 23(1) LPDP.

[329] Article 31 LPDP Regulation. It may also start an investigation acting on a complaint by the Ombudsman or consumer or user organisations.

[330] Article 29(1)(e) LPDP.

[331] Article 29(1)(d) LPDP.

[332] Article 31(3)(h) LPDP Regulation. Administrative sanctions can consist of a warning, suspension, or a fine, or the closure or cancellation of the file, register or data base, see Article 31 LPDP.

[333] Case No EX-2019-72366951- -APN-DNPDP # AAIP, available at: https://www.argentina.gob.ar/sites/default/files/rs-2020-30-apn-aaip.pdf.

[334] Article 86 of the Argentine Constitution. The functions of the Ombudsman are currently exercised by the office's Assistant Secretary-General, following the resignation of the second Ombudsman in 2009 and the end of the Deputy Ombudsman's term in 2013. In 2014, a parliamentary resolution was issued authorising the Secretary

request of an individual, any act or omission of the public administration or its agents that involves the illegitimate, defective, irregular, abusive, arbitrary, discriminatory, negligent, seriously inconvenient or inappropriate exercise of their functions, including those capable of affecting diffuse or collective interests[335]. The independence of the Ombudsperson is guaranteed by law[336], and in carrying out its investigations the Ombudsman has access to all relevant information[337].

Based on the findings of his investigation, the Ombudsman may issue warnings and recommendations, reminders of the public authority's legal and functional duties, and proposals for the adoption of new measures[338]. If the Ombudsman through his work becomes aware of potential crimes committed by public authorities, he must immediately notify the Attorney-General[339]. The Ombudsman is required to lay an annual report before Parliament with an account of the number and types of complaints submitted, those that have been rejected and the reason for their rejection, as well as those that have been investigated and their outcome[340]. According to the last figures available, the Ombudsman in 2022 initiated 234 *ex officio* investigations and received 12.210 complaints from citizens[341].

General to exercise the functions of the Ombudsman until Congress appoints a new Ombudsman. This resolution was issued by the Bicameral Commission of Congress provided for in Article 2 Law 24.284, which is responsible for the procedure to elect the Ombudsman. See Resolution 001/2014 of 23 April 2014.

[335] Article 14 Law No. 24.284 on the office of the Ombudsman, available at: https://www.argentina.gob.ar/normativa/nacional/ley-24284-680/actualizacion. Legislators, both Provincial and National, may receive complaints from interested parties, which they are required to immediately forward to the Ombudsman. The public administration and its agents include state enterprises and private companies providing public services, see Article 16 and 17 of the Law. The judiciary, the legislature, the Municipality of the City of Buenos Aires, and defence and security bodies are exempted from the scope of competence of the Ombudsman's Office (Article 16). The Ombudsman may be approached by any natural or legal person who considers themselves affected by the acts, deeds or omissions provided for in Article 14, irrespective of their nationality (see Article 18).

[336] See Article 86 of the Argentine Constitution and Article 1 Law No. 24.284. The Ombudsman has the immunities and privileges of legislators. Based on Article 12 Law No. 24.284, he may not be arrested from the day of his appointment until the day of his dismissal or suspension, except in the case of being caught 'in flagrante delicto' in the commission of an intentional crime. The Ombudsman is appointed for a period of five years, which can be renewed once, and can only be removed by Congress with the vote of two-thirds of the members present of each House, on specific grounds, set out in Article 10 Law No. 24.284 (e.g., due to supervening incapacity, for having been convicted by a final judgement for an intentional crime, or for notorious negligence in the fulfilment of the duties of the office or for having incurred in the situation of incompatibility provided for by this law). The Ombudsman has its own budget, which is approved by the Parliament (Article 36 Law No. 24.284).

[337] Article 24 Law No. 24.284. Requested information may only be refused when it is based on safeguarding an interest related to national security. Anyone who prevents the effective filing of a complaint with the Ombudsman or obstructs the investigations under his charge, by refusing to send the required reports, or prevents access to files or documentation necessary for the course of the investigation, can be held criminally liable for the crime of obstruction, as provided for in Article 239 Criminal Code (which carries a maximum sentence of imprisonment for one year), see Article 25 Law No. 24.284.

[338] Article 28 Law No. 24.284. If the recommendations are made and the public authority concerned fails to take appropriate action within a reasonable period of time or fails to inform the Ombudsman of the reasons for not adopting them, the Ombudsman may bring the background of the matter and the proposed recommendations to the attention of the relevant minister or highest authority of the entity concerned. If he fails to obtain adequate justification, he should include the matter in his or her annual or special report, mentioning the names of the authorities or officials who have adopted such an attitude.

[339] Article 26 Law No. 24.284.

[340] Article 32 Law No. 24.284.

[341] See the Ombudsman's 2022 Annual Report, available at: https://www.dpn.gob.ar/documentos/anuales/ianual2022.pdf.

Finally, different specialised bodies play a role in ensuring law enforcement authorities' compliance with data protection law, for example the General National Syndicate (SIGEN) and the General National Auditor (AGN)[342]. The SIGEN responds to the President of Argentina and has investigative powers to undertake or coordinate independent audits into, inter alia, the legality of public authorities' actions, which could include data protection law[343]. The AGN reports to the National Congress and enjoys similar powers[344].

2.2.4 Redress

The Argentinian system offers different (judicial) avenues to obtain redress, including compensation for damages.

First, individuals have a right to obtain access to and rectification or deletion ('suppression') of their data held by public authorities.

The LPDP provides that data subjects have the right to request and obtain information on their personal data included in, inter alia, public data registers or databanks[345]. In addition, every person has the right to rectify, update, and when applicable, suppress or keep confidential his or her personal data included in a data bank[346]. Both the right of access and the right to rectification and deletion may be exercised free of charge[347]. The relevant public authority may only refuse requests based on the right of access and the right to rectification and deletion in the interest of safeguarding certain important public interest (i.e., public order, the investigation of crimes and the verification of administrative violations) or to protect the rights and interests of others[348]. These exemptions are not absolute but require the relevant authority to decide on a case-by-case basis whether to invoke them, after balancing the relevant interests at stake, including the privacy interests of the individual concerned[349]. As will be explained in more detail below, individuals whose requests have been denied have the

[342] Respectively, *Sindicatura General de la Nación* and *Auditoría General de la Nación*. Both bodies were created by Law No. 24.156 on Financial Administration and National Public Sector Control Systems.
[343] Article 104 (c) Law No. 24.156.
[344] Articles 117, 119 and 130 Law No. 24.156.
[345] Article 14 LPDP. Article 14 LPDP Regulation further clarifies that the right of access enables the data subject to receive information on: (1) whether his/her data are contained in the archive, register, database or databank, (2) all the data concerning him/her that are in the archive, (3) the sources from and means by which they were obtained, (4) the purpose for which they were obtained, (5) the possible recipients and (6) whether the archive is registered pursuant to the LPDP. The Argentinian authorities have confirmed that the data subject can also obtain a copy of the data, although if this implies high costs for the controller, it is possible that s/he will have to bear such costs. Article 15 of the PDPL further specifies the requirements in terms of information to be provided to the data subject exercising his right of access. In particular, the information must be provided clearly, without any codes that might make the text difficult to read and, where applicable, enclosing an explanation of the terms used, in a language that is understood by a citizen with an average degree of education. Moreover, the information must be extensive and deal with the full record corresponding to the owner, even in case the request submitted refers to only one item of personal data. In no case shall the report disclose information referring to third parties, even if such third parties are related to the requesting party. The information may, at the owner's option, be provided in writing, by electronic, telephonic, visual, or other adequate means for such purpose.
[346] Article 16 LPDP. During the process for the verification and rectification of the relevant mistake or inaccuracy in the information, the person responsible for or the user of the data bank must either block the access to the file, or indicate, when providing the information relating thereto, that such information is subject to revision. See Article 16(6) LPDP.
[347] Article 14(3) and 19 LPDP. The right of access may only be exercised free of charge "within intervals no shorter than six months unless a legitimate interest to do otherwise is shown".
[348] Article 16(5) and 17 LPDP. The resolution so providing must be duly reasoned and notice thereof be given to the concerned individual, see Article 17(2) LPDP.
[349] See section 2.1.

possibility to pursue the special judicial remedy of 'habeas data' to gain access to their data or to have that data rectified or deleted[350].

Second, any individual may lodge a complaint with the AAIP in respect of any matter relating to the handling of personal information by a criminal law enforcement authority[351]. As described in section 2.2.3, if the AAIP finds a violation of the LPDP, it provides the relevant public authority with a decision stating that the facts investigated constitute an infraction, who is responsible for the infraction and what is the administrative sanction to be applied[352]. Decisions of the AAIP may be challenged before the courts in accordance with Title 4 of the Law on Administrative Procedure[353]. The court may declare the decision void[354]. Decisions that are declared void must be revoked or replaced by the AAIP[355].

Third, judicial redress is available to all data subjects via the constitutional right to a habeas data action. The LPDP provides the conditions for a habeas data action before courts against actions by public authorities[356]. Once the deadline for the controller to either provide the information requested by the data subject, or to correct, delete or update the information, has expired and the controller has not complied with the request, or if the data subject considers the response insufficient, s/he may initiate a judicial habeas data procedure[357]. Importantly, the Supreme Court has ruled that the standing requirement for a habeas data action against a public authority must be interpreted extensively in order to facilitate the exercise of the fundamental right to privacy as enshrined in Article 43 of the Constitution[358].

Judicial redress is also available via the general civil and administrative law actions available against public authorities, including law enforcement authorities.

First, data subjects may pursue a claim for the compensation of damages[359] in court, subject to the four basic requirements for any damages claim under Argentinian law: illegality of the damaging action; real and actual damage; cause-effect relationship between the action and the damage; and negligence, wrongful misconduct and fault. Second, a preventative action[360] would allow a data subject to request a judge to impose preventive restrictions and obligations

[350] See Article 33 LPDP and further.
[351] Article 31(3)(a) LPDP Regulation.
[352] Article 31(3)(h) LPDP Regulation.
[353] Available at: https://www.argentina.gob.ar/normativa/nacional/ley-19549-22363/actualizacion.
[354] Article 15 Law on Administrative Procedure.
[355] Article 17 Law on Administrative Procedure.
[356] Article 33, 34 and 37 LPDP.
[357] Article 14(2) LPDP.
[358] Judgement of the Supreme Court of Justice, Barcat, Abdo c/ Registro Nacional de Reincidencia dep. del Ministerio de Justicia y Seguridad y Derechos Humanos, case number 330:24, judgement of 12 October 2006. In this case, the Supreme Court granted the applicant the right to access its data in a database for law enforcement managed by the Ministry of Justice, Security and Human Rights. According to the Supreme Court: "If almost three years have elapsed without the application having been definitively established, and in the case of a procedure intended to guarantee a fundamental right, such as the right to honour, privacy and the protection of personal data, based on the third paragraph of Article 43 of the National Constitution, it is necessary to dispel the procedural concerns that deserve the way in which the dispute was brought and to resolve the issue of jurisdiction without further formality, where this is advisable for reasons of procedural economy and the delay in the decision could lead to a virtual denial of justice'" and: "the national courts have jurisdiction in federal administrative disputes to decide on the request for the deletion, rectification and updating of certain data stored in the National Register of Relief under the Ministry of Justice, Security and Human Rights of the Nation, since such judicial activity is linked to data or administrative acts carried out by public authorities".
[359] *Acción civil de daños y perjuicios*, see Article 1716 of the Civil and Commercial Code.
[360] *Acción preventiva*, Article 1711 of the Civil and Commercial Code.

on a data controller before there is specific damage, if the data subject is in a position to prove that the damage has a qualified probability to occur. Third, via a generic action[361] a data subject may request a judge to make a controller comply with any of the mandatory principles of the LPDP, even if he has not filed a complaint with the AAIP. This type of remedy is available when the habeas data action is not possible, i.e., when the action does not concern the exercise of a right of access, rectification or deletion of personal data. In practice, this type of action is most often combined with a claim for damages. Fourth, through an action for annulment[362] an individual who has been the object of a criminal investigation may challenge the court orders affecting him. This type of action can only be brought after the facts affecting his or her privacy have occurred. In case the challenge is rejected, the individual can request a review by the superior court. Moreover, under certain circumstances, the individual can become a plaintiff in the criminal proceeding. Finally, Article 52 of the Civil and Commercial Code establishes that any individual harmed in his or her personal or family privacy, honour or reputation, image or identity, or who in any way has his or her personal dignity undermined, may claim prevention and reparation of the damage suffered.

Finally, when all national redress avenues are exhausted, data subjects may lodge a case before the Inter-American Court of Human Rights for any violation of their fundamental right of privacy enshrined in the American Convention on Human Rights.

2.3 Access and use by Argentinian public authorities for national security purposes

In Argentina, two agencies may access personal data transferred from the EU to Argentina for national security purposes: the Federal Intelligence Agency (AFI) and the National Criminal Intelligence Directorate (DINICRI). The AFI is the highest-ranking intelligence agency in Argentina and the director of the so-called National Intelligence System, which consists of the AFI, the DNICRI and the National Military Intelligence Directorate (DINIEM)[363]. The AFI was established in 2015 by Law 27.126 on the creation of the Federal Intelligence Agency and Presidential Decree No. 1311/2015 approving the "New National Intelligence Doctrine", as part of a major overhaul of Argentina's intelligence services[364]. In accordance with Article 2(5) of Law 25.520 (National Intelligence Act) and Decree No. 1311/2015, the basic task of these intelligence agencies is to generate knowledge for the purpose of contributing to decision-making in relation to matters relevant to national defence and internal security[365].

[361] *Acciòn genérica*, see for instance ruling of the Federal Administrative Chamber of August 2023, CFed. CONT. ADM., Chamber V, Civil Rights Association c/EN-M Interior Op. and V-RENAPER-Ley27275 s/Ampari Ley 16.986, 16/08/2023, p. 5, TRLALEY AR/JUR/103536/2023, available at*:* https://adc.org.ar/wp-content/uploads/2023/08/sentencia-por-filtracion-de-datos-renaper-web.pdf.

[362] *Acciòn de nulidad*, see also Articles 166 and 167 Code of Criminal Procedure.

[363] Article 6 and 7 National Intelligence Act. The DINIEM is mandated to gather strategic military intelligence (see Article 10 National Intelligence Act). Article 2(4) of the Act defines 'strategic military intelligence' as "intelligence relating to knowledge of the capabilities and weaknesses of the military potential of countries of national defence interest, as well as the geographical environment of the operational strategic areas identified by the military strategic planning". According to information received, the activities of the DINIEM may not be directed at Argentinian individuals or corporations, or any person in Argentina. Therefore, the following sections focus solely on the access and use of personal data by the AFI and DINICRI.

[364] As part of this overhaul, the former Intelligence Secretariat was dissolved. See Article 24 Law 27.126.

[365] The latter notion is defined in Article 2 National Intelligence Act as "the factual situation based on the law in which the freedom, life and heritage of the inhabitants, their rights and guarantees and the full validity of the institutions of the representative, republican and federal system established by the National Constitution are protected". The notion is further specified in Annex I, Chapter I, of Decree No. 1311/2015 as "the security that covers criminal acts that violate the freedoms and rights of the individuals and of the social, constitutional and

More specifically, the AFI is tasked with producing (1) national intelligence and (2) criminal intelligence related to complex federal crimes[366]. The DINICRI is tasked with producing criminal intelligence unless it is related to complex federal crimes[367]. The relevant powers of these agencies, as regulated by the National Intelligence Act and its regulatory decree are described in the following sections.

2.3.1 Legal bases and applicable limitations/safeguards

Based on the National Intelligence Act and Decree No. 1311/2015, the AFI and DNICRI may access personal data transferred from the EU to Argentina as part of different activities, which are subject to specific limitations and safeguards following from the National Intelligence Act itself, from the LPDP, the Argentinian Constitution, the Argentina Digital Act, and case law.

Pursuant to the National Intelligence Act, the intelligence agencies must "unequivocally frame their activities within the general prescriptions of the Personal Data Protection Act 25.326"[368]. Therefore, the accessing of personal data transferred from the EU to Argentina by these agencies for national security purposes may only take place in so far this is necessary for the performance of their legal duties[369].

According to Decree No. 1311/2015, the task of the intelligence agencies is to develop "intelligence information, which comprises the body of observations and measurements obtained or gathered from public or classified sources concerning an event or relevant issues in the field of national defence or internal security"[370]. It furthermore specifies that intelligence is developed through three core institutional tasks: information gathering,

---

democratic State". More specifically, this notion encompasses (1) terrorism, (2) attacks on the constitutional order and democratic life (e.g., political and/or military groups taking up arms against the public authorities and/or the constitutional order), (3) organised crime (e.g., human, arms and drug trafficking) and (4) cybercrime (e.g., offences against the confidentiality, integrity and availability of computer systems, networks or data). The notion of 'national defence' is defined in Article 2 Law No. 23.554 on national defence as "the integration and coordinated action of all Nation forces to resolve conflicts that require the use of the armed forces, in a dissuasive or effective manner, to tackle attacks of external origin". Article 3 Law No. 23.554 furthermore provides that "the fundamental difference between the national defence and internal security must be taken into account at all times". Matters related to national defence are further specified in Annex I, Chapter I of Decree No. 1311/2015 as "possible risks of conflicts generated by aggressions of external origin perpetrated by armed forces belonging to other states against the sovereignty, territorial integrity or political independence of our country, or in any other way that is incompatible with the United Nations Charter".

[366] Article 8 National Intelligence Act. In accordance with Article 2(1) of the Act, 'national intelligence' means "the activity of obtaining, gathering, systematising and analysing specific information relating to facts, risks and conflicts affecting national defence and the internal security of the nation". Article 2(3) of the Act defines 'criminal intelligence' as "intelligence relating to specific criminal activities which, by their nature, scale, foreseeable consequences, dangerousness or manner, affect the freedom, life, property of inhabitants, their rights and guarantees and the institutions of the representative, republican and federal system established by the National Constitution".

[367] Article 9 National Intelligence Act. Both the AFI and DINICRI are expressly prohibited from using law enforcement powers and carrying out criminal investigations, see Article 4(1) National Intelligence Act, which provides that "no intelligence agency may carry out repressive tasks, possess compulsive powers, or perform police or criminal investigation duties".

[368] Article 16c National Intelligence Act.

[369] Article 23(2) LPDP provides, in so far relevant here: "The treatment of personal data with national defence or public security purposes by the armed forces, security forces, police or intelligence agencies, without the consent of the parties concerned, is limited to those cases and categories of data as are necessary for the strict compliance with the duties legally assigned to such bodies for the national defence, public security or the punishment of crimes".

[370] Decree No. 1311/2015, Annex I, Chapter II.

information management and information analysis. Specifically with regard to the AFI, the decree stipulates that the AFI may, for the purpose of the production of national intelligence, engage in "the collection, gathering and analysis of information on facts, risks and conflicts affecting national defence and internal security through the agencies that are part of the National Intelligence System"[371]. This activity involves the gathering of strategic intelligence[372] and (ii) counterintelligence[373]. Furthermore, to produce criminal intelligence relating to complex federal crimes, the AFI may engage in "the collection, systematisation and analysis of information on the criminal issues in question using AFI resources"[374].

The use of these powers is subject to limitations and safeguards that are specifically designed to prevent their (mis)use for political purposes and operations, and to ensure the protection of fundamental rights, including those guaranteed by Article 18 and 19 of the Argentinian Constitution. In particular, the Act provides that no intelligence agency may (1) exercise law enforcement powers or carry out criminal investigations (2) produce intelligence based solely on sensitive data of data subjects or (3) interfere in any way with the country's institutional, political, military, police, social or economic situation, its foreign policy, its political parties, public opinion, individuals, media or associations of any kind[375].

In terms of procedural safeguards, any intelligence activity must be ordered by the highest body of each authority[376]. Moreover, any intelligence activities involving the interception of private communications of any kind[377] may, without exception[378], only be carried out when authorised by a judicial warrant[379].

An interception warrant may only be issued when this "is necessary in the conduct of intelligence or counter-intelligence activities"[380]. Procedurally, interception requests must be submitted to federal judges with criminal competence by the Intelligence Secretariat or an official to whom that power is expressly delegated. Requests must be in writing, justified and

[371] Article 8(1) National Intelligence Act.
[372] Further specified in Annex I, Chapter II, as "intelligence based on the comprehensive analysis of the set of problems affecting national defence and internal security, which allows for the construction of a general situational diagnosis of these problems in order to establish strategic guidelines and general objectives in the area of national defence and internal security".
[373] Further specified in Annex I, Chapter II, as "intelligence oriented towards knowledge of the deployment and intelligence activities carried out by individuals, groups or agencies, national or foreign, that may affect national defence or internal security, each in its institutional sphere".
[374] Article 8(2) National Intelligence Act and Decree No. 1311/2015, Annex I, Chapter II and III.
[375] Article 4(1), (2) and (3) National Intelligence Act. The overall aim of the legislative framework to establish clear boundaries for intelligence activities is also reflected in Decree No. 1311/2015, which specifically provides that the intelligence agencies "must ensure the protection and care of the citizens and not 'spy on them'". See Annex I, Chapter I of Decree No. 1311/2015.
[376] Article 5 National Intelligence Act. For cases of emergency, the same article provides that these activities "can start, but they need to be immediately reported to the highest authorities in each of the intelligence agencies."
[377] In this context, it is important to recall that the Argentinian Supreme Court has ruled that the inviolability of communications extends to communications via the internet. See CSJN, Halabi, Ernesto c/PEN ley 25.873 and Decree 1563/04 s/ amparo, judgment of 24 February 2009.
[378] See Article 5 Argentina Digital Law: "Correspondence, understood as any communication that is made through Information and Communication Technologies (ICT), including traditional postal mail, email or any other mechanism that induces the user to presume the privacy of itself and the traffic data associated with them, carried out through telecommunications networks and services, is inviolable. Its interception, as well as its subsequent registration and analysis, will only proceed at the request of a competent judge".
[379] Article 18 National Intelligence Act.
[380] Article 18 National Intelligence Act.

must precisely indicate the telephone number(s) or e-mail address(es) or any other facilities/means, intended to be intercepted or collected[381]. As explained above (see section 2.1.1), once approved, the interception may only be conducted by or at the request of the Legal Assistance Directorate for Complex and Organised Crime, a subsidiary body of the Supreme Court[382]. An interception warrant may be granted for a period no longer than sixty days, a period which automatically expires unless it is extended by the judge (or the respective Chamber in the event of a refusal at first instance) when necessary to complete the ongoing investigation, and such an extension may only be for up to sixty days[383]. After the expiry of the time-limit for the initial collection established by judicial order, another judicial order must be issued to determine whether the retention should be prolonged or whether the data should be destroyed[384].

The role of the judge in assessing the request for an interception warrant is essentially to verify whether the warrant sought is reasonable in light of the facts put forward. This follows from guidelines, issued by the Supreme Court, on the interception of communications (see section 2.2.1)[385]. These guidelines, which address all judicial bodies, clarify that the interception of communications is "an exceptional measure that may only be authorised with a restrictive approach" and that the warrant authorising the interception must be "well founded" and "may not granted on the basis of generic terms." Moreover, based on settled case-law of the Supreme Court and the Inter-American Court of Human Rights, any interference with the inviolability of communications must be provided for by law, pursue a legitimate aim and comply with the requirements of suitability, necessity and proportionality[386].

Lastly, violations of the above-mentioned rules are subject to criminal sanctions. Those who, in the permanent or transitory development of the tasks regulated by the National Intelligence Act, "unduly intercept, seize or divert telephonic, postal, telegraphic or fax communications or any other type of information, archive, record and/or private documents whose reading is not authorised nor accessible to the public, and that have not been addressed to them" may be punished by three to ten years of imprisonment and professional disqualification for twice that time[387]. The same sentence is incurred by any official or civil servant who carries out intelligence activities prohibited by Laws No 23.554 (National Defence), Law 24.059 (Internal Security) or the National Intelligence Act[388]. Anyone who fails "to destroy or

[381] Article 18 National Intelligence Act.
[382] Article 22 National Intelligence Act. Court orders for the interception of telephone communications must be sent to the Legal Assistance Directorate for Complex and Organised Crime by means of an official letter signed by the judge, with precise and detailed instructions to guide the interception. The judge must send another official letter, indicating exclusively the numbers to be tapped, for the Legal Assistance Directorate for Complex and Organised Crime to attach it to the request to be sent to the telephone service company responsible for carrying out the interception.
[383] Article 19 National Intelligence Act.
[384] Articles 19 and 20 National Intelligence Act.
[385] Agreement 17/2019. As explained earlier, Agreement 17/2019 is set of guidelines concerning the interception of communications, issued by the Supreme Court in its capacity as head of the Argentinian judiciary, and addressed to all judicial bodies.
[386] Supreme Court, Halabi, Ernesto c/ PEN law 25,873 and decree 1563/04 on an amparo complaint, case number 332:111, judgment of 24 February 2009, recital 25; Inter-American Court of Human Rights, Escher and Others v. Brazil, Series C 200, judgment of 6 July 2009, paragraph 116, and its citation of the case of Tristan Donoso vs Panama, Series C 193, judgment of 27 January 2009, paragraph 56.
[387] Articles 42 National Intelligence Act.
[388] Article 43ter National Intelligence Act.

eliminate the records of wiretaps, copies of postal, cable and fax interceptions or of any other element that accounts for the interceptions, recordings or diversions" after having been compelled to do so by judicial order or otherwise incurs a prison sentence from two to six years and professional disqualification for twice that time[389].

2.3.2 Further use of the information collected

The processing of personal data by the AFI and DINICRI is subject to the LPDP (see sections 2.1 and 2.3.1). In addition, the National Intelligence Act sets out specific safeguards for the storage of data collected by the intelligence agencies. It stipulates that "data which, once stored, is not used for the purposes laid down by this Law, is destroyed" and prohibits the storage of data in intelligence databases "for reasons of race, religious faith, private actions, political opinion, membership of or membership of advocacy, social, human rights, trade unions, community, cooperatives, care, cultural or labour organisations, as well as their lawful activity in any sphere"[390].

With respect to the further sharing of data with other entities (within or outside Argentina), the National Intelligence Act and the LPDP (which applies to intelligence services, as explained in section 2.1) impose specific limitations. Based on Article 11 LPDP, personal data collected for national security purposes may only be shared with other public authorities for purposes directly related to the legitimate interests of the original controller and the recipient, subject to the conditions and safeguards described in section 2.2.2. Furthermore, the National Intelligence Act provides that the disclosure or dissemination of personal data, acquired by intelligence agencies in the course of their duties, requires a judicial order and a presidential authorisation pursuant to Article 16 of the Act[391], except when the disclosure or dissemination is provided for in a legal provision[392].

Based on the LPDP, the transfer of any type of personal data to third countries or international organisations which do not provide adequate levels of protection, is prohibited, subject to limited exceptions (e.g., when the transfer is made for international cooperation purposes between intelligence agencies in the fight against organized crime, terrorism and drug-trafficking)[393]. However, as explained above (see section 1.1.), these exceptions must be interpreted restrictively. Falling within the scope of one of these exceptions is not sufficient to ensure the lawfulness of the transfer; all the data protection principles, obligations and rights of the LPDP must be always complied with.

2.3.3 Oversight

The activities of Argentinian national security authorities are supervised by different bodies.

---

[389] Articles 43 National Intelligence Act.
[390] Article 16 sexies National Intelligence Act.
[391] Article 16 National Intelligence Act provides, in so far relevant here: "Access to such information shall be authorised in each case by the President of the Nation or by the official to whom that power is expressly delegated, subject to the exceptions provided for in this Law".
[392] Article 16 quáter National Intelligence Act and Article 3 Decree No. 950/2002. According to explanations received, this does not hinder the sharing of information between intelligence services and between intelligence services and other public authorities. For example, Article 15 of Law No. 23.544 requires the AFI to provide the Ministry of Defence with the information and intelligence necessary to contribute to the production of strategic military intelligence.
[393] Article 12 LPDP.

First, the AAIP oversees the activities of the AFI and DINICRI, as provided for in the LPDP and the National Intelligence Act. This oversight follows similar conditions as in a law enforcement context and for public authorities in general, as detailed in Section 2.2.3.

Second, parliamentary oversight in the area of national security is carried out by the Bicameral Commission for the Audit of Intelligence Bodies and Intelligence Activities[394]. This Commission was established in 2001 by the National Intelligence Act as an independent review mechanism composed of officials from the Chamber of Deputies and the Senate[395]. It is charged with supervising the bodies belonging to the National Intelligence System, with a view to oversee that their operation strictly complies with the constitutional, legal and regulatory requirements [396]. To perform its oversight role, the Bicameral Commission may initiate *ex officio* investigations[397]. Its oversight activities furthermore include (1) studying, analysing and assessing the execution of the National Intelligence Plan (2) studying the Annual Intelligence Activities Report[398] (3) receiving any explanations and reports deemed appropriate from government ministers (4) giving opinions on any draft legislation linked to intelligence activities, and (5) receiving complaints from natural and legal persons about abuses and wrongdoings committed by intelligence agencies[399].

The Bicameral Commission has, in principle, access to all the information or documentation it requests from the bodies that make up the National Intelligence System[400].The Bicameral Commission furthermore has the power to request classified reports containing a list of interceptions carried out within a specified period. It may request such reports from the Legal Assistance Directorate for Complex and Organised Crime, its representatives within the country and from telecom operators active in Argentina, for the purpose of controlling the legality of such interceptions[401].

The Bicameral Commission submits annual reports with recommendations to the National Executive and the Parliament. These annual reports evaluate the activities, performance, and organization of the National Intelligence System with regard to the National Intelligence Plan[402]. In 2018, the Bicameral Commission wrote a detailed opinion on a new legislative proposal to amend the National Intelligence Act[403]. In addition, in 2020-2021 the Bicameral Commission conducted an in-depth investigation into certain alleged breaches by the AFI during the period of 2016 to 2019. Its extensive report of 20 April 2021 included proposals for

---

[394] *Comisión Bicameral de Fiscalización de los Organismos y Actividades de Inteligencia del Honorable Congreso de la Nación*, created by Article 31 National Intelligence Act.
[395] Article 31 National Intelligence Act.
[396] Article 32 National Intelligence Act.
[397] Article 32 National Intelligence Act.
[398] This is a secret report, drawn up each year by the Intelligence Secretariat and forwarded to the Bicameral Commission within ten days of the beginning of the Parliament's ordinary session. See Article 33(2) National Intelligence Act.
[399] Article 33 National Intelligence Act.
[400] Article 32, 35 and 37(2) National Intelligence Act. Such access must be authorized in each case by the President or an official specially appointed to do so, Article 16 and 32 National Intelligence Act, Article 20 Decree 950/2002.
[401] Article 34 National Intelligence Act.
[402] Article 33(4) National Intelligence Act.
[403] The opinion is accessible at: https://www.leyes.congreso.gob.pe/Documentos/2016_2021/Dictamenes/Proyectos_de_Ley/02468DC14MAY20180611.pdf

structural reforms within the National Intelligence System such as the creation of a whistle-blower system[404].

Finally, SIGEN (see section 2.2.3) has the possibility to control the administrative processes and the budget execution of the AFI's public funds[405].

2.3.4 Redress

The Argentinian system offers different avenues to obtain redress, including compensation for damages.

First, individuals have a right to obtain access to and rectification or deletion ("suppression") of their data held by the AFI or DINICRI under the LPDP, subject to the same conditions as described in section 2.2.4.

Second, any individual may lodge a complaint with the AAIP in respect of any matter relating to the handling of personal information by the AFI or DINICRI, in the same way as described in section 2.2.4.

Third, judicial redress may be sought via a constitutional habeas data action against the AFI, or DINICRI, subject to the same conditions as described in section 2.2.4. For instance, in the Supreme Court case of R. P., R. D. c/Estado Nacional – Secretaría de Inteligencia del Estado, the complainant initiated a habeas data action against the former State Intelligence Service (SIDE) to gain access to information gathered by SIDE from 1961 to 1973, which he considered necessary to receive pension entitlements from the national administration (ANSES). The Supreme Court considered that information processed by intelligence organisations does not *per se* constitute classified information, and that the judiciary is authorised to have access to the documents in question and to verify whether the decision to refuse the requested access is lawful[406].

Fourth, the same judicial avenues as the ones described in section 2.2.4 (i.e., a claim for the compensation of damages, preventative action, generic action, action for annulment) are also available against the AFI and DINICRI.

Finally, once all national law remedies are exhausted, data subjects may bring their case before the Inter-American Commission of Human Rights.

---

[404] Informe Comisión Bicameral de Fiscalización de los Organismos y Actividades de Inteligencia, Espionaje Ilegal 2016-2019, available at: https://www4.hcdn.gob.ar/comisiones/especiales/cbinteligencia/Informe Comision Bicameral Inteligencia 2021-04-20.pdf. Several Decrees aimed at reforming the Federal Intelligence Agency (Decretos Nº 540/20, 987/20, 359/21, 832/21, 295/22 and 654/22) were adopted as a follow-up to the opinion.

[405] See Decree No. 52/2019, available at: https://www.argentina.gob.ar/normativa/nacional/decreto-52-2019-333546/actualizacion.

[406] Supreme Court, R. P., R. D. c/ Estado Nacional - Secretaría de Inteligencia del Estado, case number 334:445, judgement of 19 April 2011. According to information received from the Argentinian authorities, as part of the reform of the Argentinian intelligence services mentioned in section 2.3, the amount of information that is classified as confidential has been "reduced to the indispensable minimum".

III. CANADA

1. RULES APPLYING TO THE PROCESSING OF PERSONAL DATA

1.1. Relevant developments in the data protection framework of Canada

On 20 December 2001, the European Commission adopted its adequacy decision on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA)[407]. The decision covers transfers of personal data from the EU to recipients in Canada that are subject to PIPEDA. The Article 29 Working Party adopted its opinion on 20 January 2001[408].

Since the Commission adopted its adequacy finding in 2001, PIPEDA has been amended on five occasions; by the Anti-Terrorism Act (S.C. 2001, c. 41), the Public Safety Act (which entered into force in 2004, S.C. 2004, c. 15), the Public Servants Disclosure Protection Act (S.C. 2005, c. 46), Canada's Anti-Spam Legislation (S.C. 2010, c. 23) and the Digital Privacy Act (S.C. 2015, c. 32). Moreover, further interpretations and clarifications have been provided by the courts and the federal data protection authority (the Office of the Privacy Commissioner, OPC).

In June 2022, the Canadian government introduced a bill (Bill C-27) in the Canadian Parliament to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act[409]. The bill is currently being examined by the House of Commons of the Canadian Parliament, after which it will go to the Senate. The proposed Consumer Privacy Protection Act would amend PIPEDA in several ways, e.g., by codifying certain clarifications provided over the years by courts and the OPC (for instance on the validity and modalities of consent, requirements for the legitimacy/lawfulness of data processing, the right to deletion and international data transfers) and by further strengthening the powers of the OPC.

PIPEDA has a specific scope of application, which has been extended several times since the adoption of the adequacy decision[410]. Currently, PIPEDA applies to the collection, use and disclosure of personal information by an organization[411] in the course of a commercial

---

[407] Commission Decision 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act, OJ L 2, 4.1.2002, p. 13-16.

[408] Opinion 2/2001 (WP39), available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp39_en.pdf.

[409] Available at: https://lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/LegislativeSummaries/441C27E.

[410] After its adoption on 13 April 2000, PIPEDA entered into force in three stages. As from 1 January 2001, it applied to personal information, other than personal health information, that a federal work, undertaking or business, collected, used or disclosed in the course of commercial activity. It also applied to all organisations disclosing information outside a province or outside Canada and to employee data handled by a federal work, undertaking or business. As of 1 January 2002, it also covered the handling of personal health information by the abovementioned organisations. Finally, as of 1 January 2004, PIPEDA applies to any organisation that collects, uses or discloses personal information in the course of a commercial activity, whether or not it is a federally regulated business (Section 4(1) PIPEDA).

[411] PIPEDA applies to 'organisations' and does not distinguish between 'controllers' and 'processors'. Instead, Principle 1 provides that organisations remain responsible for information in their possession or custody (Section 4.1.3 of Schedule 1 PIPEDA). This includes information that has been transferred to a third party for processing. Where information is 'transferred' to a third party, the latter may only use that information for the purposes for

activity[412], as well as to the processing of personal information about employees of (or applicants for employment with) an organisation that is federally regulated[413]. Since 2015, PIPEDA also applies to processing of personal information by the World Anti-Doping Agency[414]. It does not apply to personal information handled by public authorities, non-profit organisations (unless they handle personal information for commercial purposes), individuals (to the extent they handle the information for purely personal or domestic purposes), or employee information of non-federally regulated organisations[415]. In addition, an amendment in 2015 introduced a specific exception for the processing of business contact information (e.g., name, title, work address, work contact details) solely for the purpose of communicating or facilitating communication with the individual in relation to their employment, business or profession[416]. This exception only applies to a limited number of situations (e.g., to use the work e-mail address of a lawyer to obtain legal advice) and cannot be relied upon to use information for different purposes (e.g., to use that same work e-mail address for marketing purposes)[417].

As regards its territorial scope of application, PIPEDA provides for the possibility to exempt organisations or activities from its application with respect to the processing that occurs solely

---

which it was originally collected by the transferring entity. Organisations are required to use contractual or other means to provide a comparable level of protection while the information is being processed by the third party. According to guidance from the OPC, 'comparable level of protection' does not mean that the protections must be the same but generally equivalent (see https://www.priv.gc.ca/en/privacy-topics/airports-and-borders/gl_dab_090127/). The primary means by which such protection may be ensured is through a contract (other means could include internal policies and safeguards applied throughout a corporate group, see PIPEDA case summary #2006-333, available at: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2006/pipeda-2006-333/). The guidance furthermore explains that organisations must be satisfied that third parties have policies and processes in place, including training and effective security measures, to ensure that the information is properly protected. Organisations should also have the right to audit and inspect how the third party handles and stores personal information.

[412] In accordance with Section 2(1) PIPEDA, an organisation includes an association, a partnership, a person and a trade union. A commercial activity is defined as "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists".

[413] PIPEDA refers to a federal work, undertaking or business, i.e., "any work, undertaking or business that is within the legislative authority of Parliament", see Section 2(1) PIPEDA. This includes a work, undertaking or business in connection with navigation and shipping; railway, canal, telegraph or other work that connects provinces; a line of ships that connects provinces; a ferry between provinces or between a province and third country; aerodromes, aircraft or a line of air transportation; a radio broadcasting station; a bank or authorised foreign bank; a work situated in a province but declared by Parliament to be for the general advantage of Canada or two or more provinces; a work, undertaking or business outside the exclusive legislative authority of the provinces and a work, undertaking or business to which federal laws under the Oceans Act apply.

[414] Schedule 4 and Section 4(1.1) PIPEDA.

[415] Section 4(2)(a) and (b) PIPEDA. In addition, PIPEDA does not apply to the collection, use or disclosure of personal information for purely journalistic, artistic or literary purposes (Section 4(2)(c) PIPEDA). This is a limited exception, intended to protect freedom of expression under the Canadian Charter of Rights and Freedoms. The balance between privacy and freedom of expression is ensured through other standards, such as Ethics Guidelines of the Association of Journalists, which rely on principles such as accuracy, fairness, respect for the right to privacy, transparency, etc. (see the Ethics Guidelines, available at: https://caj.ca/ethics-guidelines and the Principles for Ethical Journalism, available at https://caj.ca/images/downloads/Ethics/principles.pdf).

[416] Section 4.01 PIPEDA.

[417] See e.g.,Case Summary #2019-006, available at: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-006/. In this case, a publishing company had collected, used and shared the contact details of an individual that was presented on the website of a non-profit organisation as a contact point. The OPC found that this information did not constitute business contact information, but personal information subject to PIPEDA, as it was included on the non-profit's website for handling general inquiries from the public (not for the sole purpose of communicating or facilitating communication with the individual in relation to his employment, business or profession).

within a province that has passed legislation deemed to be substantially similar to PIPEDA[418]. In that case, this provincial legislation applies to the processing of personal information taking place within that province. Any processing that takes place across provincial or international borders or that is carried out by federally regulated businesses (regardless of where it takes place) remains subject to PIPEDA. So far, Quebec, Alberta and British Columbia have been found to have substantially similar (comprehensive) privacy legislation, while the health-related privacy laws of Ontario, New Brunswick, Nova Scotia and Newfoundland and Labrador have been declared substantially similar to PIPEDA with respect to health information. However, this does not affect personal data transferred from the EU/EEA to Canada on the basis of the adequacy decision; data transfers from the EU/EEA under the adequacy decision are considered cross-border data transfers, which are subject to PIPEDA.

While the definition of personal information under PIPEDA (i.e., "information about an identifiable individual"[419]) has not changed since the adoption of the adequacy decision, this notion has been further interpreted by the OPC, case law and guidance. In particular, it has been clarified the definition of personal information must be given a broad and expansive interpretation[420], similar to the one under Regulation (EU) 2016/679 (GDPR)[421], taking into account whether there is a serious possibility that an individual could be identified through the use of that information, either alone or in combination with other Information[422]. For example, a decision of the OPC has clarified that de-identified information remains personal information if it is still possible to link the data back to an identifiable individual[423].

Since the adoption of the adequacy decision, the main data protection principles provided by PIPEDA, which are closely aligned to the corresponding principles under EU data protection rules, have not changed. This is the case for the principle of purpose limitation (subsection 5(3)), purpose specification (Principle 4.2 of Schedule 1 PIPEDA) data accuracy (Principle 4.6 of Schedule 1), data minimisation (Principles 4.4 and 4.5, of Schedule 1), data retention (Principle 4.5 of Schedule 1), security (Principle 4.7 of Schedule 1), accountability (Principle 4.1 of Schedule 1), and transparency (Principle 4.8 of Schedule 1). At the same time, several aspects of the legal framework have been further clarified and developed, either through legislative amendments or through case law and/or guidance of the OPC.

---

[418] The procedural aspects for such a determination are laid down in the "Process for the Determination of Substantially Similar Provincial Legislation by the Governor in Council", published by Industry Canada. It is done by the Governor in Council, based on a recommendation from the Minister of Industry, which first has to consult the OPC. For a provincial law to be considered substantially similar to PIPEDA, three requirements need to be fulfilled: the law must (1) incorporate all 10 principles of Schedule 1 (which set out the data protection principles, individual rights and obligations for controllers/processors); (2) provide for an independent and effective oversight and redress mechanism with powers to investigate; and (3) restrict the collection, use and disclosure to purposes that are appropriate or legitimate.

[419] Section 2(1) PIPEDA.

[420] Examples of types of information that are considered to be personal information include, bank account numbers, credit reports, biometric information, GPS tracking information, IP addresses, patient records, etc. See https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_02/.

[421] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[422] Gordon v. Canada (Health) (2008) FC 258.

[423] Case summary 2009-018, available at: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2009/pipeda-2009-018/.

In particular, the requirements for lawfulness of processing have been further strengthened in different ways. As a general principle, PIPEDA requires the knowledge and consent of the individual for any collection, use or disclosure of personal information[424], although PIPEDA also contains certain exceptions[425] (see below). The requirements for valid consent have been reinforced by an amendment to PIPEDA introduced by the Digital Privacy Act (2015)[426], by making clear that that consent is only valid if it is reasonable to expect that individuals understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting[427]. According to the guidance of the OPC[428], this requires that individuals are provided with information on what personal information will be collected, the purpose of processing, the third parties with whom information will be shared and possible (negative) consequences for the individual (e.g., financial loss, negative effects on credit records, etc.). Organisations must provide this information in an easily accessible form, provide individuals with a clear and easily accessible choice (not) to consent, obtain new consent when making relevant changes to their privacy practices and allow consent to be withdrawn.

Moreover, case law and guidance have provided further clarifications on the form and way consent should be obtained, which may vary, depending on the circumstances and type of information[429]. A Supreme Court decision in 2016 confirmed that, in determining whether consent must be expressly given, organisations need to take into account the sensitivity of the information and the reasonable expectations of the individual, both of which depend on the specific circumstances of the case[430]. OPC guidance and decisions specify that express consent is, in principle, the most appropriate form in any circumstance[431] and must in any

[424] Principle 4.3, Schedule 1, PIPEDA. PIPEDA does not apply a general concept of data 'processing', but rather distinguishes between the collection, use and disclosure of personal information.

[425] These exceptions typically correspond to situations where it is impossible in practice to obtain consent and the processing is urgently necessary in the interest of the individual (e.g., in the context of an emergency), or where knowledge of the individual would undermine certain specific purposes of processing (e.g., in the context of a criminal investigation). For example, collection without consent is allowed where it is clearly in the interest of the individual and consent cannot be obtained in a timely way (paragraph 7(1)(a); see also the corresponding ground for use in paragraph 7(2)(d); or where knowledge or consent would compromise the availability or accuracy of the information and the collection, use or disclosure takes place for the purpose of investigating a breach of an agreement or a violation of the law (paragraphs 7(1)(b),7(2)(d) and 7(3)(d.1) PIPEDA). Similarly, organisations can for instance use and disclose personal information in the context of an emergency that threatens the life, health or security of an individual (paragraph 7(2)(b) and 7(3)(e) PIPEDA) and may disclose it to collect a debt owed by the individual, to comply with a subpoena or warrant, or to provide it to a specialised institution for the purpose of the conservation of records of historic or archival importance (paragraph 7(3)(b), (c) and (g) PIPEDA).

[426] PIPEDA already required that organisations make a reasonable effort to ensure that individuals are informed about the purposes for which the information will be used (Schedule 1, Principle 4.3.2 PIPEDA).

[427] Section 6.1 PIPEDA.

[428] Available at: https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/.

[429] For example, an application form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent; a checkoff box may be used to allow individuals to request that their names and addresses not be given to other organisations; individuals who do not check the box are assumed to consent to the transfer of this information to third parties; consent may be given orally when information is collected over the telephone; or consent may be given at the time that individuals use a product or service (Schedule 1, Principle 4.3.7 PIPEDA).

[430] Supreme Court of Canada, Royal Bank of Canada v. Trang, 2016.

[431] See https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-

event be obtained when the information is sensitive (see below on the notion of sensitivity under PIPEDA), when the processing is outside of the reasonable expectations of the individual (e.g., certain sharing of information with a third party, tracking of location), or when it creates a meaningful risk of significant harm (which is to be understood broadly, including both material and reputational impact). Implied or opt-out consent are only allowed in limited and strictly defined circumstances[432].

Since the adoption of the adequacy decision, some additional exceptions to consent have been introduced, which may permit the collection, use or disclosure of personal information without obtaining consent from the individual for specific and circumscribed purposes[433]. For example, the Digital Privacy Act (2015) introduced exceptions that allow collection and use (1) when personal information is contained in a witness statement and the collection or use is necessary to assess, process or settle an insurance claim; and (2) when personal information was produced by the individual in the course of employment, business or profession and the collection or use is consistent with the purpose for which the information was produced[434]. In addition, exceptions were introduced allowing the use and disclosure of personal information in the context of prospective and completed business transactions (e.g., in case of a merger or sale of business, but not in case of business transactions where the primary purpose or result is the purchase, sale or other acquisition or disposition, or lease, of personal information[435]) under certain conditions[436]. Finally, other exceptions were added to permit federal works,

---

bulletins/interpretations_07_consent/ and the cases cited there (in particular PIPEDA Case Summary #2003-192 and #2003-203.

[432] For example, the OPC has accepted that individuals had given implied consent to the disclosure of their data in the context of litigation or dispute resolution, where personal data had been disclosed by an organisation to obtain expert advice of a third party for the purpose of defending itself (PIPEDA Case Summary #2009-003 and #2009-016). The OPC has also clarified that an opt-out mechanism may be acceptable where: (1) The personal information is demonstrably non-sensitive in nature and context; (2) The context in which information is shared is limited and well-defined as to the nature of the personal information to be used or disclosed and the extent of the intended use or disclosure; (3) the purposes of processing are stated in a reasonably clear and understandable manner and brought to the individual's attention at the time the personal information is collected; (4) the organisation obtains consent for the use or disclosure at the time of collection, or informs individuals of the proposed use or disclosure, and offers the possibility to opt out, at the earliest opportunity; and (5) the organisation establishes a convenient procedure for opting out, with the opt-out taking effect immediately and prior to any use or disclosure of personal information for the proposed use or disclosure. See: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_07_consent/.

[433] To the extent that these exceptions concern obligations to provide personal information to criminal law enforcement or national security authorities, or to cooperate on a voluntary basis, they are described in paragraphs 7(3)(c.1), 7(3)(c.2), 7(3)(d) and 7(d.1 – 4), see sections 2.2.1 and 2.2.2.

[434] Sections 7(1)(b.1) and (b.2), as well as Section 7(2)(b.1) and (b.2) PIPEDA.

[435] Section 7.2(4) PIPEDA.

[436] In particular, organisations that are parties to a prospective business transaction (Section 7.2(1) PIPEDA) may use and disclose personal information if (1) they have entered into an agreement that requires the organisation that receives the information to use and disclose the information solely for purposes related to the transaction, to protect the information by security safeguards appropriate to the sensitivity of the information and to return or destroy the information within a reasonable time if the transaction does not proceed; and (2) the personal information is necessary to determine whether to proceed with the transaction and, if the determination is made to proceed with the transaction, to complete it. Similarly, organisations that are party to the transaction are also allowed to use and disclose personal information in relation to a completed business transaction (Section 7.2(2) PIPEDA) if (1) they have entered into an agreement that requires each of them to use and disclose the information solely for purposes for which it was collected, permitted to be used or disclosed before the transaction was completed; to protect the information by appropriate security safeguards; and to give effect to a withdrawal of consent by the individual; (2) the information is necessary for carrying on the business that was

undertakings or businesses to collect, use and disclose personal information if necessary to establish, manage or terminate an employment relationship and the organisation has informed the individual thereof[437].

Case law and guidance of the OPC have furthermore elaborated on the requirements for the legitimacy/lawfulness of data processing, regardless of whether personal information is processed on the basis of consent, or an exception applies. In particular, PIPEDA provides that any collection, use or disclosure of personal information may only take place "for purposes that a reasonable person would consider are appropriate in the circumstances"[438]. In Turner v. Telus Communications Inc, the Federal Court[439] set out a number of factors that should be taken into account to determine whether a purpose is appropriate, including the degree of sensitivity of the personal information at issue, whether the processing would be effective in meeting the organization's need, whether there are less invasive means of achieving the same ends at comparable cost and with comparable benefits and whether the loss of privacy is proportional to the benefits[440]. Consequently, organisations are required to engage in a balancing of interests of the individual and the organisation itself. In order to determine the appropriateness of a purpose, an organisation must take into account the particular facts surrounding the collection, use and disclosure.

Another area of the Canadian data protection regime that has developed since the adoption of the adequacy decision concerns the requirements with respect to security safeguards. In 2015, a mandatory data breach notification requirement was introduced, which entered into force on 1 November 2018. Organisations are now required to report breaches to the OPC and concerned individuals, if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual[441]. To determine whether that is the case, organisations have to take into account factors such as the sensitivity of the personal information, the probability that the information has been, is being or will be misused, etc.[442]. Organisations must provide the notification as soon as feasible after determining that the breach has occurred[443], maintain a record of every breach[444] and provide such records to the Privacy Commissioner upon request. Deliberately failing to report a breach or maintain data breach records are offences subject to fines[445].

PIPEDA requires organizations to be accountable for personal information under their control and sets out a number of obligations in this regard. Guidance developed by the OPC has also

---

the object of the transaction; and (3) one of the parties notifies the individual, within a reasonable time after the transaction is completed, of the disclosure of his/her information.

[437] Section 7.3 PIPEDA.

[438] Section 5(3) PIPEDA. See also https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gd_53_201805/.

[439] The Federal Court is Canada's first instance court with jurisdiction over federal matters. Its decisions can be appealed before the Federal Court of Appeal and the Supreme Court of Canada.

[440] Turner et al v. Telus Communications Inc., 2005 FC 1601.

[441] Section 10.1(1) and 10.1(3) PIPEDA. Significant harm includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property (Section 10.1(7) PIPEDA).

[442] Section 10.1(8) PIPEDA.

[443] Section 10.1(3) and (6) PIPEDA.

[444] Section 10.3(1)-(2) PIPEDA.

[445] Section 28 PIPEDA.

further clarified how the accountability requirements of PIPEDA should be implemented[446], for instance by developing privacy management programs, appointing privacy officers or offices, keeping records and establishing internal reporting mechanisms, conducting internal audit and assurance programs to monitor compliance, developing personal information inventories, conducting risk assessments and developing training and education programs.

As regards the processing of special categories of data, PIPEDA does not provide for a closed listed of categories that are subject to additional protections. Instead, PIPEDA considers any information as potentially sensitive, depending on the circumstances and context in which it is collected/used/disclosed. This has the potential to apply additional protections to a broader range of personal information depending on the circumstances. Since the adequacy decision, the OPC and the courts have considered the question of sensitivity in a variety of cases. In 2022, the OPC consolidated existing case law and OPC decisions in an interpretation bulletin clarifying that certain types of information will generally be considered sensitive because of the specific risks to individuals when said information is collected, used or disclosed. This includes information such as health and financial data, ethnic and racial origins, political opinions, genetic and biometric data, an individual's sex life or sexual orientation, and religious/philosophical beliefs[447]. Such information is subject to specific requirements as regards the form and way in which consent is obtained (see earlier) and the security measures to be put in place[448].

As regards individual rights, there have been several developments in the Canadian legal framework since the adoption of the adequacy decision. PIPEDA continues to provide individuals with rights of access[449] and correction, and, while PIPEDA in principle does not create a separate right to deletion[450], the OPC has indicated that a combination of provisions may create rights for individuals/obligations for organisations to delete personal information[451]. For example, the OPC considers that, where individuals withdraw consent[452],

---

[446] See https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-compliance-and-training-tools/gl_acc_201204/#f and the additional guidance mentioned there.

[447] See https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_10_sensible/. Other types of data, e.g., trade union membership, may also be considered sensitive depending on specific circumstances, for instance if their processing leads to a risk of discrimination.

[448] Principle 4.7 of Schedule 1.

[449] Principle 4.9. Since the Commission's adequacy decision was adopted, one additional ground for refusing an access request was added to PIPEDA in 2005 by the Public Servants Disclosure Protection Act that allows an organisation to refuse access if the personal information was created for the purpose of a disclosure or investigation under that Act (paragraph 9(3)(e) PIPEDA). The purpose of this amendment was to protect the identity of parties in disclosures and investigations about wrongdoing in public bodies.

[450] Principle 4.9.5 stipulates that an individual must be able to challenge the accuracy and completeness of his/her information and have it amended as appropriate, which may involve the correction, deletion or addition of information.

[451] According to a draft position on online reputation, the OPC indicated that a combination of principles could provide for the right to deletion. For example, the right to withdraw consent under Principle 4.3.8 (subject to certain restrictions) and an organisation's obligation to destroy personal information that is no longer needed (Principle 4.5.3), taken together, could provide such a right with respect to information the individual provided. Likewise, for information provided by others, the OPC is of the view that, under Principle 4.9.5, individuals should be provided a mechanism by which demonstrably inaccurate, incomplete or out of date information can be challenged and amended. The OPC has also taken the position that soliciting and posting of personal information for the purpose of incentivizing payment for its removal, would be considered inappropriate under

they should be able to delete information they have themselves provided to an online forum involved in a commercial activity, such as on a social network. The same reasoning has also been applied in a broader context, for instance in a case where an individual had requested deletion of personal information contained in an insurance form[453].

In addition, the entry into force of Canada's Anti-Spam Legislation (CASL) in 2014 introduced several safeguards that are relevant to the processing of personal information for direct marketing purposes[454]. CASL amended PIPEDA by limiting the possibility for processing an individual's electronic address without consent, if it is collected by the use of a computer program that is designed or marketed primarily for use in generating or searching for and collecting electronic addresses[455].

With respect to the rules in PIPEDA on international data transfers[456], certain requirements have been further interpreted and clarified by the OPC. In particular, as regards the sharing of data with a third party for processing (i.e., a 'processor') in a third country[457], the OPC has clarified that organisations are required to inform individuals of the risk that their personal information may be lawfully accessed under the laws of the third country. This approach has

---

subsection 5(3) of PIPEDA. Available at: https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-online-reputation/pos_or_201801/.

[452] If an individual withdraws consent (which is the most common legal basis under PIPEDA), the information should be deleted, unless another ground for processing still applies (e.g.,a legal obligation to retain data under financial sector legislation), see https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/ and Draft OPC Position on Online Reputation - Office of the Privacy Commissioner of Canada .

[453] Case Summary #2017-005 of 10 February 2017, available at: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2017/pipeda-2017-005/. While the concerned company initially refused, the OPC found that the request from the individual should have been treated as a withdrawal of consent to the processing. Since there was no legal obligation for the company to continue retaining the information, it had to be deleted.

[454] More generally, CASL prohibits (and subjects to administrative fines) the sending of commercial electronic messages without the recipient's consent (including by e-mail, social media and text messages); installing computer programs without the express consent of the owner of the computer system; making false or misleading representations to the public in the form of electronic messages; collecting personal information through the illegal access of a computer system; and collecting and using electronic addresses through computer programs (address harvesting).

[455] Section 7.1(2) PIPEDA.

[456] While PIPEDA does not distinguish between the sharing of personal information within Canada or the sending of personal information to other countries, it does regulate how personal information is transferred to third parties for processing on behalf of the transferring organisation (i.e., to processors) and how personal information may be disclosed to another organisation (i.e., another controller). Such scenarios may result in personal information being 'onward transferred' to organisations in other countries.

[457] Organisations may also 'disclose' personal information to third parties (which would be characterised as controller to controller). This situation is different from when personal data is 'transferred' to another organisation to conduct processing on the transferring organisation's behalf (controller to processor), governed by the accountability principle (Principle 4.1.3) which requires the transferring organisation to use contractual or other means to ensure a comparable level of protection. As explained earlier, disclosures take place with the knowledge and consent of the individual, unless one of the specific exceptions apply. While the exceptions most likely will result in disclosures within Canada, it is possible that a disclosure made pursuant to an exception could result in a transfer of personal information across international borders. Even in those exceptional cases, individuals will have been generally informed about the purpose of processing, the third parties with whom data will be shared and possible risks and other consequences at the time of collection of their data by the Canadian organisation (Guidelines for obtaining meaningful consent - Office of the Privacy Commissioner of Canada), given that the personal information will in principle have been collected from Europe on the basis of consent (see earlier).

been applied by the OPC in concrete cases that were triggered by complaints from individuals[458].

1.2. Oversight, enforcement and redress

The OPC is the independent authority charged with oversight and enforcement of PIPEDA[459]. In addition to its power to investigate complaints and undertake audits, it is also tasked with developing and conducting information programs to foster public understanding, undertaking research, encouraging organisations to comply with PIPEDA and otherwise promoting the protection of personal information under PIPEDA[460].

In terms of powers, the OPC may participate in sector- or issue-wide international privacy sweeps, issue letters of concern to organizations. With respect to its more formal enforcement authorities, it may ask an organization for access to their internal breach records, carry out audits[461] and conduct complaint investigations (in response to a complaint or on its own initiative)[462]. In carrying out audits and investigations, the OPC has access to any relevant information, may summon and enforce the appearance of persons and compel the production of evidence[463]. Upon completing an investigation or audit, the OPC issues a report setting out the findings and recommendations[464]. Since the adoption of the Commission's adequacy decision, the powers of the OPC under PIPEDA have been strengthened by amendments introduced by the Digital Privacy Act in 2015. Following this amendment, the OPC may now enter into a compliance agreement with an organisation if it believes on reasonable grounds that an organisation has violated, is about to violate or is likely to violate PIPEDA[465]. Such a compliance agreement may contain any terms the OPC deems necessary to ensure compliance and is considered a settlement with the concerned organisation. At the same time, compliance agreements do not preclude individuals from obtaining judicial redress and do not prevent the prosecution of an offence[466]. If an organisation fails to comply with the agreement, the OPC

[458] See for example PIPEDA Case Summary #2007-386, in which the Commissioner found that an organisation should have made reasonable efforts to inform the individual of the transfer of personal information to a third-party service provider, see https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2007/pipeda-2007-386/. In another case (see PIPEDA case summary #2008-394), the Commissioner held that a company in Canada that outsources personal information processing to a company that operates in another country should notify its customers that the information may be available to the government of that country or its agencies under a lawful order made in that country, see https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2008/pipeda-2008-394/.

[459] The Office consists of a Privacy Commissioner, assisted by three Deputy Commissioners. The Commissioner is appointed by the Governor in Council after approval by the Senate and House of Commons for a renewable term of seven years and may only be removed by the Governor in Council for cause on address of the Senate and House of Commons (Section 53(1)-(2) Privacy Act). This would require that the House of Commons adopts a motion for an Address requesting the removal of the Commissioner and that the Senate unites with the House in that Address. The Commissioner must engage exclusively in the duties of his/her office and may not hold any other public office for reward or engage in any other employment for reward (Section 54(1) Privacy Act).

[460] Section 24 PIPEDA.

[461] Section 18(1) PIPEDA.

[462] Section 11(1) and (2) PIPEDA.

[463] Section 12.1(1) PIPEDA (complaint investigations) and Section 18(1) PIPEDA (audits).

[464] Section 13 PIPEDA (complaint investigations) and Section 19(1) PIPEDA (audits). If the OPC considers that it is in the public interest to do so, it may make public any information that comes to its knowledge in the performance or exercise of any of its duties/powers (Section 20(2) PIPEDA). If there is evidence of a criminal offence, the OPC may report such information to the Attorney General of Canada or a province (Section 20(5) PIPEDA).

[465] Section 17.1(1) PIPEDA.

[466] Section 17.1(4) PIPEDA.

may apply to the Federal Court to obtain an order requiring the organisation to do so[467]. As explained in more detail below, the OPC actively exercises its powers to enforce compliance with PIPEDA.

As regards the possibility for individuals to obtain redress, different avenues continue to be available in the Canadian system. In particular, individuals may turn directly to organisations[468], file a complaint with the OPC[469] and obtain judicial redress (against organisations[470] or against the findings of the OPC[471]), which may lead to different types of remedies, including binding orders to bring the handling of personal information in compliance with PIPEDA and compensation for damages.

Since the adoption of the adequacy decision, the OPC has carried out a number of important investigations under PIPEDA. Among the most prominent cases are the investigation of a data breach at Equifax in 2019 (which led to the conclusion of a compliance agreement[472]), the use of facial recognition tools by Clearview in 2021 (which was a joint investigation with provincial data protection authorities that led to provincial commissioners issuing binding orders requiring Clearview to stop several practices and delete personal data that was unlawfully collected[473]), the Facebook/Cambridge Analytica scandal (as part of which the

[467] Section 17.2(2) PIPEDA. The OPC has entered into five compliance agreements. To date, it has not had to seek an order from the Federal Court to enforce any of these agreements.

[468] Principle 4.10, Schedule 1, PIPEDA. Organisations have to put in place procedures to handle complaints and inquiries (Section 4.10.2 of Schedule 1). All complaints must be investigated and, if they are found to be justified, an organisation must take appropriate measures, including, if necessary, amending policies and practices (Section 4.10.4 of Schedule 1).

[469] Section 11(1) PIPEDA. The OPC may attempt to resolve complaints by means of dispute resolution mechanisms such as mediation and conciliation (Section 12.1(2) PIPEDA.). After investigating a complaint, the OPC prepares a report with its findings and recommendations, any settlement that was reached, a request to the organisation to provide notice of action taken to implement the recommendations (if appropriate) and the recourse for the individual (Section 13 PIPEDA).

[470] After receiving the OPC's report or being notified of the discontinuation of an investigation, an individual may apply to the Federal Court for a hearing in respect of any matter in respect of which the complaint was made, or that is referred to in the OPC's report (Section 14(1) PIPEDA). The Court conducts a de novo examination of the case. The OPC may also apply to the Federal Court (with the individual's consent) or appear on behalf of the individual (Section 15 PIPEDA). In accordance with Section 16 PIPEDA, the Federal Court may, in addition to any other remedies, 1) order an organisation to correct its practices to ensure compliance; 2) order an organisation to publish a notice of any action taken or proposed to correct its practices; and 3) award damages to the complainant, including for any humiliation that was suffered. Separately, individuals may also be able claim damages by invoking a tort (e.g., the tort of inclusion upon seclusion), see Jones v. Tsige, 2012 ONCA 32, where the Ontario Court of Appeal concluded that PIPEDA did not preclude the court from recognising the tort of inclusion upon seclusion.

[471] Individuals and/or organisations may challenge decisions of the OPC pursuant to Section 18.1 of the Federal Courts Act. The Federal Court may grant relief if it would be satisfied that the Commissioner (1) acted without jurisdiction, acted beyond its jurisdiction or refused to exercise its jurisdiction; (2) failed to observe a principle of natural justice, procedural fairness or other procedure that it was required by law to observe; (3) erred in law in making a decision or an order, whether or not the error appears on the face of the record; (4) based its decision or order on an erroneous finding of fact that it made in a perverse or capricious manner or without regard for the material before it; (5) acted, or failed to act, by reason of fraud or perjured evidence; or (6) acted in any other way that was contrary to law. The Court may order to do any act or thing that was unlawfully refused, delayed or failed to be carried out, or declare invalid or unlawful, quash or set aside and refer back for determination, prohibit or restrain, a decision, order, act or proceeding.

[472] See https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-001/.

[473] See https://www.priv.gc.ca/en/opc-news/news-and-announcements/2021/an_211214/.

OPC applied to the Federal Court in 2020 to seek a binding enforcement order to ensure that Facebook's unlawful privacy practices are corrected[474]).

Its annual reports to the Parliament also show that the OPC deals with a number of complaints under PIPEDA on an annual basis: for example, the annual report of 2018-2019 refers to 380 accepted complaints, 178 closed through early resolution and 104 closed through a standard investigation[475]; the report of 2019-2020 to 289 accepted complaints, 221 closed through early resolution and 97 closed through standard investigation[476]; and the report of 2020-2021 to 309 accepted complaints, 210 closed through early resolution and 86 closed through standard investigation[477].

The OPC has also been very proactive in providing guidance on the interpretation and application of PIPEDA, including on topics such as the processing of employee data, biometric data, cloud computing, the development of mobile apps, online behavioural advertising, the processing of data from children, e-marketing, internet of things, etc.[478]. Moreover, the OPC issued several 'interpretation bulletins' that summarise the general principles that emerge from court decisions and OPC findings, e.g., on the definition of personal information, accountability, accuracy, transparency and consent[479]. The OPC also developed a number of tools to assist organisations with training and compliance efforts[480], and provides detailed information on various topics to raise awareness among data subjects (e.g., specifically targeting certain groups such as parents, teachers and seniors; on mobile devices; human resource issues; data concerning health, etc.)[481].

Finally, the OPC regularly engages with stakeholders, such as businesses (e.g., through 19 advisory engagements in the period of 2019-2020 and 13 in 2020-2021), and the Parliament (e.g., with 8 appearances before Parliamentary committees in the period of 2019-2020 and 3 in 2020-2021, and e.g., having reviewed 29 bills, laws and parliamentary studies for privacy implications during the period of 2019-2020 and 17 in 2020-2021). The OPC also advised the government and Parliament on the protection of personal data in the context of the response to the Covid-19 pandemic[482] and has been an active voice in debates about reforms of data protection legislation at both provincial and federal level[483].

---

[474] See https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-complaints-and-enforcement-process/court_p/na_fb_20200206/. The litigation before the Federal Court currently remains ongoing.

[475] Available at: https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201819/ar_201819/.

[476] Available at: https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201920/ar_201920/.

[477] Available at: https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/ar_202021/#toc5.

[478] Available at: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/issue-specific-guidance-for-businesses/?Page=1.

[479] Available at: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/.

[480] Available at: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-compliance-and-training-tools/.

[481] Available at https://www.priv.gc.ca/en/for-individuals/.

[482] See e.g., https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2020/parl_20200529/.

[483] See e.g.,the interventions of the OPC before the Committee on Institutions of the National Assembly of Quebec (https://www.priv.gc.ca/en/opc-news/speeches/2020/sp-d_20200924/) and the Special Committee to review British Colombia's Personal Information Protection Act (https://www.priv.gc.ca/en/opc-news/speeches/2021/s-d_20210622/). The OPC also commented several times on proposed legislative reforms at

2. ACCESS TO AND USE OF PERSONAL DATA TRANSFERRED FROM THE EUROPEAN UNION BY PUBLIC AUTHORITIES IN CANADA

2.1. General legal framework

The limitations and safeguards that apply to the collection and subsequent use of personal information by Canadian public authorities for criminal law enforcement and national security purposes follow from the overarching constitutional framework, specific laws regulating data access, as well as the rules that apply to the processing of personal information by the public sector.

First, access to personal information by Canadian public authorities is governed by general principles that follow from the Canadian Constitution and have been further developed through case law. In particular, Section 8 of the Canadian Charter of Rights and Freedoms (Charter), which is part of the Canadian Constitution, guarantees that "everyone has the right to be secure against unreasonable search or seizure"[484]. This provision protects against unjustified intrusions on a person's "reasonable expectation of privacy"[485], which extends to: personal privacy (i.e., physical/bodily privacy[486]), territorial privacy (i.e., of a place, in particular an individual's home[487]) and informational privacy (i.e., "the claim of individuals […] to determine for themselves when, how, and to what extent information about them is communicated to others"[488]).

According to the Supreme Court of Canada, the interception and recording of a private communication by public authorities constitutes a serious intrusion into privacy rights and

federal level, including of PIPEDA, see e.g., https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_ethi_c11_2105/.

[484] A 'search' is any action by a public authority that engages a reasonable expectation of privacy (Hunter et al. v. Southam Inc. [1984] 2 S.C.R. 145). This includes searching for tangible or intangible items, including spoken words and electronic data (See e.g., R. v. Morelli, [2010] 1 S.C.R. 253). A 'seizure' is the "taking of a thing from a person by a public authority without that person's consent" where this interferes with a reasonable expectation of privacy (R. v. Dyment, [1988] 2 S.C.R. 417 at 431; Quebec (Attorney General) v Laroche, [2002] 3 S.C.R. 708 at para 52). This includes where a person is required to produce information (e.g., R. v. McKinlay Transport Ltd., [1990] 1 S.C.R. 627 at 642 and R v Marakah, [2017] 2 S.C.R. 59), Obtaining something from a person other than the one whose rights are affected also constitutes a seizure, e.g., Dyment; R. v. Dersch, [1993] 3 S.C.R. 768. For consent to be valid, it must be fully informed (R. v. Borden, [1994] 3 S.C.R. 145) and voluntarily given (see e.g., Godbout v. Longueuil (City), [1997] 3 S.C.R. 844 at 72). A third party cannot waive the reasonable expectation of privacy of another individual by 'consenting' to a search or seizure (R v Cole, 2012 and R v Reeves, [2018] 3 S.C.R. 531).

[485] Hunter v. Southam Inc., [1984] 2 S.C.R. 145 at 159; R. v. Gomboc, [2010] 3 S.C.R. 211 at 17, 75. Whether state action interferes with a reasonable expectation of privacy and therefore constitutes a search or seizure is determined on the basis of the totality of the circumstances, taking into account (R. v. Edwards, [1996] 1 S.C.R. 128 at 45, affirmed in R v Tessling at para 19. R. v. Cole 2012 SCC 53; R v Patrick, [2009] 1 S.C.R. 579 at para 27.): (1) the subject matter of the search; (2) whether the individual had a direct interest in the subject matter (which requires the individual to demonstrate that his or her own privacy interest was breached, as opposed to the interests of third parties, Edwards at 34); (3) whether the individual had a subjective expectation of privacy in the subject matter (e.g., in case of activities taking place at one's home (Gomboc, at 25), or with respect to text messages sent to a known recipient (Jones, at 15; Marakah, at 23); and (4) whether this subjective expectation of privacy was objectively reasonable. Additional factors drawn from the Supreme Court's jurisprudence may also be taken into account, including whether the object was in the hands of third parties (and whether these had an obligation of confidentiality), the invasiveness of the method of the search (e.g., covert interception of communications), the nature of the information collected, etc. (see e.g., Cole, at 45; Tessling at 32; Patrick at 27).

[486] R. v. Tessling, at 21.

[487] See e.g., Semayne's Case, [1558-1774] All E.R. Rep. 62 (1604), at 63.

[488] Tessling at 23.

would (unless all parties to the conversation expressly consent to the recording) be considered a search within the meaning of Section 8 of the Charter, generally only permissible with prior judicial authorisation[489]. Similarly, personal computers (because of the vast amounts of information they contain, including intimate correspondence, details of financial, medical and personal situations, internet browsing histories, etc.)[490] and internet subscriber information (as it may not only relate to the person's name or address, but to his or her identity as the source or possessor of certain information) engage a high level of privacy[491].

To comply with Section 8 of the Charter, a search/seizure must be "reasonable". In principle, this requires prior judicial authorisation, when the court is satisfied that "the public's interest in being left alone by government must give way to the government's interest in intruding on the individual's privacy in order to advance the goals of law enforcement"[492]. For a warrantless search or seizure, there is therefore a presumption of "unreasonableness," which can be rebutted by the relevant public authority by establishing that the search was authorised by law, the law itself is reasonable[493], and the manner in which the search or seizure takes place is reasonable[494]. If no prior judicial authorisation is required, additional safeguards may be required, such as after-the-fact notice to the target of the search and record-keeping requirements[495]. Even when a search or seizure is authorised pursuant to a warrant or reasonable law, it can be found to be in violation of Section 8 because of the manner in which it is carried out[496]. In particular, a search or seizure must be no more intrusive than is reasonably necessary to achieve its objectives[497].

All laws and government actions at both the federal and provincial levels must conform to the Charter. As described in more detail in sections 2.2.1 and 2.3.1, the general principles following from the Charter are reflected in the specific laws that regulate the powers of law enforcement and national security authorities.

Moreover, the processing of personal information by Canadian federal public authorities (including federal criminal law enforcement authorities and national security authorities) is subject to the Privacy Act (R.S.C., 1985, c. P-21)[498]. The Act limits the collection of personal information by federal institutions to what relates directly to their programs or activities and regulates its use, disclosure and retention[499]. It reflects the principles of purpose limitation, data accuracy, transparency and storage limitation, and provides individuals with a right of

[489] R. v. Duarte [1990] 1 S.C.R. 30 at pages 42-43. Confirmed in Wakeling v United States of America, 2014 SCC 72, [2014] 3 S.C.R. 549.
[490] Morelli at 105; R. v Vu, [2013] 3 S.C.R. 657 at 24, 40-45.
[491] Spencer at 47, 51.
[492] Hunter v Southam at p. 160.
[493] A law authorising an invasion of privacy is reasonable if it strikes a proper balance between the interests of society and the rights of individuals (see e.g., R. v. Shoker, [2006] 2 S.C.R. 399 at 42-43). Relevant factors to consider in this context may include whether the law reflects the least intrusive means by which a state interest can be achieved (see e.g., Goodwin v. British Columbia (Superintendent of Motor Vehicles), [2015] 3 S.C.R. 250 at 65), whether the powers are narrowly targeted (R. v. Chehil, [2013] 3 S.C.R. 220 at 28), and the reliability of the procedure used (e.g., a method of searching that captures an inordinate number of innocent individuals cannot be reasonable, Chehil at 51).
[494] R. v. Collins, [1987] 1 S.C.R. 265 at 278.
[495] Tse, at 83-84; Chehil at 58; R. v. Fearon 2014 SCC 77, at 82.
[496] R. v. Genest, [1989] 1 S.C.R. 59; R. v. Cornell, [2010] 2 S.C.R. 142.
[497] R. v Vu, [2013] 3 S.C.R. 657.
[498] Schedule 3 of the Privacy Act.
[499] Sections 4, 7-9 of the Privacy Act.

access to their personal information and a right of correction[500]. The processing of personal information by provincial/territorial authorities (e.g., local criminal law enforcement authorities) is subject to similar personal information protection laws[501]. In particular, these laws impose limitations on the collection, use and disclosure of personal information, contain key personal information protection principles (such as transparency, accuracy, security, storage limitation and purpose limitation) and provide individuals with a right of access and correction. Moreover, all thirteen provinces and territories have an independent supervisory authority to oversee compliance and handle complaints.

These general limitations and safeguards can be invoked by individuals before independent administrative bodies (e.g., the OPC, provincial personal information protection authorities, the Civilian Review and Complaints Commission for the Royal Canadian Mounted Police and the National Security and Intelligence Review Agency) and courts to obtain redress (see sections 2.2.4 and 2.3.4).

2.2. Access and use by Canadian public authorities for criminal law enforcement purposes

In Canada, criminal law enforcement functions are carried out by different authorities. At federal and territorial[502] levels, these include the federal police force (the Royal Canadian Mounted Police, RCMP), as well as other bodies with specific competences, such as the Canada Border Services Agency, the Canada Revenue Agency, the Canadian Food Inspection Agency and the Competition Bureau. At provincial and municipal levels, criminal law enforcement functions are carried out by the RCMP or local police and peace officers. Canadian law imposes a number of limitations on the access and use of personal information for criminal law enforcement purposes by each of these authorities and provides oversight and redress mechanisms. The conditions under which such access can take place and the safeguards applicable to the use of those powers are described in the following sections.

2.2.1. Legal bases and applicable limitations/safeguards

Personal information transferred under the adequacy decision and processed by Canadian organisations subject to PIPEDA may be obtained by Canadian criminal law enforcement authorities by means of investigative measures under statutes providing for law enforcement access, the primary one being the Criminal Code or on the basis of anti-money laundering and anti-terrorist financing legislation; or through voluntary disclosures.

The Criminal Code provides Canadian criminal law enforcement authorities (at federal, provincial and municipal levels) with a legal basis to access personal information held by commercial operators through searches and seizures, the interception of communications, accessing tracking and transmission data, and the use of production orders. The Criminal Code lays down clear and precise rules on the scope and application of these measures, thereby ensuring that the interference with the rights of individuals will be limited to what is

[500] Sections 5(2), 6, 7, 8, and 12 of the Privacy Act.
[501] For an overview, see https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/provincial-and-territorial-privacy-laws-and-oversight/ and the relevant legislation referenced there.
[502] The RCMP is the police force for the three territories (Nunavut, Northwest Territories and Yukon), which do not have a separate police force.

necessary for a specific criminal investigation and proportionate to the pursued purpose. Moreover, to exercise any of these powers, prior judicial authorisation is in principle required (with certain exceptions, e.g., in emergencies, as described in more detail below)[503].

Searches or seizures may be permitted under a search warrant to take place if there are reasonable grounds to believe[504] that there is anything in a building, receptacle or place for which a connection with an offence can be established (e.g., anything that will produce evidence with respect to the commission of an offence)[505]. In terms of procedural safeguards, a search/seizure may as a general rule only take place on the basis of a court-issued warrant[506]. A search of a computer system in order to seize, reproduce or copy data, must be specifically authorised by the warrant[507]. In principle, the person subject to the search is present when the search is carried out and, where this is not the case, a copy of the warrant is left to inform the individual. Warrantless searches or seizures may take place if the conditions for obtaining a warrant exist but there are exigent circumstances that make it impracticable to obtain a warrant[508]. In accordance with case law, this will be the case if there is an "imminent danger of the loss, removal, destruction or disappearance of the evidence if the search is delayed"[509] or if there is a degree of urgency that necessitates action by law enforcement[510].

Specific limitations and safeguards apply to the interception of private communications[511], which in principle may only take place in the context of investigations of serious offences[512] and in most cases on the basis of a judicial authorisation. Procedurally, the application for the authorisation must in principle be signed by the Attorney General of the relevant province or

[503] In addition to the authorities noted (search warrants, production orders, authorizations to intercept private communications, transmission data recorder warrants, tracking warrants), there is also authority in the Criminal Code for a judge to issue a general warrant authorizing the use of a certain device, investigative technique or procedure, other measures that would, if not authorized, constitute an unreasonable search or seizure (Section 487.01(1) of the Criminal Code). Such a warrant may only be issued if the judge is satisfied that a) there are reasonable grounds to believe that an offence has been or will be committed and that information concerning the offence will be obtained through the use of the technique, procedure, device or other measure; b) it is in the best interests of the administration of justice to issue the warrant; and there is no other provision that would provide for a warrant, authorization or order permitting the technique, procedure, device or other measure. The warrant must contain terms and conditions to ensure that any search or seizure authorised by the warrant is reasonable in the circumstances (Section 487.01(3) of the Criminal Code).

[504] According to the Supreme Court, the 'reasonable grounds to believe' test is one of 'credibly based probability' or 'reasonable probability' (Baron v. R [1993] 1 S.C.R. 416 at paras 54,55). This requires a subjective and objective assessment of the facts. First, the judge must subjectively believe that there are reasonable grounds justifying the actions taken and, second, it must be objectively established that reasonable grounds do in fact exist (i.e., there must be sufficient evidence to support the belief). The totality of the circumstances should therefore be considered. See R v. Tse 2012 SCC 16 at para. 33, R v. Bernshaw 1995 1 S.C.R. 254 at para. 62, R v. Storrey 1990 1 S.C.R. 241 at paras. 16-17.

[505] This refers to the search warrant in section 487(1) of the Criminal Code.

[506] The application for a warrant and the warrant itself must contain a description of the things to be searched, the offence in respect of which the search is made, as well as the premise at which the search is to be carried out (See Form 1 and 5 referred to in the Criminal Code).

[507] Section 487(2.1) of the Criminal Code. The Supreme Court has confirmed that, because of the significant amounts of personal information they contain, computers and similar devices may only be searched if specifically authorised by a warrant. Consequently, a warrant to search a physical location may not implicitly authorise the search of electronic devices such as computers found at that location. See R. v. Vu, 2013 SCC 60.

[508] Section 487.11 of the Criminal Code.

[509] R v Grant, (1993), 84 C.C.C. (3d) 173 (S.C.C.), at 189.

[510] R v Goncalves, (1993), 81 C.C.C. (3d) 240 (S.C.C.) at 246.

[511] Interception includes listening to, recording or acquiring a communication or acquiring the substance, meaning of purport thereof (Section 183 of the Criminal Code).

[512] For example, high treason, forgery, endangering the safety of an aircraft, using explosives, participation in activities of terrorist groups, child pornography, kidnapping, etc. See Section 183 of the Criminal Code.

the Minister of Public Safety and Emergency Preparedness and submitted to a judge of a superior court of criminal jurisdiction[513]. An authorisation may be issued [514] if it is in the best interests of the administration of justice and other investigative procedures have been tried and have failed/are unlikely to succeed or the urgency of the matter is such that it would be impractical to carry out the investigation of the offence using only other investigative procedures[515]. An interception authorisation is valid for a maximum period of 60 days (one year for offences related to terrorism or criminal organizations) and may be renewed by the court once for the same period by a judge if the abovementioned conditions remain fulfilled[516]. Intercepting private communications in violation of the Criminal Code is an offence liable to imprisonment for a maximum of five years[517].

In terms of additional safeguards, the Criminal Code imposes specific reporting and transparency requirements. In particular, within 90 days after the end of the authorisation, the individual that was the object of the interception must be notified in writing and a certification of that notification must be provided to the court that authorised the interception[518]. A longer period for notification must be specifically requested when applying for authorisation and may not exceed three years[519]. Such extension may only be granted if the investigation of the offence to which the authorisation relates is ongoing and it is in the interest of justice[520]. In addition, the contents of private communications may only be used as evidence in judicial proceedings if the accused has been provided with reasonable notice of that intention together with a transcript of the communication and a statement setting out the time, place, date, and parties to the communication[521]. More generally, the Minister of Public Safety and Emergency Preparedness is required to issue an annual public report with, inter alia, the number of applications and authorisations, the number of persons identified in an authorisation against whom proceedings were commenced, the average period for which authorisation and renewals were granted, etc.[522]

Interception of private communications without a prior judicial authorisation by a police officer are permitted to take place (in the context of investigations of any offence) in two

[513] Section 185(1) of the Criminal Code. The application must provide detailed information, including on the offence under investigation, the type of communications to be intercepted and the names, addresses and occupations of the targeted individuals. Moreover, it must specify whether other investigative procedures have been tried and have failed or why it appears they are unlikely to succeed or that the urgency of the matter is such that it would be impractical to carry out the investigation - using only other investigative procedures.
[514] The warrant must itself also specify inter alia a) the offence in respect of which private communications may be intercepted; b) the type of private communication that may be intercepted; and c) the identity of the persons, if known, whose private communications are to be intercepted, as well as a general description of the place at which private communications may be intercepted and the manner of interception that may be used (Section 186(4) of the Criminal Code).
[515] Section 186(1) of the Criminal Code. The latter condition does not have to be fulfilled with respect to an offence related to terrorism or criminal organisations (Section 186(1.1) of the Criminal Code).
[516] Section 186(6) and (7), and Section 186.1 of the Criminal Code. If the urgency of the situation requires interception to start before an authorization could be obtained with reasonable diligence in accordance with the abovementioned procedure, the judge may authorize the interception in writing for a period of up to thirty-six hours (Section 188(2) of the Criminal Code). Applications for such urgency measures are made to especially appointed judges for this purpose and are followed up with a regular application under Section 185.
[517] Section 184(1) of the Criminal Code.
[518] Section 196(1) of the Criminal Code.
[519] Section 185(2)-(3) of the Criminal Code.
[520] Section 196(3) of the Criminal Code.
[521] Section 189(5) of the Criminal Code.
[522] Section 195 of the Criminal Code.

exceptional circumstances. First, this may be the case if there are reasonable grounds to believe that a) the urgency of the situation is such that an authorisation could not, with reasonable diligence, be obtained; b) the interception is immediately necessary to prevent an offence that would cause serious harm to any person or to property; and c) either the originator of the private communication or the person intended to receive it is the person who would commit the offence or is the (intended) victim[523]. In this case, the concerned individuals must be notified in the same way as was described above[524]. Second, a warrantless interception may take place by an agent of the state if a) either the originator of the communication or the person intended to receive it has consented to the interception; b) the authority believes on reasonable grounds that there is a risk of bodily harm to the person who consented to the interception; and c) the purpose of the interception is to prevent the bodily harm[525]. In that case, the content of the intercepted communications will only be admissible as evidence in court proceedings for the purposes of proceedings in which actual, attempted or threatened bodily harm is alleged[526].

In addition to intercepting the content of private communications, criminal law enforcement authorities may collect transmission data[527] if there are reasonable grounds to suspect that an offence has been or will be committed and the data will assist in the investigation[528]. Such collection may again only take place on the basis of a court-issued warrant. Case law[529] confirmed that such a warrant could be used "either to obtain names and records where the suspected phone number but not the name of the suspect is known, or alternatively, to produce the phone number and records, if any, where the police are able to provide the service provider with the name and address but not the cell phone number of the suspected person for whom they seek records".

Similarly, to collect data related to the location of a transaction, individual or thing (tracking data[530]), a warrant must be obtained. Such a warrant may authorise the use of a "tracking device" (a device, including a computer program, which may be used to obtain or record tracking data[531] or to transmit it by a means of telecommunication[532]) for a maximum period

[523] Section 184.4 of the Criminal Code. This report must also be made available to the Parliament (Section 195(4) of the Criminal Code).
[524] Section 196.1 of the Criminal Code.
[525] Section 184.1(1) of the Criminal Code.
[526] Section 184.1(2) of the Criminal Code.
[527] Defined as "data that (a) relates to the telecommunication functions of dialling, routing, addressing or signalling; (b) is transmitted to identify, activate or configure a device, including a computer program […], in order to establish or maintain access to a telecommunication service for the purpose of enabling a communication, or is generated during the creation, transmission or reception of a communication and identifies or purports to identify the type, direction, date, time, duration, size, origin, destination or termination of the communication; and (c) does not reveal the substance, meaning or purpose of the communication" (Section 492.2(6) of the Criminal Code).
[528] Sections 492.1(1) and 492.2(1) of the Criminal Code. The 'reasonable grounds to suspect' test engages the reasonable possibility, rather than probability, of crime. However, the suspicion cannot be so broad that it becomes a generalized suspicion (e.g., attached to a particular activity or location rather than a specific person). Whether or not there is a reasonable suspicion depends on the totality of the circumstances. The objective facts must be indicative of the possibility of criminal behaviour and a nexus must exist between the suspected criminal conduct and the investigative technique to be used. See R v. Chehil [2013] SCC 49, at paras. 27, 28 and 35-36.
[529] R v. Mahmood [2008] OJ No. 3922, at para. 128.
[530] Section 492.1(8) of the Criminal Code.
[531] Tracking data is defined as "data that relates to the location of a transaction, individual or thing."
[532] Section 492.1(8) of the Criminal Code.

of 60 days[533]. When used to track an individual's movement by identifying the location of a thing that is usually carried or worn by the individual, it may only be used if there are reasonable grounds to believe that an offence has been or will be committed and tracking the individual will assist in the investigation[534].

Under the Criminal Code, criminal law enforcement authorities may also obtain a production order[535] from a court, ordering a person to produce a copy of a document/prepare or produce a document containing data that is in their possession or control[536]. To issue a general production order, the judge must be satisfied that there are reasonable grounds to believe that an offence has been or will be committed, the document or data is in the person's possession or control and will produce evidence. For orders requiring the production of specific types of information, i.e., transmission data, tracking data or financial data[537], the judge must be satisfied that there are reasonable grounds to suspect that an offence has been or will be committed; the relevant information is in the persons control and will assist in the investigation of the offence[538].

As a general safeguard, warrants authorising the collection of tracking/transmission data and production orders are considered public records to which individuals can obtain access, unless a sealing order has been issued by a judge. A sealing order must be requested by a law enforcement authority at the time of applying for the warrant/order and may be issued if the disclosure would affect the course of justice (e.g., if it would compromise the identity of an informant, compromise an ongoing investigation, etc.) or the information might be used for an

[533] Section 492.1(3) and (5) of the Criminal Code. In the context of investigations in relation to organised crime and terrorism offences, a warrant may be valid for a maximum of one year, see para. 6 of the same Section.
[534] Section 492.1(2) of the Criminal Code.
[535] On the basis of the Criminal Code, the police or a judge may also compel an entity to preserve computer data (although this may not be applied to an entity that is itself the subject of the investigation of the offence, see Section 487.012(3) and 487.013(5) of the Criminal Code). In particular, the police may issue a preservation demand if there are reasonable grounds to suspect that an offence has been or will be committed or, in the case of an offence committed under a law of a foreign state, an investigation is being conducted by a person or authority with responsibility in that state for the investigation of such offences; and the computer data is in the person's possession or control and will assist in the investigation of the offence (Section 487.012 of the Criminal Code). Such a demand expires (unless revoked earlier) within 21 days in the case of an offence under Canadian law or within 90 days in case of an offence under foreign law (Section 487.012(4) of the Criminal Code). Preservation demands may not be renewed, and where continued preservation is needed, a preservation order would need to be obtained from a court. A judge may issue a preservation order under the same conditions, if the requesting police officer intends to apply or has applied for a warrant or an order in connection with the investigation to obtain a document containing the computer data (Section 487.013(1) if the Criminal Code). Preservation orders issued by a judge expire within 90 days (Section 487.013(6) of the Criminal Code). Entities subject to a preservation order or demand must destroy the computer data that would not be retained in the ordinary course of business as soon as feasible after the demand or order expires or is revoked (Section 487.0194 (1)-(2) of the Criminal Code), subject to criminal sanctions (Section 487.0199 of the Criminal Code).
[536] Section 487.014 of the Criminal Code. Entities receiving such orders may apply in writing to the judge that issued the order to revoke or change it, in accordance with Section 487.0193(1) of the Criminal Code. In that case, the entity is not required to prepare or produce the requested information until a final decision is made. The judge may revoke or amend the order if satisfied that it would be unreasonable in the circumstance to require the preparation or production of the information, or production of the information would disclose information that is privileged or otherwise protected by law (Section 487.0193(4) of the Criminal Code).
[537] This includes the account number of the person named in the order, the type of account, the status of the account and the date on which the account was opened or closed (Section 187.018(1) of the Criminal Code).
[538] See Section 487.015-487.018 of the Criminal Code.

improper purpose and this reason outweighs the importance of access to the information by the individual[539].

In addition to disclosing information pursuant to binding measures adopted under the Criminal Code, organisations subject to PIPEDA may in certain circumstances disclose information to public authorities on a voluntary basis, either on their own initiative or to comply with a request for the information. When receiving information in such cases, criminal law enforcement authorities may only use or disclose it in accordance with the requirements described in section 2.2.2. An organisation may collect and disclose personal information to a government institution on its own initiative when it has reasonable grounds to believe that the information relates to a violation of the law[540]. Organisations may also disclose personal information when receiving a request from a government institution[541] and may collect and use personal information for the purpose of such disclosure[542]. When making a request, the institution must identify its lawful authority to obtain the information. The existence of a reasonable expectation of privacy of the concerned individual is a central factor to take into account in determining whether there is such lawful authority.

Case law clarifies how these provisions are to be applied in practice. For example, the Ontario Court of Appeal found that the routine sharing of information with public authorities (in this case the informal sharing of energy consumption data by electricity provider with the police) does not comply with PIPEDA and needs to be distinguished from a situation where a service provider discloses specific information to the police with concerns that a crime has been committed[543]. The Supreme Court of Canada found that obtaining IP addresses (which can, when associated with an identity, reveal highly personal information) through a request where the police had no authority to compel compliance with that request constituted an unconstitutional search[544]. According to the Court, obtaining such information engaged a reasonable expectation of privacy and therefore constituted a search within the meaning of Section 8 of the Charter, requiring either a warrant or specific empowerment by law. The police could therefore not rely solely on PIPEDA's provisions relating to voluntary disclosures to obtain the information. Following this decision in 2014, all telecommunication providers that have published transparency reports have reported zero voluntary disclosures of subscriber information.

Finally, criminal law enforcement authorities may also indirectly receive personal information from Canada's Financial Intelligence Unit, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)[545], to which certain organisations subject to PIPEDA have to

[539] Section 467.3(1)-(2) of the Criminal Code. An application to terminate or vary a sealing order may be made to the judge who made the order or a judge of the court before which any proceedings arising out of the investigation in relation to which the warrant was obtained may be held (Section 467.3(4) of the Criminal Code).
[540] Section 7(3)(d)(i)-(ii) PIPEDA. The same applies if the information relates to national security, the defence of Canada or the conduct of international affairs.
[541] Sections 7(3)(c.1)(i) - (ii) PIPEDA.
[542] Section 7(1)(e)(i) and 7(2)(d) PIPEDA).
[543] R. v. Orlandis-Habsburgo, 2017 ONCA 649.
[544] R v. Spencer, 2014 SCC 43.
[545] FINTRAC is independent from law enforcement authorities and collects, analyses and discloses information to help detect, prevent and deter money laundering and terrorist financing activities in Canada and abroad. It was established to implement the international recommendations for combating money laundering and terrorist financing issued by the Financial Action Task Force. FINTRAC itself is subject to the Privacy Act and to specific requirements under the PCLMTFA regarding the handling of the information it receives, including e.g.,

disclose financial transaction information[546]. For example, under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCLMTFA), such organisations have to report on large electronic fund transfers[547], terrorist property[548], large cash transactions[549] and financial transactions for which there are reasonable grounds to suspect that they are related to the (attempted) commission of a money laundering or terrorist activity financing offence[550]. FINTRAC must in turn disclose financial intelligence information to criminal law enforcement authorities where it has reasonable grounds to suspect that the information would be relevant to investigating or prosecuting a money laundering or terrorist financing offence[551]. The information that may be reported includes the name of the person or entity involved in the transaction, the amount and type of currency involved, the transaction and account number, etc.[552] Information received from FINTRAC cannot be used as evidence, but is meant to support law enforcement authorities when applying for judicial authorisation of investigative measures (production orders, warrants). Any information received from FINTRAC can only be processed by a criminal law enforcement authority in accordance with the requirements described below in section 2.2.2.

2.2.2. Further use of the information collected

The processing of personal information collected by Canadian criminal law enforcement authorities is subject to the federal Privacy Act and privacy legislation at provincial/territorial level. The Privacy Act sets requirements on purpose limitation, accuracy, transparency and storage limitation[553] and specify the circumstances in which federal criminal law enforcement authorities may use or disclose personal information. Further processing (use and disclosure) without consent is only allowed under a limited number of grounds that are enumerated in the Act, e.g., when permitted by a federal statute, where necessary to comply with a warrant or subpoena, for internal audit purposes, or where the public interest in the processing clearly outweighs the invasion of privacy or where it clearly benefits the concerned individual[554]. The Act also requires public authorities to keep records of the personal information under their

---

on data retention, the destruction of information that is not required by law and the sharing of information with other (foreign) authorities (see e.g., Section 54(1)(d), Section 54(2) and Section 56.1 PCLMTFA.

[546] Entities that are required to report include accountants, casinos, financial entities, life insurance companies, brokers and agents, securities dealers, etc.

[547] I.e., of at least CAN$10 000 out of or into Canada in a single transaction or two or more transactions made within 24 hours by or on behalf of the same individual or entity Section 12(1)(b) and (c) of the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFR). This applies to financial entities, money services businesses and casinos.)

[548] I.e., property that is believed or known to be owned or controlled by or on behalf of a terrorist or terrorist group) Section 7.1 of the PCLMTFR and Section 8 of the Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism.

[549] I.e., of at least CAN$10 000 received in the course of a single transaction, or two or more cash amounts made within 24 hours by or on behalf of the same individual or entity, Section 12(1)(a) of the PCLMTFR.

[550] Section 7 PCLMTFA. This reporting obligation applies for example to financial entities; life insurance companies, brokers or agents; securities dealers, portfolio managers and investment counsellors that are provincially authorized; money services businesses; and accounting firms.

[551] Section 55(3) PCLMTFA. In addition, FINTRAC must under certain circumstances disclose information to other public authorities, such as the Canada Revenue Agency, the Canada Border Services Agency, the Communications Security Establishment and the Competition Bureau (see Section 55(3) (b) to (g) PCLMFTA.

[552] Section 55(7) PCLMFTA.

[553] See e.g., Sections 5(2), 6, 7, 8, and 12 of the Privacy Act as regards federal authorities.

[554] Section 7-8 of the Privacy Act.

control, including of the purposes for which personal information is used and the applicable retention period[555]. Similar obligations apply under provincial and territorial privacy laws.

In addition, different instruments have been adopted by the Canadian government that further specify how public authorities should protect personal information. With respect to the sharing of data with other entities (within or outside Canada), guidance of the Treasury Board of Canada Secretariat (which is responsible for developing policy instruments, including guidance, concerning the application and implementation of the federal Privacy Act) recommends to put in place information sharing agreements (legally binding agreements or arrangements/memoranda of understanding) containing appropriate personal information protection safeguards[556]. The latter for instance include purpose specification and limitation, security measures, maximum retention periods, rights of access and to request correction for individuals, conflict resolution mechanisms, etc.[557]. More generally, including under the Avoiding Complicity in Mistreatment by Foreign Entities Act, ministerial direction prohibits the disclosure of information by criminal law enforcement authorities with foreign entities where this would result in a substantial risk of mistreatment of an individual by those entities[558].

The Security of Canada Information Disclosure Act (SCIDA) permits Government institutions to share information related to threats to the security of Canada with other Canadian federal government institutions, such as federal law enforcement and security and intelligence agencies, but places strict parameters around doing so, including by requiring that the information relates to the receiving institutions mandate or responsibilities, and that disclosing would not impact personal privacy rights more than reasonably necessary in the circumstances. Disclosures under the SCIDA are also reviewed annually by the National Security and Intelligence Review Agency (NSIRA), on which a public report is tabled in Parliament.

Finally, with respect to the content of intercepted communications or the existence of such communications, the Criminal Code imposes specific limitations, subject to criminal sanctions (e.g., by prohibiting the use or disclosure without the consent of the concerned individual, except where required in the course of a criminal investigation)[559].

2.2.3. Oversight

The activities of Canadian criminal law enforcement authorities are supervised by different bodies.

First, the OPC carries out oversight of compliance with the Privacy Act by federal authorities. The OPC receives and investigates complaints from individuals, may initiate investigations on

[555] Section 10-11 of the Privacy Act.
[556] Section 4.2.11 of the Policy on Privacy Protection, available at: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12510. See also section 6.2.22 of the Directive on Privacy Practices, available at: https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=18309.
[557] https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/privacy/guidance-preparing-information-sharing-agreements-involving-personal-information.html#Toc267044420
[558] See https://www.publicsafety.gc.ca/cnt/trnsprnc/ns-trnsprnc/mnstrl-drctn-rcmp-grc-en.aspx.
[559] Section 193 of the Criminal Code.

its own initiative[560] and may more generally review processing activities of government institutions to ensure compliance with the Privacy Act. In carrying out investigations, the OPC has access to all relevant information,[561]. In particular, it may summon and enforce the appearance of persons, compel them to give oral or written evidence on oath and produce such documents and things as the OPC deems relevant to the investigation. Similarly, the OPC may enter any premises occupied by any government institution. If the OPC finds a violation of the Privacy Act, it provides the relevant agency with a report setting out the findings and recommendations[562]. Where appropriate, the OPC may also request that, within a specified time, notice must be given of any action taken or proposed to implement the recommendations (or reasons why no such action has been or is proposed to be taken). The OPC is required to report annually to the Parliament and may also make its reports on specific investigations available to the Parliament[563]. For example, in June 2021, the OPC submitted a special report to the Parliament on its investigation on the use of facial recognition technology by the RCMP[564]. The annual reports of the OPC also show that it regularly engages with law enforcement authorities, including at an early stage when new technologies are being tested or rolled out (e.g., body-worn cameras, drones), e.g., in the context of privacy impact assessments and advisory consultations[565].

Second, at provincial and territorial levels, oversight of compliance by criminal law enforcement authorities with personal information protection rules is carried out by independent Information and Privacy Commissioners, ombudspersons or review officers. Specific oversight powers may vary in each province or territory. For example, some supervisory authorities can issue binding or enforceable orders (in Alberta, British Columbia, Ontario, Quebec and Prince Edward Island), while others issue recommendations (Northwest Territories, Nova Scotia, Nunavut, Saskatchewan, Yukon) that can in some cases be enforced by a court (New Brunswick, Newfoundland and Labrador) or an independent adjudicator (Manitoba).

Third, different specialised bodies oversee the activities of the police more generally, at federal, provincial and territorial levels. In particular, the RCMP is subject to oversight by the Civilian Review and Complaints Commission for the Royal Canadian Mounted Police (CRCC)[566]. The CRCC can review any activity of the RCMP for the purpose of ensuring compliance with applicable legislation, regulations, ministerial directions, policies, procedures or guidelines, either on the basis of a complaint or on its own initiative and issue a report to the responsible Minister and the head of the RCMP with its findings and

[560] Section 29(1) and (3) of the Privacy Act.
[561] Section 34(1)-(2) of the Privacy Act. The only exceptions to this power relate to confidences of the King's Privy Council for Canada (section 34(2) of the Privacy Act) and, under certain circumstances, solicitor-client and litigation privileged materials (section 34(2.1) of the Act).
[562] Section 35(1) and 37(3) of the Privacy Act.
[563] Section 38-40 of the Privacy Act.
[564] https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/.
[565] See e.g., https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/ar_202021/#toc4 and https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201920/ar_201920/.
[566] Part VI of the Royal Canadian Mounted Police Act (RCMP Act). The members of the CRCC are appointed by order of the Governor in Council for (a renewable term of) five years and may only be removed by the order of the Governor in Council for cause (Section 25 RCMP Act. A member of the RCMP may not become a member of the CRCC.

recommendations[567]. In carrying out reviews and investigations, the CRCC has access to all relevant information[568]. In 2020-2021, the CRCC issued 322 review reports, with 239 recommendations (e.g., with operational guidance or recommending retraining or policy reviews)[569], of which 88% were accepted by the RCMP.

Similar bodies provide oversight of law enforcement agencies at provincial and territorial level, e.g., the Independent Investigations Office of British Columbia, the Law Enforcement Review Board in Alberta, the Office of the Independent Police Review Director in Ontario, the Public Complaints Commission in Saskatchewan, the Police Ethics Commissioner in Quebec, the Police Complaints Commissioner in Nova Scotia, etc.[570]

2.2.4. Redress

The Canadian system offers different avenues to obtain redress, including compensation for damages.

First, individuals have rights of access to and correction of their personal information held by public authorities.

At federal level, the Privacy Act provides individuals with a right of access to their personal information and a right of correction. Whereas these rights were in the past only available to Canadian citizens, permanent residents or individuals present in Canada[571], they have now been extended to all individuals, regardless of their nationality or place of residence[572]. As a consequence, any individual can exercise the rights of access and to request correction under the Privacy Act and has the possibility to file a complaint with the OPC if a request is refused[573]. With respect to the right of access, the relevant public authority may only refuse to disclose the requested records in limited and specific circumstances, by invoking exemptions that are either class-based or injury-based[574]. Class-based exemptions presuppose that the information is inherently sensitive, and that injury or prejudice would result from release.

---

[567] Section 45.34(1) of the RCMP Act.

[568] Section 45.39 and 45.4(2) of the RCMP Act. See also Section 45.65 et seq. with respect to investigations of complaints. While the RCMP may refuse to provide access to certain types of information (information protected by the privilege between a legal counsel and their client, information relating to a protected person (under the Witness Protection Act), medical information of RCMP members, as well as 'operational information', the CRCC may in that case request to appoint a former judge to review the requested information in light of the arguments invoked by the RCMP and the relevance thereof for the Commission. The observations of the former judge must be taken into account by the RCMP and Commission in the final decision whether or not the information can be shared. See the procedure of Section 45.41 of the RCMP Act.

[569] https://www.crcc-ccetp.gc.ca/en/annual-report-2020-2021#toc3.

[570] See the list available at: https://www.crcc-ccetp.gc.ca/en/jurisdiction.

[571] Section 12 of the Privacy Act, Privacy Act Extension Order, No. 1 and Privacy Act Extension Order, No. 2.

[572] To further strengthen the rights of individuals and to align with provincial and international practice, the Privacy Act Extension Order, No. 3 was made on 13 July 2021 and entered into force on 13 July 2022. The order extends the right of access under subsection 12(1) of the Privacy Act to any individual outside of Canada. Such individuals also benefit from the right to request correction under subsection 12(2) of the Privacy Act, since this right flows from the right of access. Before this extension order came into effect, non-Canadian nationals and non-permanent residents not present in Canada could nevertheless obtain access to their personal information held by federal authorities on the basis of the Access to Information Act through a third party present in Canada (Access to Information Act Extension Order, No. 1). In that case, the individual must provide his/her consent to the disclosure of records containing personal information concerning him/her to the third party (Section 19(2) of the ATIA).

[573] Section 29(1)(b) and (c) of the Privacy Act.

[574] See Sections 18 – 28 of the Privacy Act.

Injury-based exemptions are imposed when there is a "reasonable expectation of probable harm that would result from the disclosure of information"[575]. With a few exceptions[576], both types of exemptions are not absolute, but leave discretion to the relevant authority, which means that it has to decide on a case-by-case basis whether or not to apply the exemption, after weighing relevant factors involved, including the privacy interests of the concerned individual[577]. Individuals who have been refused access to or correction of personal information, if a complaint has been made to the Privacy Commissioner in respect of the refusal, also have the possibility to apply directly to the Federal Court for a review of the matter, under the Privacy Act[578]. In that case, the Court may order the concerned institution to grant access or correct the information.

In addition, the privacy legislation for the public sector in each province and territory grants any individual (i.e., without limitations related to nationality or residence) the right of access to his/her personal information and to have inaccurate information corrected. Moreover, individuals can request a review of a decision on an access/correction request before the competent supervisory authority. Depending on the province/territory, the rights of access/correction of individuals may be enforced directly by the supervisory authority (by issuing binding orders, e.g., in Alberta, British Columbia, Ontario, Prince Edward Island), an adjudicator (e.g., in Manitoba), or the courts (e.g., in New Brunswick, Newfoundland and Labrador, Nova Scotia, Nunavut, Québec, Saskatchewan and Yukon).

Second, individuals may file complaints with independent oversight bodies.

At the federal level, any individual may file a complaint with the Privacy Commissioner in respect of any matter relating to the handling of personal information by a criminal law enforcement authority or other federal government institution[579]. The Privacy Act does not require the individual to have been personally affected, or to demonstrate injury for a

[575] See also Section 3.2 of the Access to Information Manual of the Canada Treasury Board, available at: https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/access-information/access-information-manual.html.

[576] Only some of the class-based exemptions are mandatory (and have to be applied in all circumstances (i.e., without any balancing of interests), see also the Directive on Personal Information Requests and Correction of Personal Information, issued by the Canadian Government (available at https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32590&section=html). These concern information that was obtained in confidence from another (third country) public authority, unless the latter consents to the disclosure or makes the information public (Section 19 of the Privacy Act); information held by the OPC in the context of ongoing investigations (Section 22.1 of the Privacy Act); information handled by the Public Sector Integrity Commissioner or under the Public Servants Disclosure Protection Act (Sections 22.2 and 22.3 of the Privacy Act) or information about another individual (Section 26 of the Privacy Act).

[577] These exemptions e.g., apply to information obtained by investigative bodies in the course of lawful investigations pertaining to the detection, prevention or suppression of crime, the enforcement of any law of Canada or a province, or activities suspected of constituting threats to the security of Canada (if the relevant record came into existence less than 20 years prior to the request); information that, if disclosed, could reasonably be expected to be injurious to the conduct of international affairs, the defence of Canada, or the detection, prevention or suppression of subversive or hostile activities; if the disclosure could reasonably be expected to be injurious to the enforcement of any law of Canada or a province or the conduct of lawful investigations (paragraph 22(1)(b) of the Privacy Act). With respect to the latter exemption, the Supreme Court of Canada found that "there must be a clear and direct connection between the disclosure of specific information and the injury that is alleged." In particular, "the sole objective of non-disclosure must not be to facilitate the work of the body in question." See Lavigne v. Canada (Office of the Commissioner of Official Languages), 2002 SCC 53, [2002] 2 S.C.R. 773.

[578] Section 41 of the Privacy Act.

[579] Section 29 of the Privacy Act.

complaint to be admissible. If a complaint is well-founded, the Commissioner issues a report containing findings and non-binding recommendations, as well as, where appropriate, a request to inform the Commissioner of any action taken to Implement a recommendation within a specified time[580]. Where the described action taken or proposed to be taken to implement the recommendations would be inadequate, the OPC must inform the complainant thereof[581]. Individuals may challenge the investigations and reports of the OPC before the Federal Court, pursuant to Section 18.1 of the Federal Courts Act on procedural grounds[582]. For instance, the Federal Court may grant relief if it is satisfied that the Commissioner acted without/beyond jurisdiction; failed to observe a principle of natural justice, procedural fairness or other procedure that it was required by law to observe; erred in law; or based its report on an erroneous finding of fact that it made in a perverse or capricious manner or without regard for the material before it[583]. For example, in Oleinik v Canada (Privacy Commissioner), the Federal Court noted that "the [Privacy Commissioner's] investigation itself is amenable to review. If the report had material omissions, reached unreasonable conclusions, contained unsustainable inferences, misconstrued the factual and legal context or evinced a bias or pre-disposition on the part of the investigator, the Court could intervene."[584] The Court may, inter alia, order the OPC to do any act or thing that was unlawfully refused, delayed or failed to be carried out, or declare invalid or unlawful, quash or set aside and refer back a decision, order, act or proceeding[585].

With respect to compliance by provincial/territorial authorities with local privacy legislation, individuals may file complaints before the independent personal information protection authorities in each province/territory, which can issue binding orders (in Alberta, Quebec, British Columbia, Ontario and Prince Edward Island), orders enforceable by the courts or an adjudicator (in Manitoba, New Brunswick and Newfoundland and Labrador) or recommendations (in Yukon, Saskatchewan, Nunavut and the Northwest Territories). In Nova Scotia, an individual can appeal directly to the Supreme Court if it considers that a public authority has not complied with the recommendations of the personal information protection authority.

Third, individuals may in certain circumstances also file complaints with independent oversight bodies in the area of criminal law enforcement. For example, the CRCC handles complaints from any individual against the RCMP[586]. Individuals may complain directly to the CRCC, or first file a complaint with the RCMP and, if they are not satisfied with the outcome, request a review before the CRCC[587]. Once the investigation of a complaint is concluded, the CRCC prepares a report setting out its findings and recommendations, which is

[580] Section 35(1) of the Privacy Act.
[581] Section 35(3) of the Privacy Act.
[582] Section 18.1(4) of the Federal Courts Act.
[583] Section 18.1(4) of the Federal Courts Act.
[584] Oleinik v Canada (Privacy Commissioner) (2011 FC 1266), para. 11.
[585] Subsection 18.1(3) of the Federal Courts Act.
[586] Section 45.53(1) and 45.59(1) of the RCMP Act.
[587] Section 45.7(1) of the RCMP Act. Complaints must in principle be filed within one year after the day on which the alleged conduct occurred, although the time limit may be extended if there are good reasons for doing so and it is not contrary to the public interest (Section 45.53(5)-(6) of the RCMP Act). In deciding whether this is the case, a number of factors are taking into account, including reasonable explanations for the delay and whether the submission presents an arguable case, see https://www.crcc-ccetp.gc.ca/en/policy-extension-time-limit-submit-complaint-crcc.

shared with the responsible Minister, the RCMP and the complainant[588]. Reports of the CRCC are final and cannot be appealed or reviewed[589]. In the period 2020-2021, 3361 complaints were filed by individuals (3144 before the Commission and 201 before the RCMP), of which 2273 were admissible[590]. In the same time frame, 2254 complaints were finalised. Similarly, in 2019-2020, 3641 complaints were received, of which 2317 were admissible, and 2067 complaints were finalised. In certain provinces/territories, individuals may similarly obtain redress against law enforcement authorities before independent oversight bodies (e.g., before the Office of the Police Complaint Commissioner in British Columbia, The Saskatchewan Public Complaints Commission, the *Commissaire à la déontologie policière* in Quebec, the New Brunswick Police Commission, etc.)[591].

Fourth, different judicial remedies are available, allowing individuals to invoke the limitations and safeguards described in section 2.2.1 to obtain redress.

In particular, anyone directly affected by the improper handling of personal information by government institutions may apply for judicial review before the Federal Court, which does not require a showing of harm or injury[592].

In addition, civil proceedings for damages[593] can be brought against the federal government for torts committed by government agents, servants or members of the federal police force. While the specific details of tort law vary across provinces, generally speaking the torts of negligence, breach of confidence or intrusion on seclusion could be invoked against the federal government where it misuses personal information. For a negligence claim to succeed, the individual must establish that a duty of care existed (which requires foreseeability of harm and proximity between the parties), that there was a breach of the applicable standard of care (which requires demonstrating that the defendant's conduct fell below what would have been reasonable in the circumstances) and that this breach caused compensable harm. A successful breach of confidence claim requires establishing that the information that is the subject of the lawsuit was confidential, communicated in confidence and used in an unauthorised manner to the detriment of the plaintiff. With respect to the tort of intrusion on seclusion, a person who intentionally or recklessly intrudes, physically or otherwise, upon the seclusion of another person's private affairs or concerns may be liable if the invasion would be highly offensive to a reasonable person and causes distress, humiliation or anguish. These same principles generally also apply to civil claims against provincial or municipal authorities. Several court cases demonstrate how these principles may apply to privacy violations by public authorities. For example, in Condon v. Canada, a proposed class action based in negligence and breach of confidence for losing a hard drive containing personal information was allowed to proceed[594]. Similarly, in TDC Broadband Inc. v. Nova Scotia, compensation was successfully claimed

[588] Section 45.76(3) of the RCMP Act.
[589] Section 45.76(4) of the RCMP Act.
[590] https://www.crcc-ccetp.gc.ca/en/report-rcmp-public-complaints-2020-2021.
[591] An overview of the available redress avenues is available at: https://www.crcc-ccetp.gc.ca/en/jurisdiction. Figures on complaint handling by these bodies in 2020-2021 is available at: https://www.crcc-ccetp.gc.ca/en/report-rcmp-public-complaints-2020-2021.
[592] Section 18.1 of the Federal Courts Act.
[593] Section 3 of the Crown Liability and Proceedings Act.
[594] Condon v. Canada, 2015 FCA 159.

against a provincial government for a breach of confidence (involving the unauthorised use of confidential information)[595].

Finally, judicial remedies are available to any individual whose rights under the Charter have been violated, as a result of government action or legislation.

In particular, under Section 24 of the Charter, anyone whose rights under the Charter have been violated may apply to a court to obtain such remedy as the court considers appropriate and just in the circumstances. This may include compensation for damages, declaratory relief and injunctive relief[596]. Moreover, where the court concludes that evidence was obtained in a manner that infringed any rights or freedoms guaranteed by the Charter and the court finds that the admission of evidence would bring the administration of justice into disrepute, the evidence must be excluded[597]. For a claim under Section 24 of the Charter to be successful, an individual must a) establish an adequate factual foundation, b) bring his or her claim at the correct stage of litigation and c) persuade the court that, on a balance of probabilities, his or her Charter rights have been violated[598].

In addition, individuals can bring an action for a declaration that certain laws conflict with the Charter and are, therefore, of no force of effect under Section 52 of the Constitution Act 1867. For example, in one case the Supreme Court found that provisions of the Criminal Code were unreasonable because they did not require notification of individuals whose communications had been intercepted without a warrant[599]. Claimants may invoke Section 52 of the Constitution by alleging infringements of their own rights and freedoms; based on being affected by an allegedly unconstitutional law or administrative decision[600]; or based on "public interest standing", i.e., if there is a serious issue as to the validity of the legislation, the individual has a genuine interest in the measure's validity, and the litigation is a reasonable and effective way to bring the matter before the court[601].

2.3. Access and use by Canadian public authorities for national security purposes

In Canada, two agencies collect personal information for national security purposes.

The core mandate of the Canadian Security Intelligence Service (CSIS) is to collect foreign intelligence in Canada, investigate activities suspected of constituting threats to the security of Canada and advise the Government about these threats, which entails that CSIS is collecting, analysing and retaining information, including personal information. CSIS also has the mandate to take lawful measures to reduce threats to the security of Canada.

[595] TDC Broadband Inc. v. Nova Scotia, 2016 NSSC 206.
[596] See the overview provided at https://www.justice.gc.ca/eng/csj-sjc/rfc-dlc/ccrf-ccdl/check/art241.html.
[597] Section 24(2) of the Charter.
[598] R. v. Collins, [1987] 1 S.C.R. 265, at page 277.
[599] R. v. Tse, 2012 SCC 16.
[600] R. v. Big M Drug Mart, [1985] 1 SCR 295 at pages 313-14; Loyola High School v. Quebec (Attorney General), 2015 SCC 12 at paras 33-35.
[601] Canada (Attorney General) v. Downtown Eastside Sex Workers United Against Violence Society, [2012] 2 S.C.R. 524.

The Communications Security Establishment (CSE) is the national signals intelligence agency for foreign intelligence and the expert body for cybersecurity and information assistance[602]. Since the activities of the CSE may not be directed at Canadian individuals or corporations, or any person in Canada, it may in principle only access personal information transferred on the basis of the adequacy decision while it is in transit between the EU and Canada. The relevant powers of both agencies, as regulated by the CSIS Act and CSE Act, are described in the following sections[603].

2.3.1. Legal bases and applicable limitation/safeguards

2.3.1.1. The Canadian Security Intelligence Service (CSIS)

On the basis of the CSIS Act, CSIS may access personal information transferred from the EU to private operators subject to PIPEDA as part of different activities, each of which is subject to specific limitations and safeguards following from the CSIS Act, the Canadian Constitution (Section 8 of the Charter) and case law[604].

First, CSIS can, "to the extent strictly necessary," collect information and intelligence on activities that may on reasonable grounds be suspected of constituting threats to the security of Canada (threat investigations)[605]. Second, CSIS may, in relation to the defence of Canada or the conduct of international affairs, assist the Ministers of National Defence or Foreign

[602] The cybersecurity and information assistance aspect of CSE's mandate is to provide advice, guidance and services to help protect electronic information and information infrastructures of (federal) institutions. In addition, it provides technical and operational assistance to federal law enforcement and security agencies (such as CSIS), the Canadian Forces and the Department of National Defence.

[603] In addition to using the powers described in this section, CSIS and CSE may also receive information from private operators that is provided on a voluntary basis in accordance with PIPEDA (see section 2.2.1). CSIS may furthermore indirectly receive information on financial transactions from FINTRAC, if the latter has reasonable grounds to suspect that information it has received would be relevant to threats to the security of Canada, Section 55.1(1) PCMLTFA. The information that must be disclosed concerns, inter alia, the name of the person/entity involved in the transaction, the amount and type of currency or monetary instruments involved, the transaction number and account number, indicators of a money laundering or terrorist activity financing offence, etc. (Section 55.1(3) PCMLTFA) The reasons for each decision to disclose must be recorded in writing (Section 55.1(2) PCMLTFA). Finally, CSIS and CSE may receive information from other public authorities, if the latter are satisfied that this will contribute to the exercise of the recipient's jurisdiction in respect of activities that undermine the security of Canada, and it will not affect any person's privacy interest more than is reasonably necessary in the circumstances (Section 5 of the Security of Canada Information Disclosure Act, SCIDA). An activity that undermines the security of Canada means any activity that undermines the sovereignty, security or territorial integrity of Canada or threatens the lives or the security of people in Canada, or of any individual (Section 2(1) SCIDA). In addition, compliance must be ensured with the requirements described in section 2.2.2.

[604] CSIS may also assist the Government with security assessments (i.e. assessments of individuals seeking security clearances when this is required by the federal public service as a condition of employment) and provide information or advice relating to security matters that is relevant to the exercise of any powers or functions under the Citizenship Act or the Immigration and Refugee Protection Act (i.e. by conducting security assessments during the visa application process and the application process for refugees and Canadian citizenship), Section 13-14 CSIS Act. However, for the purpose of these tasks, the CSIS cannot make use of the warrant procedure described below to use intrusive techniques (See also X(Re) 2016 FC 1105 at para. 168).

[605] Section 12(1) CSIS Act. Section 2 of the CSIS Act defines threats to the security of Canada as a) espionage or sabotage that is directed against Canada or is detrimental to its interests (as well as activities directed toward or in support of such espionage or sabotage); b) foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person; c) activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective within Canada or a foreign state; and d) activities directed toward undermining by covered unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of, the constitutionally established system of government in Canada.

Affairs in the collection of information or intelligence within Canada in relation to the capabilities, intentions or activities of any foreign state or group of foreign states and any person other than Canadian citizens, permanent residents, or Canadian corporations (foreign intelligence collection)[606]. Third, if there are reasonable grounds to believe that a particular activity constitutes a threat to the security of Canada, CSIS may, within or outside Canada, take measures to reduce the threat (threat reduction measures), which may in certain circumstances require ancillary access to (personal) information.

For the first and second powers, CSIS must obtain judicial authorisation in the form a warrant issued by the Federal Court prior to using any techniques that would intrude more than minimally on a privacy interest protected by Section 8 of the Charter and/or otherwise violate Canadian law in the execution of the judicial authorisation[607]. This is for example the case for the interception of an individual's communications[608], obtaining detailed billing or subscriber information from communication service providers, or using cell-site simulator technology to track an individual's device. In other words, nothing in the CSIS Act authorises CSIS to violate Section 8 of the Charter. The judicial warrant obtained in this context ensures that lawful authority underlies those CSIS activities that intrude more than minimally on protected privacy interest, thus making make the activities in question compliant with Section 8 of the Charter. Likewise, the warrant may authorise activities that, absent the warrant, would otherwise contravene Canadian law.

A warrant to investigate threats to the security of Canada may be issued if (1) it is required to enable the CSIS to investigate a specific threat (i.e., "the information sought is factually related to a threat to the security of Canada")[609] and (2) other investigative procedures have been tried and have failed or are unlikely to succeed, the urgency of the matter is such that it would be impractical to carry out the investigation using only other investigative procedures, or it is unlikely that the information could be obtained without a warrant[610]. The CSIS Act lists the information that must be provided in the application for a warrant and the warrant itself, which includes the type of communication to be intercepted or the type of information, records, documents or things to be obtained; the identity of the target, if known; and a general description of the place where the warrant is to be executed[611]. In principle, a warrant may be issued for a period up to one year[612] and may be renewed by a judge, on written application by CSIS, for a period not exceeding the period for which the warrant was issued[613].

---

606 Section 16(1) CSIS Act.
607 Section 21 CSIS Act.
608 See e.g., X(Re) 2014 FCA 249 at 87.
609 X(Re) 2016 FC 1105, at 161. See also the clarification at 186 that "legitimate targets are individuals or groups of interest that are, or potentially are, related to activities constituting threats to the security of Canada […] Therefore, [incidentally collected] non-target and non-threat related third party information may only be retained for a short period of time in order to ensure that it is not related to national security. If, after such short time period, the information is determined not to be related to threats to the security of Canada as defined by section 2 of the CSIS Act, or of assistance to a prosecution, to national defence or international affairs, it must be destroyed".
610 Section 21(3) CSIS Act.
611 Section 21(2) and (4) CSIS Act
612 Section 21(5) CSIS Act. Where it is issued to enable the CSIS to investigate activities aimed at undermining (by unlawful acts), destroying or overthrowing (by violence) the constitutionally established system of government, a warrant may only be issued for a period not exceeding 60 days.
613 Section 22 CSIS Act.

The role of the judge in assessing the application for a warrant is to "ensure all requirements of the legislation are respected in the application for warrants and that the measures sought are justified in light of the facts put forward"[614]. In light of the requirements of the CSIS Act, the judge therefore assesses, inter alia, whether the information sought is "strictly necessary" to investigate a threat and whether other less intrusive techniques or procedures are not available or would not be effective[615]. Moreover, in assessing compliance with Section 8 of the Charter, the judge may look at additional elements, e.g., whether the proposed measure is no more intrusive than is reasonably necessary to achieve its objectives (i.e., whether the measure strikes an appropriate balance between the rights of the individual and the objectives being pursued by the state)[616]. The judge issuing a warrant may specify terms and conditions considered advisable in the public interest[617].

The same standard and procedure applies to deploy more intrusive investigative techniques (such as intercepting communications) as part of the CSIS' foreign intelligence collection mandate[618].

For the third power (threat reduction measures), CSIS must also obtain judicial authorisation in the form a warrant issued by the Federal Court prior to undertaking any threat reduction measure that would either limit a right or freedom guaranteed by the Charter or otherwise be contrary to Canadian law[619]. A warrant to take threat reduction measures may be issued if the measure required to reduce the threat and the measure is "reasonable and proportionate" in the circumstances of the case[620], having regard to the nature of the threat, the nature of the measures and the reasonable availability of other means to reduce the threat, as well as the reasonably foreseeable effects on third parties, including their right to privacy[621]. Moreover, the measure must comply with the Charter, e.g., the limit effected by the measure on a Charter right or freedom should not be more intrusive than is reasonably necessary to achieve its

[614] X(Re) 2016 FC 1105, at 162.
[615] Section 12(1) and 21(3) CSIS Act. Given that the decision to issue a warrant is of a discretionary nature, a judge may also take other factors into account, depending on the particular circumstances of the case (X(Re) 2014 FCA 249 at 60-61).
[616] R. v Vu, [2013] 3 S.C.R. 657.
[617] Section 21(4)(f) CSIS Act.
[618] In particular, the application for a warrant must contain the same detailed information and the judge may authorise the warrant if satisfied that a) it is required for CSIS to perform its duties and functions under section 16 (i.e. there is a link between the information sought and being able to provide the requested assistance in relation to the defence of Canada or the conduct of international affairs)and b) other (less intrusive) investigative procedures are not available or would not be effective (Section 21(2) CSIS Act). In carrying out this assessment, the judge would again take into account the requirements of the CSIS Act and the Charter, including by looking at the overall proportionality of the requested measure. In addition, any foreign intelligence collection may only take place on the written request of the Minister of National Defence or the Minister of Foreign Affairs and with the written consent of the Minister of Public Safety and Emergency Preparedness (Section 16(3) CSIS Act). In addition, CSIS' collection of foreign intelligence under section 16 can only take place within Canada (Section 16(1)).
[619] Sections 12.1(3.2), 12.1(3.4) and 21.1 CSIS Act.
[620] Section 21.1(3) CSIS Act. The application for a warrant must set out the facts relied on to justify the belief on reasonable grounds that a warrant is required to take measures to reduce a threat, as well as the reasonableness and proportionality of the proposed measures (Section 21.1(2)(a) and (c) CSIS Act). In addition, it must contain the same detailed information as required in a section 21 warrant for a section 12 or 16 investigation (see earlier).
[621] Sections 21.1(2)(c) and 22.2 CSIS Act. See also Section 12.1(2) CSIS Act.

threat reduction objectives[622]. Terms and conditions deemed advisable in the public interest may be specified in the warrant[623]. The warrant may in principle be issued for a maximum of 120 days[624] and may, upon written application, be renewed twice if the conditions continue to be fulfilled[625].

Finally, CSIS may, to support its abovementioned duties and functions, collect datasets[626] that contain personal information and that do not directly and immediately relate to activities that represent a threat to the security of Canada, where it is satisfied that the dataset is relevant to the performance of those duties and functions and the dataset is reasonably believed: to be publicly available (i.e., available to the public at the time of collection), to belong to an approved class of Canadian datasets (i.e., relating predominantly to Canadians or individuals/corporations within Canada), or to predominantly relate to non-Canadians who are outside Canada (i.e., foreign dataset) [627].

Specific substantive and procedural requirements to collect, retain, exploit and query these three types of datasets are set out in the CSIS Act and differ for each type of dataset. When it comes to the retention of a collected dataset, this report focuses on the procedural requirements applicable to foreign datasets, as this is the type of collection that is the most relevant in an adequacy context (i.e., where personal information is transferred from the EU to Canadian commercial operators and may subsequently be accessed by Canadian public authorities). In particular, once a dataset is collected, CSIS has to assess and confirm within 90 days what type of dataset (i.e., whether it is a Canadian, foreign or publicly available dataset) it concerns[628]. During this period, the dataset may in principle (see below) not be queried or exploited[629]. In the course of conducting the evaluation during the 90-day period, a limited number of CSIS staff ("designated employees")[630] may delete any extraneous, erroneous, or poor-quality information contained in the dataset. During this time, designated employees may also decrypt or translate the information in the collected dataset or apply specific privacy protection techniques[631]. During the 90-day evaluation period, a designated employee must delete any personal information from the dataset that is not relevant to the

[622] Section 12.1(3.3) CSIS Act. This derives from Section 1 of the Charter, as further interpreted in case law (see section 2.1), which guarantees rights and freedoms "subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society."
[623] Section 21.1(5)(f) CSIS Act.
[624] Except with respect to threats concerning activities toward undermining the constitutionally established system of government in Canada (for which a warrant may be issued for a maximum of 60 days, Section 21.1(6) CSIS Act).
[625] Section 22.1 CSIS Act.
[626] A dataset is defined at section 2 CSIS Act as a collection of information stored as an electronic record and characterised by a common subject matter.
[627] Sections 2, 11.02, 11.05 and 11.07(1) CSIS Act.
[628] Section 11.07(1) CSIS Act. Data incidentally collected in the execution of a warrant to investigate threats to the security of Canada may also be retained to constitute a dataset, if the judge authorising the warrant is satisfied that it is likely to assist the CSIS in the performance of its duties with respect to investigation of security threats, the adoption of threat reduction measures, or the foreign intelligence mandate (Section 21(1.1) and (3.01) CSIS Act.).
[629] Section 11.07(3) CSIS Act. Querying means "carrying out a specific search, with respect to a person or entity, for the purpose of obtaining intelligence". Exploitation means "a computational analysis of one or more datasets for the purpose of obtaining intelligence that would not otherwise be apparent". See the definitions in Section 2 CSIS Act.
[630] Defined in Section 11.01 and referencing Sections 11.04 and 11.06.
[631] Section 11.07(5) CSIS Act.

performance of the CSIS' duties and functions if its deletion does not affect the integrity of the dataset[632].

If it is determined that the information constitutes a foreign dataset, CSIS must obtain authorisation from the Minister of Public Safety (the Minister) or a designated person within the abovementioned 90-day period in order to retain the foreign dataset[633]. The Minister or designate may authorise CSIS to retain a foreign dataset when the retention is likely to assist the Service in the performance of its duties and functions and any information for which there is a reasonable expectation of privacy that relates to the physical or mental health of an individual has been removed[634]. The authorisation of the Minister must subsequently be reviewed and approved by an independent body, the Intelligence Commissioner (IC) [635]. The IC approves the authorisation by means of a reasoned decision if (s)he considers that the Minister's conclusions are reasonable, possibly by imposing specific conditions[636]. An authorisation to retain a foreign dataset may be valid for a maximum period of five years from the date on which approval from the IC is obtained[637]. If no authorisation is granted by the Minister or if the IC does not approve the ministerial authorisation, CSIS must destroy the dataset without delay[638].

Once the Minister's authorisation to retain the dataset is approved by the IC, the dataset may only be queried and exploited by a limited number of designated employees at CSIS to assist the Service in its duties and functions under specific conditions[639]. A dataset may be queried and exploited to the extent that it is strictly necessary to assist CSIS in the performance of its duties and functions in relation to threat investigations and taking threat reduction measures[640], or if required to assist the Ministers of National Defence or Foreign Affairs in collecting foreign intelligence[641]. In exigent circumstances, i.e., that require the querying of a dataset to preserve the life or safety of any individual or to acquire intelligence of significant

[632] Section 11.07(6) CSIS Act.
[633] Section 11.09(2) CSIS Act. If no authorisation is requested or obtained, the dataset must be destroyed on the day on which the 90-day period ends (Section 11.09(3) CSIS Act).
[634] Section 11.17(1) in conjunction with Section 11.1(1)-(2) CSIS Act. Such authorisation must be provided in writing and must include, inter alia, a description of the dataset, the manner in which the CSIS may update the dataset, the terms and conditions to query, exploit or destroy the data set, and any terms and conditions the Minister considers advisable in the public interest (Section 11.17(2) CSIS Act).
[635] Section 11.18 CSIS Act. The IC is a retired judge of a superior court and is appointed by the Governor in Council, on the recommendation of the Prime Minister (Section 4(1) of the Intelligence Commissioner Act, IC Act). The IC is appointed for a renewable term of five years and has exclusive authority to appoint his/her staff (Section 4(1),(2) IC Act). In reviewing requests for authorising the retention of foreign datasets, the IC has access to all information that was before the person that issued the initial authorisation, including information that is subject to any privilege (Section 23(1),(2) IC Act). The IC is prohibited from engaging in any political activity (Sections 5, 6(3) IC Act, in conjunction with Section 117 Federal Public Service Employment Act) and has exclusive authority to appoint and lay off personnel (Section 6(1) IC Act).
[636] Section 17 and 20(2) IC Act. The IC must provide a copy of each decision to the National Security and Intelligence Review Agency (NSIRA), Section 21 IC Act. Moreover, the IC must report to the Prime Minister on an annual basis on its activities, including by providing statistics on the authorisations that were approved and not approved (Section 22(1) IC Act). This report must in turn be tabled by the Prime Minister before Parliament (Section 22(3) IC Act).
[637] Section 11.17(3) CSIS Act.
[638] Section 11.19(1)-(2) CSIS Act.
[639] Section 11.2(3)-(4) CSIS Act.
[640] The same applies to assisting the Government with security assessments of individuals seeking security clearances and during the visa application process or the application process for refugees and Canadian citizenship (Section 15 CSIS Act).
[641] Section 11.2(3)-(4) CSIS Act.

importance to national security (the value of which would be diminished or lost if the CSIS would be required to comply with the ordinary authorisation procedure), the Director of the CSIS may authorise such querying even if no Ministerial authorisation to retain the dataset has been obtained (yet)[642]. However, in such cases, the IC must first review whether the assessment carried out by the Director is reasonable and must approve the decision, before the query can take place[643]. Notably, the CSIS Act does not allow for exploitation in exigent circumstances.

The results from queries or exploitation may only be retained where the collection, analysis and retention of the results are carried out in performing CSIS' functions with respect to threat investigations; where the retention is strictly necessary to assist CSIS with the taking of threat reduction measures[644]; or where the retention is required to assist the Ministers of National Defence or Foreign Affairs in collecting foreign intelligence[645]. Any query or exploitation result that does not satisfy abovementioned conditions must be destroyed without delay[646].

In terms of additional safeguards, any foreign dataset must be stored and managed separately from all other information collected and retained by CSIS. In addition, only designated employees may have access to the datasets and reasonable measures must be taken to ensure that any information to which employees have access in only communicated for the purpose of their duties and functions under the CSIS Act. Moreover, records must be kept on the rationale for their collection and retention, the details of each query and exploitation, the statutory provision under which the result of a query or exploitation is retained and the results that were retained. CSIS is also required to verify, periodically and on a random basis, if the queries, exploitations and retention of results were carried out in accordance with the CSIS Act[647]. Finally, CSIS must provide NSIRA with, inter alia, reports on the periodic verifications and the authorisations of the Director to query foreign datasets in exigent circumstances[648].

2.3.1.2. The Communications Security Establishment (CSE)

The CSE's mandate covers five aspects. First, the CSE's foreign intelligence mandate is to acquire information from or through the global information infrastructure[649], and to use, analyse and disseminate the information for the purpose of providing foreign intelligence, in accordance with the Government of Canada's intelligence priorities[650]. In addition, the CSE

[642] Section 11.22 CSIS Act.
[643] Section 11.23 CSIS Act.
[644] The same applies as regards security assessments.
[645] Section 11.21(1) CSIS Act.
[646] Section 11.21(2) CSIS Act.
[647] Section 11.24(3) CSIS Act.
[648] Section 11.25 CSIS Act.
[649] Global information infrastructure includes electromagnetic emissions, any equipment producing such emissions, communications systems, information technology systems and networks, and any data or technical information carried on, contained in or relating to those emissions, that equipment, those systems or those networks (Section 2 CSE Act).
[650] Section 16 CSE Act. Foreign intelligence is defined as "information or intelligence about the capabilities, intentions or activities of a foreign individual, state, organisation or terrorist group, as they relate to international affairs, defence or security" (Section 2 CSE Act). While there is no definition of the notion of 'international affairs', the similar term 'international relations' has been considered by Canadian courts as information that is related to Canada's relationship with foreign nations. (Canada (Attorney General) v. Canada (Commission of Inquiry) (2007), 316 F.T.R. 279 (F.C.).

provides advice, guidance and services to the Government of Canada and federal institutions with respect to cybersecurity and information assurance, and in this context may also acquire, use and analyse information from the global information infrastructure or from other sources[651]. Moreover, the CSE may carry out defensive[652] and active[653] cyber operations on or through the global information infrastructure[654]. Finally, the CSE may provide technical and operational assistance to federal law enforcement and security agencies, the Canadian Forces and the Department of National Defence[655].

The CSE may not direct activities carried out in furtherance of the foreign intelligence, cybersecurity and information assurance, defensive cyber operations or active cyber operations aspects of its mandate at Canadian individuals or corporations, or any person in Canada[656] and may not infringe the Charter[657]. Moreover, activities of the CSE as part of its foreign intelligence, cybersecurity and (defensive or active) cyber operations mandates that would otherwise contravene any Act of Parliament (including legislation in the foreign country where the activity takes place) or interfere with the reasonable expectation of privacy of a Canadian or person in Canada can only be carried out after having been authorised by the competent Minister[658] and, for foreign intelligence and cybersecurity authorisations, approved by the independent Intelligence Commissioner .

An authorisation for defensive and active cyber operations may be issued if there are reasonable grounds to believe that the activity is "reasonable and proportionate, having regard to the nature of the objective to be achieved and the nature of the activities"[659] and "the objective of the cyber operation could not reasonably be achieved by other means" and that no information will be acquired under the authorisation except in accordance with a (separately issued) foreign intelligence or cybersecurity authorisation[660].

A foreign intelligence authorisation may be issued if there are reasonable grounds to believe that[661]: (1) the activity is "reasonable and proportionate, having regard to the nature of the

[651] Section 17 CSE Act. As part of the CSE's cybersecurity mandate, the Minister may e.g., authorise the CSE to access an information infrastructure designated as of importance to the Government of Canada or of a federal institution and acquire any information originating from, directed to, stored on or being transmitted on or through that infrastructure for the purpose of helping to protect it from mischief, unauthorized use or disruption (Section 27 CSE Act).
[652] I.e., activities to help protect federal institutions' electronic information and information infrastructures; and electronic information and information infrastructures designated as being of importance to the Government of Canada (Section 18 CSE Act).
[653] I.e., to degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of a foreign individual, state, organisation or terrorist group as they relate to international affairs, defence or security (Section 19 CSE Act).
[654] Such activities may not be directed at any portion of the global information infrastructure in Canada (Section 22(2) CSE Act).
[655] Section 20 CSE Act. In providing such assistance, the CSE has the authority to exercise the same powers as federal law enforcement authorities, the Canadian Forces or the Department of National Defence, under the same conditions and subject to the same limitations (e.g., warrant requirements) as those that apply to those authorities (Section 25(1) CSE Act).
[656] Section 22(1) CSE Act.
[657] See also the Preamble of the CSE Act.
[658] Section 22 CSE Act.
[659] Section 34(1) CSE Act. The CSE must apply in writing to the Minister, setting out the facts that would allow the Minister to conclude that there are reasonable grounds to believe that the authorization is necessary and that the conditions for issuing it are met (Section 33 CSE Act).
[660] Section 34(4) CSE Act.
[661] Section 34(1) and (2) CSE Act.

objective to be achieved and the nature of the activities"[662] (which would require taking into account the benefits to be achieved by the activities and any anticipated impact on privacy interests)[663]; (2) any information acquired under the authorisation "could not reasonably be acquired by other means and will be retained for no longer than is reasonably necessary"; and (3) if the authorisation authorises the acquisition of unselected information[664]: any unselected information could not reasonably be acquired by other means.

Similarly, a cybersecurity authorisation may be issued if there are reasonable grounds to believe that, inter alia, (1) the activity is "reasonable and proportionate, having regard to the nature of the objective to be achieved and the nature of the activities"[665]; (2) any information acquired will be retained for no longer than is reasonably necessary; (3) the consent of all persons whose information may be acquired could not reasonably be obtained (in case the activity concerns the information infrastructure of federal institutions), and (4) any information acquired under the authorisation is necessary to identify, isolate, prevent or mitigate harm to electronic information or information infrastructure of federal institutions or that has been designated as being of importance to the Government of Canada.

Any authorisation issued by the Minister[666] must, inter alia, specify: (1) the activities or classes of activities that it authorises; (2) the persons or classes of persons who are authorised to carry out the activities or classes of activities; (3) any terms, conditions or restrictions that the Minister considers advisable in the public interest, or advisable to ensure the reasonableness and proportionality of any activity authorised by the authorisation; and (4) the day on which the authorisation is issued and expires[667]. In case of a foreign intelligence authorisation, it must also specify whether the activities authorised include acquiring unselected information, and any terms, conditions or restrictions that the Minister considers advisable to limit the use, analysis and retention of, and access to, unselected information[668]. An authorisation may be valid for a period not exceeding one year[669]. An authorisation may be repealed at any time by the Minister[670] or amended in case of a significant change in the underlying facts (if, taking into account the significant change, there are reasonable grounds to believe that the conditions for issuing an authorisation continue to be met)[671]. Within 90 days after the expiration of an authorisation, the CSE must provide a written report to the

[662] Section 34(1) CSE Act. The CSE must apply in writing to the Minister, setting out the facts that would allow the Minister to conclude that there are reasonable grounds to believe that the authorization is necessary and that the conditions for issuing it are met (Section 33 CSE Act).
[663] Charter statement for Bill C-59 (which proposed the CSE Act), available at: https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/ns-sn.html.
[664] This refers to information that is acquired, for technical or operational reasons, without the use of terms or criteria to identify information of foreign intelligence interest (Section 2 CSE Act).
[665] Section 34(1) CSE Act. The CSE must apply in writing to the Minister, setting out the facts that would allow the Minister to conclude that there are reasonable grounds to believe that the authorization is necessary and that the conditions for issuing it are met (Section 33 CSE Act).
[666] The application from the CSE to the Minister must be in writing and also contain detailed information, the facts that would allow the Minister to conclude that there are reasonable grounds to believe that the authorization is necessary and that the conditions for issuing it are met (Section 33 CSE Act).
[667] Section 35 CSE Act.
[668] Section 35(f) CSE Act.
[669] Section 36(2) CSE Act. Foreign intelligence and cybersecurity authorisations may be extended once by one year, which does not require a review by the IC, but notification of the IC as soon as feasible (Section 36(3)-(4) CSE Act.).
[670] Section 38 CSE Act.
[671] Section 39(1)-(2) CSE Act.

Minister on the outcome of the activities carried out, which the Minister must in turn provide to the IC and NSIRA[672].

Foreign intelligence and cybersecurity authorisations issued by a Minister are only valid if they are approved by the IC, who reviews whether the conclusions of the Minister are reasonable[673] and issues a written, reasoned decision approving or not approving the authorisation[674]. In order to carry out this review, the IC must be provided with all information that was before the Minister, including the application of the CSE, any supporting document or (written or oral) information that was considered by the Minister, the conclusions of the Minister and the authorisation itself[675]. While the term "reasonable" is not defined in this specific context, according to the IC it is to be interpreted in the same way as in administrative law jurisprudence (in the context of judicial review of administrative decisions)[676]. The IC must therefore be satisfied that the Minister's conclusions are based on a proper justification, transparent, intelligible, and justified in relation to the relevant factual and legal context[677]. In case of a significant change in any factual element that was set out in the application for an authorisation, the CSE must notify the Minister, who must in turn notify the IC and NSIRA[678]. Such amendment is only valid once approved by the IC[679].

A copy of each decision of the IC must be provided to the NSIRA to assist it in its review role[680]. According to its annual reports, in 2021 the IC approved two foreign intelligence authorisations, while finding one authorisation "partially reasonable", and approved two cyber security authorisations[681]. In 2020, the IC received (and approved) three foreign intelligence authorisations and one cybersecurity authorisation.

In emergency situations, i.e., if the Minister believes on reasonable grounds that the conditions for the authorisation are met, but the time required to obtain the IC's approval would defeat the purpose of issuing the authorisation, an authorisation may be issued and will be valid without having been approved by the IC[682]. Such an authorisation must be notified to the IC and the NSIRA as soon as feasible after it has been issued and is valid for a maximum period of five days[683].

2.3.2. Further use of the information collected

The processing of personal information by CSIS and CSE is subject to the Privacy Act (see the information provided in section 2.2.2). With respect to the further sharing of data with other entities (within or outside Canada), the Act specifically governing the activities of the CSIS and CSE impose specific limitations.

---

672 Section 52 CSE Act.
673 Section 13 IC Act.
674 Section 20(1) IC Act. The decision must be taken within 30 days (Section 20(3)(b) IC Act).
675 Section 23(1) IC Act.
676 Available at: https://www.canada.ca/en/intelligence-commissioner/annualreport.html.
677 See the IC's annual report for 2020, p. 6.
678 Section 37(1)-(3) CSE Act.
679 Section 39(3) CSE Act.
680 Section 21 IC Act.
681 Available at https://www.canada.ca/en/intelligence-commissioner/annualreport.html.
682 Section 40(1)-(2) CSE Act.
683 Section 41 and 42 CSE Act.

In accordance with the CSIS Act, CSIS may not disclose any information it has obtained except in specific, limited situations[684], e.g., (1) for the purposes of the performance of its duties and function; (2) to a police officer or Attorney General, where the information may be used in an investigation or prosecution of an offence; (3) to the Minister of Foreign Affairs, where the information relates to the conduct of international affairs of Canada; (4) to the Minister of National Defence, where the information is relevant to the defence of Canada; or (5) to any other Minister, where necessary in the public interest, which clearly outweighs any invasion of privacy that could result from the disclosure. Disclosures under the last ground have to be reported to the NSIRA. The CSE may, on the basis of the CSE Act, enter into arrangements with entities that have similar powers and duties (including of foreign states or international organisations), for the purpose furthering its mandate, including for information sharing or other cooperation[685]. An arrangement with a foreign entity must be approved by the competent Minister, after consultation with the Minister of Foreign Affairs.

The rules on data sharing under the CSIS Act and CSE Act are supplemented by the guidance of the Treasury Board of Canada on the need to put in place appropriate personal information protection safeguards in information sharing agreements/arrangements and by the Avoiding Complicity in Mistreatment by Foreign Entities Act (ACMFEA), Directions [for Avoiding Complicity in Mistreatment by Foreign Entities, and Ministerial Direction collectively addressing the disclosure of information that would result in a substantial risk of mistreatment (i.e., torture or other cruel, inhuman, or degrading treatment or punishment) of an individual by a foreign entity (as described in more detail in section 2.2.2).

2.3.3. Oversight

In Canada, the activities of national security authorities are supervised by different bodies.

First, the OPC oversees compliance of data processing by the CSIS and CSE with the Privacy Act, in the same way as described in section 2.2.3. In its annual report of 2020 - 2021, the OPC reported a rise in requests for consultation from national security authorities under the Privacy Act[686]. In exercising its oversight function over intelligence agencies, the OPC also collaborate closely with NSIRA, including on the basis of a memorandum of understanding that establishes procedures for coordination, carrying out joint reviews or investigations and information sharing[687].

Second, independent review of the activities of the CSIS and CSE (as well as any other activity that relates to national security or is referred to it by a Minister) is carried out by NSIRA[688]. The NSIRA may review any of the CSIS' and CSE's activities[689] and in this

[684] Section 19 CSIS Act.
[685] Section 54 CSE Act.
[686] https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/ar_202021/#toc4.
[687] https://www.priv.gc.ca/en/about-the-opc/what-we-do/memorandums-of-understanding/mou-nsira/. See e.g., the joint review by the OPC and NSIRA of information sharing under the Security of Canada Information Disclosure Act carried out in 2022 (https://www.priv.gc.ca/en/opc-news/news-and-announcements/2022/nr-c_220222/).
[688] See the National Security and Intelligence Review Agency Act (NSIRA Act). The NSIRA consists of a Chair and between three and six other members, appointed by the Governor in Council for one renewable term of five years from among members of the Queen's Privy Council who were not members of the Senate or the House of Commons, after consultation by the Prime Minister with the Leader of the Opposition in the House, as well as with the leader in the House of each party having at least twelve members in that House (Section 3-4 of the

context adopt any findings and recommendations it considers appropriate, including with respect to compliance with the law or ministerial directions, as well as the reasonableness and necessity of their exercise of powers[690]. In carrying out its reviews, the NSIRA is in principle entitled to access almost any information held by the CSIS and CSE with the exception of confidences of the King's Privy Council[691]. The NSIRA is required to report annually to the relevant Minister on the compliance of the activities of the two intelligence agencies with the law and applicable Ministerial Directions, as well as the reasonableness and necessity of the exercise of their powers[692]. When finding that an activity may be contrary to the law, the NSIRA must report this to the relevant Minister and to the Attorney General of Canada[693]. Moreover, the NSIRA must report annually on its findings and recommendations to the Prime Minister, who in turn is required to report to the Parliament[694]. The 2020 annual report of the NSIRA indicates that it conducted two reviews of the CSIS' activities (the use of threat reduction measures and intelligence sharing with the RCMP) and three of the CSE's activities (including of ministerial authorisations and the CSE's data retention policies and procedures for signals intelligence)[695]. The recommendations issued by the NSIRA in the context of these reviews and the response of both agencies (which accepted the recommendations) are described in the NSIRA's public annual report.

Finally, parliamentary oversight in the area of national security is carried out by the National Security and Intelligence Committee of Parliamentarians (NSICOP)[696]. The NSICOP is tasked with reviewing the legislative, regulatory, administrative, policy and financial framework for national security and intelligence, any matter relating to national security or intelligence that is referred to it by a Minister as well as any activity relating to national security or intelligence, unless it concerns an ongoing operation and the competent Minister determines that the review would be injurious to national security[697]. In the latter case, the Minister must inform the Committee that the review may be conducted once (s)he determines that review by

---

NSIRA Act). The NSIRA Rules of Procedure furthermore lay down rules on conflict of interest, which for instance require NSIRA members to withdraw from investigations in case they have any (previous) relation (personal, business, or professional) to any person affected by the investigation (Rule 4).

689 Section 8(1) of the NSIRA Act.

690 Section 8(3) of the NSIRA Act.

691 Section 9 and 10 of the NSIRA Act. The only information to which the NSIRA does not have access is a confidence of the King's Privy Council for Canada, consisting of personal consultants to the monarch of Canada on state and constitutional affairs. This includes information contained in a) any memorandum the purpose of which is to present proposals or recommendations to Council; b) any discussion paper the purpose of which is to present background explanations, analyses of problems or policy options to Council for consideration by Council in making decisions; c) any agendum of Council or a record recording deliberations or decisions of Council; d) any record used for or reflecting communications or discussions between ministers of the Crown on matters relating to the making of government decisions or the formulation of government policy; e) any record the purpose of which is to brief Ministers of the Crown in relation to matters that are brought before, or are proposed to be brought before, Council or that are the subject of communications or discussions referred to in paragraph (d); and f) draft legislation.

692 Section 32 of the NSIRA Act.

693 Section 35 of the NSIRA Act. To the extent that such a report relates to the powers of the IC, a copy must also be provided to him/her, see Section 36 of the NSIRA Act.

694 Section 38 of the NSIRA Act.

695 https://www.nsira-ossnr.gc.ca/wp-content/uploads/Annual-Report-2020-October-18-2021-FINAL-for-the-Prime-Minister-English-for-printing-1.pdf

696 See the National Security and Intelligence Committee of Parliamentarians Act (NSICOP Act). The NSICOP consists of a Chair and up to ten other committee members, each of whom must be a member of Parliament (Section 4(1) NSICOP Act). The committee members are appointed by the Governor in Council, on the recommendation of the Prime Minister, and hold office until Parliament is dissolved.

697 Section 8(1) and (2) NSICOP Act.

the NSICOP would no longer be injurious to national security, or the activity is no longer ongoing, the Minister must inform the Committee that the review may be conducted[698]. The NSICOP must inform the appropriate Minister and Attorney General of any activity related to national security that may not be in compliance with the law[699].

In conducting its tasks, the NSICOP is entitled to have access to any information under the control of a government department that is related to the fulfilment of the Committee's mandate, including information that is protected by litigation privilege, solicitor-client privilege or the professional secrecy of advocates and notaries[700]. Exceptions to this power include a confidence of the King's Privy Council, the identity of a confidential source of information to the Government, or information directly relating to an ongoing investigation carried out by a law enforcement agency that may lead to a prosecution[701]. The competent Minister may also refuse to provide information which the NSICOP is entitled to access if it constitutes special operational information and if provision of the information would be injurious to national security[702]. In that case, the Minister must provide the refusal and the reasons therefore to the NSICOP, as well as to the NSIRA[703].

The NSICOP submits annual reports with findings and recommendations to the Prime Minister[704], who submits it to Parliament, subject to possible redactions where the disclosure of specific information would be injurious to national security, national defence or international relations, or is protected by litigation privilege or by solicitor-client privilege or the professional secrecy of advocates and notaries[705]. Such reports must also contain the number of times that a Minister determined that a review would be injurious to national security and the number of times that a Minister refused to provide information in the course of a review.

2.3.4. Redress

The Canadian system offers different avenues to obtain redress, including compensation for damages.

First, individuals have a right of access and correction of their personal information held by CSIS and CSE under the Privacy Act, under the same conditions as described under section 2.2.4.

Second any individual may file a complaint with the OPC in respect of any matter relating to the handling of personal information by the CSIS and CSE, in the same way as described in section 2.2.4.

Third, any individual may file a written complaint to the NSIRA with respect to any activity carried out by CSIS or CSE[706]. The NSIRA investigates such complaints if the complainant

[698] Section 8(3) NSICOP Act.
[699] Section 31.1 NSICOP Act.
[700] Section 13 NSICOP Act.
[701] Section 14 NSICOP Act.
[702] Section 16(1) NSICOP Act.
[703] Section 16(3) NSICOP Act.
[704] Section 21(1) NSICOP Act.
[705] Section 21(6) NSICOP Act.
[706] Section 16 of the NSIRA Act.

has first complained to the Director of the CSIS/ Chief of CSE and has not received a response within a reasonable time or is not satisfied with the response, and if it is satisfied that the complaint is not trivial, frivolous, vexatious or made in bad faith (there are no further admissibility requirements and the complainant therefore does not have to demonstrate that (s)he has in fact been injured for the complaint to be handled). The NSIRA may attempt to resolve the complaint informally or conduct a formal investigation[707], and may ask the Canadian Human Rights Commission for its opinion on the complaint[708]. In the course of an investigation of a complaint, the complainant as well as the Director or concerned deputy head must be given an opportunity to give representations, present evidence and be heard[709]. Moreover, the NSIRA has the power to summon and enforce the appearance of persons and compel them to give oral or written evidence, as well as to produce all relevant documents[710]. If an individual is not satisfied with a decision of the NSIRA, he or she may apply to the Federal Court for judicial review of that decision[711]. In 2020, the NSIRA received 15 complaints against CSIS, of which it accepted three, and received one complaint against the CSE. In the same year, the NSIRA closed five complaint investigations, of which three were withdrawn by the complainant, one was resolved informally, and one was completed with a final report.

Finally, the same judicial avenues as the ones described in section 2.2.4 (i.e., review before the Federal Court, redress pursuant to Section 24 of the Charter, civil claims for damages[712], or redress under Section 52 of the Constitution) are also available against CSIS and CSE.

[707] Section 23 of the NSIRA Act.
[708] Section 26 of the NSIRA Act.
[709] Section 25(2) of the NSIRA Act.
[710] Section 27 of the NSIRA Act.
[711] Section 18.1 of the Federal Courts Act.
[712] Case law has confirmed that the activities of intelligence agencies can result in civil liability, see Abdelrazik v. Canada, [2010] F.C.J. No. 1028 (court declining to strike action alleging negligence on the part of CSIS officials).

IV. FAROE ISLANDS

1. RULES APPLYING TO THE PROCESSING OF PERSONAL DATA

1.1. Relevant developments in the data protection framework of the Faroe Islands

The Commission adopted the adequacy decision for the Faroe Islands on 5 March 2010[713], after having received the opinion of the Article 29 Working Party on 9 October 2007[714]. The decision found that, for the purposes of Article 25(2) of Directive 95/46/EC (Data Protection Directive)[715], the Faroe Islands provided an adequate level of protection for personal data transferred from the EU to recipients subject to the Faroese Act on Processing of Personal Data (APPD)[716].

At the time of the adoption of the adequacy decision, the legislative framework for the protection of personal data in the Faroe Islands consisted of the APPD, which entered into force on 1 January 2002 and was based on the standards of the Data Protection Directive. In August 2017, a process to modernise the APPD was initiated, which led to the adoption of a new Data Protection Act (DPA)[717] that entered into force on 1 January 2021. As explained in more detail below, the DPA is closely aligned with Regulation (EU) 2016/679 (GDPR)[718] and has strengthened the Faroese data protection framework in several areas. The DPA is accompanied by a special commentary, which refers to the GDPR and its recitals, in particular by specifying that the GDPR is to be used when interpreting the Act.

Like the previous APPD, the new DPA has a broad scope of application, applying to both private operators and public authorities[719]. While the definitions of 'personal data', 'controller', 'processor'[720], 'data subject' and 'processing' (which are identical to those used

[713] Commission Decision 2010/146/EU of 5 March 2010 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection provided by the Faeroese Act on processing of personal data, OJ L 58, 9.3.2010, p. 17.
[714] Opinion 9/2007 on the level of protection of personal data in the Faroe Islands, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp142_en.pdf
[715] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[716] Act No. 73 of 8 May 2001; Act on Processing of Personal Data.
[717] Act No. 80 of 7 June 2020; Act on the protection of personal data (Data Protection Act).
[718] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[719] Article 2 and 3(1) DPA and, previously, Article 3(1)-(2) APPD. As explained in more detail in section 2.1, the DPA does not apply to the processing of personal data in the course of activities carried out by Danish authorities in the Faroe Islands (such as the High Commissioner of the Faroe Islands, the Court of the Faroe Islands and law enforcement authorities). The DPA also contains a partial exclusion from the scope of application for data processing exclusively for artistic, literary or journalistic purposes and for data processing in databases with already published materials for journalistic purposes (Article 3(3)-(4) DPA). In particular, only Chapter 8 (remedies, liability and penalties), as well as Articles 41, 42 (requirements for controllers that engage a processor) and 47 (data breach notification) apply to such processing. Similar to what is provided by Article 85 GDPR, these activities are subject to specific safeguards provided by a separate act (Act No. 45 of 16 May 2006 on Media Responsibility) to reconcile the right to the protection of personal data with the freedom of expression and information. This Act in particular requires that the content and conduct of mass media is in conformity with sound press ethics (Article 34 of the Act) and provides individuals with a specific redress possibility before the Faroese Press Council (Articles 43, 44 and 49 of the Act).
[720] Already under the APPD, data processing by a processor had to be governed by a written contract between the parties, specifying that processors may only act on instructions from the controller (Article 31(2) APPD). The DPA has further clarified the relationship between controllers and processors, by listing in more detail the

in the GDPR) have not changed compared to the previous APPD[721], the DPA has brought even more convergence with the GDPR, e.g., by introducing a definition of 'pseudonymisation'[722] and further clarifying when a person is 'identifiable' by applying the same criteria of recital 26 of the GDPR[723]. The DPA has also extended the territorial scope of the Faroese data protection rules by adopting the same approach as Article 3 of the GDPR[724].

The main data protection principles and obligations that were already provided by the APPD at the time of the adoption of the adequacy decision have remained in place without substantial changes. This is the case for the principles of purpose limitation[725], data quality and proportionality[726], data retention[727] and data security[728]. At the same time, a number of principles and obligations have been further strengthened, in particular in the context of the recent reforms, e.g., the principle of lawfulness of processing, the requirements for data breach notification, the transparency obligations and the principle of accountability.

As regards the principle of lawfulness and fairness of processing, the DPA has reduced and further clarified the grounds that are available for processing, which are now identical to those listed in Article 6(1) GDPR[729]. Furthermore, the requirements for valid consent have been reinforced under the DPA, by making clear that, in addition to being freely given, specific and informed[730], consent must be unambiguous and expressed by a clear affirmative action[731].

Similarly, the DPA has strengthened the existing transparency obligations by requiring that additional information is provided to the individual (e.g., the contact details of the data protection officer, the fact that the controller intends to transfer the data to a third country, the retention period, the right to withdraw consent, the existence of automated decision-making, etc.)[732] when data is collected directly from the individual[733] or from third parties[734] and when

---

elements that should be reflected in such a contract, similar to what is provided in Article 28 of the GDPR (Article 41 DPA).

[721] See Articles 2, 6(1), (2), (6) and (7) DPA.

[722] Article 6(4) DPA.

[723] See the special commentary on Article 6(1) DPA and, previously, Article 2(1) APPD.

[724] See Article 5(2) DPA. The territorial scope of the previous APPD was more limited, as it applied to controllers not established in the Faroe Islands if (1) the processing of data is carried out with the use of equipment situated in the Faroe Islands (unless such equipment is used only for purposes of transit), or (2) the collection of data in the Faroe Islands takes place for the purpose of processing in a foreign country (i.e. where a controller that is not located in the Faroe Islands offers goods or services directly to data subjects in the Faroe Islands and in that context collects personal data) (Article 7(2) APPD).

[725] Article 7(1) lit. 2 DPA and, previously, Article 8(1) lit. 2 and 4 APPD.

[726] Article 7(1) lit. 3 and 4 DPA and, previously, Article 8(1) lit. 3 and 6, as well as Article 27 APPD.

[727] Article 7(1) lit. 5 DPA and, previously, Article 8(1) lit. 5 APPD.

[728] Article 7(1) lit. 6 DPA and, previously, Article 31(3) APPD, in conjunction with Executive Order No. 28 of 27 February 2003 on Security in relation to processing of personal data.

[729] Article 8 DPA. See also Articles 8(1) and 9 APPD, which provided two additional legal bases for processing, i.e., where the processing is subject to statutory authority (i.e., authorised or laid down by law) and when necessary for the performance of a task carried out in the exercise of official authority vested in the controller or a third party to whom the personal data are disclosed.

[730] Article 2(8) APPD defined consent as "[…] any freely given, specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."

[731] Article 6(10) DPA. Moreover, Article 9(2) DPA requires that, if consent is given in the context of a written declaration that also concerns other matters, the request for consent must be presented in a manner that is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language.

[732] Under Articles 20 and 21 APPD, controllers were required to provide the following information when collecting personal data from the individual: the name and address of the controller/his representative, the purposes of processing and its name (i.e. information on the type of processing), the recipients to whom personal

it is further processed[735]. The exceptions to transparency requirements have also been narrowed and further clarified. In particular, under the DPA, the transparency obligations do not apply in limited circumstances, e.g., if disclosing the information would endanger national security or jeopardise the investigation of a criminal offence[736]. In this respect, the special commentary clarifies that to rely on an exception, a concrete assessment should be made in each individual case. Restrictions could only be made if a concrete assessment leads to the conclusion that the information, if disclosed, would fall under one of the exceptions.

With respect to the principle of data security, the DPA expanded the requirements on reporting data breaches. While controllers were already required to notify data breaches to the Data Protection Agency[737], the DPA has clarified the modalities for such notifications, e.g., by specifying that breaches should be reported without undue delay (and where feasible within 72 hours), and exempting data breaches that are unlikely to result in a risk to the rights of individuals[738]. Moreover, the DPA introduced a requirement to notify data breaches to the concerned individuals, where it is likely to result in a high risk to their rights[739].

The DPA has also modernised the accountability requirements that applied under the previous regime (e.g., on record keeping and risk assessments)[740], by introducing an obligation to implement principles of data protection by design and by default, keep records of processing, appoint a data protection officer and carry out data protection impact assessments (and consult the Data Protection Agency prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk)[741].

In addition to the strengthening of data protection principles and obligations, the protections for special categories of data have been reinforced since the adoption of the adequacy decision. The APPD already offered additional protection for data about colour and family bonds; religion, philosophy, or political conviction; sexual life; health; trade union connections; relative social problems and other private concerns[742]. The DPA has codified the existing interpretation of "colour and family bonds," "sexual life" and "data about health" by

---

data is disclosed, whether or not the data subject is obliged to provide the data and the possible consequences failing to do so, as well as other information necessary for the data subject in order to exercise his or her rights.

[733] Article 23 DPA. Similar to Article 13(4) GDPR, this does not apply where and insofar as the data subject already has the information (see Article 23(4) DPA).

[734] Article 24 DPA. This obligation is subject to several exceptions, which are similar to the exceptions listed in Article 14(5) GDPR. Where an exception applies, the controller must take appropriate measures to protect individual rights, including by making the information publicly available (see Article 25(3) DPA).

[735] Article 23(3) DPA.

[736] Article 36(1) DPA. See also Article 22(1) APPD, which laid down exceptions to the transparency obligations under the old regime.

[737] Article 6 of Executive Order No. 28 of 27 February 2003 on Security in relation to processing of personal data. Although the Order only referred to the processing of personal that requires confidentiality/privacy the Data Protection Agency applied a wide interpretation, requiring any processing of personal data to comply with the Order.

[738] Article 47 DPA.

[739] Article 48 DPA.

[740] See Articles 4, 5, 8 and 16 of Executive Order No. 28 of 27 February 2003 on Security in relation to processing of personal data.

[741] Articles 38, 44, 49, 52 and 53 DPA.

[742] Article 2(9) APPD. The notion of "colour and family bonds" also covered data revealing racial and ethnic origin, while 'sexual life' included data concerning sexual orientation. In addition, 'data about health' covered genetic information.

explicitly mentioning data revealing racial and ethnic origin, sexual orientation and genetic data in the list of special categories of data[743] and included biometric data processed for the purpose of uniquely identifying a natural person[744]. As regards the safeguards that apply to the processing of special categories of data, the DPA has replaced the previous requirement to obtain prior authorisation from the Data Protection Agency[745] by a general prohibition on processing, only allowing the processing of such data in a limited number of situations[746]. For example, similarly to the GDPR, the DPA allows the processing of special categories of data where the data subject has given explicit consent, where processing is based on a law, where processing is necessary to protect the vital interest of the data subject, or where processing is necessary for reasons of substantial public interest[747].

The DPA has also modernised the APPD's provisions on data subject rights, which included a right to obtain information, a right of insight (i.e., access) and the rights of rectification, erasure and blocking[748]. In particular, the DPA contains updated provisions on the rights of rectification, erasure[749], restriction and object (also including a general right to object to the processing of personal data for direct marketing purposes) that correspond to the rights provided by the GDPR, both as regards the conditions under which these rights can be exercised and possible exceptions[750]. In addition, the right of access has been further strengthened, by not only requiring controllers to provide individuals with information about the processing of their data (as was already the case under the APPD)[751], but also to give access to personal data (including by providing a copy)[752]. The DPA has also further circumscribed the exceptions to the right of access, which only apply in limited circumstances, e.g., if disclosing the information would endanger national security or jeopardise the investigation of a criminal offence[753], and, according to the special commentary, must be applied on a case-by-case basis.

Moreover, the DPA introduced new rights. This includes a right for individuals not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affect them[754]. Such

[743] In addition, personal data relating to criminal convictions and offences are considered to be part of the special categories of data (Article 11(1) DPA) and benefit from specific protections.
[744] Article 11(1) DPA. Biometric data is defined in Article 6(12) DPA as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopy data".
[745] Article 10(1) APPD.
[746] Article 12, 18 and 19 DPA.
[747] Articles 12 DPA.
[748] Articles 18, 19 and 27 APPD.
[749] This for example also includes an obligation for the controller to take reasonable steps to inform other controllers that are processing information that the data subject has requested to erase (Article 28(2) DPA).
[750] Articles 27, 28, 29, 32 and 33 DPA.
[751] Under the DPA, the controller must provide the same information as under the old APPD (the name and address of the controller or his representative, the purpose of processing, the categories of personal data that is being processed, the source of personal data etc.), as well as information on the retention period, the right to lodge a complaint with the Data Protection Agency, the existence of other rights, the fact that the controller intends to transfer the data to third countries, and the existence of automated decision-making (Article 26(1) and (2) DPA).
[752] Article 26 DPA.
[753] Article 36(2) DPA. See also Article 22(1) APPD, which laid down exceptions under the old regime.
[754] Article 35 DPA.

automated decision making may only take place under certain conditions (e.g., only if authorised by law or based on the data subject's explicit consent) and subject to specific safeguards (e.g., informing the individual about the processing and the envisaged consequences)[755]. In addition, the DPA introduced a right to data portability that corresponds to the same right available under the GDPR[756].

The DPA has also introduced several changes to the rules on international transfers (onward transfers for the purpose of the adequacy decision)[757]. In particular, the regime of the APPD that allowed international transfers on the basis of a specific transfer instrument (an adequacy decision adopted by the Minister of Justice, adequate safeguards or certain statutory grounds) after obtaining prior permission from the Data Protection Agency has been updated[758]. The DPA abolished the prior authorisation requirement and allows transfers to non-EEA countries under the same conditions as the GDPR. In particular, as a general principle, the special commentary clarifies that the rules on international transfers are intended to ensure that the level of protection ensured by the DPA will not be lowered, which also applies when personal data are onward transferred from the third country to which they were transferred from the Faroe Islands.

Moreover, as was the case under the APPD, different instruments can be used for data transfers. First, the Minister of Justice can adopt an adequacy decision, for which the special commentary specifies that the same elements as those provided by Article 45 GDPR have to be taken into account and adequacy decisions adopted by the European Commission may be taken into account. In practice, the same countries that have received an adequacy decision from the Commission under the Data Protection Directive have been recognised by the Faroe Islands, with the addition of Gibraltar[759]. In addition, a transfer may take place on the basis of appropriate safeguards (by means of a legally binding and enforceable instrument between public authorities, standard data protection clauses adopted by the Minister or contractual clauses approved by the Data Protection Agency), on the condition that enforceable data subject rights and effective legal remedies are available to the data subject. In particular, the Minister has approved the standard contractual clauses for the transfer of personal data to third countries set out in the Commission implementing decision (EU) 2021/914. Finally, the DPA allows transfers on the basis of 'derogations'[760], which correspond to those provided by Article 49 GDPR and which, according to the special commentary, have a narrow scope and cannot be relied upon for regular and repeated transfers.

1.2. Oversight, enforcement and redress

The independent entity in charge of overseeing compliance with the data protection rules is the Data Protection Agency. The Agency supervises compliance of any processing activity, either on its own initiative or on the basis of complaints from data subjects[761]. In addition, it

[755] Article 23(2) lit. 6, Article 24(2) lit. 7 and Article 35 DPA.
[756] Article 31 DPA.
[757] According to the DPA, the rules on international transfers apply to any transfer of personal data to countries that are not part of the EEA (Article 59 in conjunction with Article 6(14) DPA).
[758] Article 16(1) and Article 17(2) APPD.
[759] See Executive Order No. 31 of 21 March 2019 on transfer of Personal Data to Foreign Countries.
[760] Article 62 and 63 DPA
[761] Article 68, lit. 1 DPA and, previously, Article 37, lit. 1 APPD.

carries out a number of tasks, such as promoting public awareness in relation to data protection, giving its opinion on administrative and legislative measures relating to data protection, promoting the awareness of controllers and processors of their obligations, monitoring and informing of relevant developments regarding data protection on the Faroe Islands and abroad, and publishing annual reports on its activities[762]. In performing its supervisory duties, the Agency has access to all relevant information, as well as to the premises where processing operations are carried out or administered and where data or technical equipment are stored or used[763].

Since the adoption of the adequacy decision, both the resources and powers of the Agency have been strengthened. In particular, the number of members of the Agency (i.e., the Council) has increased from three under the APPD (a chair and two other members) to five under the new DPA (a chair and four members, two of which are nominated by the Association of Municipalities and the Faroe Employer's Association)[764]. Furthermore, the number of staff members of the Agency has doubled, from three to six members of staff. To further strengthen the independence of the Council, the special commentary to the DPA provides that the members must remain free from external influence, whether direct or indirect, and may neither seek nor take instructions from anybody. In addition, the budget of the Agency has increased in the past years, from 2.0 million DKK (~ 268 000€) in 2018 and 2.445 million DKK (~ 324 000€) in 2018, to 3.252 million DKK (~ 435 000€) in 2020.

Under the former APPD, compliance with data protection requirements was ensured through a combination of different measures, including notification, prior authorisation, corrective measures (issued by the Data Protection Agency) and criminal sanctions (i.e., fines or imprisonment, imposed by the Prosecution Service)[765]. The new DPA has strengthened the enforcement powers of the Data Protection Agency, while abolishing most prior notification and authorisation requirements.

The DPA has provided the Agency with a broad range of powers, in particular to issue warnings, reprimands and orders (inter alia to discontinue processing, bring processing into compliance with the Act, implement security measures and rectify, erase or restrict processing), and to make its decisions public[766]. The DPA also introduced the possibility for the Data Protection Agency to issue a fixed penalty notice[767], i.e., a fine that may be imposed where an infringement is estimated not to result in a penalty higher than a fine, if the concerned entity admits to being guilty and accepts the fine indicated in the notice within a specified time limit. This procedure deviates from the general principle that the police, prosecution service and courts handle criminal cases and allows the settle a case without legal proceedings. Because of the criminal nature of a penalty notice, it may only be issued for infringements that are simple and where there is no evidentiary doubt.

[762] Article 68 and 74 DPA.
[763] Article 71 DPA and, previously, Article 40 APPD.
[764] Article 66 and 67(2) DPA and, previously, Article 36(3) APPD.
[765] See Article 32-35 APPD, as well as Executive Order No. 124 of 19 September 2011 on Notification and Exemption from the Rules on Authorisations.
[766] Articles 70 and 73 DPA.
[767] Article 79 DPA.

In addition to the powers of the Data Protection Agency, the new DPA has also retained a regime of criminal sanctions, e.g., for violations of the provisions on data protection principles, the obligations for controllers and processors, international transfers, and individual rights[768]. As regards the amount of fines, the special commentary provides that the Faroese authorities should take into account the same factors as those listed in Article 83(2) GDPR, i.e., the intentional or negligent character of the infringement, any action taken by the controller or processor to mitigate the damage suffered by data subjects, duration of the infringement etc. Moreover, as a starting point, the level of fines on the Faroe Islands should follow the developments in Denmark under the GDPR.

As regards possibilities for individuals to obtain redress, the Faroese system continues to offer various avenues, including the possibility to lodge a complaint with the Data Protection Agency[769], obtain judicial redress directly against controllers and processors (both private operators and public authorities)[770] and obtain compensation for damages[771].

Despite its relatively small office, the Data Protection Agency plays an active role, both when it comes to its engagement with stakeholders and exercising its oversight role.

In particular, according to information received from the Faroese authorities, the Data Protection Agency annually handles a number of files, including inspections, notifications, written questions, complaints and proposals for legislation. For example, in 2022, 379 files were handled and 319 in 2023. In the context of the Covid-19 pandemic, the Agency also advised the Faroese Government on issues relating to data protection (e.g., as regards the processing of sensitive data as part the testing strategy). Moreover, since the entry into force of the new DPA, the Data Protection Agency handled over 500 files, as part of which it received more than 22 notifications of data breaches and launched more than 28 data protection inspections. It also sent questionnaires to various controllers investigating different aspects of compliance with the new Act. This has already led to enforcement action in several cases, including reprimands and orders demanding that processing be brought into line with the new Act.

Finally, since June 2020, when the new DPA was passed by the Faroese parliament, the Data Protection Agency issued over 20 guidelines (e.g., on data protection officers, data protection in the workplace, data breaches, consent and data subject rights) and around ten templates (e.g., for notifying data breaches). The Agency also engages in various outreach activities, such as presentations and courses for both the private and public sector (so far reaching

[768] The special commentary to the DPA clarifies that, in accordance with Article 19 of the Criminal Code, this covers both intentional and negligent infringements of the DPA. For public authorities, Article 27(2) of the Criminal Code applies. This Article provides that public authorities in the Faroe Islands may not be punished for infringements committed in their exercise of official authority (e.g., when adopting a decision). Public authorities may only be punished in the exercise of activity that corresponds to or can be considered equal to activity carried through by private entities.

[769] Article 76 DPA and, previously, Article 30 APPD. Decisions of the Data Protection Agency may furthermore be appealed before the Faroese Courts on the basis of Article 255 of the Administration of Justice Act.

[770] In particular, in accordance with Article 255 of the Administration of Justice Act, any individual who has a legal interest in the outcome of a case, can bring a case before a court. According to information received from the Faroese Government, this requirement would always be fulfilled if a provision of the APPD/new DPA has been violated.

[771] Article 77 DPA and, previously, Article 46 APPD.

around 1000 participants) and launched a new website, as well as a podcast series about data protection.

2. ACCESS TO AND USE OF PERSONAL DATA TRANSFERRED FROM THE EUROPEAN UNION BY PUBLIC AUTHORITIES IN THE FAROE ISLANDS

2.1. General legal framework

The Faroe Islands enjoy a special status as an autonomous nation within the Danish Kingdom, regulated by the Home Rule Act of 1948 (Act No. 137 of 23 March 1948). Whereas certain aspects (the Constitution, the foreign exchange and monetary policy, the Supreme Court and the foreign, defence and security policy) always remain under Danish authority, the Takeover Act (Act No. 578 of 24 June 2005) provides the Faroe Islands with the possibility to assume legislative and executive power in all other areas. If the Faroe Islands decide not to take over a certain area, it remains under the jurisdiction of Denmark[772]. This is the case for the activities of the police, the prosecution service, the prison and probation service and the courts, which have not been taken over by the Faroe Islands. Given that criminal law enforcement and national security therefore remain under Danish jurisdiction, activities in these areas in the Faroe Islands are exercised exclusively by Danish authorities[773]. As explained in more detail below, these authorities are subject to laws under Danish auspices that, after having been approved by the Faroese Parliament, have been put into force in the Faroe Islands by an Executive Order of the Danish government.

The limitations and safeguards that apply to the collection and subsequent use of personal data by public authorities on the territory of the Faroe Islands for criminal law enforcement and national security purposes follow from the overarching constitutional framework of the Danish Kingdom, specific laws regulating data access, as well as rules that apply to the processing of personal data.

Firstly, Section 72 of the Danish Constitution guarantees the right to privacy. It stipulates that no house search, seizure, examination of letters and other papers, or any breach of secrecy in postal, telegraph and telephone matters may take place except under a judicial order, unless a particular exception is warranted by statute.

In addition, the European Convention on Human Rights applies to the Faroe Islands. The European Convention on Human Rights protects the right to respect for private and family life (and the right to the protection of personal data as part of it). In particular, pursuant to Article 8 of that Convention, a public authority may only interfere with the right to privacy in accordance with the law, in the interests of one of the aims set out in Article 8(2), and if proportionate in light of that aim. Article 8 also requires that the interference is "foreseeable", i.e., has a clear, accessible basis in law, and that the law contains appropriate safeguards to prevent abuse.

[772] Therefore, the below assessment is limited to the application of the law that applies in the Faroe Islands as the law of a third country. Where Danish law is applicable, reference is made to its relevant provisions.
[773] In other areas, activities are exercised by Faroese public authorities, on the basis of legislation adopted by the Faroe Islands, including the new Data Protection Act of January 2021 (See Article 5(1) DPA. All DPA requirements, as described in detail in section 1.1, apply to the activities of such authorities).

In addition, in its case law, the European Court of Human Rights has specified that any interference with the right to privacy and data protection should be subject to an effective, independent and impartial oversight system that must be provided for either by a judge or by another independent body (e.g., an administrative authority or a parliamentary body)[774]. Moreover, individuals must be provided with an effective remedy, and the European Court of Human Rights has clarified that the remedy must be offered by an independent and impartial body which has adopted its own rules of procedure, consisting of members that must hold or have held high judicial office or be experienced lawyers, and that there must be no evidential burden to be overcome in order to lodge an application with it. In undertaking its examination of complaints by individuals, the independent and impartial body should have access to all relevant information, including closed materials. Finally, it should have the powers to remedy non-compliance[775].

Therefore, through its adherence to the European Convention on Human Rights, as well as its submission to the jurisdiction of the European Court of Human Rights, the Faroe Islands is subject to a number of obligations, enshrined in international law, that frame its system of government access on the basis of principles, safeguards and individual rights similar to those guaranteed under EU law and applicable to the Member States.

Secondly, as explained in more detail in section 2.2.1 and 2.3.1, these general principles are reflected in specifics laws that regulate the access and use of personal data for criminal law enforcement and national security purposes and impose minimum safeguards. This includes in particular the Faroese Administration of Justice Act[776].

Thirdly, the processing of personal data by public authorities for criminal law enforcement and national security purposes is subject to specific data protection rules. Danish law enforcement authorities in the Faroe Islands are subject to the Act on the Processing of Personal Data by Law Enforcement Authorities that was set into force in the Faroe Islands on 1 July 2022[777]. This Act essentially transposes the legislation that was adopted by Denmark to implement Directive (EU) 2016/680 (Law Enforcement Directive) in the Faroe Islands, with minor adaptions to reflect the local conditions (for instance removing references to cooperation in/with the European Data Protection Board)[778]. It inter alia provides for key data protection principles (e.g., purpose limitation, data minimisation, data accuracy, data security), obligations for law enforcement authorities (e.g., on the processing of sensitive data, international data transfers, notification of data breaches, etc.) and rights for individuals (e.g., to obtain access, correction or deletion of personal data). In addition, the Act is complemented by several Executive Orders that have been put into force in the Faroe Islands:

[774] European Court of Human Rights, Klass and others v. Germany, Application no. 5029/71, paragraphs 17-51.
[775] European Court of Human Rights, Kennedy v. the United Kingdom, Application no. 26839/05, (Kennedy), paragraphs 167 and 190.
[776] Administration of Justice Act for the Faroe Islands (Act No. 964 of 26 June 2020).
[777] Ordinance No. 1034 of 29 June 2022 on the entry into force of the Act on the Processing of Personal Data for the Faroe Islands.
[778] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

(1) Executive Order No. 1051 of 12 September 2017 for the Faroe Islands on security measures for the protection of personal data processed by the public administration[779];

(2) Executive Order No. 1058 of 12 September 2017 for the Faroe Islands on derogating from the obligation to notify certain proceedings carried out by the public administration[780];

(3) Executive Order No. 1057 of 12 September 2017 for the Faroe Islands derogating from the obligation to notify certain proceedings conducted by the courts[781];

(4) Executive Order No. 1059 of 12 September 2017 for the Faroe Islands on security measures for the protection of personal data processed before the courts[782];

(5) Executive Order No. 442 of 16 March 2021 on Processing of Personal Data in the Central Criminal Register (Order no. 442 of 16 March 2021 for the Faroe Islands)[783].

In the area of national security, the Act on the Security and Intelligence Service[784] (ASIS) governs the activities of the Danish Security and Intelligence Service in the Faroe Islands with regard to the collection and (further) processing of personal data for national security purposes. This Act was set into force on the Faroe Islands on 1 January 2021 and mirrors the Danish Act on the Security and Intelligence Service, with some adaptations for the local Faroese situation. As explained in more detail in section 2.3.2, under the Act, all core principles (lawfulness, purpose limitation, data minimisation, data accuracy, storage limitation), individual rights and data protection obligations (e.g., rules on international transfers) apply[785]. The Act is complemented by two Executive Orders:

(1) Executive Order for the Faroe Islands on security measures to protect information about natural and legal persons processed by the Danish Security and Intelligence Service (Order No.254 of 22 February 2021, DSIS Order on security measures)[786];

(2) Executive Order for the Faroe Islands on the Danish Security and Intelligence Service's processing of information on natural and legal persons, etc. (Order No. 253 of 22 February 2021, EOFIDSIS)[787].

---

[779] This Order specifies in more detail what is required from controllers with respect to security, e.g., with respect to internal rules, instructions to staff, requirements when using processors, access management, log keeping etc.

[780] This Order provides certain exceptions from the general obligation to notify the Data Protection Authority of processing activities, e.g., personal data that is not sensitive or of a confidential nature, personal data processed in the context of staff management systems, library systems, etc.

[781] This Order exempts courts from notifying the data protection authority with respect to the processing of human resources data.

[782] This Order specifies in more detail what security measures should be put in place by courts, e.g., with respect to internal rules, the use of processors, access management, log keeping, etc.

[783] This Order regulates the processing of personal data regarding criminal cases.

[784] Ordinance No. 1623 of 17 November 2020 on the entry into force of the Act on the Security and Intelligence Service for the Faroe Islands.

[785] Sections 6a, 7 and 9a ASIS.

[786] This Order specifies the security measures the Service must take to ensure appropriate security of the data that it processes, including measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

[787] This Order contains provisions on the Service's files, databases etc. (Chapter 1); security of processing (Chapter 2); The Service's own personnel cases and security clearance cases (Chapter 3); the procedure for the

These general limitations and safeguards can be invoked by individuals before independent oversight bodies (e.g., the Danish data protection authority, the Intelligence Oversight Board) and courts to obtain redress (see sections 2.2.4 and 2.3.4).

2.2. Access and use by public authorities in the Faroe Islands for criminal law enforcement purposes

The legal framework that applies to criminal law enforcement authorities in the Faroe Islands imposes a number of limitations on the access and use of personal data for criminal law enforcement purposes and provides oversight and redress mechanisms. The conditions under which such access can take place and the safeguards applicable to the use of those powers are described in the following sections.

2.2.1. Legal bases and applicable limitations/safeguards

Personal data transferred from the EU on the basis of the adequacy decision and subsequently processed by Faroese controllers or processors may be collected by Danish authorities (i.e., the Danish police) for criminal law enforcement purposes in the context of a search or seizure, on the basis of a production order, by accessing communications or by collecting location data through telecommunications observation. The conditions, limitations and safeguards that apply to the use of these powers are laid down in the Faroese Administration of Justice Act. This Act lays down clear and precise rules on the scope of application of these measures, thereby ensuring that the interference with the rights of individuals will be limited to what is necessary for a specific criminal investigation and proportionate to the pursued purpose. As explained in more detail below, prior judicial authorisation is in principle required in order to access personal data, unless in exceptional cases specifically listed in the Act. Moreover, specific (procedural) safeguards exist to guarantee due process rights for individuals.

First, searches of places, documents (including electronic documents), objects, papers, etc.[788] may in principle only take place if the targeted person is suspected on reasonable grounds of an offence that is subject to public prosecution and the search may be presumed to be of major importance to the investigation[789]. To perform searches of accommodation, documents, papers and the content of locked objects, additional requirements must be met, i.e., the investigation must concern an offence punishable by imprisonment or there must be specific reasons to presume that evidence will be found[790]. With regard to searches concerning a person who is not a suspect, a higher threshold applies: such a search may only be conducted if the person consents to the search[791] or if the investigation concerns an offence punishable by imprisonment and there are specific reasons to presume that the search will produce

examination and approval of certain investigative measures (Chapter 4); collection and disclosure of information (Chapter 5); internal auditing (Chapter 6); information to be provided to the Intelligence Oversight Board (Chapter 7); retention for public archives (Chapter 8).

[788] Section 836(1) Administration of Justice Act.

[789] Section 837(1) Administration of Justice Act. According to the preparatory work for the Administration of Justice Act, this Section corresponds to Section 794(1) of the Danish Administration of Justice Act, which also uses the term "suspected on reasonable grounds", and is inter alia interpreted in accordance with relevant case law. For example, case law in Denmark found that an anonymous tip about the presence of narcotics in a building was not sufficient to suspect all residents (U.1999.1670.Ø) and that a search of a private property on the basis of an anonymous tip was not justified without further documented details on the tip (U.2013.3047/2).

[790] Section 837(2) Administration of Justice Act.

[791] Section 838(1) Administration of Justice Act.

evidence[792]. In all cases, a search is not allowed where, considering the purpose of the measure, the significance of the case, and the intrusion and inconvenience that the measure may be presumed to cause, the measure would be disproportionate[793].

Procedurally, searches of accommodation, documents or papers may in principle only be conducted on the basis of a court order that contains information on the specific circumstances of the case demonstrating that the abovementioned conditions are met[794]. Where the purpose of the search would be defeated by applying for a court order (i.e., if the search would no longer lead to the collection of evidence in the investigation if it would be delayed to obtain a court order), a search may take place without a court order, upon a decision of the police[795]. In principle, persons whose accommodation, premise or object is to be searched are informed of and/or present at the search (whether the search is conducted on the basis of a court order or not)[796]. This requirement may only be derogated from under certain conditions (in particular if it is of crucial importance for the investigation that the search is conducted without the knowledge of the suspect and others, and only with respect to investigations of intentional violations of certain crimes, such as crimes against the independence of the State) and on the basis of a court order[797].

Second, seizures may be conducted to secure evidence; to secure the State's claim for legal costs, confiscation and fines; to secure the victim's claim for restoration or compensation, and where the accused has evaded prosecution[798]. Any seizure may only take place as part of an investigation of an offence subject to public prosecution[799], if there is reason to presume that the object may serve as evidence or should be confiscated, or if the object was taken from someone during the offence who can claim it back[800]. A production order requiring a person who is not a suspect to produce or surrender objects may be issued under the same conditions[801]. A seizure may not take place and a production order may not be issued if the measure is disproportionate in light of the significance of the case and the loss or inconvenience that the measure is likely to cause[802]. Moreover, a seizure or production order may only be conducted/issued to the least extent necessary. If the purpose of the measure may

[792] Section 838(1) Administration of Justice Act.
[793] Section 840(1) Administration of Justice Act. This assessment must also take into account whether the search involves destruction or damage to objects, see Section 840(2) of the Act.
[794] Section 839(2) Administration of Justice Act.
[795] Section 839(3) Administration of Justice Act. Upon request from the person against whom the measure is directed, the police are required, as soon as possible, and at the latest within 24 hours, to bring the case before the court, which will then determine by court order whether the measure may be approved. The decision to conduct a search of objects other than documents and papers or of premises other than accommodation that are in the possession of a suspect is always taken by the police (Section 839(1) Administration of Justice Act). Similarly, if a search concerns accommodation, premises or objects in the possession of a suspect, and the suspect gives written consent to the search, the decision to conduct the search may also be taken by the police (Section 839(5) Administration of Justice Act).
[796] Section 841(2)-(3) Administration of Justice Act.
[797] Section 842 Administration of Justice Act.
[798] Section 844(1) Administration of Justice Act.
[799] Section 845(1) and 846(1) of the Administration of Justice Act.
[800] Section 845(1) and 846(1) of the Administration of Justice Act.
[801] Section 848(1) Administration of Justice Act.
[802] Section 849(1) Administration of Justice Act.

be achieved by less intrusive means, a written agreement to this effect may be concluded with the person against whom the measure is directed[803].

Seizures and production orders may only take place/be issued when authorised by a court order, which must contain information on the specific circumstances of the case demonstrating that the abovementioned conditions are met[804]. If the purpose of the seizure/production order would be defeated by waiting for a court order, the objects/information may be obtained without a court order[805]. In that case, the person against whom the measure is directed may request that the case is brought before the court (as soon as possible and at the latest within 24 hours) to determine whether the seizure/production order can be approved[806]. In principle, the person against whom a seizure is directed is informed thereof when the measure is initiated, unless upon a court decision finding that it is of crucial importance to the investigation that it is conducted without the knowledge of the suspect or others[807].

Third, the police may intercept communications and collect information on communications (e.g., through telephone tapping, the interception of mail, or by obtaining information on which devices are connected to a phone number or communication device)[808]. These measures may only be carried out under strict conditions: (1) there must be specific grounds for supposing that information is being passed or items sent to or from a suspect[809]; (2) the measures may be assumed to be of crucial importance to the investigation and (3) the investigation concerns an offence that is punishable by law with imprisonment of at least six years or another serious offence specified by the Act[810], or, for certain measures (telephone tapping and obtaining information on which telephones or similar communication devices within a specified area are connected to a particular telephone or other communication device), a crime that has endangered or may endanger human life or important public assets[811]. In any event, such measures may not take place where, considering the purpose of the measure, the significance of the case, and the intrusion and inconvenience that the

[803] Section 849(2) Administration of Justice Act.
[804] Section 850(1)-(2) Administration of Justice Act.
[805] Section 850(4) Administration of Justice Act. In addition, a seizure may be carried out, or a production order may be issued, without a court order, if the person against whom the measure is directed consents to the measure (Section 850(9) Administration of Justice Act).
[806] Section 850(4) Administration of Justice Act. Before the decision is taken by the court, the concerned person has the opportunity to comment (Section 850(8) Administration of Justice Act).
[807] Section 851(1) and Section 856 Administration of Justice Act.
[808] Section 812(1) Administration of Justice Act. The police may make recordings or take copies of the conversations, statements, items of mail, etc. mentioned in Article 812(1), to the extent that they are entitled to examine the contents thereof, see Article 812(2) Administration of Justice Act. In addition to the interception of communications, the police may order providers of telecommunication networks or services to preserve electronic data, including traffic data, that is stored at the time the order is issued. Such a police order must set out which data should be preserved and for how long. It may only cover data necessary for the investigation and apply as short as possible, in any event not longer than 90 days (without the possibility to extend the order), see Section 819 Administration of Justice Act.
[809] This requirement does not apply for the collection of 'extended telecommunications data', i.e., obtaining information on which telephones or similar communication devices within a specified area are connected to other telephones or communication devices, see Section 813(5) Administration of Justice Act.
[810] Section 813(1), lit. 3, (2) and (3) Administration of Justice Act. This for example includes offences against the independence and safety of the State, offences against the Constitution and supreme authorities of the State (including terrorism), the distribution of pornographic material of minors, blackmail, etc.
[811] Section 813(1) Administration of Justice Act.

measure may be presumed to cause the person or persons affected, the measure would be disproportionate[812].

Similarly, the police may obtain information from telecommunication providers on the location of a mobile telephone that is presumed to be used by a suspect ('telecommunications observation'). Such collection of location data may take place in the context of an investigation concerning an offence punishable by a term of imprisonment of at least 1.5 years, if there are specific reasons to assume that the mobile phone is used by a suspect and the measure is of major importance for the investigation[813]. Telecommunications observation may not be initiated if it would be disproportionate in light of the purpose of the interception and the importance of the case, as well as the harm and inconvenience it would likely cause to the concerned individual[814].

Specific procedural safeguards apply to the interception of communications, the collection of information about communications and the collection of location data, which may in principle only take place on the basis of a court order, which must set out the specific circumstances of the case justifying that the abovementioned conditions are met, as well as the telephone numbers, premises, addressees, or items of mail affected by the measure[815]. The court order must also specify the time period in which the measure may be conducted, which must be as short as possible, not exceeding four weeks, unless extended by another court order[816]. Exceptionally, the police may collect (information on) communications without a court order, where obtaining the order would defeat the purpose of the measure, in which case approval from the court must be sough as soon as possible and no later than 24 hours after the measure is implemented[817].

Moreover, when an application to a court is made by the police for the authorisation of measures concerning communications (including the interception of communications and the collection of location data), a lawyer must be appointed to represent the concerned individual, who is entitled to access the materials provided by the police, attend hearings and provide comments[818]. In addition, the concerned individual must in principle be notified by the court within 14 days after the measure has ended[819]. Such notice may only be dispensed with or deferred upon a decision of a court and after having provided the appointed lawyer with the opportunity to comment, if it would prejudice an ongoing investigation or the protection of

[812] Section 814(1) Administration of Justice Act.
[813] Section 825(5) Administration of Justice Act.
[814] Section 825(7) Administration of Justice Act.
[815] Section 815(1) and 825(8) Administration of Justice Act. For the investigation of certain serious crimes (e.g., crimes against the independence of the state and security or against the state constitution and the highest state authorities), the court order may also state the name of the person concerned by the measure (the suspect), see Article 815(2) of the Act. In this case, the police must in principle notify the court as soon as possible after the expiry of the period within which the measure was carried out of any telephone numbers intercepted that were not listed in the court order. Such a notification must indicate the specific reasons for supposing that the telephone numbers concerned are being used to pass messages to or from the suspect.
[816] Section 815(3) and 825(8) Administration of Justice Act.
[817] Section 815(4) and 825(8) Administration of Justice Act.
[818] Sections 816-817 and 825(8) Administration of Justice Act.
[819] Section 821(1) and (3) and 825(8) Administration of Justice Act. This notification requirement does not apply when information is obtained on which telephones or similar communication devices within a specified area are connected to a particular telephone or other communication device (Section 821(5) Administration of Justice Act).

confidential information on the police's investigative methods, or if other circumstances argue against notification[820].

Fourth, on the basis of a court order, the police may read data in an information system that is not publicly accessible with the aid of programs or other equipment (data reading) where (1) there are specific grounds for supposing that the information system is being used by a suspect in connection with certain serious crimes (i.e., crimes punishable with imprisonment of at least six years or crimes against the independence of the State and security or against the State constitution and the highest State authorities) and (2) the measure may be assumed to be of crucial importance to the investigation[821]. Data reading may not take place where, considering purpose of the measure, the significance of the case, and the intrusion and inconvenience that the measure may be presumed to cause the person or persons affected, the measure would be disproportionate[822]. The safeguards mentioned above for the collection of communications (i.e., on exceptional collection without a court order, the appointment of a lawyer and the notification of concerned individuals) also apply to data reading[823].

Finally, certain entities in the Faroe Islands are required to report information (including personal data) to criminal law enforcement in accordance with rules on the prevention of money laundering and the financing of terrorism. In particular, the Act on Measures to prevent Money Laundering and Financing of Terrorism (Money Laundering Act)[824] requires certain entities (e.g., banks, fund brokers, payment service providers, investment management companies, etc.) to investigate complex and unusually large transactions, as well as all unusual patterns of transactions and activities that have no clear economic or demonstrable lawful purpose, in order to determine whether there is suspicion or reasonable grounds to presume that those transactions or activities are or have been connected to money laundering or financing of terrorism[825]. They must immediately notify the Public Prosecutor for Serious Economic and International Crime when they suspect, or have reasonable grounds to presume, that a transaction is or has been connected to money laundering or financing of terrorism[826]. Similarly, the Royal Decree on Specific Measures to combat Terrorism requires entities covered by the Money Laundering Act to immediately notify the Danish Money Laundering Secretariat of a transaction or request that has or has had a connection to persons or entities mentioned on the lists of names used in connection with Denmark's implementation of the sanctions under United Nations Security Council Resolution No 1373 of 28 September 2001[827].

2.2.2. Further use of the information collected

[820] Section 821(4) Administration of Justice Act.
[821] Section 826 (1) Administration of Justice Act.
[822] Section 826(2) Administration of Justice Act.
[823] Section 826(3)-(4) Administration of Justice Act.
[824] Act no. 651 of 8 June 2017 on Measures to prevent Money Laundering and Financing of Terrorism (Money Laundering Act) (set into force for the Faroese Islands by royal decree no. 813 of 12 August 2019).
[825] Section 25(1) Money Laundering Act.
[826] Section 26(1) Money Laundering Act.
[827] Royal decree for the Faroese Islands no. 1149 of 24 September 2020 on Specific Measures to combat Terrorism.

The processing of personal data collected by law enforcement authorities in the Faroe Islands is subject to the Act on the Processing of Personal Data by Law Enforcement Authorities[828]. As explained above, this Act essentially mirrors (with some minor adjustments to take the Faroese context into account, e.g., by removing references to cooperation with/in the European Data Protection Board) the Danish Act on the Processing of Personal Data by Law Enforcement Authorities[829], which has transposed the Law Enforcement Directive into the Danish legal order. Therefore, the legal framework that applies in the Faroe Islands to the processing of personal data by criminal law enforcement authorities is based on the framework that applies in the EU. It provides for key data protection principles (e.g., purpose limitation, data minimisation, data accuracy, data security, accountability)[830], imposes data protection obligations on law enforcement authorities (e.g., prohibiting the processing of sensitive data unless this is necessary for the protection of vital interests of individuals or the data is manifestly made public by the individual;[831] to report data breaches[832], keep records of processing activities[833], appoint a data protection officer[834] etc.) and imposes specific conditions for transfers of personal data to third countries or international organisations (in particular allowing transfers to countries/organisations for which the European Commission has adopted an adequacy decision under the Law Enforcement Directive, or, in the absence thereof, on the basis of an international agreement containing data protection safeguards or a self-assessment of all the circumstances of the transfer carried out by the controller)[835].

In addition, more specific requirements on the use of information collected by criminal law enforcement authorities follow from the Administration of Justice Act. For example, the Act provides that any information incidentally obtained by the police in the context of a search or the collection of (information on) communications may not be used as evidence in court, unless a court decides otherwise if other investigative measures are unlikely to provide evidence in the case and the case concerns an offence that is punishable by imprisonment for at least 1.5 years (for information obtained through the collection of communications) or 6 years (for information obtained through a search) [836]. Moreover, under the Administration of Justice Act, any material obtained through the collection of (information on) communications must be destroyed if it proves not to be relevant to the investigation[837].

2.2.3. Oversight

The activities of Danish criminal law enforcement authorities in the Faroe Islands are supervised by different bodies.

First, oversight of the processing of personal data by Danish criminal law enforcement authorities in the Faroe Islands is carried out by the Danish data protection authority (Danish

[828] Available in Danish at: https://www.kunngerdaportalur.fo/Umbraco/surface/Document/GetDocument?id=4278
[829] Act No. 410 of 27 April 2017.
[830] Section 4 Act on the Processing of Personal Data by Law Enforcement Authorities.
[831] Section 10 Act on the Processing of Personal Data by Law Enforcement Authorities.
[832] Section 13 Act on the Processing of Personal Data by Law Enforcement Authorities
[833] Section 10 Act on the Processing of Personal Data by Law Enforcement Authorities.
[834] Section 14 Act on the Processing of Personal Data by Law Enforcement Authorities.
[835] Section 34 Act on the Processing of Personal Data by Law Enforcement Authorities.
[836] Section 822 and 843 Administration of Justice Act.
[837] Section 824(4) Administration of Justice Act.

DPA), under the Act on the Processing of Personal Data by Law Enforcement Authorities[838]. The Danish DPA may investigate compliance with the Act, on the basis of complaints from individuals or on its own initiative[839]. It has access to all information relevant to its activities and may conduct on-site inspections[840]. In terms of remedial powers, the Danish DPA may issue opinions that planned processing activities are likely to infringe the Act, may order processing operations to comply with the Act, or may temporarily or definitely restrict/prohibit the processing of personal data[841]. Non-compliance with an order of the Danish DPA is punishable by a criminal fine imposed by a court[842].

Second, the activities of the Danish criminal law enforcement authorities in the Faroe Islands are subject to the general oversight of the Danish Ombudsman, the Danish Independent Police Complaint Authority and the Danish Audit Office.

The Danish Parliamentary Ombudsman is elected by the Danish Parliament to investigate, at its own initiative or acting on a complaint by an individual, whether public authorities act unlawfully or otherwise commit errors or derelictions in the discharge of their duties[843]. The Ombudsman is independent from the Parliament[844] and may only be dismissed by the Parliament if (s)he ceases to enjoy its confidence[845]. The Ombudsman has jurisdiction over all parts of the public administration, with the exception of courts[846]. In conducting investigations, the Ombudsman has access to all relevant information and can access all relevant premises[847]. The Ombudsman may express criticism, issue recommendations and otherwise state his/her views of a case, but cannot take legally binding decisions[848]. If the Ombudsman's investigation of a case reveals errors or derelictions of major importance, it must be reported to the Parliament's Legal Affairs Committee, as well as to the minister, municipal council or regional council concerned.

The Independent Police Complaints Authority is an independent body with the power to investigate, on the basis of complaints or on its own initiative, allegations of police misconduct (including in the Faroe Islands)[849]. In conducting an investigation of possible misconduct, the Authority has access to all relevant information[850]. Unless an investigation is

[838] Under the previous law, the Danish DPA for instance carried out oversight activities of the police in November 2021, focusing on inter alia data security, the deletion of personal data and rights of individuals.
[839] Section 40(1), (6), (10) and (12) Act on the Processing of Personal Data by Law Enforcement Authorities.
[840] Section 41(1) Act on the Processing of Personal Data by Law Enforcement Authorities.
[841] Section 42(1) Act on the Processing of Personal Data by Law Enforcement Authorities.
[842] Section 50(2) Act on the Processing of Personal Data by Law Enforcement Authorities.
[843] See Chapters 1, 4, 5 and 7 of the Danish Ombudsman Act.
[844] Section 10 Danish Ombudsman Act.
[845] Section 3 Danish Ombudsman Act.
[846] Chapter 2 Danish Ombudsman Act.
[847] Chapter 6 Danish Ombudsman Act.
[848] Section 22 Danish Ombudsman Act.
[849] Chapter 107 and 108 Administration of Justice Act. The Authority is headed by a Police Complaints Council, whose members are appointed by the Minister of Justice for a four year renewable term, upon the recommendation of different bodies: a Chair that must be a High Court judge (upon the recommendation of the High Courts), an attorney (upon the recommendation of the Danish Bar and Law Council), a professor in law and two representatives of the general public (upon the recommendation of the National Association of Local Authorities and the Danish People's Information Council), see Section 118b Danish Administration of Justice Act. In accordance with Section 150(2) Administration of Justice Act, the Authority exercises its functions with complete independence.
[850] Section 1060(1) Administration of Justice Act.

terminated[851], the Authority issues a decision within a reasonable time, in which it may include comments on the conduct of the police[852]. The Authority may also initiate an investigation into allegations of criminal offences committed by the police, either upon a complaint from an individual or *ex officio,* when there is a reasonable suspicion that police personnel in service have committed a criminal offense which is subject to prosecution by the public authorities[853]. In this context, the Authority has access to all relevant information and may use the investigatory powers, including the coercive powers, which are available to the police,[854]. When an investigation is completed, the Authority sends the case to the public prosecutor for a decision on possible prosecution[855]. In addition, the Authority shares an annual report on its investigation with the Danish Attorney General[856]. According to the 2022 annual report of the Authority, it handled 17 cases concerning the Faroe Islands in 2022, including two criminal cases concerning the unlawful disclosure of information[857].

The Danish Audit Office is an independent body headed by an Auditor General, who is appointed by the Speaker of the Danish Parliament and approved by the Parliament's Standing Orders Committee[858]. While the main role of the Audit Office is to conduct financial audits, it may also examine whether government-funded agencies and enterprises comply with applicable laws and regulations and on the efficiency and effectiveness of the administration. For example, in 2020, the Audit Office published a report on the outsourcing of sensitive and confidential personal data by central government IT systems[859].

2.2.4. Redress

Individuals whose personal data is collected by criminal law enforcement authorities in the Faroe Islands have access to different avenues to obtain redress, including compensation for damages.

First, individuals have a right to obtain access to, correction[860] of and deletion[861] of their data processed by criminal law enforcement authorities under the Act on the Processing of

[851] The investigation can e.g., be terminated if there are grounds for bringing charges against the accused or the defendant is suspected of a criminal offense and demands the case be treated as a criminal case. See Section 1069(1) Administration of Justice Act.
[852] Section 1070-1071(1) Administration of Justice Act. If no decision has been made within 6 months, the complainants and defendants must be notified.
[853] Section 1077(1) Administration of Justice Act.
[854] Section 1079 Administration of Justice Act.
[855] Section 1081(1) Administration of Justice Ace. The Authority may appeal decisions of the public prosecutor's office on possible prosecution to the Prosecutor General.
[856] Section 1081(2) Administration of Justice Act.
[857] Available at: https://politiklagemyndigheden.dk/wp-content/uploads/2023/05/Politiklagemyndigheden-Aarsberetning-2022.pdf.
[858] Section 1(1) Danish Auditor General Act. The Auditor General is appointed for a term of six years, with a possible renewal of four years. He/she may only be dismissed by the Speaker of the Parliament upon recommendation of the Public Accounts Committee, with the approval of the Standing Orders Committee of the Parliament.
[859] Available at: https://uk.rigsrevisionen.dk/media/2105518/15-2019.pdf.
[860] Pursuant to Section 17(1) Act on the Processing of Personal Data by Law Enforcement Authorities, a criminal law enforcement authority is required, upon request from an individual, to rectify without undue delay any incorrect information and to complement any incomplete information (where the latter is possible without jeopardising the purpose of the processing). The authority is also required to inform other entities from whom the data originated of any corrections.

Personal Data by Law Enforcement Authorities[862]. The exercise of the right of access may be postponed, restricted or refused if providing access would be prejudicial to (1) official or legal inquiries, investigations or procedures, (2) the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, (3) the protection of national security, (4) the protection of public security or (5) the protection of the rights of the data subject or others[863]. In response to a request for erasure, the authority may instead restrict the processing of personal data where the accuracy of the data is contested by the data subject and the accuracy/inaccuracy cannot be ascertained, or the data must be maintained for the purposes of evidence[864]. In case of a postponement/restriction/refusal, a law enforcement authority has to inform the individual of the reasons thereof or indicate to the individual that it is not possible to disclose whether or not personal data regarding him/her are being processed[865]. In both cases, the individual has to be informed about the possibility to appeal the decision, or to request that the Danish DPA exercises the rights on behalf of the individual (the outcome of which can in turn be appealed before a court)[866].

Second, any individual may lodge a complaint concerning the processing of their data by a criminal law enforcement authority with the Danish DPA[867]. In response to a complaint, the latter may make use of all of the investigatory and remedial powers described in the previous section. Decisions or inaction of the Danish DPA can be appealed before the Danish courts[868]. The court may annul administrative decisions and return the decision to the specific authority (cassation) or replace an administrative decision with a new decision[869].

Third, any individual can lodge a complaint about the actions of Danish criminal law enforcement authorities in the Faroe Islands, including the collection and use of personal data, before the Danish Parliamentary Ombudsman, who can make use of the powers described in the previous section. Similarly, individuals can turn to the Independent Police Complaints Authority, which can make use of the powers described in the previous section to investigate and handle complaints or allegations of criminal offences concerning activities of Danish criminal law enforcement authorities[870].

Fourth, individuals can also directly invoke the Act on the Processing of Personal Data by Law Enforcement Authorities against criminal law enforcement authorities in court to obtain judicial redress[871]. This also includes the possibility to obtain compensation for material or

---

[861] In case of an erasure of data in response to a request from an individual, the authority must inform any recipients of the data thereof (Section 17(6) Act on the Processing of Personal Data by Law Enforcement Authorities).
[862] Section 15 and 17 Act on the Processing of Personal Data by Law Enforcement Authorities.
[863] Section 16(1), in conjunction with Section 14(1) Act on the Processing of Personal Data by Law Enforcement Authorities
[864] Section 17(3) Act on the Processing of Personal Data by Law Enforcement Authorities.
[865] Section 16(3) and Section 17(6) Act on the Processing of Personal Data by Law Enforcement Authorities.
[866] Section 40(1)(10) Act on the Processing of Personal Data by Law Enforcement Authorities.
[867] Section 48(1) Act on the Processing of Personal Data by Law Enforcement Authorities.
[868] Section 48(2) Act on the Processing of Personal Data by Law Enforcement Authorities and Section 63(1) of the Danish Constitution.
[869] See Article 63(1) of the Danish Constitution.
[870] In accordance with Section 1058(3) Administration of Justice Act, a complaint must be lodged within 6 months of the occurrence of the matter to which the complaint relates, although this time limit may be disregarded by the Authority in exceptional cases.
[871] Section 48(3) Act on the Processing of Personal Data by Law Enforcement Authorities.

immaterial damage suffered as a result of unlawful data processing by a criminal law enforcement authority[872].

Fifth, different judicial redress avenues are available to individuals to challenge the unlawful use of investigative measures (e.g., search, seizure, intervention with the secrecy of communications, etc.). In particular, disputes on the lawful use of investigatory powers may be brought before the court during an investigation, in which case an individual can invoke Section 72 of the Danish Constitution[873]. Furthermore, depending on the circumstances, unlawfully obtained evidence may be ruled inadmissible by the court in the criminal case[874]. In addition, any individual who, in the course of criminal proceedings, has been subjected to investigative measures may obtain compensation for financial damage, mental suffering, inconvenience, disturbance or deterioration of position or condition as a result of these measures[875]. The Prosecution Service decides whether to award a claim for damages[876]. If the claim for damages is refused, the claimant can, within two months of notification of the refusal, request that the claim is brought before the district court[877].

Finally, any individual may obtain judicial redress before the European Court of Human Rights against the unlawful collection of his/her data by Danish criminal law enforcement authorities in the Faroe Islands, provided that all available domestic remedies have been exhausted.

2.3. Access and use by public authorities for national security purposes

Personal data transferred from the EU to the Faroe Islands based on the adequacy decision may be accessed for national security purposes by the Danish Security and Intelligence Service (DSIS) on the basis of legislation put into force in the Faroe Islands and Faroese implementing rules[878]. The DSIS, which is part of the police, is primarily tasked with preventing, investigating and combating crimes against the independence and security of the State, as well as crimes against the constitution and supreme State authorities[879]. In addition, the DSIS performs several other tasks in the area of national security, such as informing the Minister of Justice of matters relating to internal security, collecting intelligence on threats to the country, and drawing up threat assessments[880]. As described in more detail below, the

[872] Section 49 Act on the Processing of Personal Data by Law Enforcement Authorities.
[873] Section 763(1) Administration of Justice Act.
[874] Section 763(1) Administration of Justice Act.
[875] Section 1050, conjunction with Section 1049 Administration of Justice Act.
[876] Section 1053 (1) Administration of Justice Act.
[877] Section 1054 Administration of Justice Act. For instance, in one case, the Danish Eastern High Court ruled in favour of DKK 75 000 (approx. EUR 10 000) in compensation due to four police raids of a company and long-term and extensive seizure of business documents (U.2005.103Ø or TfK2004.685/1Ø).
[878] This report focuses on the legal framework that applies in the Faroe Islands. It therefore does not describe the collection and use of personal data by the Danish Defence Intelligence Service (DDIS), which is regulated exclusively by Danish law (that has not been put into force on the Faroe Islands). The DDIS, which falls under the Danish Ministry of Defence, is Denmark's foreign affairs intelligence service and military intelligence service. The DDSIS' interception of communications may not target authorities, companies, organisations or individuals within the Danish territory, including the Faroe Islands (Section 13 of the Danish Defence Act). Moreover, according to written information received from the Faroese government, there is currently no legal basis that would allow controllers and processors in the Faroe Islands to voluntarily disclose information in case it would be requested by the DDSIS.
[879] Article 1(1) ASIS. See also Chapters 12 and 13 of the Criminal Code.
[880] Article 1(2)-(7) ASIS.

collection of personal data by the DSIS in the Faroe Islands, as well as the further use of such data, is regulated by the ASIS, the Faroese Administration of Justice Act and Faroese Executive Orders.

2.3.1. Legal bases and applicable limitations/safeguards

The ASIS lays down the different powers of the DSIS (described in more detail below), as well as the overarching conditions and limitations that apply to the use of each power. Importantly, while the ASIS provides the DSIS with a legal basis to collect information (including personal data), the DSIS can only make use of coercive measures – such as carrying out a search/seizure, issuing a production order, or intercepting communications – in accordance with the conditions, limitations and safeguards of the Administration of Justice Act described in section 2.2.1[881]. As a result, the same requirements as the ones that apply to criminal law enforcement activities of the Police, also apply to the national security activities of the DSIS. For example, the information must be important in the context of a specific criminal investigation, the DSIS must comply with the principle of proportionality, prior judicial authorisation must in principle be obtained, and individuals must in principle be notified about the collection of their data (e.g., within 14 days after the interception of communications), etc.

More generally, the DSIS is, as any other public authority, subject to principles of general administrative law, including the principle of proportionality. This means, inter alia, that the means and methods used by the DSIS to collect or obtain personal data must be appropriate for that purpose, that less intrusive means and methods must be deemed not to be sufficient, and that the method chosen must not be disproportionate to the purpose for which the data are collected or obtained[882].

In accordance with the ASIS, the DSIS provides that it may open "inquiries" into natural and legal persons, if the inquiry is likely to be relevant for the performance of its tasks relating to the prevention and investigation of crimes against the independence and security of the State or against the constitution, or if the inquiry is necessary for the performance of its other tasks[883]. An inquiry is an activity aimed at specifically selected natural or legal persons for the purpose of collecting or obtaining information about them. The actual collection of personal data in the context of an inquiry may only take place if additional conditions are met.

First, the Act provides that the DSIS may collect and obtain data that may be relevant to its activities[884]. Based on the preparatory work for the Danish DSIS Act (on which the Faroese Act is based), the "collection" of personal data means accessing data that is readily available (e.g., information available on the internet), while "obtaining" personal data means accessing data that is not readily available but can be obtained by contacting a third party such as a public authority, association, organisation or private person[885]. According to an evaluation

[881] Section 6 ASIS.
[882] Danish Ministry of Justice, Report on the experience with the PET Law, June 2022 (PET report), p. 16. The report is available in Danish at https://www.justitsministeriet.dk/pressemeddelelse/justitsministeriet-offentliggoer-rapport-om-evaluering-af-pet-loven/.
[883] Section 5 ASIS.
[884] Section 3 ASIS.
[885] PET report, p. 12.

report of the Danish Ministry of Justice on the activities of the DSIS, the criterion "may be relevant" implies that data may only be collected or obtained by the DSIS if the data is likely to have an impact on the effectiveness of the Service[886]. In any event, a third party receiving a request is not obliged under the ASIS to disclose personal data to the DSIS[887]. Whether the requested data can be disclosed must therefore be determined based on the legal grounds for processing set out in the applicable data protection legislation, in this case the Faroese Data Protection Act. The only way for the DSIS to compel the third party to disclose data is by following the procedures of the Administration of Justice Act (e.g., to obtain a production order)[888].

Second, the DSIS may obtain data from other public authorities (including in the Faroe Islands)[889], which are obliged to disclose the data if the DSIS considers that the data are likely to be relevant to the performance of its tasks relating to the prevention and investigation of crimes against the independence and security of the State, as well as crimes against the constitution. The criterion "likely to be relevant" implies that there must be a more specific presumption that the data which the Service wishes to obtain will have an impact on the performance of the Service's tasks[890]. In other words, there must be a certain probability (and not a remote possibility) that the data may contribute to the Service's performance of those tasks[891].

Additional limitations and safeguards follow from the EOFIDSIS, which for instance requires that the collection of particularly sensitive health data (e.g., information on psychiatric diagnoses) and data on groups of persons who are not identified in advance may only take place with the prior approval of the head or general counsel of the DSIS[892]. When obtaining data on groups of unidentified persons, the DSIS is required, as soon as circumstances permit, to assess whether the persons to whom the data relates are relevant for its tasks. To the extent this is deemed not to be the case, the irrelevant data must be deleted immediately[893]. In addition, the use of coercive investigative measures must always be approved by the head or general counsel of the DSIS or their deputies[894]. If the measure in question requires a court

[886] PET report, p. 12.
[887] See the proposal for legislative act LSF 161 in parliamentary session 2012/1, p. 88: https://www.retsinformation.dk/eli/ft/201212L00161 (Only available in Danish).
[888] Section 848(1) Administration of Justice Act. See the proposal for legislative act L 23 in parliamentary session 2015-16, p. 8: https://www.ft.dk/ripdf/samling/20151/lovforslag/l23/20151_l23_som_fremsat.pdf (Only in available in Danish).
[889] Section 4 ASIS. Based on this provision, the DSIS can only request data that is already available to the other authority or that it should receive in the future. It does not oblige the other authority to obtain information from a third party that it otherwise would not have had a reason to obtain. See proposal to legislative act L 23 in parliamentary session 2015-16, p. 9: https://www.ft.dk/ripdf/samling/20151/lovforslag/l23/20151_l23_som_fremsat.pdf (Only in available in Danish).
[890] Under Section 4 ASIS, the DSIS may obtain information on persons at a stage where there is no basis (yet) for a concrete suspicion, including grounds for initiating a criminal investigation or bringing criminal charges, but where there may nevertheless be reasons for presuming a suspicion, for example because the concerned individual is associated with a group of persons or an organisation that is under investigation by the DSIS. See PET report, p. 12.
[891] PET report, p. 12.
[892] Section 10(2) EOFIDSIS.
[893] Section 10(1) EOFIDSIS.
[894] Article 9(1) EOFIDSIS.

order, the approval must be given before the case is referred to the court in accordance with the rules of the Administration of Justice Act[895].

As stressed above, the provisions of the ASIS on the possibility for the DSIS to open inquiries and in that context collect information do not by themselves authorise the DSIS to initiate criminal investigations or to make use of coercive powers such as searches, seizures, production and the interception of communications (or collection of information on communications). The latter may only be carried out if all relevant legal requirements are fulfilled, i.e., under (1) the ASIS (e.g., establishing the relevance or necessity of the collection for the performance of the DSIS' tasks), (2) the EOFIDSIS (e.g., as regards internal approval) and (3) the Administration of Justice Act (e.g., relevance/importance to a specific criminal investigation, compliance with the principle of proportionality, need to obtain prior authorisation from a court, obligation to notify concerned individuals, etc.).

2.3.2. Further use of the information collected

The processing of personal data collected by the DSIS is also governed by the ASIS, which imposes the principle of purpose limitation, data minimisation, data accuracy and limited data retention[896]. With respect to data retention, the ASIS generally requires the DSIS to delete data on natural persons where no new information has been obtained in connection with the inquiry or investigation in the last 15 years[897]. Data may only be kept longer where the data is needed on imperative grounds relating to the performance of the DSIS' tasks, in which case the DSIS must inform the Intelligence Oversight Board (see below) thereof[898]. However, if the DSIS becomes aware that there is no longer a legal basis to keep data before the abovementioned retention period has expired (i.e., because the data is no longer relevant to the performance of its tasks relating to the investigation of certain crimes or the data is no longer necessary for the performance of the DSIS' other tasks), that data must be deleted immediately[899]. This obligation does not apply where the information is included in documents for which there is still a legal basis for the processing[900]. The DSIS must carry out regular spot checks on the deletion of data, on which it is required to regularly report to the Intelligence Oversight Board[901].

The DSIS is also required to have technical and organisational measures in place to ensure the security of the data it processes, in accordance with the DSIS Order on security measures[902]. This includes having internal rules on inter alia physical security measures, access control and authorisation schemes, guidance on the use of computer equipment, etc., which must be reviewed at least annually[903]. More generally, the EOFIDSIS requires the DSIS to regularly

[895] Article 9(2) EOFIDSIS. In particular, as regards the initiation of telephone interception or the obtaining of telecommunications data based on court orders relating to a named person rather than a specific telephone number, in accordance with Article 815(2) Administration of Justice Act, prior approval must be given by the head or general counsel of the DSIS or their deputies in each case where measures are taken in respect of new telephone numbers, see Article 9(3) EOFIDSIS.
[896] Section 6 ASIS.
[897] Section 9(1) ASIS.
[898] Section 9(2) ASIS, in conjunction with Section 14 EOFIDSIS.
[899] Section 9a (1) ASIS.
[900] Section 9a (2) ASIS.
[901] Section 12 and 18 EOFIDSIS.
[902] Section 3 DSIS Order on security measures.
[903] Section 4 DSIS Order on security measures.

carry out spot checks on deletion, logging, opening of investigations, obtaining of data, investigative measures and transfer of data[904] and report on such checks to the Intelligence Oversight Board[905].

Under the ASIS, the further sharing of personal data with other entities is subject to specific requirements. First, the DSIS may share data with the Danish Defence Intelligence Service if such sharing may be relevant to the performance of the tasks of both services[906]. The disclosure of information to other entities (within or outside the Faroe Islands) may take place only (1) in compliance with all data protection principles (e.g., purpose limitation, data minimisation, data accuracy); (2) if the individual has given consent, the disclosure is likely to be relevant to the performance of the DSIS' tasks relating to the prevention and investigation of crimes against the independence and security of the State or against the constitution, or the disclosure is necessary for the performance of its other tasks and (3) when the disclosure is presumed reasonable following a case-by-case assessment (which, according to the preparatory work on the ASIS, requires to examine in particular, the content of the information, the purpose of the disclosure and an assessment of the damaging effect that such disclosure could cause for the concerned individual)[907]. An additional requirement applies to sensitive personal data, which may only be transferred to foreign authorities with the prior approval of the head or general counsel of the DSIS or their deputies[908].

Finally, when making use of the powers under the Administration of Justice Act, the same limitations under that Act as the ones described in Section 2.2.2, e.g., as regards the use of intercepted communications as evidence or the deletion thereof when the information is not relevant for the investigation, also apply to data processed by the DSIS.

2.3.3. Oversight

The activities of the DSIS are supervised by different bodies.

First, compliance by the DSIS with the ASIS, including its requirements on the processing of personal data, is overseen by the independent Danish Intelligence Oversight Board[909]. The Board can investigate compliance with the ASIS (and the rules established under the ASIS,

[904] Section 12 EOFIDSIS.
[905] Section 18 EOFIDSIS.
[906] Section 10(1) ASIS.
[907] Section 10(2) and (4), in conjunction with Section 6a and 7 ASIS. See also https://www.logting.fo/mal/mal/?id=194.
[908] Section 11 EOFIDSIS.
[909] The status and independence of the Board are laid down the Danish Act on the Security and Intelligence Service (DASIS). The Board is composed of five members, appointed by the Minister of Justice after consultation of Parliamentary Committee on the Intelligence Services (see below) for a renewable period of four years (Section 16(1) DASIS). The chair of the Board, a judge of the High Court, is appointed on the basis of a recommendation from the presidents of the High Courts of Eastern and Western Denmark (Section 16(2) DASIS). It follows from the preparatory work pertaining to Section 16 that it should not be possible to appoint members who have or have held prominent positions in a political party, who are staff in the central administration, or who served in intelligence agencies (See proposal for legislative act L 161 of parliamentary session 2012-13, p. 73-74: 20121_l161_som_fremsat.pdf(ft.dk) (Only available in Danish). In particular, there may be no circumstances casting doubt on the complete impartiality of the persons concerned. A Board member may only be dismissed by the Minister of Justice if the person in question requests so or if the prerequisites for the appointment are no longer met (Section 16(3) DASIS). In accordance with Section 17 DASIS, the Board exercises its functions with complete independence.

such as the EOFIDSIS)[910] on its own initiative or on the basis of a complaint from an individual[911]. For example, in 2021, the Board inter alia carried out checks of compliance by the DSIS with the requirements for obtaining information from other public authorities, the data retention requirements, the rules for data sharing with third parties, as well as data security[912]. In carrying out its oversight activities, the Board can access all relevant information (including by ordering the DSIS to provide any information or material relevant to its activities, to access the premises of as well as the data processed by the DSIS)[913]. In addition, the DSIS is required to regularly report to the Board, e.g., about the collection of personal data from public authorities and about its regular internal audits concerning data deletion, logging, the opening of investigations, obtaining of data, the use of investigative measures and transfers of data[914]. The Board may issue an opinion with recommendations to the DSIS, which may also be provided to the Minister of Justice[915]. If, in exceptional cases, the DSIS does not comply with a recommendation of the Board, it must notify the Board and immediately submit the matter to the relevant minister for decision[916]. If also the minister decides not to follow the recommendation of the Board, the Government must notify the Parliamentary Committee for the Intelligence Services[917].

Second, the DSIS is more generally subject to independent oversight by the Danish Parliamentary Ombudsman, who can make use of all the powers described in section 2.2.3.

Third, the DSIS, as a part of the Danish police, is also subject to the oversight of the Independent Police Complaints Authority, which can make use of all the powers described in section 2.2.3.

Fourth, the Danish National Audit Office also has the power to supervise the activities of the DSIS, under the same conditions as described in section 2.2.3.

Finally, the DSIS is subject to specific parliamentary oversight by the Danish Parliamentary Committee for the Intelligence Services[918]. To this end, the Government must provide the Committee with an annual update on the activities of the intelligence services, including the DSIS, and keep it informed of significant circumstances of a security nature and foreign policy issues relevant to the activities of the intelligence services[919]. The Committee may also

[910] The Board does not supervise compliance with the Administration of Justice Act, which is subject to the supervision of courts and other oversight bodies that are competent for criminal law enforcement authorities, see below (see Section 18 ASIS).
[911] Section 18 ASIS.
[912] See the Board's annual report on the DSIS for 2021, available at: https://www.tet.dk/wp-content/uploads/2022/06/PET_UK_2021_web.pdf.
[913] Section 20 ASIS.
[914] Section 15 EOFIDSIS and Section 18, in conjunction with Section 12 EOFIDSIS.
[915] Section 19(1) ASIS.
[916] Section 19(3) ASIS.
[917] Section 19(1) ASIS. See also Section 3(3) of Act no. 378 of 6 July 1988 on the establishment of a committee on the Danish Defence Intelligence Service and the Danish Security and Intelligence Service as amended by Act no. 632 of 12 June 2013 (Intelligence Services Committee Act).
[918] The Committee consists of five Members of Parliament appointed by the political parties represented in the Danish Parliament. It is headed by a chairperson elected by the Committee members, see Section 1(2) Intelligence Services Committee Act.
[919] Section 2 Intelligence Services Committee Act. In addition, the government is required to submit the annual report of the DSIS to the Committee prior to its publishing, see Section 2(6) Intelligence Services Committee Act.

request information from the government on the activities of the intelligence services, including statistical information[920]. Finally, prior to issuing guidelines on the activities of the intelligence services, the government must inform the Committee of their content[921]. The Committee may, either orally or in writing, provide the government with its opinion on all the matters under its consideration[922]. However, since the members of the Committee are bound by a duty of confidentiality, the recommendations of the Committee are not made public[923].

2.3.4. Redress

Individuals can make use of different avenues to obtain redress against the DSIS, including compensation for damages.

First, individuals may request the Intelligence Oversight Board to investigate whether the Service is processing personal data about them "without justification"[924]. Following such a request, the Board must ensure that this is not the case and inform the person concerned thereof[925]. In particular, the Board will, on the basis of a request from an individual, verify whether the DSIS complies with the ASIS, including for instance with the applicable data protection principles (e.g., purpose limitation, data accuracy, data minimisation). If during its investigation the Board finds that the Service is processing personal data without a legal basis (or no longer has a legal basis for the processing), the DSIS is obliged to delete that data under the ASIS[926]. In addition, in case "special circumstances so warrant", the Board may also order the Service to provide the data subject full or partial access to personal data about him/her processed by the Service[927]. For example, in 2021, the Board received 35 requests from individuals, which led to a finding that data was processed unlawfully in six cases, after which the data was deleted by the DSIS[928]. Decisions of the Board in response to a request from an individual can be challenged before the Danish courts in accordance with Section 63(1) of the Constitution to obtain judicial review, as described in section 2.2.4.

In addition, while under the ASIS individuals are in principle not entitled to have direct access to data processed by the DSIS or to know whether the DSIS is processing such data, the DSIS may provide full or partial access to data upon request "if special circumstances so warrant", i.e., where the individual has a vital interest in having access to the data, e.g., if it could have serious psychological harmful effects if the person is not informed that he or she is not registered with the Service, or in cases where unlawful processing of personal data has caused a person significant financial or non-financial damage[929].

---

[920] Section 2(3) Intelligence Services Committee Act. The Committee may furthermore ask the Minister for Justice and the Minister for Defence to arrange for the heads of the intelligence services to be present at a committee meeting to answer questions, see Section 2(4) Intelligence Services Committee Act.
[921] Section 2(5) Intelligence Services Committee Act.
[922] Section 4(1) Intelligence Services Committee Act. Based on Section 4(2) Intelligence Services Committee Act, it may furthermore report to the Danish Parliament on its activities, including on the matters under consideration by the Committee. The report may be made public.
[923] Section 6e Intelligence Services Committee Act.
[924] Section 12(2) and 13(2) and (3) ASIS.
[925] Section 13(1) ASIS.
[926] Section 13(2) ASIS.
[927] Section 13(3) ASIS.
[928] See the Board's annual report on the DSIS for 2021, p. 28.
[929] See proposal for legislative act LFS 161 of parliamentary session 2012/1, p 108-109: available at: https://www.retsinformation.dk/eli/ft/201212L00161.

Second, any individual can lodge a complaint about the actions of Danish national security authorities in the Faroe Islands, including the collection and use of personal data, before the Danish Parliamentary Ombudsman, who can make use of the powers described in the previous section.

Third, individuals can turn to the Independent Police Complaints Authority, which can make use of the powers described in the previous section to investigate and handle complaints concerning activities of Danish national security authorities[930].

Fourth, the same judicial avenues as the ones described in section 2.2.4 (e.g., invoking Section 72 of the Danish Constitution, claiming compensation for damages suffered because of the unlawful use of investigative measures under the Administration of Justice Act) are also available against the DSIS.

Finally, any individual may obtain judicial redress before the European Court of Human Rights against the unlawful collection of his/her data by the DSIS, provided that all available domestic remedies have been exhausted.

[930] In accordance with Section 1058(3) Administration of Justice Act, a complaint must be lodged within 6 months of the occurrence of the matter to which the complaint relates, although this time limit may be disregarded by the Authority in exceptional cases.

V. BAILIWICK OF GUERNSEY

1. RULES APPLYING TO THE PROCESSING OF PERSONAL DATA

1.1. Relevant developments in the data protection framework of Guernsey

On 21 November 2003 the European Commission adopted a decision in which the Bailiwick of Guernsey was considered as providing an adequate level of protection for personal data[931]. The Article 29 Working Party had adopted a positive opinion on the level of protection of personal data in Guernsey on 13 June 2003[932]. At the time, the legal framework for the protection of personal data was set out in the Data Protection (Bailiwick of Guernsey) Law 2001 (Data Protection Law 2001), which was closely aligned with the UK's Data Protection Act 1998. The latter had been enacted to give effect to the provisions of Directive 95/46/EC (Data Protection Directive)[933].

Since the adoption of the Commission's adequacy decision, Guernsey has significantly modernised its data protection framework, in particular by adopting the Data Protection (Bailiwick of Guernsey) Law 2017 (Data Protection Law). The Data Protection Law was intended to bring the Guernsey regime in line with Regulation (EU) 2016/679 (GDPR)[934]. It applies in full since 26 May 2019[935].

The Data Protection Law is complemented by several Ordinances and Regulations. The most important one is the Data Protection (Law Enforcement and Related Matters) (Bailiwick of Guernsey) Ordinance, 2018 (LEO), which regulates the processing of personal data by competent authorities for criminal law enforcement and national security purposes[936].

---

[931] Commission Decision 2003/821/EC of 21 November 2003 on the adequate protection of personal data in Guernsey, OJ L 308, 25.11.2003, p. 27-28.

[932] Opinion 5/2003 on the level of protection of personal data in Guernsey (WP79), available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp79_en.pdf

[933] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[934] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[935] While the Data Protection Law came into force on 25 May 2018, a one-year transition period was foreseen for certain obligations.

[936] In addition, the Data Protection (Commencement, Amendment and Transitional) (Bailiwick of Guernsey) Ordinance, 2018 (CAT Ordinance) introduced several modifications to the Data Protection Law and other ordinances. The Data Protection (Authorised Jurisdiction) (Bailiwick of Guernsey) Ordinance, 2019 was adopted to ensure the free flow of data between Guernsey and the UK during the Brexit transition period. Two further statutory instruments entered into force on 25 May 2018. First, the Data Protection (International Cooperation and Assistance) (Bailiwick of Guernsey) Regulations, 2018 provides the Data Protection Authority with additional functions in relation to international cooperation and mutual assistance. Second, the Data Protection (General Provisions) (Bailiwick of Guernsey) Regulations, 2018 regulates administrative matters such as the registration of controllers/processors, registration fees, payment of levies and contains certain rules regarding the transfer of personal data. The General Provision Regulation 2018 also introduces certain exemptions and amends existing exemptions under the Data Protection Law. The General Provisions Regulation 2018 has been amended five times after it was adopted: by the Data Protection (General Provisions) (Bailiwick of Guernsey) (Amendment) Regulations, 2019, the Data Protection (General Provisions) (Bailiwick of Guernsey) (Amendment No. 2) Regulations, 2019; the Data Protection (General Provisions) (Bailiwick of Guernsey) (Amendment) Regulations, 2020; the Data Protection (General Provisions) (Bailiwick of Guernsey) (Amendment No. 2) Regulations, 2019; and the Data Protection (General Provisions) (Bailiwick of Guernsey) (Amendment No. 3) Regulations, 2020.

With the adoption and full entry into force of the Data Protection Law and the abovementioned Ordinances and Regulations, the Guernsey data protection regime has been significantly strengthened. As set out in more detail below, the Data Protection Law mirrors the provisions of the GPDR with respect to all of its key aspects. In particular, in areas where the GDPR has enhanced the protection of personal data when compared to the protection offered by its predecessor, the Data Protection Directive, the Data Protection Law of Guernsey has been strengthened as well.

Like the Data Protection Law 2001, the new Data Protection Law has a broad scope of application, applying to both private operators and public authorities[937]. While the definitions of 'personal data', 'controller', 'processor', 'data subject' and 'processing'[938] (which are identical to those used in the GDPR) have not changed, the Data Protection Law has brought even more convergence with the GDPR, e.g., by introducing a definition of 'pseudonymisation'[939] and further clarifying when a person is "identifiable" by applying the same criteria of recital 26 of the GDPR[940]. Also the territorial scope of the Law has been extended to cover the processing of personal data by controllers or processors not established in Guernsey, subject to the same conditions that are set out in Article 3 of the GDPR[941]. This confirms the intention of the Guernsey legislator to strengthen the effectiveness of Guernsey's data protection regime.

The main data protection principles (i.e., the principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality) were already present in the Data Protection Law 2001 and are present also in the modernised Law[942]. Some of them have been further strengthened, e.g., the principle of lawfulness of processing, the transparency obligations, the security principle and the principle of accountability.

In particular, as regards the principle of lawfulness, the requirements for valid consent have been reinforced, by making clear that, in addition to being freely given, specific and informed, consent must be unambiguous and expressed by a clear affirmative action[943]. Similarly, the Data Protection Law has strengthened the existing transparency obligations by requiring that additional information is provided to the individual (e.g., the contact details of the data protection officer, the fact that the controller intends to transfer the data to a third country, the retention period, the right to withdraw consent, the existence of automated decision-making,

[937] The Guernsey data protection regime applies to the processing of personal data wholly or partly by automated means, or to processing other than by automated means, if the personal data forms or is intended to form part of a filing system, see Section 2(2) Data Protection Law. 'Processing' is defined in Section 111 (1) Data Protection Law as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means." This includes collection, recording, organisation, structuring or storage, adaptation or alteration, retrieval, consultation or use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, or restriction, and erasure or destruction of personal data.
[938] Section 111(1) Data Protection Law. 'Personal data' is defined as "any information relating to an identified or identifiable individual". In the context of the Law 'individual' means a living natural person. A 'controller' is a person, which, alone or jointly with others, determines the purposes and means of the processing of personal data. A 'processor' processes personal data on behalf of a controller.
[939] Section 111(1) Data Protection Law.
[940] Paragraph 1 of Schedule 9 to the Data Protection Law.
[941] Sections 2(3) and 3(b) Data Protection Law.
[942] Section 6 Data Protection Law.
[943] Section 10 Data Protection Law.

etc.) when data is collected directly from the individual[944] or from third parties[945] and when it is further processed[946].

With respect to the principle of data security, the Data Protection Law has introduced the obligation to notify data breaches[947], which was previously not present in the Guernsey regime. As also required by the GDPR, in case of a personal data breach, the controller must, as soon as practicable, and in any event, within 72 hours after becoming aware of the breach (unless the latter is not practicable), notify the personal data breach in writing to the Authority. If a personal data breach is likely to pose a high risk to the significant interests of a data subject, written notice must be provided also to the data subject.

In terms of accountability, the obligations have been fully aligned with the GDPR and requirements that were not present in the Data Protection Law 2001 have been introduced: The Data Protection Law contains the obligations to implement principles of data protection by design and by default[948], to keep records of processing[949], to designate a data protection officer[950], and to conduct impact assessments[951]. Like the GDPR, the Data Protection Law follows a risk-based approach, and the scope of the obligations is tailored to the risks for the rights and freedoms of natural persons.

In addition to the strengthening of data protection principles and obligations, the protections for special categories of personal data have been reinforced since the adoption of the adequacy decision. The Data Protection Law 2001 already offered additional protection for information about the racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, about membership in a trade union or other labour organisation, about physical or mental health and the commission or alleged commission of an offence[952]. The Data Protection Law extends this protection to biometric and genetic data[953]. As regards the safeguards that apply to the processing of special categories of data, the Data Protection Law allows the processing of special categories of data only in specific circumstances, and, in certain cases requires the processing to be accompanied by additional safeguards[954]. That was already the case under the Data Protection Law 2001[955].

---

[944] Section 12 and Schedule 3 of the Data Protection Law. Similar to Article 13(4) GDPR, this does not apply where and insofar as the data subject already has the information (see Section 12(5) of the Data Protection Law).
[945] Section 13 and Schedule 3 of the Data Protection Law. This obligation is subject to several exceptions, which are similar to the exceptions listed in Article 14(5) GDPR. Where an exception applies, the controller must take appropriate measures to protect individual rights, including by making the information publicly available (see Section 13(5) Data Protection Law).
[946] Section 13(2A) Data Protection Law.
[947] Section 42 Data Protection Law.
[948] Section 32 Data Protection Law.
[949] Section 37(1) Data Protection Law and Part III General Provisions Regulation 2018.
[950] Section 47 Data Protection Law.
[951] Section 44 Data Protection Law.
[952] Section 2 Data Protection Law 2001.
[953] Section 111(1) Data Protection Law.
[954] Part II and III of Schedule 2 to the Data Protection Law. For example, similarly to the GDPR, the Data Protection Law allows the processing of special categories of data where the data subject has given explicit consent, where processing is based on a law or where processing is necessary to protect the vital interest of the data subject.
[955] Schedule 3 to the Data Protection Law 2001.

In terms of rights, Part III of the Data Protection Law provides individuals with all of the key data protection rights, notably the right of access, rectification, and erasure[956], and it also provides for a right to restriction[957] and objection[958]. In addition, the Law provides for a right not to be subject to decisions based on automated processing[959].

Compared to the previous legislation, the Data Protection Law has strengthened the rights of individuals in several ways. The right of access not only requires controllers to provide individuals with information about the processing of their data (as was already the case under the Data Protection Law 2001[960]), but also to give access to personal data (including by providing a copy)[961]. Moreover, additional grounds to object to processing have been added[962]. For instance, individuals have a right to object to the processing of their personal data where such processing is based exclusively on grounds of public interest or on the legitimate interest of the controller[963]. In addition, the data subject no longer has to apply to a court to order the rectification and erasure of their personal data, as was required under the Data Protection Law 2001, but instead can make a request directly to the controller[964].

Importantly, new rights have been introduced in the Guernsey Data Protection Law. This includes a right for individuals not to be subject to a decision that is based solely on automated processing and affects the significant interests of the data subject.[965]. Such automated decision making may only take place under certain conditions (e.g., only where authorised by law or based on the data subject's explicit consent) and subject to specific safeguards (e.g., informing the individual about the processing, the logic involved and the envisaged consequences, allowing the data subject to obtain human intervention)[966]. In addition, the Data Protection Law introduced a right to data portability that corresponds to the same right available under the GDPR[967].

As is the case in the GDPR, the data subject rights are subject to certain restrictions intended to allow the balancing of the data protection interests of individuals with objectives of general public interest and with the fundamental rights and freedoms of others.

First, Part I of Schedule 8 allows the restriction of individual rights based on the nature of the personal data being processed. These restrictions apply automatically whenever one of the listed categories of personal data is being processed. The categories are listed in an exhaustive manner and cover a narrowly construed set of situations, such as the provision of references in confidence by the controller in the context of the education, employment or appointment of

[956] Section 21 Data Protection Law.
[957] Section 22 Data Protection Law.
[958] Sections 17 to 19 Data Protection Law. The Guernsey Data Protection Laws grants a right to object in three situations: where processing takes place in the public interest, for direct marketing purposes, and for historical or scientific purposes.
[959] Section 24 Data Protection Law.
[960] Section 7 Data Protection Law 2001.
[961] Section 15 Data Protection Law.
[962] Pursuant to Sections 10 and 11 Data Protection Law 2001, the data subject was entitled to request from the controller to cease or not to begin any processing that would be likely to cause unwarranted damage or distress to him or to another, and any processing for purposes of direct marketing.
[963] Section 18 Data Protection Law.
[964] Sections 20 and 21 Data Protection Law.
[965] Section 24(1) and (5) Data Protection Law.
[966] Section 24(2) and (3) Data Protection Law.
[967] Section 14 Data Protection Law.

the data subject, or personal data recorded by a candidate during an examination or marking. These categories are not only very limited in scope, but also do not typically cover situations where personal data is transferred to Guernsey from the EU.

Second, Part II of Schedule 8 sets out restrictions on grounds of prejudice. They can be invoked only when (and to the extent that) the application of the provisions "would be likely to prejudice" the legitimate aim pursued. For example, controllers can restrict data subject rights to the extent that their application would be likely to prejudice the combat effectiveness of the armed forces of the Crown[968], or would be likely to prejudice judicial independence or the conduct of judicial proceedings[969].

The Data Protection Authority of Guernsey has issued interpretative guidance that clearly frames the application of the exemptions. It clarifies the scope of the different exemptions, including by means of examples, which helps to prevent these exemptions being misunderstood and applied in an overly broad manner. It also explains how the requirements of necessity and proportionality should be applied with respect to a specific exemption[970].

With respect to international transfers of personal data, i.e., concerning the potential onward transfer of personal data that has been transferred from the EU, Guernsey has reorganised and clarified its transfer regime and put in place a system that is very similar to the rules on international transfers set out in Chapter V of the GDPR in terms of structure and requirements. Section 55 of the Data Protection Law lays down a prohibition on transferring data to unauthorised jurisdictions, except when specifically authorised by the Law. Authorised jurisdictions are Member States of the European Union, as well as any country or international organisation for which the European Commission has determined that it ensures an adequate level of protection within the meaning of Article 45(2) of the GDPR[971].

The Data Protection Law further clarifies that countries which have been found adequate by the European Commission are only considered as authorised jurisdictions as long as the

---

[968] Paragraph 6 of Part II of Schedule 8 to the Data Protection Law.

[969] Paragraph 11 of Part II of Schedule 8 to the Data Protection Law.

[970] The guidance is available at: https://www.odpa.gg/information-hub/organisations/exemptions/. First, it clarifies that "Exemptions should be applied narrowly to specific personal data in specific circumstances. There should be no 'blanket' application of exemptions. Consideration should be on a case-by-case basis taking into account the type of personal data, the purpose of the processing and any adverse impact of the application of the exemption on the data subject. […] Exemptions should be carefully considered, and their use fully justified. In accordance with the accountability requirements of the Law and the expectations of the Authority, all decisions to rely on an exemption should be documented and controllers should be prepared to share that documentation with the Authority." Second, the Data Protection Authority makes clear that controllers have to assess whether it is necessary and proportionate to invoke an exemption in relation to the specific data subject right and the specific set of personal data in question. Third, with respect to the prejudice test, the Data Protection Authority explains that in order to rely on the restriction "it is necessary to demonstrate that the purpose of processing that personal data would likely be prejudiced (e.g., to do so would have a damaging or detrimental effect on what is being done) if the designated provision was complied with". Moreover, the guidance confirms that the prejudice test is a high threshold, requiring a "very significant and weighty chance of prejudice".

[971] Pursuant to Section 111(1) Data Protection Law, an 'authorised jurisdiction' can also be a 'designated jurisdiction'. A 'designated jurisdiction' is defined in Section 111(1) Data Protection Law as the United Kingdom, a country within the United Kingdom, any Crown Dependency and any sector within the former categories, where designated by an Ordinance made by the Parliament of Guernsey. Such designation was made for the United Kingdom by The Data Protection (Authorised Jurisdiction) (Bailiwick of Guernsey) Ordinance, 2019 during the Brexit transition period. The Ordinance expired on 31 December 2021 pursuant to an amendment made by the Data Protection (Authorised Jurisdiction) (Bailiwick of Guernsey) (Amendment) Ordinance, 2020.

adequacy finding is still in force[972]. Guernsey has thus ensured an automatic alignment between the adequacy decisions of the EU and its own data transfer authorisations.

Sections 56, 57 and 59 of the Data Protection Law set out the conditions for transfers to unauthorised jurisdictions. Section 56 allows transfers if the controller or processor is satisfied of the existence of appropriate safeguards and of a mechanism for data subjects to enforce their rights and obtain effective legal remedies against the recipient. The instruments that can be used to provide such safeguards are similar to those provided in Article 46 of the GDPR: (1) a legally binding and enforceable agreement between public authorities, (2) binding corporate rules[973], (3) standard data protection clauses[974], (4) an approved code of conduct and (5) an approved certification mechanism[975].

Under the conditions laid down in Section 57, personal data can be transferred to unauthorised jurisdictions if authorised by the Data Protection Authority[976]. Section 57 explicitly requires the Authority to take into account any opinions or decisions of the European Data Protection Board in determining whether to authorise a transfer. In this area, Guernsey has thus ensured that beyond the alignment of the law itself, also the interpretation of the law remains in line with the interpretation within the EU.

Finally, transfers can take place on the basis of certain statutory grounds listed in Section 59(1) of the Data Protection Law[977]. These statutory grounds for transfers overlap to a large extent with the derogations for specific situations listed in Article 49 of the GDPR. Moreover, the Guernsey authorities have confirmed that a transfer under Section 59(1) would need to be justified on a case-by-case basis, i.e., each instance of transfer, and each piece of personal data transferred would need to fulfil the specific statutory conditions in the relevant provision of Section 59(1) in order for the transfer to be lawful. They have also confirmed that Section 59(1) of the Data Protection Law has to be interpreted in a manner equivalent to Article 49 of the GDPR to preclude systematic or repetitive transfers.

---

[972] See the definition of 'authorised jurisdiction' in Section 111(1) Data Protection Law. After the EU-U.S. Privacy Shield was invalidated by the Court of Justice of the European Union, the Guernsey Data Protection Authority alerted organisations in Guernsey that they could no longer rely on the Privacy Shield for their transfers of personal data. See press release of 24 July 2020, available at: https://www.odpa.gg/news/news-article/?id=feff8843-a322-eb11-a813-000d3a2012fa.

[973] These can be approved by the Guernsey Data Protection Authority or by one of the authorities in the EU on the basis of Article 47 GDPR. So far, the Guernsey Authority has not approved any binding corporate rules.

[974] Pursuant to Section 111(1) Data Protection Law, standard data protection clauses are those adopted by the Commission on the basis of the GDPR or the Data Protection Directive, or those approved by the Guernsey Data Protection Authority. The latter has not yet approved any such clauses.

[975] An approved code of conduct or an approved certification mechanisms have to be each combined with binding and enforceable commitments of the recipient to apply the relevant safeguards in the mechanism, including as regards data subject rights.

[976] An authorisation can be granted if the safeguards listed in Section 56(2) Data Protection Law are in place or if safeguards are ensured by contractual clauses, and there is a mechanism in place for data subjects to enforce their data subject rights and obtain effective legal remedies against the recipient, see Section 57(2)(a) and (b) Data Protection Law.

[977] Pursuant to Section 59(1) Data Protection Law, personal data may be transferred to an unauthorised jurisdiction for instance where required by an order or a judgment of a court or tribunal having the force of law in Guernsey, where required by a decision of a Guernsey public authority based on an international agreement imposing an international obligation on Guernsey, where explicit consent of the individual has been obtained, where necessary for the performance of a contract with or in the interest of a data subject, or where necessary to protect the vital interests of the data subject or of another individual and the data subject is incapable of giving consent or the controller cannot reasonably be expected to obtain the explicit consent of the data subject.

1.2. Oversight, enforcement and redress

Guernsey has also reformed its system of oversight and enforcement of the Data Protection Law. Oversight and enforcement are carried out by the Data Protection Authority (the Authority), which replaces the Commissioner under the Data Protection Law 2001[978]. The Authority is composed of a chairman, four to eight other voting members (the Members), and a commissioner (an ex officio and non-voting member)[979]. Compared to the previous Commissioner, the independence of the Authority has been significantly strengthened in several ways.

First, the independence of the Authority is explicitly provided by Section 62 of the Data Protection Law, which requires it to act independently, free from direct or indirect external influence and without seeking or taking instructions from any person. Second, the Authority now enjoys a status of a legal person separate from its members[980]. Third, the Law lays down specific requirements for the appointment and dismissal of the Members and the Commissioner. The Members are appointed by resolution of the Parliament of Guernsey among individuals nominated by a Parliamentary Committee[981]. The Commissioner, which is the chief executive of the Authority, is appointed by the Authority itself[982]. They must have the qualifications, experience and skills necessary to exercise and perform their functions, in particular in the area of data protection. In addition, the Members must have a strong sense of integrity and must be able to maintain confidentiality[983].

Members can only be removed from office by a resolution of the Parliament of Guernsey, on the basis of a report and recommendation from the Parliamentary Committee, on the basis that the specific conditions for dismissal as set out in the Law are met[984]. The conditions for the dismissal of the Commissioner by the Authority are equally set out in the Law[985]. The

[978] Parts XI and XII Data Protection Law. The general functions of the Authority include oversight and enforcement of the Data Protection Law, promoting awareness (among the public, controllers and processors), as well as issuing opinions, guidance and public statements. In addition, the Authority may engage in international co-operation, including by developing international cooperation mechanisms and providing international mutual assistance. See Sections 61 to 65 Data Protection Law.

[979] Schedule 6, Paragraph 1 Data Protection Law. At present, the Authority is composed of a chairperson and six voting members.

[980] Section 60(1) Data Protection Law. This means that the Authority can directly employ staff, where in the past it relied on the government to do so and could only employ civil servants, and that it can separate its banking arrangements and internal audits from the government. See also Annual Report 2018 of the Office of the Data Protection Authority, p. 13.

[981] The Committee is the States of Guernsey Committee for Home Affairs, which is a committee of the States of Guernsey. It consists of a President and four members who are members of the Parliament and up to two non-voting members appointed by the Committee who are not to be members of the Parliament.

[982] Schedule 6, Paragraph 5 Data Protection Law.

[983] Schedule 6, Paragraph 1(3) Data Protection Law. The Code of Practice for Members of the Guernsey Data Protection Authority sets out ethical values and further rules on standard of conduct of the Members of the Authority.

[984] Members can only be dismissed on grounds of serious misconduct, conviction of a criminal offence, bankruptcy, incapacity because of physical or mental illness, other inability to perform their duties, or ineligibility, see Paragraph 2(1) of Schedule 6 to the Data Protection Law. The Committee can only recommend dismissal based on a serious misconduct if a panel consisting of three or more individuals (none of whom is a member of the Parliament of Guernsey, the Committee or the Authority) appointed by the Committee determines the Member to be guilty of a serious misconduct. Paragraph 2(2) of Schedule 6 to the Data Protection Law.

[985] Paragraph 5(6) of Schedule 6 to the Data Protection Law. The Commissioner can only be removed on grounds of serious misconduct, conviction of a criminal offence, bankruptcy, physical or mental illness, or if otherwise unable or unfit to perform the Commissioner's duties.

Commissioner may not engage in any other employment, occupation or business, or receive any benefits other than the salary, allowances and other expenses awarded by the Authority, except with the approval of the Authority[986].

The Data Protection Law has also equipped the Authority with additional investigatory and enforcement powers that are very similar to those foreseen in the GDPR. In particular, the Authority can conduct audits[987], investigate individual complaints[988] and carry out general inquiries on its own initiative[989]. In carrying out its functions, the Authority has access to all relevant information[990]. Upon finding of a violation of the Data Protection Law, the authority can impose various sanctions, ranging from warnings and reprimands to binding orders (for instance to discontinue processing, bring processing into compliance with the Law, rectify, erase or restrict processing or suspend the transfer of personal data)[991].

Moreover, the Authority can impose administrative fines for certain violations of the Law[992]. The fines must be effective, proportionate and have a deterrent effect[993]. As regards the amount of fines, the Authority has to take into account the same factors as those listed in Article 83(2) GDPR, i.e., the intentional or negligent character of the infringement, any action taken by the controller or processor to mitigate the damage suffered by data subjects, duration of the infringement etc.[994]. In addition, several violations of the Data Protection Law continue to constitute offences and may therefore be subject to criminal sanctions[995].

As regards possibilities for individuals to obtain redress, the Guernsey system continues to offer various avenues, including the possibility to lodge a complaint with the Authority[996], to obtain judicial redress directly against controllers and processors (both private operators and

[986] Paragraph 5(8) of Schedule 6 to the Data Protection Law.
[987] Paragraph 9 of Schedule 7 to the Data Protection Law.
[988] Sections 67 and 68 Data Protection Law.
[989] Section 69 Data Protection Law.
[990] Paragraph 1 of Schedule 7 Data Protection Law.
[991] Sections 71 to 73 Data Protection Law. Failure to comply with an order from the Authority is an offence under the Law.
[992] Section 74 Data Protection Law: these violations are (1) failure to verify the validity of consent of a child under 13 years of age under section 10(2)(f), (2) failure to inform the data subject of anonymisation, in breach of section 11(1)(b), (3) breach of any duty imposed on the person concerned by any provision of Part IV (except section 31), V, VI, VII (except section 46) or VIII (duties of controllers and processors, administrative duties, security of personal data, data protection impact assessments and prior consultation, data protection officers) (4) breach of the duty imposed on an accredited monitoring body by section 53(2), (5) breach of any duty imposed on the person concerned by section 6(1) on accountability, including a breach of the data protection principle relating to lawfulness of processing, (6) breach of any duty imposed on the person concerned under Part III, (fa) failure to comply with an order of the Authority under section 73(2), (7) transfer of personal data to a person in an unauthorised jurisdiction in breach of section 55, or (h) breach of any provision of any Ordinance or regulations made under the Law imposing a duty on a controller or processor). For example, in 2020, the Authority imposed two fines, one of £80 000 and one of £10 000. More information is available at: https://www.odpa.gg/actions-weve-taken/.
[993] Section 74(3) Data Protection Law.
[994] Section 74(2) Data Protection Law.
[995] This for example applies to obtaining personal data or disclosing personal data to another person without consent of the controller (or selling that personal data), obstructing the Authority, failing to comply with an order of the Authority, providing false, deceptive or misleading information to the Authority , and impersonating an Authority official, Sections 87 to 89 Data Protection Law.
[996] Section 67 Data Protection Law.

public authorities)[997] and obtain compensation for damages[998]. In addition, individuals can obtain judicial redress against decisions of the Authority[999].

Despite its relatively small size, the Authority plays an active role, both when it comes to its engagement with stakeholders and exercising its oversight role. The Authority handles a number of files, including inspections, notifications, written questions and complaints each year. For example, between 25 May and 31 December 2018, the Authority handled 34 complaints and conducted 30 investigations[1000]. In 2019, the Authority handled 67 complaints and conducted 50 investigations, which led to a breach determination in 8 cases and reprimands being imposed in 6 cases. Moreover, the Authority held 11 public events and organised sessions for organisations every two weeks, in which it provided information and advice[1001]. In 2020, the Authority issued seven reprimands, one warning, two fines and one order and again dealt with a number of complaints and investigations[1002]. The Authority also engages in various outreach activities on an ongoing basis, such as presentations for both the private and public sector, for instance on data protection for start-ups and small businesses, on individual rights or on how to respond to data subject access requests[1003].

2. ACCESS TO AND USE OF PERSONAL DATA TRANSFERRED FROM THE EUROPEAN UNION BY PUBLIC AUTHORITIES IN GUERNSEY

2.1. General legal framework

The limitations and safeguards that apply to the collection and subsequent use of personal data for purposes of criminal law enforcement and national security follow from Guernsey's international obligations in the area of fundamental rights and personal data protection, from the rules that apply to the processing of personal data by the public sector, as well as from specific laws regulating access to data by Guernsey public authorities.

First, as an exercise of power by a public authority, government access in Guernsey must be conducted in full respect of the law. The ratification of the European Convention of Human Rights by the United Kingdom has been extended to Guernsey since 1953[1004]. The right to respect for private and family life (and the right to data protection as part of that right) is protected by the Human Rights (Bailiwick of Guernsey) Law 2000, which incorporates the European Convention on Human Rights into Guernsey law[1005]. Article 8 of the Convention provides that any interference with privacy must be in accordance with the law, in the interests of one of the aims set out in Article 8(2) and proportionate in light of that aim.

[997] Section 79 Data Protection Law.
[998] Section 79(3) Data Protection Law.
[999] Sections 82 and 83 Data Protection Law.
[1000] See Annual report May-Dec 2018, available at: https://www.odpa.gg/about/our-governance/annual-reports/.
[1001] See Annual report 2019, available at: https://www.odpa.gg/about/our-governance/annual-reports/.
[1002] See Annual report 2020, available at: https://www.odpa.gg/about/our-governance/annual-reports/. More details on the Authority's enforcement action, including on actions taken in 2021, are provided on the Authority's website, available at: https://www.odpa.gg/actions-weve-taken/.
[1003] For recent courses and presentations, see for example the events set out on the website of the Authority, available at: https://www.odpa.gg/events/.
[1004] See Declaration contained in a letter from the United Kingdom's Permanent Representative to the Council of Europe, dated 23 October 1953, registered at the Secretariat General on 23 October 1953 – available at: https://www.coe.int/en/web/conventions/full-list2?module=declarations-by-treaty&numSte=005&codeNature=0.
[1005] Section 1(1) and (2) Human Rights (Bailiwick of Guernsey) Law 2000.

Article 8 also requires that the interference is "foreseeable", i.e., have a clear, accessible basis in law, and that the law contains appropriate safeguards to prevent abuse.

In addition, in its case law[1006], the European Court of Human Rights has specified that any interference with the right to privacy and data protection should be subject to an effective, independent and impartial oversight system that must be provided for either by a judge or by another independent body[1007] (e.g., an administrative authority or a parliamentary body).

Moreover, individuals must be provided with an effective remedy, and the European Court of Human Rights has clarified that the remedy must be offered by an independent and impartial body which has adopted its own rules of procedure, consisting of members that must hold or have held high judicial office or be experienced lawyers, and that there must be no evidential burden to be overcome in order to lodge an application with it. In undertaking its examination of complaints by individuals, the independent and impartial body should have access to all relevant information, including closed materials. Finally, it should have the powers to remedy non-compliance[1008].

Second, the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) also applies in Guernsey[1009]. Article 9 of Convention 108 provides that derogations from the general data protection principles, the rules governing special categories of data and data subject rights are only permissible when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences, or for protecting the data subject or the rights and freedoms of others.

Therefore, through adherence to the European Convention of Human Rights and to Convention 108, Guernsey is subject to a number of obligations, enshrined in international law and that frame its system of government access on the basis of principles, safeguards and individual rights similar to those guaranteed under EU law and applicable to the Member States. Furthermore, as far as the ECHR is concerned, compliance with these obligations is subject to the judicial control of the European Court of Human Rights.

Third, the Guernsey Parliament has adopted specific provisions for the processing of personal data for law enforcement purposes, i.e., the Data Protection (Law Enforcement and Related Matters) (Bailiwick of Guernsey) Ordinance, 2018 (LEO). The material scope of the LEO is similar to the one of the Law Enforcement Directive. It applies to the processing of personal data by competent authorities[1010] for the purposes of the prevention, investigation, detection

[1006] According to Section 2(1)(a) Human Rights (Bailiwick of Guernsey) Law 2000, a court or tribunal in Guernsey that is determining a question which has arisen in connection with a Convention right must take into account any judgment, decision, declaration or advisory opinion of the European Court of Human Rights.
[1007] European Court of Human Rights, Klass and others v. Germany, Application no. 5029/71, paragraphs 17-51.
[1008] European Court of Human Rights, Kennedy v. the United Kingdom, Application no. 26839/05, (Kennedy), paragraphs 167 and 190.
[1009] Declaration contained in a letter from the Permanent Representative of the United Kingdom to the Council of Europe, dated 26 August 1987, handed to the Secretary General at the time of deposit of the instrument of ratification, on 26 August 1987, available at: https://www.coe.int/en/web/conventions/full-list?module=declarations-by-treaty&numSte=108&codeNature=0.
[1010] Competent authorities in Guernsey are listed in Section 50(a) LEO and include the States (i.e. the executive governments of the islands of Guernsey, Alderney and Sark, see also Section 111(1) Data Protection Law), a

or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security or national security, as well as for exercising or performing any power or duty conferred or imposed on a public authority by a criminal proceeds enactment[1011].

Furthermore, the data protection principles of lawfulness and fairness[1012], purpose limitation[1013], data minimisation[1014], accuracy[1015], storage limitation[1016] and security[1017] are retained in the LEO in similar terms as in the Law Enforcement Directive. In essence, the processing of personal data by a competent authority for a law enforcement purpose is permitted only if and to the extent that it is carried out in the context of a function imposed by law and the data subject has given consent, the processing is necessary for the performance of a task carried out by the authority, or an enactment authorises or requires such processing[1018]. In addition, the LEO imposes specific transparency obligations[1019] and recognises the same

---

public committee, a holder of public office, a statutory body, a court or tribunal of Guernsey, any person hearing or determining an appeal, or conducting a public inquiry, under any enactment, the salaried police force of the Island of Guernsey, a parish Douzaine, and any person exercising powers similar to the aforementioned persons in any country other than Guernsey. Competent authorities are also any other person who exercises a function of public nature for a criminal law enforcement purpose, in respect of Guernsey or any other country, and any other prescribed person. The abovementioned authorities are considered as competent authorities under the LEO only when exercising or performing a function conferred or imposed on the person by law or by a States Resolution for a law enforcement purpose.

[1011] Sections 50 LEO and 111(1) of the Data Protection Law. The criminal proceeds enactments, which are listed in the LEO, authorise and govern the tracing, freezing, seizure and forfeiture of the proceeds of crime. The personnel involved in these processes and procedures are usually criminal law enforcement officers. However, in Guernsey these processes and procedures are carried out by way of civil procedures and proceedings.

[1012] Section 5 LEO. The processing of personal data by a competent authority for a law enforcement purpose is permitted only if and to the extent that it is carried out in the context of a function imposed by law and (1) the data subject has given consent, (2) the processing is necessary for the performance of a task carried out by the authority, or (3) an enactment authorises or requires such processing.

[1013] Section 6 LEO. Section 6(2) LEO allows for secondary processing of data for law enforcement purposes only if the consent of the data subject has been obtained, if it is for a historical or scientific purpose (related to the secondary law enforcement purpose), or the secondary processing is carried out in the context of a controller discharging a function imposed by law. In any case, such secondary processing must be necessary and proportionate to the secondary law enforcement purpose.

[1014] Section 7 LEO

[1015] Section 8 LEO. In addition, as required also by the LED, competent authorities must make a clear distinction between personal data relating to different categories of data subjects, such as persons suspected of having committed an offence, persons convicted of a criminal offence, persons who are victims of a criminal offence and witnesses.

[1016] Section 9 LEO.

[1017] See Section 10, as well as Sections 32 and 33 LEO. Section 3 LEO furthermore lists the provisions of the Guernsey Data Protection Law that apply to personal data processed for criminal law enforcement purposes. These are the provisions on the territorial and material scope, household exemptions, the nature of consent (except in the case of criminal data), rules regarding anonymised data (except the notification requirement), the duties of controllers and processors to keep records, make returns and cooperate with the Authority, all the provisions on the Authority and civil and criminal proceedings.

[1018] Section 5 of the LEO. Pursuant to Schedule 2 LEO, stricter conditions apply to the processing of special category data. The processing of such data is lawful when the data subject has given consent and the controller has put in place appropriate safeguards for the significant interests of the data subject. Alternatively, the processing is lawful where the processing is strictly necessary for the criminal law enforcement purpose, appropriate safeguards are in place and at least one condition specified in Schedule 2 (e.g., the information was made public by the data subject; processing is necessary in order to comply with an order or a judgment of a court; legal proceedings; processing is necessary for the discharge of any functions of a court or tribunal acting in its judicial capacity; obtaining legal advice; etc.) is fulfilled.

[1019] Section 12 LEO requires that data subjects are provided with information on the identity and contact details of the controller/controller's representative and the data protection officer, the purposes for processing, data subject rights, the complaints mechanism and the possibility of requesting the Authority to bring civil

data subject rights as the LED[1020]. In particular, individuals enjoy a right of access[1021], correction[1022] and deletion[1023] and have the right not to be subject to automated decision-making[1024]. Competent authorities are also required to implement data protection by design and default[1025], to keep records of processing activities[1026], and, in certain situations, to conduct data protection impact assessments and to pre-consult the Data Protection Authority[1027]. Moreover, they are required to put in place appropriate measures to ensure security of processing[1028] and are subject to specific obligations in case of a data breach, including notification of such breaches to the Authority and data subjects[1029]. Like in the Law Enforcement Directive, there is also a requirement for a controller (unless it is a court or other judicial authority acting in a judicial capacity) to designate a data protection officer who assists the controller in complying with its obligations as well as monitoring that compliance[1030]. Finally, the LEO contains specific provisions on international transfers of personal data[1031]. The provisions substantially echo those in the Law Enforcement Directive. Essentially, transfers to "unauthorised jurisdictions"[1032] are prohibited unless they are necessary for a law enforcement purpose and based on appropriate safeguards[1033]. In the absence of appropriate safeguards, transfers to unauthorised jurisdictions are only possible in

---

proceedings before a court. The controller has two options: (1) publish the information, or (2) give the information directly to (i.e., notify) the data subject. Moreover, when reasonable in a specific case in order to enable a data subject to exercise his or her rights, the controller Is obliged to provide further information, including on the legal basis for processing, the expected storage period for the data (or the criteria to determine the same), categories of recipients and any other Information necessary to enable the data subject to exercise the data subject rights.

[1020] Similarly to Article 12 LED, Section 23 LEO further specifies the modalities for exercising these rights, allowing competent authorities to refuse to comply with a request from an individual or to charge a reasonable fee for complying with the request if the request is manifestly unfounded, frivolous, vexatious, unnecessarily repetitive or otherwise excessive. Moreover, pursuant to Section 19 LEO, the rights of access, correction and deletion do not apply to the processing of judicial data in the course of a criminal investigation. Judicial data refers to personal data contained in a judicial decision or in other documents, relating to the crime-related investigation or (as the case may be) the proceedings relating to a criminal offence within or outside the Bailiwick, which are created by or on behalf of a court or other judicial authority.

[1021] Section 13 LEO. In addition, Section 13 provides individuals with a right to obtain a confirmation as to whether or not personal data relating to the individual is being processed, as well as to access that data and obtain information relating to its processing (e.g., on the purpose, categories of personal data concerned, the source of the personal data, the recipients, etc.).

[1022] Section 14 LEO.

[1023] Section 15 LEO.

[1024] Section 17 LEO.

[1025] Section 27 LEO.

[1026] Section 3(1)(d) LEO and Section 37 Data Protection Law.

[1027] Sections 37 and 38 LEO.

[1028] Sections 32 and 33 LEO.

[1029] Sections 34 and 35 LEO.

[1030] Section 39 to 42 LEO.

[1031] Sections 43 to 47 LEO.

[1032] Pursuant to Section 50(1) LEO, authorised jurisdictions are Guernsey, the EU Member States, any country or any international organisation that the Commission has determined ensures an adequate level of protection within the meaning of Article 36 LED and any designated jurisdiction. Such designation was made for the United Kingdom by The Data Protection (Authorised Jurisdiction) (Bailiwick of Guernsey) Ordinance, 2019 during the Brexit transition period. The Ordinance expired on 31 December 2020.

[1033] Section 43(1) in conjunction with Section 44 LEO. Appropriate safeguards are in place where provided by a legal instrument binding the intended recipient, such as a legally binding and enforceable agreement between the controller and the recipient, or where the controller, having assessed all the circumstances surrounding the transfer, concludes that appropriate safeguards exist to protect the data. The controller is required to keep detailed written records of any transfer relying on appropriate safeguards, and when relying on appropriate safeguards on the basis of the circumstances surrounding the transfer, the controller must notify the Authority of the categories of data transferred on that basis.

specific circumstances that are listed in the law in an exhaustive manner and correspond to the 'derogations' set forth in the Law Enforcement Directive[1034].

Under similar conditions as under the Law Enforcement Directive, Section 24 of the LEO specifies that certain specific provisions of the LEO[1035] may be restricted to the extent that and as long as, having regard to the significant interests of the data subject, the restriction is a necessary and proportionate measure for one of the purposes listed in the law[1036].

Moreover, Schedule 3 to the LEO imposes the same restrictions (where relevant in the context of the LEO) to specific provisions[1037] of the LEO as the ones provided by the Data Protection Law[1038]. First, Schedule 3 allows the restriction of individual rights based on the nature of the personal data being processed. These restrictions apply automatically whenever one of the listed categories of personal data is being processed. These categories are listed in an exhaustive manner and cover a very limited, narrowly construed set of situations. In addition, they do not typically cover situations where personal data is transferred to Guernsey from the EU[1039]. Second, Schedule 3 sets out restrictions on grounds of prejudice. They can be invoked only when and to the extent that the application of the provisions "would be likely to prejudice" the legitimate aim pursued. For example, controllers can restrict data subject rights to the extent that their application would be likely to prejudice the combat effectiveness of the armed forces of the Crown[1040], or would be likely to prejudice judicial independence or the conduct of judicial proceedings[1041]. As explained in section 1.1., the Data Protection Authority of Guernsey has issued interpretative guidance that clearly frames the application of the restrictions. It clarifies the scope of the different restrictions, including by means of examples, which helps to prevent them being misunderstood and applied in an overly broad

[1034] Section 45 LEO sets out the special circumstances in which international transfers can take place in the absence of appropriate safeguards, i.e. for the protection of vital interests of individuals, to safeguard legitimate interests of the data subject, to prevent immediate and serious threats to the public or national security of any country, in individual cases for a law enforcement purpose, and in individual cases in the context of legal proceedings and legal advice relating to a law enforcement purpose.

[1035] The provisions that may be restricted are those that concern the provision of information to the data subject, i.e., the transparency obligations and the data subject's right to access.

[1036] Pursuant to Section 19 LEO, these purposes are to avoid obstructing official or legal inquiries, investigations or procedures; to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties; to protect public security; to protect national security; or to protect the significant interests of others. In case of restriction, the controller must provide the data subject as soon as practicable with a statement informing about the restriction, along with the reasons and the possible redress avenue.

[1037] Most of the restrictions allow the restriction of provisions in Part III LEO, i.e., the data subject rights, as well as of the data protection principles that correspond to these rights. The exemption on public security in paragraph 18 of Schedule 3 allows the restriction of Parts II to VIII LEO, i.e., of the provisions on the data protection duties and principles, the data subject rights, the duties of controllers and processors, the security of personal data, data protection impact assessments and prior consultation, data protection officers and on transfers to other jurisdictions.

[1038] Only those exemptions provided by the Data Protection Law that are not relevant in the context of the LEO have not been included in Schedule 3, such as confidential references given by the controller, judicial and crown appointments, examination and marking data, management forecasting or planning, financial service data, trusts exemption and exemption on journalism, art, literature and academia.

[1039] The exemptions apply automatically to privileged items and to personal data withheld by a court or tribunal, see paragraphs 3 and 15 of Schedule 3 to the LEO.

[1040] Paragraph 4 of Schedule 3 to LEO.

[1041] Paragraph 7 of Schedule 3to the LEO.

manner. It also explains how the requirements of necessity and proportionality should be applied with respect to specific restrictions[1042].

The processing of personal data for national security purposes in Guernsey is either subject to the provisions of the Data Protection Law described in Section 1.1., or to the provisions of LEO as described above. As explained above, the LEO applies to the processing of personal data by a competent authority, including for the purpose of safeguarding against or preventing threats to national security. The Data Protection Law applies if the processing of personal data for national security purposes is not conducted by a competent authority. While both the LEO[1043] and the Data Protection Law[1044] provide for an exemption from specified provisions for national security purposes, these provisions may only be restricted to the extent that their application would be likely to prejudice national security. In addition, the application of these exemptions has been clarified through detailed guidance. As recalled above for restrictions applicable in the field of criminal law enforcement, in particular, relying on the exemption must be necessary and proportionate in a democratic society. The exemption cannot be invoked in a blanket manner but can be relied upon only the basis of a case-by-case analysis and considering the actual consequences of applying the relevant provision. Controllers must be able to show that there is a real possibility of an adverse effect on national security if the relevant provision is applied. All decisions to rely on an exemption have to be documented and controllers must be prepared to share that documentation with the Data Protection Authority[1045].

Moreover, according to paragraph 18(2) of Schedule 3 to the LEO and paragraph 18(2) of Schedule 8 to the Data Protection Law, a certificate signed by Her Majesty's Procureur can confirm the legality of the reliance on the restriction[1046]. That means that the certificate serves as conclusive evidence of the fact that a restriction from one or more provision specified in the certificate is required for the purposes of national security. It is important to note that the

[1042] The guidance specifically refers to the restrictions set out in the Data Protection Law. As these overlap with the exemptions provided by the LEO (see footnote 35), the guidance applies in the same manner to the interpretation of the restrictions in the LEO. The guidance is available at: https://www.odpa.gg/information-hub/organisations/exemptions/. First, it clarifies that "Exemptions should be applied narrowly to specific personal data in specific circumstances. There should be no 'blanket' application of exemptions. Consideration should be on a case-by-case basis taking into account the type of personal data, the purpose of the processing and any adverse impact of the application of the exemption on the data subject. […] Exemptions should be carefully considered, and their use fully justified. In accordance with the accountability requirements of the Law and the expectations of the Authority, all decisions to rely on an exemption should be documented and controllers should be prepared to share that documentation with the Authority." Second, the Data Protection Authority makes clear that controllers have to assess whether it is necessary and proportionate to invoke a restriction in relation to the specific data subject right and the specific set of personal data in question. Third, with respect to the prejudice test, the Data Protection Authority explains that in order to rely on the restriction "it is necessary to demonstrate that the purpose of processing that personal data would likely be prejudiced (e.g., to do so would have a damaging or detrimental effect on what is being done) if the designated provision was complied with". Moreover, the guidance confirms that the prejudice test is a high threshold, requiring a "very significant and weighty chance of prejudice".

[1043] Pursuant to Paragraph 18 of Schedule 3 LEO, the application of the provisions in Parts II to VIII may be restricted, provided that the applicable conditions are fulfilled.

[1044] Pursuant to paragraph 18 of Schedule 8 Data Protection Law, the application of the provisions in Parts II to XII and XV may be restricted, provided that the applicable conditions are fulfilled.

[1045] See the Guernsey Data Protection Authority's guidance on exemptions, available at: https://www.odpa.gg/information-hub/guidance/exemptions/.

[1046] To date, no such certificate has been issued under Guernsey current data protection framework, nor under its predecessor, the Data Protection (Bailiwick of Guernsey) Law, 2001.

national security certificate does not provide for an additional ground for restricting data protection rights and obligations for national security reasons. In other words, the controller or processor can only rely on a certificate when it has concluded that it is necessary to rely on the national security restriction which, as explained above, must be applied on a case-by-case basis[1047]. Even if a national security certificate applies to the matter in question, the Guernsey Data Protection Authority can investigate whether or not reliance on the national security restriction was justified in a specific case[1048]. Moreover, any person directly affected by the issuing of a certificate may appeal to the Royal Court. The Royal Court will review the decision to issue a certificate and decide whether there were reasonable grounds for issuing it. The Court can consider a wide range of issues, including necessity, proportionality and lawfulness, having regard to the impact on the rights of data subjects and balancing the need to safeguard national security. As a result, the Court can quash the certificate or determine that the certificate does not apply to specific personal data which is the subject of the appeal[1049].

It follows from the above that limitations and conditions are in place under the applicable Guernsey legal provisions, as interpreted by the Guernsey Data Protection Authority, to ensure that these exemptions and restrictions remain within the boundaries of what is necessary and proportionate to protect criminal law enforcement and national security.

2.2. Access and use by Guernsey public authorities for criminal law enforcement purposes

In Guernsey, criminal law enforcement functions are carried out by the Island Police Force, which is headed by the Chief Officer. Guernsey law imposes a number of limitations on how the Police Force has access to and uses personal data for criminal law enforcement purposes, and it also provides oversight and redress mechanisms in this area. The conditions under which access to personal data can take place and the safeguards applicable to the use of these powers are assessed in the following sections.

2.2.1. Legal bases and applicable limitations/safeguards

Personal data transferred under the adequacy decision and processed by organisations in Guernsey may be obtained by Guernsey criminal law enforcement authorities by means of investigative measures under the Police Procedures and Criminal Evidence (Bailiwick of Guernsey) Law 2003 (PPCE), on the basis of the Regulation of Investigatory Powers (Bailiwick of Guernsey) Law 2003 (RIPL), or on the basis of anti-money laundering legislation[1050].

[1047] See the Guernsey Data Protection Authority's guidance on exemptions, available at: https://www.odpa.gg/information-hub/organisations/exemptions/.

[1048] Section 4(2) LEO and Section 6(2)(g) Data Protection Law require the controller to be in a position to demonstrate that it has complied with the law. This implies that an intelligence service would need to demonstrate to the Data Protection Authority that when relying on the restriction, it has considered the specific circumstances of the case.

[1049] Paragraph 18(4) to (11) Data Protection Law and paragraph 18(4) to (11) Data Protection Law.

[1050] In addition, under Guernsey law, UK authorities can lawfully operate in Guernsey to access personal data for criminal law enforcement purposes where these operations are not prohibited by Guernsey law, or the operations are specifically authorised by legislation in force in Guernsey. For the powers that can be exercised in Guernsey by UK authorities, see the Commission Implementing Decision of 28.6.2021 pursuant to Regulation (EU)

The PPCE provides the Guernsey police with a legal basis for accessing personal data held by commercial operators through searches and seizures. The PPCE lays down detailed rules on the scope and application of these measures, aimed at ensuring that the interference with the rights of individuals will be limited to what is necessary for a specific criminal investigation and proportionate to the pursued purpose. Searches and seizures may only take place on the basis of a court-issued search warrant[1051] and the issuing of such warrant is subject to specific procedural and substantive requirements.

More specifically, a police officer may apply for a search warrant to the Bailiff[1052] or an appropriate judicial officer in Alderney or Sark[1053]. An application for a warrant must set out the grounds for the application, the premises to be searched and, as far as practicable, the articles or persons to be sought[1054].

A search warrant may be issued only if the Bailiff/judicial officer is satisfied that there are reasonable grounds[1055] to believe that (1) a serious arrestable offence[1056] has been committed; (2) there is material which is likely to be of substantial value to the investigation of the offence; (3) the material is likely to be relevant evidence; and (4) it does not consist of or include items that are subject to legal professional privilege or otherwise excluded[1057].

In terms of formal requirements, the warrant must specify the identity of the person who applied for it, the date of issuance, the enactment under which it is issued, the premise to be searched and, in as far as practicable, the articles or persons to be sought[1058]. The police

---

2016/679 on the adequate protection of personal data by the United Kingdom, available at: https://commission.europa.eu/system/files/2021-06/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_en.pdf.

[1051] Pursuant to Sections 12 and 13 PPCE, warrantless searches may only take place in exceptional circumstances that do not appear relevant in the context of data transfers covered by an adequacy decision adopted under the GDPR. In particular, a police officer may search a premise for the purpose of (1) executing a warrant of arrest; (2) arresting a person for an arrestable offence; (3) recapturing any person whomsoever who is unlawfully at large and whom he is pursuing; or (4) saving life or limb or preventing serious damage to property. In addition, a warrantless search may take place on a premise occupied or controller by a person under arrest, if the police have reasonable grounds to suspect that there is evidence on the premise that relates to that offence, or a connected/similar offence.

[1052] The Bailiff is the most senior judge of Guernsey's Royal Court and is also the President of the Court of Appeal.

[1053] In Alderney the appropriate judicial officer is the Chairman of the Court of Alderney or, if he is absent or unable to act, a Jurat of the Court of Alderney authorised by him to act in that capacity on his behalf. In Sark the appropriate judicial officer is the Seneschal of Sark or, if he is absent or unable to act, his deputy.

[1054] Section 10(2) PPCE.

[1055] The test of 'reasonable grounds to believe' for the exercise of a power contains both a subjective and objective element. First, the officer making the application needs to genuinely believe that a serious arrestable offence has been committed, and second, there must be an objective basis for that belief. It sets a higher standard to satisfy than 'reasonable suspicion', which is the basis for a police officer's arrest of a suspect, see Blackstones Criminal Practice (2019 edition) D1.4.

[1056] Section 90 and Schedule 4 PPCE set out which offenses qualify as 'serious arrestable offence', covering for instance treason, murder, manslaughter, rape, kidnapping etc.

[1057] In addition, one of the following conditions must be met: (1) it is not practicable to communicate with any person entitled to grant entry to the premises; (2) it is practicable to communicate with a person entitled to grant entry to the premises but it is not practicable to communicate with any person entitled to grant access to the evidence; (3) entry to the premises will not be granted unless a warrant is produced; and (4) the purpose of a search may be frustrated or seriously prejudiced unless a police officer arriving at the premises can secure immediate entry to them.

[1058] Section 10(6) PPCE.

officer carrying out the search must provide the occupier of the searched premise with the warrant, or in case the latter is not present, leave a copy of the warrant[1059].

A police officer who is lawfully on any premises may seize anything at that premise if (s)he has reasonable ground for believing that it has been obtained in consequence of the commission of an offence and that it is necessary to seize it in order to prevent it being concealed, lost, damaged, altered or destroyed[1060]. Moreover, the police officer may require any information which is stored in electronic form and is accessible from the premises to be produced in a form in which it can be taken away and in which it is visible and legible, provided that (s)he has reasonable grounds for believing that it is evidence in relation to an offence which he is investigating or any other offence, or that it has been obtained in consequence of the commission of an offence, and that it is necessary to do so to prevent it being concealed, lost, damaged, tampered with or destroyed[1061].

Specific limitations and safeguards also apply to the use of investigatory powers by public authorities in Guernsey. The use of investigatory powers to obtain information on communications is governed by the Regulation of Investigatory Powers (Bailiwick of Guernsey) Law 2003 (RIPL)[1062]. The RIPL regulates notably the interception of communications, acquisition of communications data (i.e., metadata stored by the service providers), the use of surveillance (such as covert investigations), and the investigation of electronic data protected by encryption (for example to obtain passwords allowing access to electronic devices) by a specified list of public authorities.

Section 1 RIPL introduces a general principle of confidentiality of communications by providing that it is an offence to intercept communications in the course of their transmission by means of a public postal service or a public or private telecommunication system without lawful authority[1063]. Sections 1(5) and 5 RIPL further clarify that to be lawful, any

[1059] Section 11 PPCE.
[1060] Section 14 PPCE.
[1061] According to Section 16 PPCE, the police officer who seizes anything must, if requested by the occupier of premises, provide in reasonable time that person with a record of what he has seized. The police officer must also grant access to or supply a photograph or a copy of the seized item at the request of the person who had custody of the item before it was seized. There is no obligation to grant access or to supply a photograph or photo if the officer in charge has reasonable ground for believing that to do so would prejudice the investigation, the investigation of any other offence or any related criminal proceeding. Pursuant to Section 17 PPCE, anything that has been seized by the police may be retained as long as is necessary in all the circumstances.
[1062] The RIPL is supplemented by a number of Codes of Practice dealing with the following matters: (1) Accessing Communications Data, (2) Covert Human Intelligence Sources, (3) Covert Surveillance, (4) Interception of Communications, and (5) Interception of Communications – Postal. The Codes of Practice provide guidance on, amongst other things, the procedures to be followed before the interception of communications or acquisition of communications data can take place. They were issued and brought into force under Section 61(1) RIPL by the Regulation of Investigatory Powers (Codes of Practice) (Bailiwick of Guernsey) Order 2004. Pursuant to Section 62(1) RIPL the Codes of Practice are admissible in civil and criminal proceedings. If any provision of the Codes of Practice appears relevant to a question before a court, it must be taken into account.
[1063] The same applies to communications transmitted by means of a private telecommunication system, i.e. any telecommunication system which, without itself being a public telecommunication system, is (1) attached, directly or indirectly and whether or not for the purposes of the communication in question, to a public telecommunication system, and (2) there is apparatus comprised in the system which is both located in the Bailiwick and used (with or without other apparatus) for making the attachment to the public telecommunication system.

interception of communications must be authorised by an interception warrant[1064] issued by Her Majesty's Procureur[1065].

An interception warrant is issued on application by certain persons specifically listed in the law[1066] if the Procureur is satisfied that it is necessary for one of the purposes listed in Section 5(3) RIPL. These include the purpose of preventing or detecting serious crime[1067]. Importantly, the law explicitly requires that the conduct that would be authorised must be proportionate to what is sought to be achieved by that conduct[1068]. In considering the necessity and proportionality of the measure, the Procureur must take into account whether any alternative means could be reasonably used to obtain the information[1069]. In addition, Section 2.5 of the Code of Practice on Interception of Communications further clarifies that this requires a balance of the intrusiveness of the interference against the need for it in operational terms. The interception of communications will not be proportionate if it is excessive in the circumstances of the case. In addition, any interception should be carefully managed to meet the objective in question and must not be arbitrary or unfair[1070].

In accordance with Section 7 RIPL, the warrant must either name or describe one person as the interception subject or specify a single set of premises as the premise in relation to which the interception is to take place. The warrant must also describe the communications for which interception is authorised, including the addresses, numbers, apparatus or other factors used to identify the communications[1071]. An interception warrant ceases to have effect after 3 months beginning with the day of the warrant's issue, unless it is renewed. A renewal may be

[1064] Interception without warrant is only lawful in specific limited circumstances set out exhaustively in Sections 3 and 4 RIPL, for instance if the sender and the intended recipient of the communication have consented to the interception, the interception is carried out by a provider of postal or telecommunication services and connected to the purpose of providing that service, or if it is carried out for the purpose of obtaining information about the communications of a person who is or is reasonably believed to be in a country or territory outside of Guernsey, provided that the law of that country or territory requires the interceptor to carry out, secure or facilitate the interception in question. Any interception conducted by public authorities under Sections 3 and 4 RIPL must be done in accordance with the Human Rights (Bailiwick of Guernsey) Law 2000 (in particular Article 8 of the European Convention of Human Rights incorporated by that Law), the Data Protection Law and the LEO.

[1065] Pursuant to Section 67(3) RIPL, any reference to Her Majesty's Procureur includes Her Majesty's Comptroller. The Procureur and Comptroller are independent from the government and are appointed by way of Warrant under the hand of the Sovereign.

[1066] These are the Chief Officer of the Island Police Force, the Chief Officer of Customs and Excise (of Guernsey), the Director General of the Security Service, the Chief of the Secret Intelligence service, the Director of GCHQ, and a person who, for the purpose of any international mutual assistance agreement, is the competent authority of a country or territory outside the Bailiwick.

[1067] Section 67(3) RIPL defines 'serious crime' as offences which involve the use of violence, result in substantial financial gain or constitute conduct by a large number of persons in pursuit of a common purpose, or for which a person over 21 with no previous convictions could reasonably be expected to be sentenced to imprisonment for three years or more.

[1068] Section 5(2)(b) RIPL.

[1069] Section 5(4) RIPL.

[1070] Section 2.5, Interception of Communications Code of Practice (made pursuant to Section 61 of the Regulation of Investigatory Powers (Bailiwick of Guernsey) Law, 2003, available at: https://www.guernseylegalresources.gg/CHttpHandler.ashx?documentid=52506.

[1071] Section 7(3) RIPL. Under Sections 7(4) and (5) RIPL, these specifications are not required for the interception of 'external communications', i.e., communications sent or received outside the British Islands where the Procureur has issued a certificate certifying that the examination of certain described intercepted material is necessary. According to the Guernsey authorities, such certificate has never been issued.

authorised by Her Majesty's Procureur only where (s)he is satisfied that the warrant remains necessary for the purposes described in Section 5(3) RIPL[1072].

The RIPL also regulates the acquisition of communications data. The acquisition of communications data is not aimed at obtaining the content of a communication, but aimed at obtaining information such as traffic data, information about the use of a postal service or telecommunications service, and any other information held or obtained by a postal service/telecommunication service in relation to persons to whom the service is provided[1073].

Persons designated with respect to a specific public authority[1074] may obtain communications data by giving notices to a postal or telecommunications operator, requiring the operator to obtain and/or disclose relevant data[1075]. A notice may only be issued if the designated person believes that it is necessary to obtain communications data for one of the specific purposes listed exhaustively in the law, including for the purpose of preventing or detecting crime or of preventing disorder[1076].

Importantly, the notice or authorisation may only be granted if the designated person believes that obtaining the data in question is proportionate to what is sought to be achieved[1077]. According to the Code of Practice on Accessing Communications Data, this means that even if an action that interferes with a Convention right is directed at pursuing a legitimate aim, this will not justify the interference if the means used to achieve the aim are excessive in the circumstances[1078]. Any interference with a Convention right must be carefully designed to meet the objective in question and must not be arbitrary or unfair[1079]. Even taking all these considerations into account, in a specific case interference may still not be justified because the impact on the individual or group is too severe[1080].

The notice must be issued in writing and specify the communications data to be obtained, the grounds on which it is necessary to obtain the data, the office, rank or position held by the person issuing the notice, and the manner in which any disclosure required by the notice is to

[1072] Section 8(1)-(3) RIPL.
[1073] 'Communications data' is defined in Section 67(3) RIPL.
[1074] In accordance with Section 20 RIPL, the designated persons are the Chief Officer of the Island Police Force (for the Island Police Force), the Chief Officer of Customs and Excise (for Customs and Excise) and Her Majesty's Procureur (for any other public authority within Guernsey and any of the Intelligence Services).
[1075] Section 18 RIPL. Pursuant to Section 18(9) RIPL, such notices may include a requirement to keep secret the issuing of the notice, its contents, and the measures carried out in pursuing the notice. The violation of this provision is deemed to be an offence under Section 18(10) RIPL.
[1076] Pursuant to Section 18(2) RIPL, the notice or authorisation can also be issued if it is in the interests of the economic well-being of the Bailiwick (as specified by the Code of Practice on Accessing Communications Data, only to the extent relevant in the interest of national security), in the interests of public safety, for the purpose of protecting public health, for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department, for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health, or for any other purpose which is specified by the responsible government committee. The committee has specified two additional purposes for obtaining communications data: inquiry into circumstances around a person's death, and discharge of functions of the Guernsey Financial Services Commission under any international agreement or memorandum of understanding endorsed by the International Organisation of Securities Commission.
[1077] Section 18(5) RIPL.
[1078] Section 4.4 Code of Practice on Accessing Communications Data, available at: https://www.guernseylegalresources.gg/CHttpHandler.ashx?documentid=52505.
[1079] Section 4.4 Code of Practice on Accessing Communications Data.
[1080] Section 4.4 Code of Practice on Accessing Communications Data.

be carried out[1081]. The effect of a notice is limited and unless it is renewed, it ceases to require that data be obtained one month after the date on which the notice is given[1082]. A notice may be renewed before the end of the period of one month under the same conditions as described above[1083].

Finally, Part III RIPL covers the investigation of electronic data protected by encryption and allows for the issuing of notices requiring the disclosure of the key to encrypted information that is lawfully within the possession of the authorities (such as to obtain passwords allowing access to electronic devices). Such notices may be given where any protected information has come into possession of authorities[1084] and a person with the appropriate permission[1085] reasonably believes that a key to the protected information is in the possession of a person and that the imposition of a disclosure requirement in respect of the protected information is necessary for one of the purposes listed exhaustively in the law, notably in the interest of national security or for the purpose of preventing or detecting crime[1086]. In addition, the person imposing the disclosure requirement must believe on reasonable grounds that the measure is proportionate to what is sought to be achieved and that it is not reasonably practicable to obtain possession of the protected information in an intelligible form without the disclosure requirement[1087]. The notice must be given in writing or in a manner that produces a record[1088] and must describe the protected information to which the notice relates, must specify the office, rank or position held by the person giving it, must specify the time by which the notice is to be complied with and must set out the disclosure that is required by the notice and the form and manner in which it is to be made[1089].

In Guernsey, criminal law enforcement authorities can also obtain personal data from business organisations in the context of investigations into whether a person has engaged in or benefited from criminal conduct, or into the whereabouts of the proceeds of criminal conduct.

These powers are governed by the Criminal Justice (Proceeds of Crime (Bailiwick of Guernsey) Law, 1999 (POCL). In addition, the Drug Trafficking (Bailiwick of Guernsey) Law, 2000 (DTL) introduces similar powers in connection with investigations into whether a person has carried on or has benefited from drug trafficking, the whereabouts of the proceeds of drug trafficking, or drug money laundering.

In accordance with these laws, the Bailiff can, on an application of a police officer, make orders to make material available, issue search warrants to obtain that material where a

[1081] Section 19(2) RIPL.
[1082] Section 19 (4) to (7) RIPL.
[1083] Section 19(6)-(7) RIPL. If the person who has given the notice is satisfied that it is no longer necessary on these grounds or no longer proportionate to what is ought to be achieved, the person shall cancel the notice, pursuant to Section 19(8) RIPL.
[1084] By any of the means listed in Section 46(1) RIPL, such as the exercise of a statutory power to seize, detain, inspect, search or otherwise to interfere with documents or other property or the exercise of any statutory power to intercept communications.
[1085] Pursuant to Schedule 2 RIPL, a person has the appropriate permission if a written permission for the giving of Section 46 notices has been granted by a person holding judicial office, or when information has come to the possession of the authorities by a conduct authorized by warrant and the warrant contained permission for the giving of Section 46 notices in relation to protected information to be obtained under the warrant.
[1086] Section 46(2) and (3) RIPL.
[1087] Section 46(2)I and (d) RIPL.
[1088] Section 46(4)(a).
[1089] Section 46(4)(b) – (g).

production order is not appropriate or not complied with, make customer information orders and account monitoring orders.

Each type of order is subject to strict formal and substantial requirements. In essence, the scope of such orders is always limited to one individual or one set of premises, they must contain specific mandatory information, and they may only be issued for limited purposes.

For instance, under the POCL, the Bailiff can make an order[1090] to make material available if there are reasonable grounds for suspecting that a specified person has engaged in or benefited from criminal conduct, there are reasonable grounds for suspecting that the material is likely to be of substantial value to the investigation, and does not consist of or include items subject to legal professional privilege or excluded material[1091], and there are reasonable grounds for believing that it is in the public interest that the material should be produced or that access to it should be given[1092].

The Bailiff can issue a search warrant[1093] under the POCL authorising a police officer to enter and search specific premises, provided that the same conditions as described above are met and an order to make material available has not been complied with, or it would not be appropriate to make such an order. Where a police officer has entered premises in the execution of a search warrant, he or she may seize and retain any material, other than items subject to legal professional privilege or excluded material, which is likely to be of value to the investigation. All applications for production orders and search warrants must have the consent of Her Majesty's Procureur.

A customer information order requires a financial services business[1094], on a notice given by Her Majesty's Procureur or a police officer, to provide any customer information[1095] that the institution has relating to a person specified in the application[1096], in such manner, and by such time, as they require[1097]. An account monitoring order requires the financial services business specified in the application to provide account information specified in the order to

[1090] Section 45 POCL.
[1091] Excluded material includes personal records which a person has acquired or created in the course of any trade, business profession or other occupation, human tissue taken for the purposes of diagnoses or medical treatment and journalistic material.
[1092] In relation to any material that consists of information contained in a computer, such an order requires to produce the material in a form in which it can be taken away and in which it is visible and legible, or to give access to the material in a form in which it is visible and legible.
[1093] Section 46 POCL.
[1094] The financial services businesses are defined in Schedule 1 to the POCL and include for instance lending, financial leasing, operating a money service business, currency exchange and cheque cashing, facilitating or transmitting money or value through an informal money or value transfer system or network, issuing, redeeming, managing or administering means of payment, including credit, charge and debit cards, cheques, travellers' cheques, money orders and bankers' drafts and electronic money, providing financial guarantees or commitments, trading in money market instruments, foreign exchange, exchange, interest rate or index instruments, and commodity futures, transferable securities or other negotiable instruments or financial assets, participating in securities issues and the provision of financial services related to such issues, etc.
[1095] Customer information is defined in Section 48B POCL and section 67B DTL as information about whether the person holds an account or safe deposit box at the financial services business and other relevant information such as the account or safety box number, the person's name, date of birth and address, the date on which the person began to hold the account, if the person has ceased to hold the account the date of cessation, such evidence of the person's identity as was obtained by the financial services business under or for the purposes of any legislation relating to money laundering etc.
[1096] Section 48A POCL and section 67A DTL.
[1097] Section 48A(6)POCL and section 67A(6) DTL.

an appropriate officer, for the period[1098], in a manner, and by the time stated in the order[1099]. The conditions for issuing these orders are identical to the ones described above[1100].

Under the Disclosure (Bailiwick of Guernsey) Law, 2007 (DL) obligations are placed on financial services businesses[1101] and other (non-financial services) businesses to disclose certain information[1102] to a prescribed police officer, where they know or suspect, or have reasonable grounds for knowing or suspecting, that another person is engaged in money laundering or that certain property is or is derived from the proceeds of criminal conduct[1103].

Importantly, any disclosure of personal data obtained on the basis of the abovementioned provisions has to comply with the Data Protection Law, and the further processing by criminal law enforcement authorities of personal data obtained through such disclosures is subject to the provisions of the LEO.

2.2.2. Further use of the information collected

The further use of data collected by Guernsey criminal law enforcement authorities on one of the grounds referred to in Section 2.2, as well as the sharing of such data with a different authority for purposes other than the ones for which it was originally collected (so-called 'onward sharing'), is subject to safeguards and limitations.

First, the processing of personal data by law enforcement authorities in Guernsey is governed by the provisions of the LEO as described in section 2.1. With respect to onward sharing, Article 6(2) of the LEO, like the Law Enforcement Directive, allows that personal data collected for a law enforcement purpose may be further processed (whether by the original controller or by another controller) for any other (secondary) law enforcement purpose if the data subject has given its consent to the further processing, if the further processing is for a historical or scientific purpose, or if the controller processes the data for the secondary purpose in the context of discharging a function imposed by law, and the processing is necessary and proportionate to that secondary purpose. In this case, all the safeguards provided by the LEO and the Data Protection Law (referred to in section 2.1) apply to the processing carried out by the receiving authority.

When law enforcement authorities in Guernsey intend to share personal data processed under the LEO with law enforcement authorities of a third country, specific requirements apply[1104]. These requirements are very similar to those set out by the Law Enforcement Directive.

[1098] The period stated in an account monitoring order must not exceed the period of 90 days beginning with the day on which the order is made (Section 48H(7) POCL, 67H(7)DTL).
[1099] Section 48H(6) POCL, section 67H(6) DTL.
[1100] Such orders can also be made in connection of an investigation into money laundering or drug money laundering, if there are reasonable grounds for suspecting that the person specified in the application for the order has committed a money laundering offence or an offence under Section 57, 58 or 59 DTL, and the above-mentioned conditions are met, see Sections 48C and 48(I) POCL, Sections 67C and 67I DTL.
[1101] See definition in Schedule 1 to the POCL, footnote 86.
[1102] The information that needs to be disclosed includes any information or document relating to the knowledge, suspicion or reasonable grounds for suspicion that the person in respect of whom the disclosure is made is engaged in money laundering or that certain property is or is derived from the proceeds of any person's criminal conduct, and any fact or matter upon which such knowledge, suspicion or reasonable grounds for suspicion is based, see Section 3A DL.
[1103] Sections 1 and 3 DL.
[1104] Sections 43 to 47 LEO.

Transfers of personal data to "unauthorised jurisdictions" (essentially jurisdictions other than the EU Member States and any country or international organisation that the European Commission has found to ensure an adequate level of protection within the meaning of Article 36 of the LED)[1105] can only take place if they are necessary for a law enforcement purpose and based on appropriate safeguards[1106]. In the absence of appropriate safeguards, transfers to unauthorised jurisdictions are only possible in specific circumstances that are listed in the law in an exhaustive manner, e.g., for the protection of vital interests of individuals, to safeguard legitimate interests of the data subject, to prevent immediate and serious threats to the public or national security of any country, in individual cases for a law enforcement purpose, and in individual cases in the context of legal proceedings and legal advice relating to a law enforcement purpose[1107].

Second, the different laws that allow for data collection by criminal law enforcement authorities in Guernsey impose specific limitations and safeguards as to the use and further dissemination of the information obtained in exercising the powers they grant.

As regards the powers of search and seizure under the PPCE, the police officer who seizes anything must, if requested by the occupier of premises, provide in reasonable time that person with a record of what he has seized. The police officer must also grant access to or supply a photograph or a copy of the seized or retained item at the request of the person who had custody of the item before it was seized[1108]. Importantly, anything that has been seized by the police may not be retained longer than necessary in the circumstances[1109].

With respect to the interception of communications, Sections 12 and 13 RIPL set out the safeguards that need to be applied to material intercepted on the basis of a warrant. In particular, the Procureur must make arrangements to ensure that the dissemination of the intercepted material (i.e., the number of people who can access it, the extent to which the material is disclosed or copied, the number of copies[1110], etc.) is limited to the minimum necessary for the purposes authorised by the warrant. Each copy made of any of the materials must be destroyed as soon as there are no longer any grounds for retaining it as necessary for any of the authorised purposes[1111]. Intercepted material may be shared with authorities of a

[1105] Section 50 LEO.
[1106] Section 43(1) in conjunction with Section 44 LEO. Appropriate safeguards are in place where provided by a legal instrument binding the intended recipient, such as a legally binding and enforceable agreement between the controller and the recipient, or where the controller, having assessed all the circumstances surrounding the transfer, concludes that appropriate safeguards exist to protect the data. The controller is required to keep detailed written records of any transfer relying on appropriate safeguards, and when relying on appropriate safeguards on the basis of the circumstances surrounding the transfer, the controller must notify the Authority of the categories of data transferred on that basis.
[1107] Section 45 LEO.
[1108] Section 16 PPCE.
[1109] Section 17 PPCE.
[1110] 'Copy' is defined as (1) any copy, extract or summary of the material or data which identifies itself as the product of an interception; or (2) any record referring to an interception which is a record of the identities of the persons to or by whom the intercepted material was sent, or to whom the communications data relates.
[1111] Something is considered necessary for the authorised purposes if it continues to be necessary (or is likely to become necessary) (1) for the purpose for which the warrant was issued; (2) for facilitating the carrying out of any of the functions of the Attorney General in relation to interceptions; (3) for facilitating the carrying out of any functions in relation to interceptions by the Commissioner or of the Tribunal; or (4) to ensure that a person conducting a criminal prosecution has the information needed to determine what is required of that person by his or her duty to secure the fairness of the prosecution.

country or territory outside of Guernsey only if the Procureur has made arrangements that ensure corresponding limitations, to the extent that the Procureur seems fit, and that prevent any disclosure that would not be lawful within Guernsey[1112].

These safeguards are further specified in the Codes of Practice on the Interception of Communications. In particular, the Code of Practice requires all intercepted material to be handled in accordance with the arrangements made by the Procureur, the details of which must be made available to the Investigatory Powers Commissioner (see section 2.2.3 below)[1113]. All intercepting agencies are required to keep detailed records of interception warrants for which they have applied[1114]. The Code further requires intercepted material, as well as copies and summaries of the material, to be handled and stored securely to minimise the risk of loss or theft. In particular, it must be inaccessible to persons without the required level of security clearance, and this requirement for secure storage also applies to communications service providers. It also requires intercepted material to be securely destroyed as soon as it is no longer needed for any of the authorised purposes and retained material to be reviewed at appropriate intervals to confirm that its retention is justified and valid.[1115]

Concerning the acquisition of Communications Data, the Code of Practice on Accessing Communications Data provides that applications and notices for communications data must be retained by the relevant public authority until they have been audited by the Investigatory Powers Commissioner. The public authority should also keep a record of the dates on which an authorisation or notice is started and cancelled. The Code furthermore provides that communications data, as well as all copies, extracts and summaries of it, must be handled and stored securely[1116].

For the investigation of electronic data protected by encryption, Section 51 RIPL sets out additional safeguards. In particular, it requires all persons involved in such investigations to make arrangements in order to ensure that any key disclosed in the context of the investigation is used only for obtaining access to information to which the investigation relates, that the use and retention of the key are proportionate to what is sought to be achieved, that the key is stored in a secure manner and that it is destroyed as soon as it is no longer needed[1117].

Finally, under the DL any information obtained by Her Majesty's Procureur or a police officer under this law or any other enactment, or in connection with the carrying out any of their respective functions, may be disclosed to any other person only if the disclosure takes place for a specified purpose, notably for the prevention, detection, investigation or prosecution of criminal offences, whether in Guernsey or elsewhere, the carrying out the functions of the Guernsey Financial Services Commission or a body in another country or territory which carries out any similar function to the Commission, or for the carrying out of any functions of

[1112] Section 12(6) and (7) RIPL.
[1113] Section 6.1, Interception of Communications Code of Practice.
[1114] Section 4.16, Interception of Communications Code of Practice.
[1115] Section 6.2 to 6.9, Interception of Communications Code of Practice.
[1116] Section 7, Accessing Communications Data Code of Practice.
[1117] Section 51 RIPL.

any intelligence service. Any such disclosure must not contravene the Data Protection Law or LEO[1118].

2.2.3. Oversight

Different bodies carry out oversight of the activities of criminal law enforcement authorities.

First, the processing of personal data by competent authorities for criminal law enforcement purposes is subject to the oversight of the Data Protection Authority, whose independence is enshrined in law[1119]. The tasks and powers of the Data Protection Authority mirror those set out in Article 46 and 47 of the LED[1120]. To perform those tasks, the Data Protection Authority may investigate complaints, conduct inquiries into the processing of personal data by criminal law enforcement authorities[1121], issue recommendations, make a determination of a violation of the Law and impose sanctions[1122]. These sanctions can include reprimands, warnings or corrective orders (e.g., requiring the authority to bring processing in compliance with the Law, rectify or erase data, cease the processing, etc.). In determining which order to impose, the Authority must have regard to different factors, such as the nature, gravity and duration of the violation, whether the violation was intentional or negligent, the degree of cooperation with the Authority to remedy the breach, any other action taken to mitigate any damage suffered by data subjects etc.[1123].

According to information provided by the Data Protection Authority, since the entry into force of the LEO, the Authority has been involved in 17 complaints, two inquiries and 11 self-reported data breaches that concerned data processing carried out by law enforcement authorities. The Authority issued one enforcement notice against a law enforcement authority in a case that concerned the unlawful sharing of data. The notice required the authority to review safeguarding and associated data sharing procedures. The Data Protection Authority also regularly engaged with law enforcement authorities by providing guidance and advice.

Second, the use of investigatory powers under the RIPL is overseen by the Investigatory Powers Commissioner. Under Part IV of the RIPL, the Bailiff must appoint a judge of the Court of Appeal (of Guernsey) as the Investigatory Powers Commissioner. The Commissioner is responsible for reviewing the activities under the RIPL, including the issuing of interception warrants, notices for the collection of communications data and investigations of electronic data protected by encryption[1124]. All persons involved in the use of investigatory powers are required to disclose or provide to the Commissioner all documents and information that the Commissioner may require for the purpose of enabling him to carry out his functions[1125]. The Commissioner is in turn required to prepare an annual report on the use

[1118] Section 8(4)(a) DL.
[1119] Section 3(1)(f) LEO in conjunction with Section 62 Data Protection Law.
[1120] Section 3(1)(f) LEO in conjunction with Parts XI and XII Data Protection Law.
[1121] Section 3(1)(f) LEO in conjunction Sections 68 and 69 Data Protection Law.
[1122] Section 3(1)(f) LEO in conjunction Section 72 Data Protection Law. The Authority cannot impose administrative fines on competent authorities processing personal data for criminal law enforcement purposes, see Schedule 1 LEO.
[1123] Schedule 1 LEO, which modifies Section 73(7) and (7A) Data Protection Law.
[1124] Section 53 RIPL.
[1125] Section 54(1) RIPL.

of investigatory powers for submission to the Bailiff of Guernsey[1126]. The Bailiff must lay before the Royal Court a copy of every annual report made by the Commissioner[1127]. The Commissioner's report is also made public. If it appears to the Commissioner that there has been a contravention of the RIPL or insufficient safeguards have been put in place for intercepted communications, he/she must report that to the Bailiff[1128].

As described in the Commissioner's recent annual reports, the overwhelming majority of warrants requested and granted in Guernsey are in support of the activities of the Guernsey Police and the Guernsey Border Agency and for the purpose of preventing or detecting crime, notably drug trafficking and related anti-money laundering. In his annual reports, the Commissioner found that warrants had been issued for properly identified statutory purposes, in respect of the principles of necessity and proportionality and in compliance with procedural requirements. He also noted that the safeguards required by Sections 12 and 51 RIPL had been implemented in a satisfactory manner. In a limited number of instances, the Commissioner noted that he had made recommendations for further practical improvements[1129].

2.2.4. Redress

As regards the processing of personal data by law enforcement authorities in Guernsey, redress mechanisms are available under the data protection legislation, under the Human Rights Act 2001 and under the RIPL. This series of mechanisms provide data subjects with effective administrative and judicial means of redress, enabling them in particular to ensure their rights, including the right to have access to their personal data, or to obtain the rectification or erasure of such data.

First, data subjects have the right to lodge a complaint with the Data Protection Authority concerning the processing of their personal data by criminal law enforcement authorities[1130]. The Authority has the power to determine breaches of the LEO and impose necessary sanctions. It also has the power, on request by a data subject or on its own initiative, to bring proceedings before a court in respect of any breach or anticipated breach of the Law. Following such complaint, the court can make any order, relief and remedy it considers just

[1126] Section 54(4) RIPL.
[1127] Section 54(6) RIPL.
[1128] Section 54(2) and (3) RIPL.
[1129] The Reports of the Investigatory Powers Commissioner covering the years 2016 to 2021 are available at: https://guernseyroyalcourt.gg/CHttpHandler.ashx?id=154063&p=0, https://guernseyroyalcourt.gg/CHttpHandler.ashx?id=148330&p=0, https://guernseyroyalcourt.gg/CHttpHandler.ashx?id=148328&p=0, https://guernseyroyalcourt.gg/CHttpHandler.ashx?id=125594&p=0, https://guernseyroyalcourt.gg/CHttpHandler.ashx?id=115492&p=0, https://guernseyroyalcourt.gg/CHttpHandler.ashx?id=107429&p=0. In 2021, the Commissioner noted that a more detailed confidential report had been provided that included recommendations on how to improve the practice in relation to the acquisition of communications data, see para. 63 of the 2021 report. In 2020, the Commissioner made recommendations in relation to the operation and management of covert human intelligence sources, see para. 67 of the 2020 report. In 2019, recommendations concerned the authorisation of direct surveillance, see para. 76 of the 2019 report. In 2018, the Commissioner recommended measures to improve the quality of applications for interception warrants, see para. 57 of the 2018 report. In 2017, recommendations for practical improvement concerned direct surveillance and covert human intelligence sources, see paras. 64 and 67 of the 2017 report.
[1130] Section 3(1)(f) LEO in conjunction with Section 67 Data Protection Law.

under the circumstances, including an award of compensation to any person who suffers damage as a result of the breach, an injunction or interim injunction to restrain any actual or anticipated breach of an operative provision, and a declaration that a breach was committed[1131].

Second, individuals can obtain judicial redress against decisions of the Authority. This includes the possibility to challenge an action or inaction of the Authority before a court, e.g., decisions not to investigate a complaint, or decisions finding that there has been no violation of the Law. Moreover, an individual can appeal to court against any failure of the Authority to provide written notice that a complaint is either being investigated or not being investigated, within the time period specified in the Law, or if the complaint is being investigated, written notice of the progress and, where applicable, the outcome of the investigation within the time period specified in the Law[1132]. If a determination of the Authority is appealed, the court has the power to confirm or annul the determination of the Authority and remit the matter back to the Authority for reconsideration and make any other order it considers just[1133].

Third, under Section 79 of the Data Protection Law, individuals can also obtain judicial redress against criminal law enforcement authorities directly before the courts. In particular, if there is a breach of the operative provisions of the Law and the breach causes damage to another person, it is actionable in court by that person[1134].

Fourth, as far as any person considers that their rights, including rights to privacy and data protection, have been violated by public authorities, individuals can obtain redress before the Guernsey courts under the Human Rights Law 2001. Under Section 6(1) of the Human Rights Law, it is unlawful for a public authority to act in a way which is incompatible with rights provided in the law[1135]. A person who claims that a public authority has acted (or proposes to act) in a way which is unlawful under Section 6(1) can bring proceedings against the authority under this Law in the appropriate court or tribunal, when he or she is (or would be) a victim of the unlawful act[1136]. If the court finds any act of a public authority to be unlawful, it can grant such relief or remedy, or make such order, within its powers as it considers just and appropriate[1137].

Finally, any individual may obtain judicial redress before the European Court of Human Rights against the unlawful collection of his/her data by criminal law enforcement authorities, provided that all available domestic remedies have been exhausted.

[1131] Section 3(1)(f) in conjunction with Section 85 Data Protection Law.
[1132] Section 3(1)(f) in conjunction with Section 82 Data Protection Law.
[1133] Section 3(1)(f) in conjunction with Section 83 Data Protection Law.
[1134] Section 3(1)(f) in conjunction with Section 79(2) Data Protection Law.
[1135] However, the act of the public authority is not unlawful if as the result of one or more provisions of primary legislation, the authority could not have acted differently or in the case of one or more provisions of, or made under, primary legislation which cannot be read or given effect in a way which is compatible with the Convention rights, the authority was acting so as to give effect to or enforce those provisions, see Section 6(2) Human Rights Law.
[1136] Section 7(1) Human Rights Law. According to Section 7(5) Human Rights Law a person is a victim of an unlawful act only if he would be a victim for the purposes of Article 34 of the Convention if proceedings were brought in the European Court of Human Rights in respect of that act.
[1137] Section 8(1) Human Rights Law.

For violations of the RIPL, individuals can obtain redress before the Interception of Communications Tribunal. This redress avenue is described in section 2.3.4 below.

2.3. Access and use by Guernsey public authorities for national security purposes

In Guernsey, access to information transferred under the adequacy decision for purposes of national security can take place in the form of the interception of communications, the acquisition of communications data and the investigation of data protected by encryption on the basis of the RIPL[1138].

2.3.1. Legal bases and applicable limitations/safeguards

The interception of communications, acquisition of communications data and investigation of data protected by encryption on the basis of the RIPL may not only take place in the context of criminal investigations, but also when necessary in the interests of national security or to safeguard the economic well-being of the Bailiwick[1139]. The use of these powers for those purposes is subject to the same substantive and procedural limitations and safeguards as described in section 2.2.1 in the context of criminal law enforcement, notably the need for independent authorisation, requirements of necessity and proportionality and limitation to specific communications or information[1140].

Moreover, although the notion of "economic well-being" may appear broad, Section 5 RIPL sets out that an interception warrant can only be considered necessary for the purpose of safeguarding the economic well-being of Guernsey if the purpose is to obtain information relating to the acts or intentions of persons outside Guernsey[1141]. In addition, the Code of Practice on the Interception of Communications further specifies that Her Majesty's Procureur can only issue an interception warrant for the purpose of safeguarding the economic well-being of Guernsey if he considers, on the basis of the facts of each case, that there is a direct link between the economic well-being of the Bailiwick and national security[1142]. Similarly, the Code of Practice on Accessing Communications Data sets out that communications data

[1138] These powers can be exercised by the Island Police Force, Customs and Excise (of Guernsey), and the UK intelligence services. The safeguards under the RIPL apply also to any UK authorities making use of powers under the RIPL, notably the requirements for the issuing and implementation of interception warrants, restrictions on the use and disclosure of intercepted material, and the right of complaint to the Tribunal. The Human Rights Law, the Data Protection Law and the LEO also apply to any actions taken and decisions made by UK authorities acting under the RIPL. In addition, any safeguards and limitations in UK law (including legislation governing intelligence services or data protection) apply concurrently to the UK authorities. For the powers that can be exercised in Guernsey by UK intelligence services and the limitations and safeguards provided by UK law, see the Commission Implementing Decision of 28.6.2021 pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data by the United Kingdom, available at: https://commission.europa.eu/system/files/2021-06/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_en.pdf.

[1139] Sections 5(3)(a) and (c), 18(2)(a) and (c) and 46(3)(a) and (c) RIPL.

[1140] Differently from what is described in Section 2.2.1, when relating to the interception of communications in the interest of national security or the safeguarding of Guernsey's economic well-being, a warrant can be renewed for up to six months, see Section 8(4) RIPL.

[1141] Section 5(5) RIPL.

[1142] Section 5.4 Interception of Communications Code of Practice. An example of a situation where it might be possible to rely on this ground to authorise an interception would be a threat to Guernsey's critical national infrastructure that would impact Guernsey's economic interests (e.g., through an attack on Guernsey's essential electricity or communications infrastructure).

can only be obtained for the purpose of the economic well-being of Guernsey if, on the basis of the facts of each case, the economic well-being is related to national security[1143].

2.3.2. Further use of the information collected

The further use of personal data obtained in the interests of national security is governed either by the provisions of the LEO or of the Data Protection Law, as described in section 2.1[1144]. Section 6(2) of the LEO allows that personal data collected for a law enforcement purpose (within the meaning of the LEO) may be further processed for any other (secondary) law enforcement purpose only if the data subject has given its consent to the further processing, if the further processing is for a historical or scientific purpose, or if the controller processes the data for the secondary purpose in the context of discharging a function imposed by law, and the processing is necessary and proportionate to that secondary purpose. Pursuant to Sections 5and 6(1)(b) of the LEO, data processing must be lawful and fair, and data must not be further processed in a manner that is incompatible with the purpose for which it was collected.

Moreover, specific requirements apply when personal data is shared with authorities outside of Guernsey[1145]. As described in more detail in sections 1.1, 2.1 and 2.2.2, these requirements are very similar to those set out by the EU's data protection framework. Transfers of personal data to "unauthorised jurisdictions" (essentially jurisdictions other than the EU Member States and any country or international organisation that the European Commission has found to ensure an adequate level of protection)[1146] can only take place if they are based on appropriate safeguards[1147]. In the absence of appropriate safeguards, transfers to unauthorised jurisdictions are only possible in specific circumstances that are listed in the law in an exhaustive manner[1148].

In addition, the RIPL, complemented by the relevant Codes of Practice, sets out specific safeguards for the further use and sharing of data obtained on the basis of its provisions. These involve particular arrangements to ensure that the dissemination of material obtained is limited to the minimum necessary for the purposes pursued with the authorisation. Material must be handled and stored securely to minimise the risk of loss or theft and must be destroyed as soon as there are no longer any grounds for retaining it as necessary for any of the authorised purposes. Retained material must be reviewed at appropriate intervals to confirm that its retention is justified and valid. All agencies exercising powers on the basis of the RIPL are required to keep detailed records of warrants or authorisations for which they have applied[1149]. Intercepted material may be shared with authorities of a country or territory

[1143] Section 4.2 Accessing Communications Data Code of Practice.
[1144] The LEO applies to the processing of personal data by a competent authority, including for the purpose of safeguarding against or preventing threats to national security. The Data Protection Law applies if the processing of personal data for national security purposes is not carried out by a competent authority. While both the LEO and the Data Protection Law provide for an exemption from specified provisions for national security purposes, these provisions may only be restricted if necessary and proportionate and to the extent that their application would be likely to prejudice national security.
[1145] Sections 43 to 47 LEO, Sections 55 to 59 Data Protection Law.
[1146] Section 50 LEO, Section 111(1) Data Protection Law.
[1147] Section 43(1) in conjunction with Section 44 LEO, Section 56 Data Protection Law.
[1148] Section 45 LEO, Section 59(1) Data Protection Law.
[1149] Sections 12, 13 and 51 RIPL, Section 4.16, Interception of Communications Code of Practice, Section 7, Accessing Communications Data Code of Practice.

outside of Guernsey only if arrangements are in place to ensure corresponding limitations and to prevent any disclosure that would not be lawful within Guernsey[1150].

2.3.3. Oversight

Government access for national security purposes in Guernsey is overseen by different bodies. The Data Protection Authority oversees the processing of personal data in light of the LEO and the Data Protection Law, while specific oversight on the use of the investigatory powers under the RIPL is provided by the Investigatory Powers Commissioner.

The processing of personal data carried out for national security purposes is governed by the provisions of both the LEO and the Data Protection Law. The general functions and powers of the Guernsey Data Protection Authority are laid down in Section 61 *et seq.* of the Data Protection Law in conjunction with Schedule 7 to the Data Protection Law[1151]. The tasks include, but are not limited to, monitoring and enforcement, promoting public awareness, advising the Guernsey parliament and government and other institutions on legislative and administrative measures, promote the awareness of controllers and processors of their obligations, provide information to a data subject concerning the exercise of the data subject's rights, handle complaints, conduct investigations, issue guidance etc. The Authority has the powers to notify controllers of an alleged infringement and to issue warnings that a processing is likely to infringe the rules, issue reprimands, ban processing or order the controller to take certain actions[1152]. While the Data Protection Law[1153] allows exemptions from certain provisions, including from those that concern the Authority, for national security purposes, these provisions may only be restricted on a case-by-case basis to the extent that their application would be likely to prejudice national security and if necessary and proportionate (as explained in section 2.1).

Furthermore, as described in section 2.2.3 above, the Investigatory Powers Commissioner oversees the application of the RIPL i.e., the interception of communications, the acquisition of communications data and the investigation of data protected by encryption. In his recent annual reports, the Commissioner noted that the overwhelming majority of warrants in Guernsey were requested and granted in support of the activities of the Guernsey Police and the Guernsey Border Agency and for the purpose of preventing or detecting crime[1154].

2.3.4. Redress

[1150] Section 12(6) and (7) RIPL, see also section 2.2.2 above.
[1151] Pursuant to Section 3(1)(f) LEO, the provisions regarding the Authority in the Data Protection Law apply also to processing of personal data that falls within the scope of the LEO.
[1152] Sections 72 and 73 Data Protection Law.
[1153] Pursuant to paragraph 18 of Schedule 8 Data Protection Law, the application of the provisions in Parts II to XII and XV may be restricted, provided that the applicable conditions are fulfilled.
[1154] The Reports of the Investigatory Powers Commissioner covering the years 2016 to 2021 are available at: https://guernseyroyalcourt.gg/CHttpHandler.ashx?id=154063&p=0, https://guernseyroyalcourt.gg/CHttpHandler.ashx?id=148330&p=0, https://guernseyroyalcourt.gg/CHttpHandler.ashx?id=148328&p=0, https://guernseyroyalcourt.gg/CHttpHandler.ashx?id=125594&p=0, https://guernseyroyalcourt.gg/CHttpHandler.ashx?id=115492&p=0, https://guernseyroyalcourt.gg/CHttpHandler.ashx?id=107429&p=0.

First, an individual who believes that his or her rights under the LEO have been (or are about to be) breached can make a complaint to the Data Protection Authority, which exercises oversight over processing by competent authorities (as described in section 2.3.3 above). Redress mechanisms under the LEO and the Data Protection Law include breach determinations or sanctions issued by the Authority, and civil proceedings before a court, in which a court can make any order, relief and remedy it considers just under the circumstances, including an award of compensation to any person who suffers damage as a result of the breach, an injunction or interim injunction to restrain any actual or anticipated breach of an operative provision, and a declaration that a breach was committed (as described in section 2.2.4 above).

Individuals can also obtain redress for violations of the RIPL before an independent Tribunal established by Section 56 RIPL[1155].

The Tribunal is the appropriate forum for any complaint by a person, including any individual in the EU, who believesthat conduct under the RIPL has taken place in relation to him, his property or his communications[1156], including conduct by or on behalf of any of the UK intelligence services, conduct in connection with the interception of communications in the course of their transmission, conduct in connection with the collection of communications data, or conduct in connection with the investigation of data protected by encryption[1157]. In addition, the complainant is required to believe that the conduct has taken place either in "challengeable circumstances"[1158] or has been carried out by or on behalf of the intelligence services[1159].

When considering a complaint, it is the duty of the Tribunal to investigate whether surveillance has taken place in relation to the complainant, as well as the authority for such surveillance, if any[1160]. The Tribunal determines whether any errors of law, errors of fact or procedural errors have been committed, or whether there has been any other irregularity, such as a lack of proportionality[1161]. All persons involved in the exercise of powers under the RIPL

[1155] In accordance with Schedule 3 to the RIPL, the Tribunal consists of five members appointed by the Royal Court of Guernsey, each of whom must be (1) an Advocate of the Royal Court of Guernsey or Jersey, (2) a member of the Bar in England, Scotland or Northern Ireland, or (3) a solicitor of the Supreme Court of Judicature of England and Wales, a solicitor in Scotland or a solicitor of the Supreme Court of Northern Ireland, in each case of not less than ten years standing. The members are appointed for a term of 5 years and can be reappointed. A member of the Tribunal may only be removed from office by the Royal Court.

[1156] On the standard of the 'belief' test, in the absence of relevant case law in Guernsey, UK case law is likely to be persuasive. In Human Rights Watch v Secretary of State [2016] UKIPTrib15_165-CH, paragraph 41, the Investigatory Powers Tribunal, by referring to the European Court of Human Rights case law, held that the appropriate test is whether in respect of the asserted belief that any conduct falling within Subsection 68(5) of RIPA 2000 has been carried out by or on behalf of any of the intelligence services, there is any basis for such belief, such that the individual may claim to be a victim of a violation occasioned by the mere existence of secret measures or legislation permitting secret measures, only if he is able to show that due to his personal situation, he is potentially at risk of being subjected to such measures.

[1157] Section 56(4)(a) RIPL.

[1158] Pursuant to Section 56(7) and (8) RIPL, conduct has taken place in 'challengeable circumstances' if it has taken place with authority (e.g., on the basis of an interception warrant, an authorisation/notice for the acquisition of communications data, etc.), or if the circumstances are such that it would not have been appropriate for the conduct to take place without authority, or at least without proper consideration having been given to whether such authority should be sought.

[1159] Section 56(4)(b) RIPL.

[1160] Section 58 RIPL.

[1161] Section 58(2) and (3) RIPL.

are required to provide to the Tribunal all such documents and information that the Tribunal may need to carry out its functions[1162]. The Tribunal also has the power to require the Investigatory Powers Commissioner to provide the Tribunal with all such assistance (including the Commissioner's opinion as to any issue to be determined by the Tribunal) as the Tribunal think fit[1163]. The Commissioner must be kept informed about the proceedings and any determination, award, order, or other decision made in relation to those proceedings[1164].

If the Tribunal makes a determination in favour of the complainant, the Tribunal must provide the complainant with a summary of that determination including any findings of fact. The tribunal must also give notice to the complainant if no determination has been made in his/her favour[1165]. The Tribunal has the power to issue interim orders and to provide any such award of compensation or other order as it thinks fit. This may include an order quashing or cancelling any warrant or authorisation and an order requiring the destruction of any records of information obtained in exercise of any power conferred by a warrant or authorisation, or otherwise held by any public authority in relation to any person[1166]. According to Section 58(8) RIPL, a determination, award, order, or other decision of the Tribunal, is not subject to appeal[1167].

Finally, as also described in section 2.2.4 above, as far as individuals consider that their rights, including rights to privacy and data protection, have been violated by public authorities, they can obtain redress before the Guernsey courts under the Human Rights Law 2001. In addition, any individual may obtain judicial redress before the European Court of Human Rights against the unlawful collection of his/her data for national security purposes, provided that all available domestic remedies have been exhausted.

[1162] Section 59(6) and (7) RIPL.
[1163] Section 59(2) RIPL.
[1164] Section 59(3) RIPL.
[1165] Section 59(4) RIPL.
[1166] Section 58(7) RIPL.
[1167] According to the Guernsey authorities, the Tribunal has so far made a determination in the case of one complaint. The decision of the Tribunal was not made public. Pursuant to Rule 6(1) of the Investigatory Powers Tribunal Rules 2006 adopted under Section 60 RIPL (available at: http://www.guernseylegalresources.gg/CHttpHandler.ashx?id=70618&p=0) the Tribunal has a duty to ensure, amongst other things, that no information is disclosed which is contrary to the public interest or prejudicial to the prevention, detection, investigation or prosecution of serious crime.

VI. ISLE OF MAN

1. RULES APPLYING TO THE PROCESSING OF PERSONAL DATA

1.1. Relevant developments in the data protection framework of the Isle of Man

On 28 April 2004 the Commission adopted a decision in which the Isle of Man was considered as providing an adequate level of protection for personal data transferred from the EU[1168]. The Article 29 Working Party had adopted a positive opinion on the level of protection of personal data in the Isle of Man on 21 November 2003[1169]. At the time, the legal framework for the protection of personal data in the Isle of Man was set out in the Data Protection Act 2002, which entered into force on 1 April 2003. The Data Protection Act 2002 was closely aligned with the UK's Data Protection Act 1998 that had been enacted in the UK to give effect to the provisions of Directive 95/46/EC (Data Protection Directive)[1170].

Since the adoption of the adequacy decision, the Isle of Man has further modernised and significantly strengthened its data protection framework through a comprehensive reform. The Data Protection Act 2002 was replaced with new legislation that closely aligns the Isle of Man regime with the EU's current data protection legislation. In particular, the Isle of Man has incorporated most of the provisions of Regulation (EU) 2016/679 (GDPR)[1171] into its own legal order while making only minor adjustments on specific aspects, in particular to adapt the framework to the local context. The recitals of the GDPR have also been maintained in the new data protection framework to assist with contextualising and interpreting relevant provisions.

The Isle of Man main data protection framework now consists of:

(1) the Data Protection Act 2018, which enables the Isle of Man to apply EU instruments relating to data protection (including, but not limited to the GDPR, Directive (EU) 2016/680 (Law Enforcement Directive)[1172], Directive (EU) 2016/681 (PNR Directive)[1173] and Directive (EU) 2016/1148 (NIS Directive[1174]) as part of the law of the Isle of Man[1175];

[1168] Commission Decision 2004/411/EC of 28 April 2004 on the adequate protection of personal data in the Isle of Man, OJ L 151, 30.04.2004, p. 48-51.
[1169] Opinion 6/2003 on the level of protection of personal data in the Isle of Man (WP82), available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp82_en.pdf.
[1170] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[1171] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[1172] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.
[1173] Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.
[1174] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
[1175] The Data Protection Act 2018 entered into force on 15 May 2018.

(2) the Data Protection (Application of GDPR) Order 2018[1176] and Data Protection (Application of LED) Order 2018[1177] (Applied GDPR and Applied LED, respectively)[1178], which stipulate that the GDPR and the Law Enforcement Directive apply as part of the law of the Isle of Man, subject to the modifications laid down in those orders; and finally

(3) the GDPR and LED Implementing Regulations 2018 (Implementing Regulations), which provide supplementing provisions for the implementation of both of the above-mentioned orders[1179].

More specifically, the Applied GDPR retains the broad scope of application of the GDPR[1180]. Like the GDPR, the Applied GDPR covers the processing of personal data wholly or partly by automated means, or other processing, if the personal data forms part of a filing system[1181]. Moreover, the GDPR's definitions of 'personal data,' 'processing'[1182], 'pseudonymisation' 'controller' and 'processor' have been retained without modifications in the Applied GDPR. Concerning its territorial scope, the Applied GDPR covers the processing of personal data by controllers or processors established in the Isle of Man[1183], under identical conditions to those set out in Article 3 of the GDPR. It has also been extended to cover the processing of personal data by controllers or processors not established in the Isle of Man, subject to the same

[1176] The Order was amended by Data Protection (application of GDPR) (Amendment) Order 2019 that came into force on 20 November 2019.
[1177] The Order was amended by Data Protection (application of LED) (Amendment) Order 2019 that came into force on 20 November 2019.
[1178] The Applied GDPR and the Applied LED came into force on 16 May 2018.
[1179] The GDPR and LED Implementing Regulations 2018 came into force on 1 August 2018. They were amended by the GDPR and LED Implementing Regulations (Amendment) Regulations 2018 which entered into force on 1 February 2019.
[1180] Like the GDPR, the Applied GDPR does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity (Article 3 Applied GDPR in conjunction with Article 2(2)I GDPR). In addition, the processing of personal data solely for journalistic, artistic, academic and literary purposes is exempt from several provisions of the Applied GDPR and the Implementing Regulations (the data protection principles, legal grounds for processing, the transparency obligations, rights of the data subjects, obligation to notify data breaches and the rules on international transfers). This exception applies, to the extent that the controller reasonably believes that the application of those provisions would be incompatible with such purposes, where the processing is carried out with a view to the publication of journalistic, academic, artistic or literary material and the controller reasonably believes that the publication of the material would be in the public interest (Paragraph 22 of Schedule 9 of the Implementing Regulations). In determining whether an exception to the Applied GDPR and the implementing Regulations would be justified, because the publication of personal data would be in the public interest, the controller must take into account the special importance of the public interest to preserve freedom of expression and information. Moreover, the controller must have regard to any of the codes of practice or guidelines that is relevant to the publication in question (e.g., The Editors' Code of Practice and the National Union of Journalists Code of Conduct.
[1181] Article 3 Applied GDPR in conjunction with Article 2(1) GDPR.
[1182] Article 3 Applied GDPR in conjunction with Article 4(2) Applied GDPR. The Implementing Regulations extend the scope of application of part of the Isle of Man's data protection legislation (See Reg. 19 Implementing Regulation), (including the Applied GDPR, the Applied LED and the Implementing Regulations) to the manual and unstructured processing of personal data held by certain public authorities. Such public authorities are defined in the Freedom of Information Act 2015 and include the Cabinet Office and the government departments, Isle of Man constabulary, Statutory boards (for example Office of Fair Trading, Isle of Man Financial Services Authority, Isle of Man Post Office and Communications Commission), publicly-owned companies (such as Isle of Man Film Ltd and Isle of Man National Transport Ltd), other public authorities (such as Attorney General's Chambers, Clerk of Tynwald and Financial Intelligence Unit) and all local authorities.
[1183] Article 3 and Article 3(2) of Schedule 1 to the Applied GDPR in conjunction with Article 3(1) GDPR.

conditions that are set out in Article 3(2) of the GDPR; thereby strengthening the effectiveness of the Isle of Man data protection regime[1184].

The Data Protection Act 2002 already contained the data protection principles that were set out in the Data Protection Directive. The Applied GDPR retains those principles – namely, the principles of lawfulness and fairness[1185]; transparency[1186]; purpose limitation[1187]; data minimisation, accuracy and storage limitation[1188]; security, integrity and confidentiality[1189] and accountability[1190]. At the same time, it further strengthens several principles by introducing concrete obligations to implement them. In particular, the Applied GDPR introduces the obligation to notify data breaches subject to the same conditions as in the GDPR[1191], and reinforces accountability requirements by establishing obligations such as record keeping, data protection by design and default, data protection impact assessments and data protection officers[1192].

The Applied GDPR also guarantees the same data subject rights as enshrined in the GDPR, i.e., the rights of information, access, rectification, erasure, restriction, objection, and portability[1193]. The provisions establishing these rights have been retained without changes. Concerning the specific rights to object to direct marketing[1194], and not to be subject to automated individual decision-making[1195], Isle of Man law now also fully mirrors the GDPR.

As is the case in the GDPR, the data subject rights in the Isle of Man are subject to certain restrictions[1196] intended to allow the balancing of the data protection interests of individuals

[1184] Article 3 Applied GDPR in conjunction with Article 3(2) GDPR.
[1185] Article 3 Applied GDPR in conjunction with Articles 5(1)(a) and 6(1) GDPR. Reg. 10 of the Implementing Regulations complements Article 6(1)I GDPR by providing that the processing of personal data under Article 6(1)I GDPR includes processing of personal data that is necessary for the administration of justice, the exercise of a function of Tynwald, the exercise of a function conferred on a person by an enactment or the exercise of a function of the Crown, a department or a Statutory Board. With respect to consent (one of the grounds for lawful processing), the Applied GDPR also retains the conditions provided in the Article 7 GDPR, unmodified. In the context of the provision of information society services pursuant to Article 3 Applied GDPR in conjunction with Article 8 GDPR, a child's consent is lawful only when the child is at least 13 years old or, where the child is below that age, the processing is lawful only if that consent is given or authorised by the holder of parental responsibility.
[1186] Article 3 Applied GDPR in conjunction with Articles 13 and 14 GDPR.
[1187] The purpose limitation principle provided in Article 5(1)(b) GDPR has been retained without changes in the Applied GDPR. The conditions on further compatible processing in Article 6(4)(a) – I GDPR have also been retained with no modifications in the Applied GDPR.
[1188] The Applied GDPR does not introduce any changes on the principles of data minimisation, accuracy and storage limitation (as provided in Article 5I – I GDPR).
[1189] Concerning data security, the principle of integrity and confidentiality (Article 5(f) GDPR) is retained in the Applied GDPR without any modifications.
[1190] The principle of accountability provided in Article 5(2) GDPR has been retained in the Applied GDPR without modifications and the same applies to Article 24 on the responsibility of the controller.
[1191] Article 3 Applied GDPR in conjunction with Articles 33 and 34 GDPR.
[1192] Article 3 Applied GDPR in conjunction with Articles 25, 30 35, 36 and 37 – 39 GDPR.
[1193] Article 3 Applied GDPR in conjunction with Articles 13 – 20 GDPR.
[1194] Article 21 GDPR on the data subject's right to object has been retained in the Applied GDPR with no modifications.
[1195] Article 3 Applied GDPR in conjunction with Article 22 GDPR. Reg. 16 of the Implementing Regulations adds that when automated decision-making is required or authorised by law, the controller must, as soon as reasonably practicable, notify the data subject in writing that such a decision has been taken. The data subject has a right to obtain a reconsideration of the decision, or to a new decision not based solely on automated processing.
[1196] The restrictions are set out in Schedule 9 to the Implementing Regulations.

with objectives of general public interest and with the fundamental rights and freedoms of others.

Some of those allow the restriction of individual rights based on the nature of the personal data being processed. They apply automatically whenever one of the listed categories of personal data is being processed. These categories are listed in an exhaustive manner and cover a narrowly construed set of situations, such as data processing for the purpose of assessing a person's suitability for certain specific offices (e.g., judicial appointments or appointment made by the Crown)[1197], the processing of personal data for purposes of providing confidential references[1198] or where personal data consists in marks or other information processed for the purpose of determining the result of an exam[1199]. These categories are not only (very) limited in scope, but also do not typically cover situations where personal data is transferred to the Isle of Man from the EU.

The majority of the restrictions have to be based either on grounds of prejudice or can only be invoked to the extent that the application of a certain right would interfere with a protected interest at stake, i.e., a public interest or the rights and freedoms of others. Restrictions subject to the prejudice test can be invoked only when (and to the extent that) the application of the provisions "would be likely to prejudice" the legitimate aim pursued. For example, controllers can restrict data subject rights to the extent that their application would be likely to prejudice the prevention or detection of crime or the assessment or collection of any tax or duty[1200], or would be likely to prejudice the combat effectiveness of any of the armed forces of the Crown[1201].

The Isle of Man Information Commissioner, as well as the Attorney General's Chambers together with the Cabinet Office, have issued interpretative guidance that clearly frames the application of the exemptions. It clarifies the scope of the different exemptions, including by means of concrete examples, which should help preventing that they are misunderstood and applied in an overly broad manner. It also explains how the requirements of necessity and proportionality should be applied with respect, in general, to the "likely to prejudice" or "to the extent" standard, and for specific exemptions[1202]. Finally, and importantly, the guidance

[1197] Paragraph 11 and 12 of Schedule 9 to the Implementing Regulations.
[1198] Paragraph 17 of Schedule 9 to the Implementing Regulations.
[1199] Paragraph 18 of Schedule 9 to the Implementing Regulations.
[1200] Paragraph 1(1) of Schedule 9 to the Implementing Regulations.
[1201] Paragraph 14 of Schedule 9 to the Implementing Regulations.
[1202] The guidance is available at: https://www.inforights.im/media/1972/appended-restrictions-exemptions.pdf. First, it clarifies that "[…] the general obligation in respect of rights is to facilitate the exercise of those rights" and that "the application of any restriction/exemption must be considered on a case-by-case basis as departure from the general requirements to comply with rights and principle is only to the minimum extent necessary" (pp. 1 and 9). In this context, the type of personal data, the purpose of the processing and any adverse consequences of the application of the exemption on the data subject must be taken into account (p. 9). Second, it clarifies that decisions on restrictions should be taken at a senior level, the reasons for the decisions should be documented and, where appropriate, explained to the data subject (pp. 3 and 9). Third, with respect to the exemptions that apply "to the extent" that their application would be "likely to prejudice" or otherwise interfere with a protected interest, the guidance clarifies that "the determination of the "extent" is a question of fact to be decided in the light of all the circumstances of each specific case". In this respect, the interference with the rights conferred on the data subject must be proportionate to the reality as well as the potential gravity of the public interests involved (see R (on the Application of Lord) v Secretary of State for the Home Department [2003] EWHC 2073). The 'likely to prejudice' test implies that there is a substantial probability (rather than a mere risk) that complying with the provision would noticeably damage" one or more of the protected interests at stake (p. 3). In

explicitly states that it should be read in conjunction with the Guidelines 10/2020 on restrictions under Article 23 of the GDPR that have been issued by the EDPB[1203].

The current Isle of Man regime for special categories of personal data is similar to that of the GDPR. The Applied GDPR recognises as special categories of data all data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic and biometric data, and data concerning a natural person's sex life or sexual orientation. The processing of such data is prohibited unless specific exceptions apply, which correspond to those in the GDPR[1204]. Moreover, the processing of special categories of data is subject to additional requirements, in particular the obligation to appoint a data protection officer in case of large-scale processing[1205] and to conduct a data protection impact assessment[1206]. Finally, the Applied GDPR retains without modification the GDPR's prohibition on automated individual decision-making on the basis of special categories of data[1207].

In the field of international transfers of personal data, the legal framework of the Isle of Man is closely aligned with Chapter V of the GDPR and therefore ensures continuity of protection for the onward transfer of personal data that was originally received from the EU. In particular, the Applied GDPR incorporates Chapter V of the GDPR into the Isle of Man legal framework with certain adaptations to the local context (e.g., by deleting references to binding corporate rules and to procedures before the EDPB)[1208] and is complemented by the Implementing Regulations, which further specify under which conditions international data transfers can take place. Transfers of personal data to third countries or international organisations are prohibited except if the country or international organisation benefits from an adequacy decision, if appropriate safeguards that meet the requirements of Article 46 of the GDPR are in place, or if one of the derogations set out in the Implementing Regulations apply[1209].

With respect to adequacy, the Applied GDPR and Implementing Regulations refer to decisions adopted by the European Commission[1210]. As a result, controllers and processors in the Isle of Man can transfer personal data freely, without having to put in place specific safeguards, to all countries and territories for which the Commission has adopted an adequacy finding. Appropriate safeguards may be provided by a legally binding and enforceable instrument between public authorities or bodies, standard contractual clauses, an approved

---

particular, "the degree of risk must be such that there may be very well be prejudice to those interests even if the risk falls short of being more probable than not" (p. 11).

[1203] https://www.inforights.im/media/1972/appended-restrictions-exemptions.pdf, p. 1.

[1204] Article 3 Applied GDPR in conjunction with Article 9 GDPR. In this respect, the Implementing Regulations (Reg. 12 in conjunction with Schedule 2) further specify in which situations it is possible to rely on the ground that allows the processing of special categories of data for reasons of substantial public interest. This includes where the processing is necessary for the purposes of protecting a natural person from neglect or physical, mental or emotional harm; for an insurance purpose or for the purposes of preventing fraud.

[1205] Article 3 Applied GDPR in conjunction with Article 37(1)I GDPR.

[1206] Article 3 Applied GDPR in conjunction with Article 35(3)(b) e GDPR.

[1207] Article 3 Applied GDPR in conjunction with Article 22(4) GDPR.

[1208] Article 3 Applied GDPR in conjunction with Articles 44 to 49 GDPR.

[1209] Reg. 68 and 69 Implementing Regulations.

[1210] See Article 3 Applied GDPR in conjunction with Article 45 GDPR and the following link: https://inforights.im/organisations/data-protection-law-2018/transfers-to-third-countries.

code of conduct or an approved certification scheme[1211]. The Information Commissioner has so far not issued specific standard contractual clauses but has instead directed controllers and processors to use the standard contractual clauses adopted by the European Commission[1212]. Moreover, subject to prior authorisation by the Information Commissioner, an international transfer can be carried out on the basis of ad hoc contractual clauses or administrative arrangements between public authorities[1213]. Finally, in specific situations (i.e., as an exception to the general rule that an adequacy decision or appropriate safeguards should be in place), data transfers may take place on the basis of one of the grounds listed in the Implementing Regulations[1214]. These 'derogations/exceptions' correspond to those of Article 49 GDPR, while providing for certain specifications as regards the situations in which they may apply[1215].

1.2. Oversight, enforcement and redress

Since the adoption of the adequacy decision, oversight and enforcement of compliance with the Isle of Man data protection law have been strengthened, notably by reinforcing the supervisory authority's independence and by extending its powers.

Oversight and enforcement of the Applied GDPR and the Implementing Regulations are now carried out by the Information Commissioner, whose appointment and powers are governed by the Freedom of Information Act 2015. The Commissioner is explicitly mandated to perform his or her functions and powers independently and, in doing so, not to be subject to the direction of Tynwald (the Isle of Man parliament), its Branches or the Council of Ministers[1216]. The Commissioner is appointed by the Council of Ministers for a term of up to 5 years. Only candidates with appropriate qualifications, skills and competence can be appointed[1217], and the candidate has to be approved by Tynwald[1218]. The Information Commissioner may be removed before the end of his or her term only for very specific reasons set out in law[1219], and the Freedom of Information Act covers cases where the office may become vacant[1220].

[1211] Article 3 Applied GDPR in conjunction with Article 46(2) GDPR.

[1212] https://inforights.im/organisations/data-protection-law-2018/transfers-to-third-countries/.

[1213] According to Reg. 69 Implementing Regulations, in determining whether to authorise a transfer, the Information Commissioner must have regard to factors that include, but are not limited to, any opinions or decisions of the European Data Protection Board under Article 64, 65 or 66 GDPR that appear to the Information Commissioner to be relevant.

[1214] Schedule 10 of the Implementing Regulations.

[1215] For example, para. 1 of Schedule 10 of the Implementing Regulations provides that a transfer may take place where specifically required by a judgment of a court or tribunal having the force of law in the Isle of Man; para. 5 clarifies that a transfer may take place where "necessary for reasons of substantial public interest", which will be considered to be the case if the transfer is permitted or required under an enactment applicable in the Isle of Man; and para. 7 explains that a transfer may take place if necessary to protect the vital interests of an individual, if the data subject is physically or legally incapable of giving consent or has unreasonably withheld consent, or the controller or processor cannot reasonably be expected to obtain the explicit consent.

[1216] Section 53 Freedom of Information Act.

[1217] According to Paragraph 3 of Schedule 2 of the Freedom of Information Act, the Information Commissioner holds office for a term of up to five years and is automatically eligible for re-appointment for a second term of up to 5 years on expiry of the first term. The Commissioner can be further appointed for a third term of up to 5 years if the Council of Ministers is satisfied that it is in the public interest to do so.

[1218] Schedule 2 Freedom of Information Act 2015.

[1219] If the person holding the office of Information Commissioner (1) has not carried out the duties of the office in a competent manner; (2) is incapacitated either mentally or physically from carrying out the duties of the

The functions and powers of the Information Commissioner have been aligned with those of supervisory authorities under the GDPR. In particular, the Information Commissioner may issue enforcement and penalty notices for violations of provisions of the Applied GDPR and Implementing Regulations on data protection principles, lawfulness of processing, transparency and individual rights, obligations for controllers and processors and the rules on international transfers, or for non-compliance with an information notice, an assessment notice or an enforcement notice[1221]. The Information Commissioner also has the power to bring proceedings before a court in respect of a failure to comply with its notices and order compliance[1222]. Certain violations of data protection legislation may also constitute offences and lead to criminal sanctions such as fines, imprisonment, or both[1223]. This would for example be the case when information is altered or erased with the intention of preventing disclosure of information that any person has requested to access, or with the intention of preventing the controller or processor from supplying the information requested by the Information Commissioner[1224].

Avenues for redress for violations of the Applied GDPR and the Implementing Regulations are available to data subjects under the same conditions as those provided by the GDPR[1225]. In essence, data subjects have a right to an effective judicial remedy both before courts and before the Information Commissioner. The Data Protection Tribunal is the competent forum to hear appeals against decisions from the Information Commissioner[1226]. Obtaining judicial redress directly before the Data Protection Tribunal against controllers and processors[1227] is also possible, under the cause of action of breach of statutory duty (i.e., for violations of a data subjects' right).

Taking into account of the size of the territory for which it has jurisdiction, the office of the Information Commissioner has been active in exercising its different functions. For example, in 2021, the Information Commissioner received 112 personal data breach reports and 44

---

office; (3) has neglected to carry out all or any of the duties of the office; (4) has failed to comply with the restrictions on other employment and professional activity; (5) has failed to comply with any term or condition of the appointment; (6) has engaged in conduct incompatible with the office of Information Commissioner; (7) has taken leave of absence not provided for by the terms and conditions of the appointment; or (8) has been convicted of an offence and by reason of that conviction shown himself not to be a fit and proper person to continue to hold the office. See Paragraph 7 of Schedule 2 Freedom of Information Act.

[1220] Namely, if the person holding the office (1) dies; (2) gives the Chief Minister written notice of resignation; (3) accepts nomination to become a member of Tynwald; (4) is compulsorily detained as a patient in a hospital; (5) has a receiver appointed in respect of his or her property; (6) becomes bankrupt or makes a composition or arrangement with his or her creditors; (7) is convicted of an offence involving corruption; or (8) is convicted of an offence and sentenced to custody. See Paragraph 8 of Schedule 2 Freedom of Information Act.

[1221] According to Reg. 112(1) Implementing Regulations, the penalty notice requires the person to pay to the Information Commissioner an amount specified in the notice. In determining whether to give a penalty notice to a person and determining the amount of the penalty, the Information Commissioner must have regard to the matters listed in Article 83(1) and (2) GDPR, that have been retained without modifications in Reg. 112(2) of the Implementing Regulations. Under Reg. 114(1) of the Implementing Regulations, the maximum amount of the penalty that may be imposed by a penalty notice is £1 000 000.

[1222] Reg. 117 Implementing Regulations.

[1223] Reg. 126 to 129 Implementing Regulations.

[1224] Reg. 128 and 129 Implementing Regulations.

[1225] The Applied GDPR retains the rules in Article 77 to 79 GDPR without material modifications.

[1226] According to Reg. 120 of the Implementing Regulations, the Data Protection Tribunal is an independent judicial body established under the provisions of the Data Protection Act 2002 and is maintained under Reg. 119 Implementing Regulations.

[1227] Article 3 Applied GDPR in conjunction with Article 79 GDPR and Reg. 124 of the Implementing Regulations.

complaints, engaged in four investigations and issued three information notices, five reprimands, and three enforcement notices. In 2022, it handled 225 breach reports and 32 complaints, carried out seven investigations and issued two information notices, three warnings, one reprimand, three enforcement notices and one penalty notice[1228].

Moreover, the Information Commissioner has issued several guidance documents for organisations, for instance concerning specific categories of controllers (such as churches, religious organisations or small businesses), specific processing activities (e.g., in the context of cloud computing services), or on specific obligations (e.g., on carrying out data protection impact assessments)[1229]. To facilitate the exercise of rights by individuals, the Information Commissioner has also developed dedicated guidance and template letters (e.g., for submitting access requests)[1230], as well as an online tool for submitting complaints to the Information Commissioner[1231].

2. ACCESS TO AND USE OF PERSONAL DATA TRANSFERRED FROM THE EUROPEAN UNION BY PUBLIC AUTHORITIES IN THE ISLE OF MAN

2.1. General legal framework

The limitations and safeguards that apply to the collection and subsequent use of personal data for purposes of criminal law enforcement and national security follow from the Isle of Man's international obligations in the area of fundamental rights and personal data protection, from the rules that apply to the processing of personal data by the public sector, as well as from specific laws regulating access to data by Isle of Man public authorities.

First, the right to the protection of personal data forms part of the right to respect for private and family life enshrined in the Human Rights Act 2001, which incorporates into Isle of Man law the rights stemming from the European Convention of Human Rights[1232]. According to the Human Rights Act 2001, all actions of public authorities must be in compliance with the Convention[1233], and all primary and subordinate legislation shall be read and given effect in a way that is compatible with the Convention's rights[1234]. Article 8 of the Convention provides that any interference with privacy must be in accordance with the law, in the interests of one of the aims set out in Article 8(2) and proportionate in light of that aim. Article 8 also requires that the interference is "foreseeable", i.e., have a clear, accessible basis in law, and that the law contains appropriate safeguards to prevent abuse.

[1228] See the periodic reports for 2019 to 2023 available at: https://inforights.im/organisations/about-us/functions-of-the-commissioner/compliance-activity/. On the issuing of a penalty notice, see also the Information Commissioner's press statement, available at: https://inforights.im/organisations/latest-news-updates/2022/aug/penalty-imposed-on-manx-care/.

[1229] Available at the following link: https://www.inforights.im/document-library/data-protection-law-2018/?Page=1&.

[1230] https://www.inforights.im/individuals/data-protection/how-to-exercise-your-rights/making-a-subject-access-request/.

[1231] Available at: https://www.inforights.im/complaint-handling/how-to-make-a-complaint-to-the-information-commissioner/data-protection-complaints/.

[1232] The ratification of the European Convention of Human Rights by the United Kingdom has been extended to the Isle of Man since 1953, see Declaration contained in a letter from the Permanent Representative of the United Kingdom, dated 23 October 1953, available at: https://www.coe.int/en/web/conventions/full-list?module=declarations-by-treaty&numSte=005&codeNature=4&codePays=UK.

[1233] Section 6 Human Rights Act 2001.

[1234] Section 3 Human Rights Act 2001.

In addition, in its case law[1235], the European Court of Human Rights has specified that any interference with the right to privacy and data protection should be subject to an effective, independent and impartial oversight system that must be provided for either by a judge or by another independent body[1236] (e.g., an administrative authority or a parliamentary body). Moreover, individuals must be provided with an effective remedy, and the European Court of Human Rights has clarified that the remedy must be offered by an independent and impartial body which has adopted its own rules of procedure, consisting of members that must hold or have held high judicial office or be experienced lawyers, and that there must be no evidential burden to be overcome in order to lodge an application with it. In undertaking its examination of complaints by individuals, the independent and impartial body should have access to all relevant information, including closed materials. Finally, it should have the powers to remedy non-compliance[1237].

Second, the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) applies to the Isle of Man by virtue of the United Kingdom's membership to this convention[1238]. Article 9 of Convention 108 provides that derogations from the general data protection principles (Article 5 Quality of data), the rules governing special categories of data (Article 6 Special categories of data) and data subject rights (Article 8 Additional safeguards to the data subject) are only permissible when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences, or for protecting the data subject or the rights and freedoms of others.

Therefore, through adherence to the European Convention of Human Rights and submission to the jurisdiction of the European Court of Human Rights, the Isle of Man is subject to a number of obligations, enshrined in international law, that frame its system of government access on the basis of principles, safeguards and individual rights similar to those guaranteed under EU law and applicable to the Member States.

Third, the processing of personal data by criminal law enforcement authorities in the Isle of Man is subject to the rules of the Applied LED, which essentially replicates the Law Enforcement Directive. The material scope of the Applied LED is identical to the one of the Law Enforcement Directive. It applies to the processing of personal data by competent authorities[1239] for the purposes of the prevention, investigation, detection or prosecution of

[1235] According to Section 2(1)(a) Human Rights Act 2001, a court or tribunal determining a question which has arisen under this Act in connection with a Convention right must take into account any judgment, decision, declaration or advisory opinion of the European Court of Human Rights.
[1236] European Court of Human Rights, Klass and others v. Germany, Application no. 5029/71, paragraphs 17-51.
[1237] European Court of Human Rights, Kennedy v. the United Kingdom, Application no. 26839/05, (Kennedy), paragraphs 167 and 190.
[1238] See Declaration contained in a letter from the Permanent Representative of the United Kingdom, dated 13 January 1993, registered at the Secretariat General on 21 January 1993, available at: https://www.coe.int/en/web/conventions/full-list?module=declarations-by-treaty&numSte=108&codeNature=0.
[1239] Competent authorities in the Isle of Man are listed in Schedule 1 to the Implementing Regulations and include the Chief Constable of the Isle of Man Constabulary and any other police force established by the Department of Home Affairs pursuant to section 1 of the Police Act 1993, and the Financial Intelligence Unit established pursuant to the Financial Intelligence Unit Act 2016. Moreover, Regulation 28 of the Implementing Regulations extends the LED's scope to any other person, to the extent that the person has statutory functions for any of the law enforcement purposes.

criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security[1240]. Furthermore, the data protection principles of lawfulness and fairness, purpose limitation, data minimisation, accuracy, storage limitation and security are retained in the Applied LED in the exact same terms as in the LED[1241]. In essence, the processing of personal data by a competent authority is only permitted when necessary for a law enforcement purpose, and only in accordance with a law specifying at least the objectives of the processing, the personal data to be processed, and the purposes of the processing[1242]. In addition, the Applied LED imposes specific transparency obligations[1243] and recognises the same data subject rights as the Law Enforcement Directive without any modifications[1244]. In particular, data subjects enjoy a right to access[1245], correction[1246] and deletion[1247] and have the right not to be subject to automated decision-making[1248]. Competent authorities are also required to implement data protection by design and default[1249], to keep records of processing activities[1250], and, for certain processing operations, to carry out data protection impact assessments and to pre-consult the Information Commissioner[1251]. Moreover, they are required to put in place appropriate measures to ensure security of processing[1252] and are subject to specific obligations in case of a data breach, including notification of such breaches to the Information Commissioner and data subjects[1253]. Like in the Law Enforcement Directive, there is also a requirement for a controller (unless it is a court or other judicial authority acting in a judicial capacity) to designate a data protection officer who assists the controller in complying with its obligations as well as monitoring that compliance[1254]. Finally, the Applied LED contains specific provisions on international

[1240] Article 1(1) Applied LED; Regulation 29 and 27 Implementing Regulation.
[1241] Article 4(1) Applied LED.
[1242] Article 8 Applied LED. Pursuant to Article 10 Applied LED, stricter conditions apply to the processing of special category data and it is permitted only where it is strictly necessary and the processing is authorised by the law of the Island, the processing is for the purpose of protecting the vital interests of the data subject or of another natural person or the processing relates to data which are manifestly made public by the data subject. Additional conditions are set out in the Schedule 12 (e.g., the information was made public by the data subject; processing is necessary for the purposes of preventing fraud, processing is necessary when a court or other judicial authority is acting in its judicial capacity; legal proceedings; obtaining legal advice; etc.).
[1243] Article 13 Applied LED.
[1244] Similarly to Article 12 Law Enforcement Directive, Regulation 41 of the Implementing Regulations further specifies the modalities for exercising these rights, allowing competent authority to charge a reasonable fee or refuse to comply with a request from an individual if the request is manifestly unfounded or excessive, in particular because of its repetitive character. Moreover, pursuant to Regulations 44 and 45(6) Implementing Regulations, the Isle of Man Council of Ministers can by regulations (which require Tynwald approval) restrict, wholly or partly, the data subject's rights of access and the controllers obligation to inform the data subject in writing about any refusal of the right to rectification or erasure, "to the extent that, and for so long as such a partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned, in order to (1) avoid obstructing official or legal inquiries, investigations or procedures; (2) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties; (3) protect public security; (4) protect national security; or (5) protect the rights and freedoms of others." To date, no such regulations have been adopted.
[1245] Article 14 Applied LED.
[1246] Article 16(1) Applied LED.
[1247] Article 16(2) Applied LED.
[1248] Article 11 Applied LED.
[1249] Article 20 Applied LED.
[1250] Article 24 Applied LED.
[1251] Articles 27 and 28 Applied LED.
[1252] Article 29 Applied LED.
[1253] Articles 30 and 31 Applied LED.
[1254] Article 32 Applied LED.

transfers of personal data to a third country or an international organisation[1255]. The provisions substantially echo those in the Law Enforcement Directive. Essentially, transfers are prohibited unless the receiving country benefits from an adequacy decision by the European Commission, or if appropriate safeguards are in place[1256]. Transfers are still possible in the absence of an adequacy decision or appropriate safeguards, but only in specific circumstances listed in an exhaustive manner and identical to those set forth in the LED[1257].

Under identical conditions as under the Law Enforcement Directive, the Implementing Regulations specify that certain specific provisions of the Applied LED[1258] may be restricted to the extent that the application of those provisions would be likely to prejudice any of the matters mentioned in Article 1(1) of the Applied LED (i.e., the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security)[1259].

The Isle of Man Information Commissioner and the Attorney General's Chambers and Cabinet Office have clarified through guidance how the law enforcement exemption functions in practice[1260]. Importantly, the guidance stresses that the exemptions must not be applied in a blanket manner, but "on a case-by-case basis", i.e., where necessary and proportionate for law enforcement purposes in light of all the circumstances of the specific case. Finally, in the absence of specific judicial authority in the Isle of Man, the guidance refers to the case law of the High Court of England and Wales where it has been held that the term "likely" connotes a degree of probability where there is a very significant and weighty chance of prejudice to the identified public interests[1261].

The processing of personal data for national security purposes in the Isle of Man is subject to the provisions of the Applied GDPR and the Implementing Regulations that are described in section 1 above[1262]. At the same time, Regulation 22 of the Implementing Regulations

[1255] Articles 35 to 39 Applied LED.
[1256] Regulation 72 of the Implementation Regulations provides that appropriate safeguards are in place where provided by a legally binding instrument, or where the controller, having assessed all the circumstances surrounding transfers of personal data, concludes that appropriate safeguards exist to protect the data.
[1257] Regulation 73 sets out the derogations for specific situations in which international transfers can take place in the absence of an adequacy decision or of appropriate safeguards, that is for the protection of the vital interests of individuals, to safeguard the legitimate interests of the data subject, to prevent an immediate and serious threat to public security, in individual cases for a law enforcement purpose, and in an individual case for the establishment, exercise or defence of legal claims relating to any law enforcement purpose.
[1258] The provisions that can be restricted are the following: (1) Article 4(1)(a), except to the extent to which the processing requires compliance with Article 8 Applied LED; (2) Article 13 and regulation 42 (information to be made available or given to the data subject); (3) Article 14 and regulation 43 (right of access by the data subject); (4) Article 16 and regulation 45 (right to rectification or erasure and restriction of processing); (5) Article 18 and regulation 47 (rights of the data subject in criminal investigations and proceedings).
[1259] Paragraph 30, Part 8 of Schedule 9 Implementing Regulations. When invoking an exemption to the right of access, the controller is required to document the factual or legal reasons on which the decision to rely on the exemption was based, and to make that information available to the Manx Information Commissioner, see Paragraph 30(3) of Schedule 9 Implementing Regulations.
[1260] Information Commissioner's Guidance on "Exemptions from certain provisions," Appendix "Further guidance produced by the Attorney General's Chamber's and Isle of Man Cabinet Office," available at: https://www.inforights.im/media/1972/appended-restrictions-exemptions.pdf.
[1261] Information Commissioner's Guidance on "Exemptions from certain provisions," Appendix "Further guidance produced by the Attorney General's Chamber's and Isle of Man Cabinet Office," pp. 16-18.
[1262] Compared to the GDPR, the scope of the Applied GDPR has been modified by omitting the exclusions in Article 2(2)(a) GDPR (processing in the course of activities which fall outside the scope of Union law) and

provides for an exemption from specified provisions of the Applied GDPR and the Implementing Regulations[1263] when such exemption is required for the purpose of safeguarding national security or for defence purposes. The application of this exemption has been clarified through detailed guidance by the Isle of Man Information Commissioner and the Attorney General's Chambers and Cabinet Office[1264]. In particular, relying on the exemption must be necessary and proportionate in a democratic society. The exemption cannot be invoked in a blanket manner but can be relied upon only the basis of a case-by-case analysis and considering the actual consequences of applying the relevant provision of the Applied GDPR. Controllers must be able to show that there is a real possibility of an adverse effect on national security if the relevant provision is applied. All decisions to rely on an exemption have to be documented and controllers must be prepared to share that documentation with the Information Commissioner[1265].

Moreover, according to Regulation 23 of the Implementing Regulations, controllers may apply for a certificate signed by the Chief Minister which certifies that the restriction of the specific provisions listed under Regulation 22 is required to the protection of national security. It is important to note that the national security certificates do not provide for an additional ground for restricting data protection rights for national security reasons. In other words, the controller or processor can only rely on a certificate when it has concluded it is necessary to rely on the national security exemption which, as explained above, must be applied on a case-by-case basis[1266]. Even if a national security certificate applies to the matter in question, the Isle of Man Information Commissioner can investigate whether or not reliance on the national security exemption was justified in a specific case[1267].

Any person directly affected by the issuing of the certificate may appeal to the Isle of Man Data Protection Tribunal[1268] against the certificate[1269] or, where the certificate identifies data

---

Article 2(2)(b) GDPR (processing by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU).

[1263] According to Regulation 22 Implementing Regulations, the application of the following provisions may be restricted: (1) Chapter II Applied GDPR (data protection principles), except the principle of lawfulness and the legal grounds for the processing under Article 6 (lawfulness of processing) and Article 9 (processing of special category data); (2) Chapter III Applied GDPR (rights of data subjects); (3) in Chapter IV Applied GDPR Article 33 (notification of personal data breach to the Information Commissioner) and Article 34 (communication of personal data breach to the data subject); (4) Chapter V Applied GDPR (transfers of personal data to third countries of international organisations); (5) in Chapter VI Applied GDPR Article 57(1)(a) and (6) (Information Commissioner's duties to monitor and enforce the Applied GDPR and to conduct investigations) and Article 58 (investigative, corrective, authorisation and advisory powers of Information Commissioner); (7) Chapter VIII Applied GDPR (remedies, liabilities and penalties) except for Article 83 (general conditions for imposing administrative fines) and Article 84 (penalties); (8) in Part 6 Implementation Regulation, regulation 84 (general functions of the Information Commissioner), paragraphs (3) and (8); and regulation 84, paragraph (9), so far as it relates to Article 58(2)(i) Applied GDPR.

[1264] Information Commissioner's Guidance on "Exemptions from certain provisions," Appendix "Further guidance produced by the Attorney General's Chamber's and Isle of Man Cabinet Office".

[1265] Information Commissioner's Guidance on "Exemptions from certain provisions," Appendix "Further guidance produced by the Attorney General's Chamber's and Isle of Man Cabinet Office," pp. 9 and 13-15.

[1266] Information Commissioner's Guidance on "Exemptions from certain provisions," Appendix "Further guidance produced by the Attorney General's Chamber's and Isle of Man Cabinet Office," pp. 15-16.

[1267] Article 5(2) Applied GDPR requires the controller to be in a position to demonstrate that it has complied with the DPA 2018. This implies that an intelligence service would need to demonstrate to the ICO that when relying on the exemption, it has considered the specific circumstances of the case.

[1268] In accordance with Regulation 119 of the Implementing Regulations, there continues to be an Isle of Man Data Protection Tribunal which consists of a chairperson and two other members, appointed in accordance with the Tribunals Act 2006.

by means of a general description, challenge the application of the certificate to specific data[1270]. The tribunal will review the decision to issue a certificate and decide whether there were reasonable grounds for issuing the certificate. It can consider a wide range of issues, including necessity, proportionality and lawfulness, having regard to the impact on the rights of data subjects and balancing the need to safeguard national security. As a result, the tribunal can quash the certificate or determine that the certificate does not apply to specific personal data which is the subject of the appeal[1271].

It follows from the above that limitations and conditions are in place under the applicable Isle of Man legal provisions, as interpreted by the Isle of Man government and the Isle of Man Information Commissioner, to ensure that these exemptions and restrictions remain within the boundaries of what is necessary and proportionate to protect criminal law enforcement and national security.

2.2. Access and use by Isle of Man public authorities for criminal law enforcement purposes

In the Isle of Man, criminal law enforcement functions are carried out by the police force, officially called the Isle of Man Constabulary, which is headed by the Chief Constable. In the specific case of financial crime, the responsible authority is the Financial Intelligence Unit (FIU)[1272]. The law of the Isle of Man imposes a number of limitations on the access to and use of personal data for criminal law enforcement purposes, and it provides oversight and redress mechanisms in this area. The conditions under which access to personal data can take place and the safeguards applicable to the use of these powers are assessed in the following sections.

2.2.1. Legal bases and applicable limitations/safeguards

Personal data transferred under the adequacy decision and processed by organisations in the Isle of Man may be obtained by Isle of Man criminal law enforcement authorities by means of investigative measures under the Police Powers and Procedures Act 1998, on the basis of the Interception of Communications Act 1988, or on the basis of anti-money laundering and anti-terrorist (financing) legislation, including through (voluntary) disclosures.

The Police Powers and Procedures Act 1998 (PPP Act) provides the Isle of Man police with a legal basis for accessing personal data held by commercial operators through searches and seizures. The PPA Act lays down detailed rules on the scope and application of these measures, aimed at ensuring that the interference with the rights of individuals will be limited to what is necessary for a specific criminal investigation and proportionate to the pursued purpose. Searches and seizures may only take place on the basis of a court-issued search

[1269] Regulation 23(3) Implementing Regulations.
[1270] Regulation 23(5) Implementing Regulations.
[1271] Regulation 23(4) and (7) Implementing Regulations.
[1272] The Financial Intelligence Unit is an autonomous agency in the Isle of Man competent for gathering financial intelligence on the Isle of Man. More specifically, the FIU is responsible for (1) receiving, gathering, analysing, storing and sharing information about financial crime (whether in the Island or elsewhere); (2) assisting with the prevention and detection of crime, and in particular, financial crime; (3) cooperating with law enforcement agencies; and (4) contributing to the reduction of crime, and in particular, financial crime and to the mitigation of its consequences, see Section 5 FIUA.

warrant[1273] and the issuing of such warrant is subject to specific procedural and substantive requirements.

More specifically, a police officer must apply for a search warrant to a Justice of the Peace[1274]. An application for a warrant must set out the grounds for the application, the legal basis for issuing the warrant and, as far as practicable, the persons and premises[1275] to be searched[1276]. In case the application would request authorisation for more than one search entry, it should also indicate the maximum number of entries desired[1277].

A search warrant may be issued only if the Justice of the Peace is satisfied that: (1) a serious offence[1278] has been committed and there is material on the premises to be searched which is likely to be of substantial value to the investigation of the offence, or a person has in his possession any property in respect of which an offence has been committed; (2) the material or the property is likely to be relevant evidence; and (3) it does not consist of excluded material or items subject to legal privilege[1279].

In terms of formal requirements, the warrant must specify the name of the person who applies for it, the date of issuance, the enactment under which it is issued, and the particular premises to be searched, or (in the case of an all-premises warrant) the person who is in occupation or control of the premises to be searched, together with any premises under that person's

[1273] Pursuant to Sections 20 and 21 PPP Act, warrantless searches may only take place in exceptional circumstances that do not appear relevant in the context of data transfers covered by an adequacy decision adopted under the GDPR. In particular, a police officer may search premises for the purpose of (1) executing a warrant of arrest or a warrant of commitment; (2) arresting a person for an offence triable on information; (3) recapturing any person who is unlawfully at large and whom he is pursuing; or (4) saving life or limb or preventing serious damage to property. In addition, a warrantless search may take place of any premises occupied or controlled by a person under arrest, if the police officer has reasonable grounds to suspect that there is evidence, other than items subject to legal privilege, on the premises that relates to that offence, or a connected/similar offence.

[1274] In the Manx justice system, 'Justices of the Peace' are magistrates, appointed by the Lieutenant Governor on behalf of the Crown, who have judicial powers in the Isle of Man Courts.

[1275] The warrant can apply to one or more sets of premises occupied or controlled by a person specified in the application (specific premises warrant) or any premises occupied or controlled by a person specified in the application (all premises warrant). If the application is for an all premises warrant, it must specify (1) as many sets of premises desired to enter and search as it is reasonably practicable to specify; (2) the person who is in occupation or control of those premises; (3) why it is necessary to search more premises; and (4) why it is not reasonably practicable to specify all the premises desired to enter and search. The Justice of the Peace must also be satisfied that, because of the particulars of the offence, there are reasonable grounds for believing that it is necessary to search premises occupied or controlled by the person in question and not specified in the application in order to find the material sought, and that it is not reasonably practicable to specify in the application all the premises that might need to be searched.

[1276] Section 18(2) PPP Act.

[1277] The warrant may authorise entry to and search of premises more than once if the Justice of the Peace is satisfied that it is necessary to authorise multiple entries in order to achieve the purpose for which the warrant is issued. If it authorises multiple entries, the number of entries authorised may be unlimited or limited to a maximum (sections 1C and 1D PPP Act).

[1278] Serious offences are defined in Section 79 PPP Act in conjunction with Schedule 3 to the PPP Act and include offences such as treason, murder, manslaughter, rape, possession of firearms with intent to injure etc.

[1279] Section 11(1) PPP Act. In addition, pursuant to Section 11(3) PPP Act, one of the following conditions must be met in relation to each set of premises specified in the application: (1) it is not practicable to communicate with any person entitled to grant entry to the premises; (2) it is practicable to communicate with a person entitled to grant entry to the premises but it is not practicable to communicate with any person entitled to grant access to the evidence; (3) entry to the premises will not be granted unless a warrant is produced; or (4) the purpose of a search may be frustrated or seriously prejudiced unless a police officer arriving at the premises can secure immediate entry to them.

occupation or control that can be specified and that are to be searched. The warrant must also identify, as far as it is practicable, the articles or persons to be sought[1280].

According to Section 22 PPP Act, a police officer who is lawfully on any premises may furthermore seize anything at those premises, including any information which is stored in electronic form[1281], if he has reasonable grounds for believing[1282] that it has been obtained in consequence of the commission of an offence or that the item is evidence in relation to an offence which he is investigating or any other offence, and that it is necessary to seize it in order to prevent it being concealed, lost, damaged, altered or destroyed[1283].

Importantly, the Isle of Man Department of Home Affairs has adopted a code of practice for searches and the seizure and treatment of property by police officers which sets out additional limitations and safeguards[1284]. The Code notably stresses that "[t]he right to privacy and respect for personal property are key principles of the Human Rights Act 2001. Powers of entry, search and seizure should be fully and clearly justified before use because they may significantly interfere with the occupier's privacy. Officers should consider if the necessary objectives can be met by less intrusive means. Powers to search and seize must be used fairly, responsibly, with respect for people who occupy premises being searched or are in charge of property being seized and without unlawful discrimination"[1285]. The Code also specifies in more detail the requirements for making an application for a search warrant, in particular the need to check the accuracy of information on which an application for a search warrant is based[1286].

Specific limitations and safeguards also apply to the interception of communication in the course of transmission by post, by means of a courier service or a public telecommunication system[1287]. The interception of communications is regulated in the Interception of

[1280] Section 18(6) PPP Act.

[1281] The police officer may require that information to be produced in a form in which it can be taken away and in which it is visible and legible or from which it can readily be produced in a visible and legible form, see Section 22(4) PPP Act.

[1282] On the interpretation of the 'reasonable grounds to believe' test, Manx courts are likely to follow English precedent in the absence of case law from Manx courts. Under English case law, the test is understood to require suspicion (rather than proof). See R H and ors (minors) [1996] 1 All ER 1 at pages 20 (para f) to 21 (para a), per Lord Nicholls.

[1283] According to Section 24 PPP Act, the police officer who seizes anything must, if requested by the occupier of premises, provide in reasonable time that person with a record of what he has seized. The police officer must also grant access to or supply a photograph or a copy of the seized or retained item at the request of the person who had custody of the item before it was seized. Pursuant to Section 25 PPP Act, anything that has been seized by the police officer may be retained as long as is necessary in all the circumstances.

[1284] The legal basis and value of the Code of Practice are set out in Sections 75 and 76 PPP Act. Pursuant to these provisions, the Code of Practice has to be approved by Tynwald. A police officer shall be liable to disciplinary proceedings for a failure to comply with any provision of the code and the code shall be admissible as evidence in all criminal and civil proceedings The current Police Powers and Procedures Code is set out in the Police Powers and Procedures Codes Order 2014 [SD 2014/0363], available at: https://www.tynwald.org.im/links/tls/SD/2014/2014-SD-0363.pdf.

[1285] Police Powers and Procedures Code, Code B, paragraphs 1.3 and 1.3A.

[1286] Police Powers and Procedures Code, Code B, paragraph 3.1 et seq.

[1287] Pursuant to the IOCA, 'public telecommunication system' has the same meaning as in the Telecommunications Act 1984. Section 2(1) of the Telecommunications Act 1984 defines 'telecommunication system' as a system for the conveyance, through the agency of electric, magnetic, electro-magnetic, electro-chemical or electro-mechanical energy, of (1) speech, music and other sounds; (2) visual images; (3) signals serving for the impartation (whether as between persons and persons, things and things or persons and things) of any matter otherwise than in the form of sounds or visual images; or (4) signals serving for the actuation or

Communications Act 1988 (IOCA). Section 1 IOCA introduces a general principle of confidentiality of communications by providing that it is an offence to intentionally intercept communications. Section 1 further clarifies that to be lawful, any interception of communications must be authorised by a warrant issued by the Chief Minister under section 2 IOCA[1288]. The Chief Minister can only issue a warrant if s/he considers that the warrant is necessary in the interests of national security or for the purpose of preventing or detecting serious crime[1289]. Importantly, in considering the necessity of a warrant, the Chief Minister must assess whether the information sought to be obtained could reasonably be acquired by other, less intrusive means[1290]. Before issuing or renewing a warrant the Chief Minister is required to consult the Attorney General, i.e., obtain legal advice from the Government's principal legal adviser on whether the conditions for issuing a warrant are fulfilled.

As the further conditions, limitations and safeguards that apply to the issuing of interception warrants are identical for interception carried out for law enforcement and for national security purposes, they are addressed in detail in the section on access and use of personal data by Isle of Man public authorities for national security purposes.

In the Isle of Man, criminal law enforcement authorities can also obtain personal data from business organisations in the context of financial and asset recovery investigations. These powers are governed by the Proceeds of Crime Act 2008 (POCA) which covers confiscation investigations[1291], money laundering investigations[1292], civil recovery investigations[1293], and detained cash investigations[1294]. During such investigations, police officers[1295] may request a Deemster[1296] to issue several types of orders: production orders[1297], search and seizure

---

control of machinery or apparatus .In accordance with Section 7 of the Telecommunications Act 1984, public telecommunication systems are telecommunication systems the running of which is authorised by a licence and which have been designated as a public telecommunication system by order of the Council of Ministers.

[1288] Interception without warrant is only lawful in specific limited circumstances, i.e., when intercepting with the consent of the sender or recipient (Section 1(2)(b) IOCA) and in case of limited administrative and enforcement purposes (Section 1(3)(a) and (b) IOCA).

[1289] Section 2(2) IOCA. The notion of 'serious crime' is defined in Section 33(4) of the Regulation of Surveillance Act 2006 as covering conduct for which a person who has attained the age of twenty-one and has no previous convictions could reasonably be expected to be sentenced to custody for a term of 3 years or more, or conduct which involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose.

[1290] Section 2(3) IOCA. See also Report of the Interception of Communications Commissioner for the year that ended on 31st December 2018, available at: https://www.gov.im/media/1367579/ioc-commissioners-report-for-the-year-ended-31122018-gd2019-0020.pdf.

[1291] Under Section 159(1) POCA, a confiscation investigation is an investigation into whether a person has benefited from his or her criminal conduct, or the extent or whereabouts of the benefit from his or her criminal conduct.

[1292] Under Section 159(5) POCA, a money laundering investigation is an investigation into whether a person has committed a money laundering offence or an ancillary money laundering offence.

[1293] Under Section 159(2) POCA, a civil recovery investigation is an investigation into whether property is recoverable property or associated property, who holds the property, or its extent or whereabouts.

[1294] Under Section 159(4) POCA, a detained cash investigation is an investigation for the purposes of recovery of cash (under Chapter 3 Part 1 POCA) into the derivation of cash detained or a part of such cash, or whether cash detained, or a part of such cash, is intended to be used in unlawful conduct.

[1295] Police officers are not the only persons able to request such orders and warrants. Under Sections 169(5) and 170(12) POCA, an appropriate person is (1) a police officer or a customs officer, if the warrant is sought for the purposes of a confiscation investigation or a money laundering investigation; (2) a person authorised by the Attorney General, if the warrant is sought for the purposes of a civil recovery investigation; or (3) a police officer or a customs officer, if the warrant is sought for the purposes of a detained cash investigation.

[1296] Deemsters are full-time judges on the Isle of Man.

warrants[1298], disclosure orders[1299], customer information orders[1300], and account monitoring orders[1301]. Each type of order is subject to strict formal and substantial requirements. In essence, the scope of such orders is always limited to one individual or one set of premises, they must contain specific mandatory information, and they may only be issued for limited purposes. For example, search and seizure warrants must specify the subject of the investigation (a person or property), they must state that the order is sought for the purposes of the investigation and in relation to material specified in the application, and that the person specified in the application appears to be in possession or control of that material[1302]. Then, a Deemster may only issue the order if there are reasonable grounds to believe or suspect[1303] that there is related material specified in the warrant[1304] on the premises[1305], and that, for instance, in the case of a money laundering investigation, the person specified in the application has committed a money laundering offence or an ancillary money laundering offence[1306].

The Anti-Terrorism and Crime Act 2003 (ATCA) provides the Isle of Man police with specific powers to obtain information in the course of terrorism investigations, including by conducting searches and seizures, by obtaining customer information and through account monitoring orders. These powers can generally be exercised only on the basis of a search warrant issued by a Justice of the Peace under similar procedural and substantive conditions as regular warrants[1307]. However, in the specific context of anti-terrorism, warrantless searches are allowed on the basis of a written order from a police officer of at least the rank of chief inspector, but only in case of serious emergency requiring immediate action[1308].

[1297] Sections 162 – 168 POCA. Production orders require a specified person to produce material in their possession or control or give access to that material within the period stated in the order.
[1298] Sections 169 – 173 POCA. Search and seizure warrants are used to obtain that material where a production order is not available, or not complied with.
[1299] Sections 174 – 179 POCA. Disclosure orders require a specified person to answer questions, provide specified information, and/or produce specified documents.
[1300] Sections 180 – 186 POCA. Customer information orders require a financial institution to provide customer information in relation to persons specified in the order.
[1301] Sections 187 – 192 POCA. Account monitoring orders require a financial institution to provide specified account information for a specified period.
[1302] Section 169(2) and (3) POCA.
[1303] The tests of reasonable ground to 'believe' or 'suspect' are synonymous and used interchangeably, both are considered language of suspicion. See R H and ors (minors) [1996] 1 All ER 1 at pages 20 (para. f) to 21 (para. a), per Lord Nicholls.
[1304] Section 170(6) – (10) POCA.
[1305] Section 169(3) POCA.
[1306] Sections 169(6) and 170 POCA.
[1307] Part V and Schedule 5 to ATCA. Such a warrant authorises a police officer to enter the premises covered by the warrant, to search the premises and any person found there, and to seize and retain any relevant material, which is found on a search. The warrant does not authorize the seizure and retention of items subject to legal privilege. A Justice of the Peace may issue a warrant only if satisfied (1) that the warrant is sought for the purposes of a terrorist investigation; (2) that there are reasonable grounds for believing that there is material on the premises to which the application relates which is likely to be of substantial value, whether by itself or together with other material, to a terrorist investigation and which does not consist of or include excluded material, items subject to legal privilege, or special procedure material; (3) that the issue of a warrant is likely to be necessary in the circumstances of the case; and (4) in the case of an application for an all premises warrant, that it is not reasonably practicable to specify in the application all the premises which the person specified occupies or controls and which might need to be searched. Under sub-paragraph 3 of Schedule 5 to ATCA, the material is relevant if the police officer has reasonable grounds for believing that (1) it is likely to be of substantial value, whether by itself or together with other material, to a terrorist investigation, and (2) it must be seized in order to prevent it from being concealed, lost, damaged, altered or destroyed.
[1308] Paragraph 14 of Schedule 5 to the ATCA.

Furthermore, a police officer, or a person authorised in writing by the Attorney General, may also request account monitoring orders to a High Court judge[1309]. Such an order may not exceed 90 days[1310], is subject to formal requirements[1311], and may only be issued if the tracing of the terrorist property is desirable for the purposes of the investigation and will enhance its effectiveness[1312]. Lastly, the police also have the power to obtain customer information orders[1313]. Such orders may be issued by a High Court judge under the same conditions as an account monitoring order[1314].

Finally, criminal law enforcement authorities in the Isle of Man, including the FIU, may obtain personal data through (voluntary) disclosure by private individuals, business organisations or public authorities.

In terms of disclosures to the FIU, Sections 142 – 144 POCA introduce an obligation to disclose information related to suspected money laundering when a person obtained that information in the course of a business in the so-called regulated sector[1315]. Section 14 ACTA similarly imposes a duty on the regulated sector to disclose information where there are reasonable grounds for knowing or suspecting that another person has committed an offence related to financing of terrorism[1316]. Section 11 of the ACTA requires any other person that believes or suspects, based on information which comes to his or her attention in the course of a business or employment, that another person has committed an offence related to the financing of terrorism, to disclose this suspicion, and the information on which it is based. According to Section 12 ACTA, any person may disclose to the FIU a suspicion or belief that any money or other property is terrorist property (or is derived from terrorist property), as well as any matter on which the suspicion or belief is based. Pursuant to the Financial Intelligence Unit Act 2016 (FIUA), any person may disclose information if the disclosure is made for the purposes of the exercise of any functions of the FIU[1317]. The FIU then has the power to request additional information from certain entities or individuals[1318], but only when it reasonably considers that, for the proper fulfilment of any of its functions, it is necessary or expedient to seek additional information from the person in question[1319].

In terms of disclosures to the Isle of Man police, Section 26 ACTA imposes a duty on any person to disclose specific information which he or she knows or believes to be of material

[1309] Schedule 4 to the ATCA.
[1310] Paragraph 2(5) of Schedule 4 to the ATCA.
[1311] According to Paragraph 2(2) of Schedule 4 to the ATCA, the application for an account monitoring order must state that the order is sought against the financial institution specified in the application and in relation to information related to an account or accounts held at the institution by the person specified in the application. According to paragraph 2(3), the application for an account monitoring order may specify information relating to all accounts held by the person specified in the application at the specified financial institution, particular descriptions of accounts held, or particular accounts.
[1312] Paragraph 2(1) of Schedule 4 to the ATCA.
[1313] Schedule 6 to the ATCA.
[1314] Paragraph 5 of Schedule 6 to the ATCA.
[1315] The regulated sector is defined in paragraph 2 of Schedule 4 to the POCA and includes financial services, insurance businesses, collective investment schemes, an administrator or trustee of a retirement benefits scheme, external accountants, tax advisers, payroll agents; etc.
[1316] These include fund-raising, use of money or other property and facilitating funding for the purposes of terrorism, and money laundering related to terrorist property (Sections 7-10 ACTA).
[1317] Section 24(1) FIUA.
[1318] Section 18 FIUA.
[1319] Section 18(1)(b) FIUA.

assistance in preventing the commission of an act of terrorism, or in securing the apprehension, prosecution or conviction of another person, in the Isle of Man, for an offence involving the commission, preparation or instigation of an act of terrorism. In addition, Section 56 ACTA provides that public authorities may (voluntarily) disclose certain information obtained under other Isle of Man legislation[1320]. In that case, no disclosure of information can be made unless the public authority is satisfied that making the disclosure is proportionate to what is sought to be achieved by it[1321].

Importantly, any disclosure of personal data on the basis of the abovementioned provisions has to comply with the Applied GDPR and the Implementing Regulations, and the further processing by criminal law enforcement authorities of personal data obtained through such disclosures is subject to the provisions of the Applied LED and the Implementing Regulations.

2.2.2. Further use of the information collected

The further use of data collected by Isle of Man criminal law enforcement authorities on one of the grounds referred to in Section 2.1.1, as well as the sharing of such data with a different authority for purposes other than the ones for which it was originally collected (so-called 'onward sharing'), is subject to safeguards and limitations.

First, the processing of personal data by law enforcement authorities in the Isle of Man is governed by the provisions of the Applied LED and the Implementing Regulations as described in section 2.1. With respect to onward sharing, Article 4(2) of the Applied LED, like the LED, allows that personal data collected for a law enforcement purpose may be further processed (whether by the original controller or by another controller) for any other law enforcement purpose, provided that the controller is authorised by law to process data for the other purpose and the processing is necessary and proportionate to that purpose. In this case, all the safeguards provided by the Applied LED, the Applied GDPR and the Implementing Regulations (referred to in section 2.1) apply to the processing carried out by the receiving authority.

Second, the different laws that allow for data collection by criminal law enforcement authorities in the Isle of Man impose specific limitations and safeguards as to the use and further dissemination of the information obtained in exercising the powers they grant.

As regards the powers of search and seizure under the PPP Act, the police officer who seizes anything must, if requested by the occupier of premises, provide in reasonable time that person with a record of what he has seized. The police officer must also grant access to or supply a photograph or a copy of the seized or retained item at the request of the person who

[1320] See Schedule 10, which lists the information (obtained on the basis of other laws) that may be disclosed. This includes e.g., information obtained under the Telecommunications Act, Police Act, Consumer Protection Act, etc. Information can be disclosed for the purpose of (1) any criminal investigation which is being or may be carried out, whether in the Isle of Man or elsewhere; (2) criminal proceedings which have been or may be initiated, whether in the Isle of Man or elsewhere; (3) the initiation or bringing to an end of any such investigation or proceedings; or for (4) facilitating a determination of whether any such investigation or proceedings should be initiated or brought to an end.
[1321] Section 56(3) of the ATCA.

had custody of the item before it was seized[1322]. Importantly, anything that has been seized by the police may not be retained longer than necessary in the circumstances[1323].

With respect to the interception of communications, Section 6 of the IOCA sets out the safeguards that need to be applied to intercepted material. Notably, when issuing an interception warrant, the Chief Minister is required to make arrangements to limit the dissemination of the material to the minimum necessary for the purposes authorised by the warrant. In particular, the Chief Minister must limit the extent to which the material is disclosed, the number of persons to whom any of the material is disclosed, the extent to which the material is copied as well as the number of copies made of any of the material[1324]. In addition, the IOCA explicitly provides that the material may not be retained for longer than necessary to fulfil the purpose for which it was obtained[1325].

In terms of investigative measures carried out in the context of terrorism offenses and money laundering, the ATCA allows the sharing of information with any of the British intelligence services for the purpose of the exercise by that service of any of its functions, but only if such sharing is not in violation of the data protection legislation or prohibited by the IOCA[1326].

Finally, the Criminal Justice Act 1991 provides the rules on mutual legal assistance in criminal matter[1327]. The Attorney General may provide evidence located on the Isle of Man to a third country's court or prosecuting authority if there are reasonable grounds to suspect that an offence according to that third country's law has been committed, and if proceedings or an investigation are ongoing about that offence[1328]. The Attorney General must request a warrant to a Deemster before granting access to the evidence[1329]. For the warrant to be granted, the offense in the third country would need to also be recognised as such under Isle of Man law had it taken place on the Island, and there needs to be reasonable grounds to suspect that the evidence is located on premises on the Island[1330].

2.2.3. Oversight

Different bodies have oversight over the processing of personal data by criminal law enforcement authorities in the Isle of Man.

First, the Information Commissioner, whose independence is enshrined in law[1331], oversees the application of the Applied LED and the Implementing Regulations[1332]. The tasks and

[1322] Section 24 PPP Act.
[1323] Section 25 PPP Act.
[1324] Section 6 IOCA. Under Section 11 IOCA, a copy is defined as any of the following, whether or not in documentary form (1) any copy, extract or summary of the material; and (2) any record of the identities of the persons to or by whom the material was sent, and cognate expressions shall be construed accordingly.
[1325] Section 6(3) IOCA.
[1326] Section 58A(3) ATCA and Article 7 in conjunction with Schedule 2 Applied GDPR.
[1327] Importantly, the Proceeds of Crime (External Investigations) Order 2011 (secondary legislation made under the POCA) extends the investigative measures in accordance with POCA, for use in response to mutual legal assistance requests from other jurisdictions.
[1328] Section 21(3) Criminal Justice Act 1991.
[1329] Section 22 Criminal Justice Act 1991
[1330] Section 22(1) Criminal Justice Act 1991.
[1331] The Applied LED retains the rules of Article 42 Law Enforcement Directive on the independence of the supervisory authority without modification. The Information Commissioner must remain free from external

powers of the Information Commissioner mirror those set out in Article 46 and 47 of the Law Enforcement Directive. To perform those tasks, the Information Commission may issue several types of notices and orders and has the power to bring court proceedings for non-compliance with such notices or orders[1333]. Information notices require a controller or processor to disclose the information the Commissioner needs for the discharge of his or her functions under the data protection legislation[1334]. Assessment notices permit to verify a controller or processor's compliance with data protection legislation, for instance by allowing on-site investigations and access to any data processing equipment, any document, material or information[1335]. Enforcement orders permit to compel a person to take or refrain from taking certain actions, for example in relation to the data protection principles, data subjects' rights, or the obligation to notify data breaches[1336]. According to information provided by the Isle of Man authorities, since the entry into force of the Applied LED and the Implementing Regulations, the Information Commissioner has investigated several complaints that concerned the Isle of Man Constabulary. In two cases, minor compliance issues were detected, such as non-compliance with a data subject's request for access to personal data. Those issues were rectified further to the Commissioner's advice. The Information Commissioner also regularly engages with law enforcement authorities by providing guidance and advice, notably to the authorities' data protection officers.

Second, the Interception of Communications Commissioner oversees the application of the IOCA, i.e., the interception of communications for the purposes of national security and of detecting and preventing serious crime[1337]. The functions of the Commissioner are to keep under review the activities of the Chief Minister relating to his functions under the IOCA and the adequacy of the safeguards implemented in connection with interception under the IOCA. The Interception of Communications Commissioner must also assist the Interception of Communications Tribunal (see section 2.2.4) for the purpose of enabling it to carry out its functions under the IOCA[1338].

Every person holding office under the Crown, a person engaged in the business of the Post Office or a person in the running of a courier service or a public telecommunications system is required to disclose to the Interception of Communication Commissioner all documents or information that the Commissioner may require for the purpose of enabling him to carry out his functions[1339].

---

influence, whether direct or indirect, and neither seek nor take instructions from anybody. Furthermore, the Commissioner must refrain from any action incompatible with his or her duties.

[1332] Regulation 79 Implementing Regulations.

[1333] Regulation 117 Implementing Regulations.

[1334] Regulation 101 Implementing Regulations.

[1335] Regulation 104(2) Implementing Regulations.

[1336] Regulation 106 Implementing Regulations.

[1337] The role of the Interception of Communications Commissioner is established by the IOCA. In accordance with Section 9(1) IOCA, the Commissioner is appointed by the Governor and must be "a fit and proper person".

[1338] Section 9(1) IOCA.

[1339] Section 9(3) IOCA.

The Interception of Communication Commissioner is required to prepare an annual report to the Governor in Council[1340]. A copy of every annual report must be submitted to the Isle of Man parliament (Tynwald) and made public[1341].

If it appears to the Interception of Communication Commissioner that there has been a contravention of rules governing the issuance of interception warrants which has not been the subject of a report made by the Tribunal under the IOCA (see section 2.2.4), or that the safeguards that have been put in place in relation to the retention and disclosure of the intercepted material are inadequate, (s)he must report to the Governor in Council[1342].

Pursuant to the Commissioner's recent annual reports, interception warrants in the Isle of Man have been issued for the purposes of the detection and prevention of serious crimes. The Commissioner found that the warrants had been issued in respect of the principles of necessity and proportionality and in compliance with procedural requirements, notably the need to consult the Attorney General before the issuing of a warrant. Finally, she found that the safeguards required by Section 6 IOCA had been implemented in a satisfactory manner, while noting in her latest annual report of 2020 that the related policies and procedures had been recently updated by the Cabinet Office in cooperation with the Constabulary, leading to an improvement in the practical aspects of the procedure[1343].

2.2.4. Redress

As regards the processing of personal data by law enforcement authorities in the Isle of Man, redress mechanisms are available under the data protection legislation, the Human Rights Act 2001 and under the IOCA.

This series of mechanisms provide data subjects with effective administrative and judicial means of redress, enabling them in particular to ensure their rights, including the right to have access to their personal data, or to obtain the rectification or erasure of such data.

First, pursuant to Regulation 122 of the Implementing Regulations, data subjects have the right to lodge a complaint with the Information Commissioner if the data subject considers that, in connection with personal data relating to him or her, there is an infringement of the data protection legislation. The Information Commissioner has the power to assess the compliance of the controller and processor with the Applied LED and the Implementing Regulations and require them to take necessary steps in case of non-compliance[1344].

[1340] Section 9(6) IOCA.
[1341] Section 9(7) IOCA. Under section 9(8) IOCA, the Governor in Council may exclude certain matters from the copy of the report as laid before Tynwald, if he considers, after consultation with the Commissioner, that the publication of any matter in an annual report would be prejudicial to national security or to the prevention or detection of crime.
[1342] Section 9(5) IOCA.
[1343] The Reports of the Interception of Communications Commissioner for the years ending on 31st December 2016, 2018, 2019 and 2020 are available at: https://www.tynwald.org.im//business/opqp/sittings/Tynwald%2020162018/2017-GD-0008.pdf, https://www.gov.im/media/1367579/ioc-commissioners-report-for-the-year-ended-31122018-gd2019-0020.pdf, https://www.tynwald.org.im/business/opqp/sittings/20182021/2020-GD-0080.pdf, https://www.tynwald.org.im/business/opqp/sittings/20212026/2021-GD-0096.pdf.
[1344] See Regulations 100 et seq. of the Implementing Regulations.

Second, the Implementing Regulations provide the right to a remedy against the Information Commissioner if it fails to take appropriate steps[1345] to respond to a complaint made by the data subject. More specifically, the complainant can apply to the Data Protection Tribunal, which can issue an order requiring the Information Commissioner to take any steps specified in the order or to provide the requested information to the data subject[1346].

Third, data subjects can also invoke violations of the data protection rules by criminal law enforcement authorities directly before the courts[1347]. If, on an application by a data subject, a court is satisfied that there has been an infringement of the data subject's rights under the data protection legislation, the court may order the controller or processor to take or refrain from taking steps specified in the order. Moreover, a person who suffers damage by reason of a contravention of a requirement of the data protection legislation is entitled to compensation for that damage from the competent authority. A controller or processor is not liable if it proves that it is not in any way responsible for the event giving rise to the damage[1348].

Fourth, as far as any person considers that their rights, including rights to privacy and data protection, have been violated by public authorities, individuals can obtain redress before the courts of the Isle of Man under the Human Rights Act 2001[1349]. If the court finds any act of a public authority to be unlawful, it can grant such relief or remedy, or make such order, within its powers as it considers just and appropriate[1350]. The court can also declare a provision of primary legislation to be incompatible with a right provided by the Human Rights Act[1351]. Finally, after having exhausted national remedies, a person, non-governmental organisation or groups of individuals can obtain redress before the European Court of Human Rights for violations of the rights guaranteed under the European Convention of Human Rights[1352].

For violations of the IOCA, individuals can obtain redress before the Interception of Communications Tribunal. This redress avenue is described in section 2.2.4 below.

2.3. Access and use by Isle of Man public authorities for national security purposes

[1345] The Commissioner is required to take appropriate steps to respond to the complaint, including by investigating the subject matter of the complaint, to inform about the outcome of the complaint and about the complainant's right to seek redress before a tribunal, see Regulation 122(3) and (4) of the Implementing Regulations.
[1346] Regulation 123(3) Implementing Regulations.
[1347] Regulation 124 Implementing Regulations.
[1348] Regulation 125 Implementing Regulations.
[1349] Under Section 6(1) Human Rights Act it is unlawful for a public authority to act in a way which is incompatible with the respect for the rights provided in that law. An individual who claims that a public authority has acted (or proposes to act) in a way which is unlawful under Section 6(1) can bring proceedings against the authority in the appropriate court or tribunal, or rely on the rights concerned in any legal proceedings, when he or she is (or would be) a victim of the unlawful act.
[1350] Section 8(1) Human Rights Act.
[1351] However, the declaration of incompatibility does not affect the validity, continuing operation or enforcement of the provision in respect of which it is given, and is not binding on the parties to the proceedings in which it is made, see Section 4 Human Rights Act.
[1352] Article 34 of the European Convention of Human Rights provides that "The Court may receive applications from any person, non-governmental organisation or group of individuals claiming to be the victim of a violation by one of the High Contracting Parties of the rights set forth in the Convention or the Protocols thereto. The High Contracting Parties undertake not to hinder in any way the effective exercise of this right".

In the Isle of Man, access to information transferred under the adequacy decision for purposes of national security takes place in the form of the interception of communications on the basis of the IOCA[1353]. It is the Isle of Man Constabulary that carries out such interception.

2.3.1. Legal bases and applicable limitations/safeguards

The IOCA provides the legal framework for the interception of communications in the course of transmission by post, by means of a courier service or a public telecommunication system. The IOCA introduces a general principle of confidentiality of communications and makes it a criminal offence to intentionally intercept communications[1354]. This is reflected in the fact that interception is lawful only when carried out on the basis of a warrant[1355]. An interception warrant is issued by the Chief Minister and requires the person to whom it is addressed to intercept the communications described in the warrant or to disclose the intercepted material to such persons and in such manner as are described in the warrant[1356]. An interception warrant can only be issued if the Chief Minister considers that the information sought to be obtained could not reasonably be acquired by other, less intrusive means[1357]. Before issuing or renewing a warrant the Chief Minister is required to consult the Attorney General, i.e., obtain legal advice from the Government's principal legal adviser on whether the conditions for issuing a warrant are fulfilled. A register of warrants must be maintained, including details of every warrant, and of every amendment, renewal and cancellation thereof, and details of every consultation of the Attorney General[1358].

In accordance with Section 3 IOCA, the warrant must require the interception of communications in relation to one particular person named or described in the warrant or in relation to a single set of premises named or described in the warrant. The warrant must also describe the communications for which interception is required by references to addresses, numbers, apparatus or other factors to be used for identifying those communications[1359].

[1353] For the powers that can be exercised in the Isle of Man by UK intelligence services, see the Commission Implementing Decision of 28.6.2021 pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data by the United Kingdom, available at: https://commission.europa.eu/system/files/2021-06/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_en.pdf. The Isle of Man Regulation of Surveillance Act 2006 covers activities that are not relevant in the context of data transfers from the EU to the Isle of Man under the adequacy decision, such as surveillance in the form of covert human intelligence. It does not cover the interception of communications in the course of their transmission by means of a telecommunication system, unless the communication is sent by, or intended for, a person who has consented to the interception of communications and there is no interception warrant under the Interception of Communications Act 1988 authorising the interception, see Section 3(5) Regulation of Surveillance Act 2006.

[1354] Section 1 IOCA.

[1355] Section 2(1) IOCA. Interception without warrant is only lawful in specific limited circumstances, i.e., when intercepting with the consent of the sender or recipient (Section 1(2)(b) IOCA) and in case of limited administrative and enforcement purposes (Section 1(3)(a) and (b) IOCA).

[1356] Section 2(1) IOCA.

[1357] Section 2(3) IOCA. See also Report of the Interception of Communications Commissioner for the year that ended on 31st December 2018, available at: https://www.gov.im/media/1367579/ioc-commissioners-report-for-the-year-ended-31122018-gd2019-0020.pdf.

[1358] Section 6(4) and (5) IOCA.

[1359] Section 3(3) IOCA. These specifications are not required for the interception of a communication sent or received outside the British Islands (i.e., 'external communications'), where the Chief Minister has issued a certificate certifying that the examination of certain described intercepted material is necessary, see Section 3(2) IOCA. To date, no such certificate has been issued.

Unless it is renewed, a warrant ceases to have effect two months after its issuance. The Chief Minister may, at any time before the end of the relevant period, renew the warrant if he considers that the warrant continues to be necessary (on the same grounds for which it was issued)[1360]. If the Chief Minister considers that any factor specified in a warrant is no longer relevant for identifying the communications authorised to intercept, he must amend the warrant by deleting that factor[1361].

2.3.2. Further use of the information collected

The further use of personal data obtained in the interests of national security is governed by the provisions of the Applied GDPR and the Implementing Regulations as described in sections 2.1 and 1[1362]. In particular, pursuant to Articles 5(1)(a) and (b) of the Applied GDPR, such processing must be lawful, and data must not be processed in a manner that is incompatible with the purpose for which it was collected. The controller can process the data for another purpose, different from that for which the data was collected, when it is compatible with the original one and provided that the controller is authorised by law to process the data.

In addition, the IOCA sets out specific safeguards for the further use and sharing of data obtained through the interception of communications, including for the sharing of such data with third countries. Section 6 IOCA specifies that the Chief Minister has the duty to make arrangements to limit the dissemination of the material obtained to the minimum necessary for the purposes authorised by the warrant. In particular, the Chief Minister must limit the extent to which the material is disclosed, the number of persons to whom any of the material is disclosed, the extent to which the material is copied as well as the number of copies made of any of the material[1363]. In addition, the IOCA explicitly provides that the material may not be retained for longer than necessary to fulfil the purpose for which it was obtained[1364].

2.3.3. Oversight

Government access for national security purposes in the Isle of Man is overseen by different bodies. The Information Commissioner oversees the processing of personal data in light of the Applied GDPR and the Implementing Regulations, while specific oversight on the use of the interception powers under the IOCA is provided by the Interception of Communications Commissioner, which oversees interception both for law enforcement and for national security purposes.

[1360] The renewed warrant cease to have effect at the end of one month beginning with the day on which it was renewed, Section 4(6)(b) IOCA.
[1361] Section 5(1) and (3) IOCA.
[1362] While controllers can be exempt from some of these provisions pursuant to Regulation 22 of the Implementing Regulations to the extent that such exemption is required for the purposes of national security, such exemption must be assessed case-by-case and can be invoked only as far as the application of a particular provision would have negative consequences for national security (see section 2.1). Moreover, as any processing for a different purpose must be authorised by law, Isle of Man authorities must have a clear legal basis for the further processing.
[1363] Section 6 IOCA. Under Section 11 IOCA, a copy is defined as any of the following, whether or not in documentary form (1) any copy, extract or summary of the material; and (2) any record of the identities of the persons to or by whom the material was sent, and cognate expressions shall be construed accordingly.
[1364] Section 6(3) IOCA.

The processing of personal data carried out for national security purposes is governed by the Applied GDPR and the Implementing Regulations. The general functions and powers of the Information Commissioner are laid down in Articles 57 and 58 of the Applied GDPR. The tasks include, but are not limited to, monitoring and enforcement, promoting public awareness, advising Tynwald, the government and other institutions on legislative and administrative measures, promote the awareness of controllers and processors of their obligations, provide information to a data subject concerning the exercise of the data subject's rights, handle complaints, conduct investigations etc. The Commissioner has the powers to notify controllers of an alleged infringement and to issue warnings that a processing is likely to infringe the rules, issue reprimands, ban processing or order the controller to take certain actions. While Regulation 22 of the Implementing Regulations provides an exception to certain tasks and powers of the Commissioner if this is required for the purposes of safeguarding national security, these exceptions apply only if necessary and proportionate and on a case-by-case basis (as explained in section 2.1).

Furthermore, as described in section 2.1.3 above, the Interception of Communications Commissioner oversees the application of the IOCA, i.e., the interception of communications for the purposes of national security and for detecting and preventing serious crime[1365]. (S)he reviews the activities of the Chief Minister relating to his functions under the IOCA and the adequacy of the safeguards implemented in connection with interception under the IOCA and assists the Interceptions of Communications Tribunal (see section 2.2.4)[1366]. The Commissioner prepares an annual report to the Governor in Council[1367], a copy of which must be submitted to the Isle of Man parliament and made public[1368]. If it appears to the Commissioner that there has been a contravention of rules governing the issuance of interception warrants or that safeguards that have been put in place in relation to the retention and disclosure of the intercepted material are inadequate, (s)he must report to the Governor in Council[1369].

Pursuant to the Commissioner's recent annual reports, no interception warrants since 2016 have been issued in the interest of national security[1370].

2.3.4. Redress

Individuals can obtain redress for violations of the IOCA before the Interception of Communications Tribunal.

[1365] The role of the Interception of Communications Commissioner is established by the IOCA. In accordance with Section 9(1) IOCA, the Commissioner is appointed by the Governor and must be "a fit and proper person".
[1366] Section 9(1) IOCA.
[1367] Section 9(6) IOCA.
[1368] Section 9(7) IOCA. Under section 9(8) IOCA, the Governor in Council may exclude certain matters from the copy of the report as laid before Tynwald, if he considers, after consultation with the Commissioner, that the publication of any matter in an annual report would be prejudicial to national security or to the prevention or detection of crime.
[1369] Section 9(5) IOCA.
[1370] The Reports of the Interception of Communications Commissioner for the years ending on 31st December 2016, 2018, 2019 and 2020 are available at: https://www.tynwald.org.im//business/opqp/sittings/Tynwald%2020162018/2017-GD-0008.pdf, https://www.gov.im/media/1367579/ioc-commissioners-report-for-the-year-ended-31122018-gd2019-0020.pdf, https://www.tynwald.org.im/business/opqp/sittings/20182021/2020-GD-0080.pdf, https://www.tynwald.org.im/business/opqp/sittings/20212026/2021-GD-0096.pdf.

Any person, including any individual in the EU, who believes[1371] that communications sent to or by him have been intercepted, can apply to the Interception of Communications Tribunal for an investigation. The Tribunal has been established in accordance with Section 8 IOCA and it is independent from the executive[1372]. When receiving an application, the Interception of Communications Tribunal must investigate whether there is or has been a relevant[1373] warrant or certificate, and where this is the case, whether there has been any violation of the rules under the IOCA in relation to that warrant or certificate. The Tribunal may only reject applications that appear to be frivolous or vexatious.

If the Interception of Communications Tribunal concludes that there has been a violation of the rules of the IOCA, it must notify the applicant about its conclusions, report its findings to the Governor in Council and, if appropriate, make an order to (1) quash the relevant warrant or the relevant certificate; (2) delete copies of the intercepted material; (3) direct the Treasury to pay to the applicant a compensation[1374]. The Interception of Communications Tribunal must also notify the applicant in case it comes to the conclusion that there has been no contravention of the rules of the IOCA. According to Section 8(8) IOCA the decision of the Tribunal is not subject to appeal.

Finally, as also described in section 2.1.4 above, as far as individuals consider that their rights, including rights to privacy and data protection, have been violated by public authorities, they can obtain redress before the courts of the Isle of Man under the Human Rights Act 2001. In addition, any individual may obtain judicial redress before the European Court of Human Rights against the unlawful collection of his/her data for national security purposes, provided that all available domestic remedies have been exhausted.

[1371] On the standard of the 'belief' test, in the absence of relevant case law in the Isle of Man, UK case law is likely to be persuasive. In Human Rights Watch v Secretary of State [2016] UKIPTrib15_165-CH, paragraph 41, the Investigatory Powers Tribunal, by referring to the European Court of Human Rights case law, held that the appropriate test is whether in respect of the asserted belief that any conduct falling within Subsection 68(5) of RIPA 2000 has been carried out by or on behalf of any of the intelligence services, there is any basis for such belief, such that the individual may claim to be a victim of a violation occasioned by the mere existence of secret measures or legislation permitting secret measures, only if he is able to show that due to his personal situation, he is potentially at risk of being subjected to such measures.

[1372] In accordance with Schedule 1 IOCA, the Tribunal has three members, who are appointed by the Governor. The Chairman of the Tribunal must be an advocate of not less than 10 years' standing. The members are appointed for a term of 5 years and can be reappointed. A member of the Tribunal may only be removed from office by the Governor at his or her own request, or on the basis of a resolution of Tynwald. Every person holding office under the Crown or engaged in the business of the Post Office, in the running of a courier service or a public telecommunication system is obliged to disclose or give to the Tribunal such documents or information as they may require for the purpose of enabling them to carry out their functions.

[1373] A warrant is a relevant warrant in relation to an applicant if the applicant is named or described in the warrant, or the communications described in the warrant are likely to be, or to include communications from him or intended for him (Section 8(9) IOCA).

[1374] Section 8(4) and (5) IOCA.

VII. STATE OF ISRAEL

1. RULES APPLYING TO THE PROCESSING OF PERSONAL DATA

1.1. Relevant developments in the data protection framework of Israel

On 31 January 2011 the European Commission adopted a decision in which the State of Israel, as defined in accordance with international law, was considered as providing an adequate level of protection for personal data[1375]. The Article 29 Working Party had provided its opinion on the level of protection for personal data in Israel on 1 November 2009[1376]. At the time, the legal framework for the protection of personal data in Israel was set out in the Privacy Protection Law 5741 - 1981 (PPL) and Regulations. The PPL was first passed in 1981 and applies to both the public and the private sector.

Since the adoption of the Commission's adequacy decision, Israel's framework for the protection of privacy and personal data has been significantly strengthened through a number of developments at legislative, regulatory and enforcement level. In particular, as described in more detail below, Israel adopted Privacy Protection (Data Security) Regulations, 5777-2017 (Data Security Regulations) which apply to the public and to the private sector and are aimed at improving the level of data security across all sectors by setting general legally binding standards[1377]. In addition, Israel introduced specific safeguards to reinforce the protection of personal data transferred from the European Economic Area by adopting Privacy Protection Regulations (Instructions for Data that was Transferred to Israel from the European Economic Area), 5783-2023 (Privacy Protection Regulations)[1378]. Moreover, Israeli Courts have clarified and further reinforced the existing framework in several judgments that interpret the

[1375] Commission Decision 2011/61/EU of 31 January 2011 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data, OJ L 27, 1.2.2011, p. 39–42. The decision on the adequate protection of personal data by the State of Israel is to be applied in accordance with international law and is without prejudice to the status of the Golan Heights, the Gaza Strip and the West Bank, including East Jerusalem, under the terms of international law. See Article 2(2) of the adequacy decision. Recital 14 of the decision furthermore provides that onward transfers to a recipient outside the State of Israel, as defined in accordance with international law, should be considered as transfers of personal data to a third country. Consequently, transfers from the State of Israel to territories beyond its internationally recognised borders should be subject to the same legal safeguards applicable to onward transfers.

[1376] Opinion 6/2009 on the level of protection of personal data in Israel (WP165), available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp165_en.pdf.

[1377] Privacy Protection (Data Security) Regulations, 5777-2017, adopted on 5 April 2017, available at: https://www.gov.il/BlobFolder/legalinfo/data_security_regulation/en/PROTECTION%20OF%20PRIVACY%20REGULATIONS.pdf. The Regulations apply to all databases, whether or not they are subject to a registration requirement under the PPL.

[1378] Privacy Protection Regulations (Instructions for Data that was Transferred to Israel from the European Economic Area), 5783-2023, published in the Official Gazette (*Reshumut*) on 7 May 2023, available at: https://www.gov.il/en/departments/legalInfo/datatransferredisrael2023. As provided for by Article 36 PPL, the Regulations have been approved by the Constitution, Law and Justice Committee of the Israeli Parliament (*Knesset*) and promulgated by the Minister of Justice. Their scope of application is set out in Regulation 2(a) of the Privacy Protection Regulations. They apply to data that is in a database in Israel that has been transferred from the European Economic Area, except for data that a natural person directly provided on his initiative, as well as to any other data in a database in Israel that contains such data. In accordance with Regulation 9(1), the Regulations entered into application on 7 August 2023 with respect to data received in a database in Israel on or after the day of the publication of the Regulations, and will enter into force one year from the date of their publication with respect to data received in a database in Israel before that day.

right to privacy set out in the Basic Law[1379] and the provisions of the PPL. Finally, Israel's Privacy Protection Authority (PPA)[1380] has clarified important elements of the data protection system in Israel through the adoption of guidelines, opinions and directives, for instance on the interpretation of the term 'data' and on the right of access.

While the developments in terms of guidance, interpretation and case law that are described in more detail below contribute to an increased level of data protection in Israel, codifying these developments in legislation would be important to enhance legal certainty and solidify the protection for personal data. The ongoing debate on a draft bill that would amend the PPL[1381] seems to offer such an opportunity.

More specifically, since the adoption of the adequacy decision, the PPL's scope of application has been further clarified in various judgments, government resolutions and opinions of the PPA.

In the Israeli system, personal data is protected in accordance with Chapters A and B of the PPL. Chapter A protects the right to privacy more generally, while Chapter B specifically regulates the protection of data in databases.

Chapter A of the PPL prohibits certain infringements of privacy[1382] by reference to categories such as "information on a person's private affairs"[1383], as well as "a matter that relates to a persons' intimate life"[1384] and "other data obtained in a way which infringes privacy under the provisions of the Article"[1385]. Since the adoption of the adequacy decision, the categories used in Chapter A of the PPL have been further clarified by Israeli courts. For example, courts have confirmed that data such as residential address and telephone number also constitute

[1379] In Israel there is no codified constitution, but there are Basic Laws which have been given constitutional status by the Supreme Court of Israel. The right to privacy is enshrined in Article 7 of the Basic Law: Human Dignity and Liberty.
[1380] As described in more detail in section 1.2, the PPL foresees that the oversight over the protection of privacy is carried out by the so-called Registrar, who, pursuant to Article 7 PPL, is a person qualified to be appointed as a Magistrates Court judge and is appointed by the Government to operate the databases register. By decision of the government of Israel of 2006, this Registrar was integrated into the Israeli Law, Information and Technology Authority (ILITA), which was created by that same decision. The role of the Head of ILITA was assigned to the Registrar, see Article 10(e) PPL and Article 4(A) of Government Resolution No. 1890 of 2 October 2022. ILITA was later renamed as Privacy Protection Authority.
[1381] Privacy Protection Bill (Amendment No. 14), 5722-2022, amending the Protection of Privacy Law, 5741-1981, submitted to the Knesset on 5 January 2022. On 3 April 2023 the Israeli Ministerial Committee on Legislation decided to apply to the Knesset for the application of the rule of continuity for the advancement of the Privacy Protection Bill (Amendment No. 14), 5722-2022, after its progress had been stalled due to the dissolution of the Knesset. On 29 May 2023 the Parliament decided to apply the rule of continuity for advancement of the Bill and the Bill was allocated to the Constitution Law and Justice Committee.
[1382] While the list of infringements is in principle exhaustive, several elements are construed broadly to cover a range of possible infringements. See for instance Article 2(8) PPL, which prohibits the infringement of the duty of confidentiality in respect to a person's private affairs, whether it was explicitly or implicitly prescribed in an agreement; or Article 2(9), which prohibits the use or passing on of information on a person's private affairs, for a purpose other than for which it was provided. In addition, the Supreme Court has ruled that, beyond the protection specifically provided by Article 2, Israeli common law continues to apply (HCJ Jane Doe 6650/04, Kalanswa Case 7541-04-14 and CA John Doe 8954/11). With respect to public authorities, infringements of privacy other than those listed in Article 2 PPL may be considered a violation of Article 7 of the Basic law: Human Dignity and Liberty.
[1383] Article 2(9) PPL.
[1384] Article 2(11) PPL.
[1385] Article 2 (10) PPL.

"information of a person's private affairs" and are protected under the law[1386]. Moreover, a person's bank account number[1387], credit card number[1388], personal calls log[1389], and a person's application to the authorities for filing a complaint[1390] were considered as information on a person's private affairs.

In Chapter B, the notion of 'database' is defined as "a collection of data, kept by magnetic or optic means, and intended for computer processing", which has been interpreted broadly to apply to any type of data stored digitally[1391]. Article 7 PPL defines the term 'data' as data on personality, personal status, intimate affairs, state of health, economic state, vocational qualifications, opinions, and beliefs of a person. To ensure more comprehensive protection, Article 7 PPL has been interpreted broadly by Israeli courts to apply to almost any kind of data. For example, the case law rejected the claim that foreclosure orders are not 'data' as defined in the PPL and held that, in the digital age which enables enhanced searches and processing of data and cross-referencing, the definition of private data must be interpreted more broadly[1392]. In another ruling, the Supreme Court[1393] rejected the claim that national identity numbers do not constitute 'private data' as defined by the PPL and found that a national identity number is not just a "sequence of numbers", but rather an identifier that, in combination with additional data, can be used to conclude more personal data such that "the person and the ID number becomes identical"[1394].

Such broad approach has also been adopted in two resolutions adopted by and binding on the Israeli government, reflecting its understanding of the term 'data.' One of them concerns the right to public access to documents in government databases[1395]. It exempts personal 'identifiable data' from the government's obligation to grant access, and personal 'identifiable data' is defined broadly to include un-identified data that can be potentially identifiable if combined with additional data. The second resolution concerns the promotion of "Digital Health" and requires certain safeguards to be provided in future legislation in this field[1396]. Some of these safeguards are tailored depending on the level of identifiability of the data concerned.

[1386] For a person's address as part of his private affairs, see AdminA 2820/13 Rosenberg v. Enforcement and Collection Authority, 67(1) 1 (2014), para 23. In AdminC 67403-01-19 Har-Shemesh v. Freedom of Information Law Officer (published in Nevo, 7.4.2019), it was held that a person's mobile phone number is at the heart of his private affairs.

[1387] CA 439/88 Registrar of Databases v. Moshe Ventura 48(3) PD 808 (1994).

[1388] CA 27045-11-11 Yanusov v. Pelephone Communication Ltd. (published in Nevo, 14 May 2014).

[1389] AdminA 7678/16 Drucker v. Freedom of Information Law Officer in the Prime Minister's Office (published in Nevo, 7. August 2017)

[1390] CivC (Tel Aviv Magistrate) 27044-10-11 Schwartz v. Nachum (Published in Nevo, 28. July 2014).

[1391] Article 7 PPL. See also para. 6.2-6.3 of Guideline no. 1/2017 of the Database Registrar regarding the "Application of the Provisions of the Privacy Protection Law on the Right to Access Voice Recordings and Other Digital Data".

[1392] AdminC 244867-02-11 I.D.I Insurance Company Ltd. v. Ministry of Justice the Israeli Law, PPA – the Registrar of Databases (Jul. 7, 2012), as upheld by the Israeli Supreme Court in Admin A 7043/12 I.D.I. Insurance Company Ltd. v. Ministry of Justice the Israeli Law, PPA – the Registrar of Databases, 15 January 2014.

[1393] The Supreme Court of Israel is the country's highest judicial authority and has the authority to issue definitive rulings on the interpretation of the law. Such rulings are considered a binding source of law.

[1394] HCJ 6824/07 Adel Manna v. Tax Authority, 10 December 2010.

[1395] Government Resolution 1933 regarding 'open data' of the government's databases, 30. August 2016.

[1396] Government Resolution 2733 regarding the promotion of Digital Health, 11 June 2017.

Finally, such broad interpretation has also been reflected in Directives and Opinions issued by the PPA. According to PPA Directive No. 4/2012, the provisions of Chapter B of the PPL apply to identified or identifiable data about a person. In the context of security and surveillance cameras, the PPA's interpretation , in line with Directive No. 4/2012, is that the use of such cameras in the public domain and the storage of the footage captured by these cameras constitute a database, even if the identity of the people appearing in the footage is unknown to the camera owner, in light of the possibility to cross-reference data from different databases, such as the camera owner's client database[1397]. In an opinion issued in December 2022[1398], the PPA quoted the opinion of Israel's Attorney General filed in the Greenberg case, in which it was asserted that the provisions of the Privacy Protection Law apply to data "as long as it is possible by reasonable means to identify the data subject". The Attorney General further stated that "data should be treated as identifiable data about a person, as long as it is possible, with reasonable effort, to identify the data subject (the client). In this context, one should take into account the possibility of re-identifying the data subjects, even when the data is supposed to be anonymous" [1399]. In addition, the PPA's opinion of December 2022 quoted the Israeli Supreme Court in the Gottesmann case, where it ruled that "[e]ven information that is shown anonymously might establish a connection with a specific person. […] it is therefore not necessary for a person's name or picture to appear alongside the publication; it suffices for it to be possible by some means to connect the information with a specific person by "reverse engineering"[1400]. This is thus an approach which is similar to the one to be carried out under Regulation (EU) 2016/679 (GDPR)[1401].

In addition, since the adoption of the adequacy decision, several of the data protection principles provided by the PPL have been further clarified through case law, guidance of the PPA, or the adoption of regulations.

As regards the principle of lawfulness, the Israeli data protection regime requires that the collection and processing of personal data is made on the basis of the data subject's consent or based on an authorisation by law[1402]. Importantly, the conditions for obtaining an individual's

[1397] See also Paragraph 2.7, PPA Directive no. 4/2012 "The use of security and surveillance cameras and the databases of the footage captured by them", and paragraphs 9-10 in the opinion attached thereto, both available at: https://www.gov.il/he/departments/policies/surveillance_cameras_guidelines.

[1398] Privacy Protection Authority Legal Opinion "What are 'Data' and 'Information on a Person's Private Affairs' According to the Privacy Protection Law", 20 December 2022, available at: https://www.gov.il/BlobFolder/rfp/information_definition_public_hearing/en/PPA's%20Opinion%20-%20What%20are%20Data%20and%20Information%20on%20a%20Person's%20Private%20Affairs.pdf.

[1399] Paragraphs 40 and 46 in the Attorney General's opinion of 29 April 2018 in CivC 22141-03-15 Greenberg v. Cellcom (judgment of 5.3.2020).

[1400] CA 1697/11 Gottesman v. Vardi, 23 January 2013, available at: https://versa.cardozo.yu.edu/opinions/gottesman-v-vardi.

[1401] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[1402] With respect to consent, Chapter A PPL prohibits infringements of privacy without the individual's consent and thus recognises that consent can be a legitimate ground for the processing of personal data. Moreover, the information requirement set out in Article 11 PPL stipulates that where data is collected from an individual, the individual needs to be informed whether (s)he is under a legal obligation to provide the information, or whether the provision of the information depends on the individual's consent. Pursuant to Article 3 PPL, consent must be informed. Article 35 PPL stipulates that "the provisions of this Law shall not derogate from the provisions of any other Law". From this provision, as well as from case law, it follows that the collection and processing of personal data can also be based on an authorization by a law. The Israeli Supreme Court has clarified with respect to public authorities that according to the principle of 'legality of authority' each administrative authority

consent have been further developed in case law of the Israeli courts, aligning them more closely with the conditions required by EU law. In *Isakov Inbar v. The State of Israel, the Commissioner for Women Labor Law*[1403], the court clarified that the monitoring of an employee's email account requires the employee's explicit, specific, informed and freely given consent to the infringement of privacy. With respect to a purely private email account, the court held that in view of the inherent power asymmetry in the employer-employee relationship, it had to be presumed that any consent to the monitoring of such an account had not been given freely, so that such monitoring activities could not be based on consent alone, but could take place only pursuant to a court order. The case law further specified the concept of freely given consent, stressing that consent would not be freely given in case of any coercion, whether direct or indirect, such as the sanctioning of an employee[1404]. It also set out the requirements for appropriately informing an individual, notably that the information to the individual would have to be clear and include all relevant details, such as the nature of the data collected, the applicable retention period, where the data would be stored and who would have access to it, how it would be secured etc.

The purpose limitation principle is recognised both in Chapter A and in Chapter B of the PPL. In Chapter A, Section 2(9) PPL sets out that the "use or passing of information on a person's private affairs for a purpose other than which was provided" in the absence of the individual's consent constitutes an infringement of privacy, as well as a felony under Section 5 PPL and a civil wrong under Section 4 PPL. As mentioned above, the term 'a person's private affairs' has been interpreted broadly by Israeli courts[1405], thus ensuring a wide scope of application for the purpose limitation principle. In Chapter B PPL, Section 8(b) PPL stipulates that "no person shall use the data in a database which must be registered under this Section, except for the purposes for which the database was established". The purpose limitation principle has been upheld also by Israeli courts, for example in the *IDI* case[1406], in which it was ruled that data obtained by a company in connection with a foreclosure could not be used for the purpose of assessing the individual's eligibility for car insurance, as such use violated the purpose limitation provisions of the PPL.

---

must act solely within the powers vested in it by law. When an administrative act may lead to an infringement of individual rights, there must be a clear and explicit legal authority in primary or secondary legislation allowing this act, and the legislative authority must comply with the Basic law: Human Dignity and Liberty, see PCA 2558/16 Jane Doe v. Compensation Officer - Ministry of Defence (5 November 2017).

[1403] National Labor Court 90/08 Tali Isakov Inbar v. The State of Israel, the Commissioner for Women Labor Law (Feb. 8, 2011).

[1404] Collective Dispute Appeal 7541-04-14 The New Workers' General Federation v. the Kalanswa Municipality (May 5, 2017).

[1405] 'Information on a person's private affairs' has been interpreted to cover any data related to the private life, e.g., name, address, telephone number, place of work, identity, friends, relations with spouse and family, see CA 439/88 Registrar of Databases v. Moshe Ventura 48(3) PD 808 (1994. In a later Supreme Court ruling, AdminA 398/07 The Movement for Freedom of Information v. The State of Israel – Tax Authority 63(1) PD 284 (2008), the Court considered with respect to these items that the decision whether they are considered as 'a person's private affairs' in accordance with the provisions of the Privacy Protection Law should be examined in each case according to its circumstances and its context, and with the aspiration to attain the right to privacy, while at the same time not causing a substantial violation of other rights, such as the freedom of speech, accessibility of the public to information and more. see AdminA 9341/05 The Movement for Freedom of Information v. the Governmental Companies Authority (May 5, 2009).

[1406] AdminC (TA) 244867-02-11 I.D.I Insurance Company Ltd. v. Ministry of Justice the Israeli Law, PPA – the Registrar of Databases (Jul. 7, 2012), as upheld by the Israeli Supreme Court, AdminA 7043/12 I.D.I. Insurance Company Ltd. v. Ministry of Justice the Israeli Law, PPA – the Registrar of Databases (Jan. 15, 2014).

The principle of data security and confidentiality is reflected in Articles 16, 17, 17A and 17B of the PPL. Article 7 PPL defines 'data security' as the "protection of the integrity of data, or protection of the data from exposure, use or copying, all when done without due permission". Article 16 PPL protects the confidentiality of data by setting out that data may not be disclosed by an employee, manager or possessor of a database except in certain specific circumstances, such as for performing his work or pursuant to a court order. Article 17 specifies that a database owner, the possessor of a database and the manager of a database are each responsible for the security of a database. Article 17A provides for access restrictions in order to prevent unauthorised access to databases, and Article 17B obliges specific bodies[1407] to appoint a Security Officer, who is also personally responsible for the security of the database. Moreover, since the adoption of the adequacy decision, the Data Security Regulations have established mechanisms aimed at strengthening data security in both the private and public sectors by making it part of the management routines of all organizations processing personal data, and more specifically, by creating awareness, accountability and working procedures. In particular, the Data Security Regulations classify databases into different categories according to the level of risk created by the processing activity. This level of risk is defined by the data sensitivity, the number of data subjects and the number of authorised access holders. The duties of the database owners are determined in accordance with the level of risk. Among others, the Data Security Regulations contain obligations concerning the mapping of data processing activities[1408], data security protocol[1409], "data security risk evaluation"[1410], physical security measures[1411] and access controls[1412], as well as an obligation to notify severe "data incidents" to the PPA, and to the data subjects if so instructed by the PPA[1413].

In addition, several data protection principles that were previously recognised only implicitly in the PPL have been codified in the Privacy Protection Regulations and/or the Data Security Regulations and have thus been significantly strengthened after the adoption of the adequacy decision.

While the principle of data quality/data accuracy was previously not set out as an independent principle, but recognised implicitly in the context of the right to rectification provided in Article 14 PPL[1414], for data that has been transferred to Israel from the EU, Regulation 5 of

[1407] Public bodies, bodies that operate several databases and bodies that carry out data processing with specific risks for the individual, see Article 17B PPL.
[1408] Article 5 Data Security Regulations.
[1409] Article 4 Data Security Regulations.
[1410] Article 5 Data Security Regulations.
[1411] Article 6 Data Security Regulations.
[1412] Articles 7, 8, 9 and 10 Data Security Regulations.
[1413] Article 11 Data Security Regulations.
[1414] Article 14 PPL stipulates that "A person who reviewed the data about himself, and found it to be incorrect, incomplete, unclear or not up to date, may request the database owner, and if he is a foreign resident – the possessor, to correct or delete the data." The principle of data quality and data accuracy has also been recognised by Israeli courts. In one case, the respondents had failed to make it clear in their application to register a database "whether and how a person could ascertain whether his name appears in the database, and request that the data be corrected or deleted from the database; in addition, no deletion and updating mechanism, for the passage of time, has been established within the database". The Supreme Court justice found that "a correction and adjustment mechanism on the one hand, and a deletion and updating mechanism on the other, are essential to ensure the accuracy and reliability of the data compiled and ensure the mitigation of the risk of harm to both the relevant individuals and to the public.", see CA 439/88 Registrar of Databases v. Moshe Ventura 48(3) PD 808 (1994).

the Privacy Protection Regulations now explicitly requires the database controller to have in place an organizational, technological or other mechanism, the purpose of which is to ensure that the data in the database is correct, complete, clear and updated. If the database controller finds, on the basis of, inter alia, the abovementioned mechanism, that the database contains data that is not correct, complete, clear or updated, he is required to take reasonable measures in the circumstances of the case for the purpose of rectifying or deleting the data.

Also the principle of limited data retention has been reinforced through the adoption of the Privacy Protection and the Data Security Regulations[1415]. For data that has been transferred to Israel from the EEA, Regulation 4 of the Privacy Protection Regulations requires the database controller to have in place an organizational, technological or other mechanism, the purpose of which is to ensure that the database does not include data that is no longer necessary for the purpose for which it was collected or retained, or for any other purpose for which it may be retained in accordance with any law (referred to as data that is not necessary). If the database controller finds, on the basis of, inter alia, the abovementioned mechanism, that data that is not necessary is kept in the database, he is required to delete the said data at the earliest opportunity in the circumstances of the case[1416]. In addition, Regulation 2(c) of the Data Security Regulations provides that database owners must annually examine if the data stored in their databases is excessive for the purpose of each database.

Finally, the principle of transparency was so far only reflected in the PPL through the right to information. Article 11 PPL provides that if data is collected from a person for use in a database, this person needs to be informed about whether (s)he is under a legal obligation to provide the data or whether the provision of data depends on his or her volition and consent, about the purpose of the collection and the recipient of the data, as well as the purpose of any further sharing of the data. To enhance transparency for data subjects in the EU whose personal data is transferred to Israel, Regulation 6 of the Privacy Protection Regulations now imposes additional transparency requirements. A database controller in Israel who received data about a person is required to provide the said person, whether directly or indirectly through the entity that provided the data from the EU, with information about the identity of the database controller and the database manager, their addresses and contact information, the purpose of the data transfer, the type of the data that was transferred, and the data subject rights that are available in the Israeli framework[1417]. The information must be provided as

[1415] Previously, the principle of limited data retention could only be implied from Article 8(b) PPL. This provision sets out that data in databases can only be used for the purposes for which the database was established, which could imply that data can no longer be used (including the storage) if the use (including the storage) is no longer necessary for the purpose for which the database was established.

[1416] Pursuant to Regulation 4(c) of the Privacy Protection Regulations, the obligation to delete is subject to exemptions for purposes similar to those for which an exemption to the right to deletion is granted also under EU law. In addition, these exemptions can only be invoked to the extent necessary and proportionate. More specifically, the obligation to delete, to the extent necessary and proportionate in the circumstances of the case, does not apply if actions that assure that it is impossible, by applying reasonable measures, to identify the data subject, were performed with respect to the said data, or to the extent the use of the data is necessary and proportionate for exercising the right of freedom of expression including the public's right to know, protecting a public interest, including for archiving purposes, scientific research or statistical research, conducting a legal proceeding or ensuring debt collection, addressing fraud, theft or other incidents affecting the integrity of the data processing operation, or for fulfilling an obligation resulting from an international agreement to which the Government of Israel is a party.

[1417] The right to deletion pursuant to Regulation 2 of the Privacy Protection Regulations, the right to access pursuant to Article 13 PPL, and the right to correction pursuant to Article 14 PPL.

soon as possible after receiving the data and no later than one month as of the date of receiving the data[1418]. In this way, the Privacy Protection Regulations ensure that individuals in the EU continue to be informed of the specific controllers processing their information and are able to exercise their rights vis-à-vis the relevant entities.

In addition to the strengthening of data protection principles, the protections for special categories of personal data in Israel have been reinforced since the adoption of the adequacy decision. The PPL already offered stronger protections[1419] for data on the personality, intimate affairs[1420], state of health, economic state, opinions, and beliefs. In addition, in the *Kalanswa* case, the court ruled that biometric fingerprints taken in the workplace constitute sensitive personal data and confirmed also more generally that biometric data would normally be considered sensitive data[1421]. Moreover, the Israeli Genetic Data Law, 5761-2000 (Genetic Data Law) recognises the sensitivity of genetic data and sets out additional safeguards for their processing[1422]. For instance, consent to the processing of genetic data must be given in writing and there are specific rules for the storage of genetic data[1423]. The above is also reflected in the Data Security Regulations, which refer to biometric and genetic data as data with special sensitivity that require at least the medium level of protection[1424]. Finally, for

[1418] See Regulation 6(a) and (b) of the Privacy Protection Regulations. Regulation 6(c) of the Privacy Protection Regulations allows certain limited and qualified exceptions to these additional transparency obligations that are essentially equivalent to those provided under EU data protection legislation. More specifically, the obligation to inform, to the extent necessary and proportionate in the circumstances of the case, does not apply (1) if the database controller has reasonable grounds to assume that the particulars of the information to be provided are already known to the data subject, (2) if the contact information of the data subject is not known to the database controller, or the implementation of the duty to inform involves an unreasonable burden on the database controller, taking also into account the possibility to cooperate with the data exporter, (3) if there is a duty of confidentiality prescribed by law or a prohibition by law on the disclosure of the data, (4) if there is a legal provision that regulates the disclosure of the information to be provided, (5) if exercising the duty to inform may harm a person's life, health or body, (6) if exercising the duty to inform may harm journalistic activities or reveal the source of information for journalistic activity, or (7) if exercising the duty to inform will affect the rights of a person in a degree exceeding the harm caused to the data subject as a result of failure to disclose the information to be provided.

[1419] In accordance with Article 8(c)(2) PPL, databases containing data that is considered sensitive pursuant to Article 7 PPL must always be registered. In addition, the Data Security Regulations require an increased level of data security for databases that contain sensitive data, see Article 1(3) First schedule to the Data Security Regulations.

[1420] As confirmed by the case law of Israeli courts, data concerning a natural person's sex life or sexual orientation is covered by the category of data on intimate affairs. See for example Supreme Court ruling in HCJ 3809/08 The Association for Civil Rights in Israel v. the Israel Police (2012), where the Court found, in relation to Criminal Procedure Law, that "surveillance of a person, even if for a criminal investigation, may reveal other details, the knowledge of which is a violation of a person's privacy and his intimate affairs, such as health problems, consumer habits, sexual orientation, and so on."

[1421] Collective Dispute Appeal 7541-04-14 The New Workers' General Federation v. the Kalanswa Municipality (May 5, 2017).

[1422] See Articles 1, 11, 12, 15, 16 and 28G of the Genetic Data Law.

[1423] Articles 11 and 15 Genetic Data Law.

[1424] Article 1(3)(c) and (g), First Schedule to the Data Security Regulations. The Data Security Regulations lay down detailed obligations on how to maintain a record of accesses to a database and of events such as security breaches, on the obligation for controllers and processors (including the obligation to detail in written agreements between controllers and processors the purpose of processing, the type of processing operations authorised, the obligation for the processor to return or destroy data at the end of the processing), on periodical auditing, risk evaluations and penetrability tests, the obligation for a controller to adopt written security procedures binding all employees and organs of their organisation, to vet the qualification of employees and train them on data protection legislation and requirements before granting them access to a database (for databases of medium or high security level, training must be repeated periodically), to take measures to make sure only permitted authorized users use the database and database systems, the duties of data security officers, as well as technical aspects such as limiting the possibility to connect mobile devices to databases, or to connect database

data that has been transferred to Israel from the EU, Regulation 7 of the Privacy Protection Regulations extends the protections for sensitive data also to data regarding a person's ethnic origin and to data regarding trade union membership, so that all data considered sensitive under EU law now benefit from additional protections also under the Israeli framework.

Since the adoption of the adequacy decision, also the data protection rights of individuals have been strengthened in several ways.

The right of access is guaranteed in Article 13(a) PPL, which sets out that "every person is entitled to review, in person, or through a representative authorised by him in writing, or through his legal guardian, any data regarding such person which is kept in a database[1425]." The PPA has further clarified this right in a guideline issued in 2017[1426]. This guideline notably specifies that the right of access should be granted with respect to data in any format or file type, including video, text messaging or voice recordings. The guideline also confirms that data subjects benefit from the right of access with respect to data stored by their service provider. Finally, the guideline clarifies that under the right of access, data subjects should have the right to receive data in a digital format that may be read, heard or viewed by publicly available software, via email, secure website or any other digital means. In the past, the Israeli Supreme Court had already aligned the scope of the right of access in Israel with the scope of this right in the EU legal framework, interpreting the right of access as including the right of the data subject to receive a copy of the data[1427].

The right to rectification is provided for by Article 14 PPL, according to which a person who reviewed data about himself and found it to be incorrect, incomplete, unclear, or not up to date, may request the database owner to correct or delete the data. Pursuant to Article 14(c) PPL, the database owner may refuse to comply with such request for rectification, but the PPA's Directive No. 2/2012 clarifies that in view of the explicit language of Articles 13, 14 and 31A(4) PPL, a refusal to grant the right to rectification under this Directive with no grounds provided or not made in good faith will be considered by the PPA as a violation of that right[1428]. Moreover, pursuant to Article 15 PPL, an individual can appeal before a Court the refusal to grant the right to rectification[1429]. Finally, for data that has been transferred to Israel from the EU, the Privacy Protection Regulations require the database controller to have in place an organizational, technological or other mechanism to ensure that the data in the

---

systems to the internet or a public network. Also, the proposed draft Privacy Protection Bill (Amendment No. 14) that would amend the PPL recognises biometric and genetic data as categories of 'especially sensitive data'.

[1425] In the Israeli legal framework, the right of access can – subject to certain conditions and limitations - be restricted for data in specific databases that are listed in Article 13(e) PPL. For instance, the rules on access to data in databases may be disapplied with respect to a database of a security agency, to a database of the Prisons Service, to a database of a tax authority, or where the State security, its foreign relations or the provisions of any law require that data of a person is not disclosed to him. The conditions for and limitations to the application of these restrictions are described in Section 2.2.1. Additional rules with respect to the right of access are set out in the Privacy Protection Regulations (Terms of Review of Data and Procedures on Appeal for Refusal of Request for Review) – 5741-1981). The Regulations provide the conditions for review of personal data (Articles 1 and 3), the payment method (Article 6 sets the amount of 20 Old Shekels– less than 1€) and the legal procedure challenging the rejection of such request before a magistrate court (Articles 8, 9, 10).

[1426] PPA Guideline No. 1/2017 regarding the scope of the PPL on the right to access voice recordings, video and digital data, available at: https://www.gov.il/he/departments/policies/right_of_access.

[1427] HCJ 7256/95 Fishler v. Israel Police Commissioner, IsrSC 50(5) 1, (1996).

[1428] PPA Directive No. 2/2012, available at: https://www.gov.il/he/departments/policies/recruitment_guidelines.

[1429] See also Article 8 of the Protection of Privacy Regulations (Terms of Review of Data and Procedures on Appeal for Refusal of Request for Review).

database is correct, complete, clear and updated, and to take reasonable measures for the purpose of rectifying or deleting the data if the database controller finds that the database contains data that is not correct, complete, clear or updated[1430].

The right to deletion of personal data in the Israeli system was so far only available under Article 14 PPL, i.e., in cases where data is found to be incorrect, incomplete, unclear or not up to date. In addition, data subjects could obtain the deletion of their data by filing a complaint with the PPA[1431] or by bringing a case before court[1432]. With the adoption of the Privacy Protection Regulations, the right to deletion has been significantly strengthened for data that has been transferred to Israel from the EU. Regulation 3(a) of the Privacy Protection Regulations explicitly requires the database controller to delete data on request of the data subject if the data was created, obtained, accrued or collected in contravention of the provisions of any law, if the further use of the data is in violation of the law, or if the data is no longer necessary for the purposes for which it was created, obtained, accrued or collected. Pursuant to Regulation 3(b) of the Privacy Protection Regulations, a request to delete data may only be refused in certain limited and specific situations and subject to the requirements of necessity and proportionality[1433].

With respect to the transfer of personal data abroad, certain requirements in the Privacy Protection (Transfer of Databases Abroad) Regulations (Transfer Regulations)[1434] have been further interpreted and clarified by the PPA. In addition, the Data Security Regulations have established additional accountability obligations for controllers with respect to international transfers.

[1430] Regulation 5 of the Privacy Protection Regulations.

[1431] If the PPA finds that the PPL or other regulations promulgated thereunder have been violated, it can act to stop or prevent the violation. For instance, in a series of decisions against data traders and their clients taken between 2015 and 2017, the PPA ordered the deletion of data that had been illegally obtained from the Israeli population registry and other sources, see https://www.gov.il/he/departments/news/data_rings and https://www.gov.il/he/Departments/news/teleall. The PPA may also decide, if appropriate, to refer the case to a court.

[1432] Article 29(a)(4) PPL provides that the Court may order "the destruction of data which was illegally received, or prohibition of use of said data, or the surplus data as defined in section 23E, or it may give any other order with regards to the data." For example, in the Kalansawa case the Court ordered the deletion of the municipality employees' biometric data, after having held that the data had been unlawfully collected, CDA 7541-04-14 The New Workers' General Federation v. the Kalanswa Municipality (5 May 2017). In addition, Israeli courts ordered the destruction of data on the basis of Article 29 PPL for instance in CivC (Jerusalem Magistrate) 21933-11-17 Shorshan v. Kerem Nevot Ltd. (PBC) (published in Nevo, 24.6.2020) and CrimC (Tel Aviv Magistrate) 19578-11-14 The State of Israel v. A (published in Nevo, 27.7.2016.

[1433] Similarly to the situations in which a request for deletion may be refused under the EU legal framework, a database controller in Israel may refuse a request to delete data to the extent the use of the data is necessary and proportionate for exercising the right of freedom of expression, including the public's right to know, for performing a legal obligation or exercising an authority by operation of the law, for protecting a public interest, including for archival purposes, scientific research or statistical research, for conducting a legal proceeding or ensuring debt collection, for addressing fraud, theft or other incidents affecting the integrity of the data processing operations, or for fulfilling an obligation resulting from an international agreement to which the Government of Israel is a party. See Regulation 3(b) of the Privacy Protection Regulations.

[1434] Article 1 of the Transfer Regulations provides that the transfer abroad of data from databases in Israel is prohibited, unless the law of the country to which the data is transferred ensures a level of protection that is not lower than the level of protection provided for by Israeli law, and provided that certain principles listed in the Regulations apply. It is the responsibility of database controllers to assess the level of data protection and the application of the listed principles in the country where the data is received. Article 2 of the Transfer Regulations provides for a limited and exhaustive list of situations in which data may be transferred abroad even if the law of the country to which the data is transferred does not ensure an equivalent level of protection.

As regards Article 3 of the Transfer Regulations, which sets out the safeguards that need to be ensured for data that is transferred abroad[1435], the PPA has clarified in a legal opinion[1436] that the scope and content of the guarantee required by that Article can include different but sufficient assurances to ensure the privacy of the data subjects, taking into account the scope of the data, its sensitivity and other relevant circumstances, even if these assurances are not completely identical to the Israeli privacy and data protection legislation.

In addition, in an effort to align the Israeli transfer regime more closely with the respective rules at EU and international level, the PPA clarified that Article 3 should not be understood as prohibiting the onward transfer of data that has been received from Israel, provided that (1) the owner of the database in Israel from which the data was originally transferred had given written consent to the onward transfer to a third party, (2) that the onward transfer itself was done lawfully, i.e., based on consent of the data subjects or authorised by law; and (3) if the data were transferred to the third party directly from Israel, the transfer would comply with the conditions set out in Article 1 or Article 2 of the Transfer Regulations so that some continuity of protection is ensured.

As regards accountability requirements, the Data Security Regulations compel the data controller to define in the "database definitions document" (which describes key aspects of the database and the processing activities carried out) also the details of a possible transfer abroad[1437]. In particular, the database definitions document needs to specify "details of transferring the database or material parts thereof outside the State borders or using the data outside the State borders, the purpose of transfer, destination country, manner of transfer and identity of the transferee".

1.2. Oversight, enforcement and redress

Oversight and enforcement of the PPL is ensured by the PPA[1438]. While being part of the administrative structure of the Israeli Ministry of Justice[1439], the PPA carries out its functions

[1435] Pursuant to Article 3 of the Transfer Regulations, in any case of transfer of personal data abroad (both under Article 1 and Article 2 of the Transfer Regulations), the database controller must ensure that the recipient of the data undertakes in writing to apply adequate measures in order to protect the privacy of the data subjects and guarantee that the data shall be transferred to no other person, whether in the recipient's country or in another.

[1436] PPA Draft Legal Opinion - Article 3 of the Privacy Protection (Transfer of Data to Databases Abroad) Regulations, 5761-2001, available at: https://www.gov.il/BlobFolder/rfp/transfer_of_data_abroad_interpretation_draft/he/transfer%20of%20data%20abroad%20interpretationdraft.pdf.

[1437] Article 2(a)(4) of the Data Security Regulations.

[1438] The PPL foresees that oversight over the protection of privacy is carried out by the so-called Registrar. Pursuant to Article 10(c) PPL, the Registrar is responsible for supervising compliance with the provisions of the PPL (i.e., Chapter A and Chapter B of the PPL) and of the regulations thereunder. By resolution of the government of Israel of 2006 (available at: https://www.gov.il/he/departments/policies/2006_des4660), the Registrar was integrated into the Israeli Law, Information and Technology Authority (ILITA), which was created by that same decision. The role of the Head of ILITA was assigned to the Registrar. In order to better reflect the Authority's activities and increase public awareness as to its mission, ILITA was renamed as Privacy Protection Authority in 2017. The Head of the PPA is appointed by the Government and, pursuant to Article 7 PPL, needs to be a person at least qualified to be appointed as a Magistrates Court judge. In line with the relevant applicable rules, the Minister of Justice selects the candidate for the position of the Head of the PPA, but he can only select a candidate from among those that have been recommended by a 'search committee'. The Civil Service Commissioner's Office determines and publishes the characteristics of the position and the conditions to be fulfilled by the candidates, such as qualifications and professional experience. The search committee then evaluates the candidates' qualifications and capabilities under the equal opportunity principle underlying public

independently. Since the adoption of the adequacy decision, this independence has been strengthened.

More specifically, as formally clarified by a Resolution adopted by the Israeli government in October 2022 and its accompanying Explanatory Notes[1440], the PPA is "independent in exercising the powers vested in the Head of the Authority for performing its duties", which notably means that it "is not subordinate to the ministerial level or to intervention from outside the Authority." Moreover, the Government Resolution clarifies that within the Ministry of Justice's budget, the PPA's operational budget must be managed separately.

In addition to its independence, also the PPA's role and powers have been reinforced since the adoption of the adequacy decision. First, the PPA has been equipped with additional powers[1441] under the Data Security Regulations. Pursuant to Article 11(d) of the Data Security Regulations, in cases of severe security events[1442] the database owner is required to immediately notify the PPA and report on the measures taken following the event. The PPA is entitled to order a database owner to notify the security event to any data subject who may be harmed by the event. Moreover, in specific circumstances the PPA may impose additional requirements on a database in order to strengthen its security or may exempt certain databases from specific provisions[1443]. Second, to reflect its increasing role and its wide-ranging tasks, the PPA's budget and number of staff members have increased significantly[1444]. Third, Israeli courts have clarified the PPA's powers to issue guidelines and enforce them, stressing that these powers are to be construed broadly and are not limited to what is set forth explicitly in the law. According to the courts, the PPA is entitled to exercise its discretion in an individual case or according to a general policy determined in accordance with the professional interpretation of the PPL. Thus, it is within the authority of the PPA to issue guidelines and

---

tenders. Once the Minister of Justice has selected a candidate among those recommended by the search committee, the Israeli government needs to approve the appointment.

[1439] Pursuant to Article 10(d) and (e), the Minister of Justice is required to establish, with approval by the Knesset Constitution, Law and Justice Committee, a supervisory unit to supervise the databases, their registration and the data security therein and the Registrar shall head that supervisory unit.

[1440] Independence of the Privacy Protection Authority, Government Resolution No. 1890 of 2 October 2022 (Government Resolution No. 1890), available at: https://www.gov.il/he/departments/policies/dec1890-2022. An unofficial English translation of the Government Resolution No. 1890 is available at: https://www.gov.il/en/departments/legalInfo/resolution1890. In the Israeli system, government resolutions are binding on all parts of the government. Government Resolution No. 1890 also specifies the qualification required for being appointed as Head of the PPA, i.e., to be qualified to be appointed as District Court Judge (rather than as Magistrate Court Judge, as provided by Article 7 PPL).

[1441] Under the PPL, in order to carry out its functions, the staff of the PPA can notably request relevant information and documents from any person involved, as well as enter, search and seize any object in any place for which there are reasonable grounds to believe that a database is operated therein. The PPA can act on the basis of individual complaints or on its own initiative. If a possessor or owner of a database has infringed any provision of the PPL or fails to comply with a demand from the PPA, the PPA may suspend or cancel the registration of a database, and thus suspend or prohibit the processing of data in this database. See Article 10 PPL.

[1442] Pursuant to Article 11(a) of the Data Security Regulations, a security incident is defined as any event that raises concern for the breach of data integrity, the unauthorized use of data or a deviation from authorization.

[1443] Article 20 of the Data Security Regulations.

[1444] According to information provided by the Israeli authorities, the PPA's budget had increased by 65% to 15 million NIS in May 2019 and was further increased to more than 17 million NIS in 2022. Moreover, between 2016 and 2023 the PPA received additional 33 staff members.

corrective orders to database controllers, processors and managers, reflecting the PPA's interpretation to the provisions of the law[1445].

As regards possibilities for individuals to obtain redress, the Israeli system continues to offer various avenues. A person claiming data about him or her was used contrary to the PPL may lodge a complaint with the PPA[1446] and may apply directly to court if a request for access or rectification is refused[1447]. Moreover, a person claiming data about him was used contrary to the provisions under the PPL, can apply to the court with a civil tort lawsuit when the defendants are civil entities[1448]. When the defendant is a government agency, the individual may file an administrative petition, either to the Supreme Court or to the Administrative Court.[1449]. Where a violation of the PPL constitutes a criminal offence, individuals can also submit a criminal complaint or a private criminal indictment against another individual pursuant to Article 68 of the Israeli Criminal Procedure Law (combined version) 5742-1982. In the Israeli system, individuals can also obtain damages for violations of the PPL[1450]. Finally, in addition to any other penalty and relief, the court may, in a criminal or civil trial for infringement of any provision of the PPL, issue an order, for instance on the destruction of the information that was illegally received or on the prohibition of the use of such information[1451].

The PPA plays a very active role in the interpretation and enforcement of data protection law, both when it comes to its engagement with stakeholders and when exercising its oversight role. Its activities include the issuing of opinions and guidelines, enforcement actions and the promotion of legislation[1452]. Since the adoption of the adequacy decision, the PPA issued numerous guidelines, position papers and legal opinions. Among other, it published guidelines on the Data Security Regulations, on the right to access, on the use of surveillance cameras in the public domain, on workplace surveillance, on the use of outsourcing services for data processing, on privacy protection during recruitment procedures and on the use of voter registers during elections. Most recently, in 2022, the PPA updated its policy regarding the receipt of reports on data security incidents, requiring serious incidents to be reported

[1445] AdminC (TA) 24867-02-11 I.D.I. Insurance Company Ltd. v. Ministry of Justice the Israeli Law, Information and Technology Authority – the Registrar of Databases, (Jul. 7, 2012), Nevo Legal Database, at para. 3 of the judgment of Judge Agmon-Gonen, that was upheld by the Supreme Court in AdminA 7043/12 I.D.I. Insurance Company Ltd. v. Ministry of Justice the Israeli Law, Information and Technology Authority – the Registrar of Databases (Jan. 15, 2014), Nevo Legal Database.

[1446] As confirmed by Article 2(D) of Government Resolution No. 1890, one of the PPA's duties is to "handle public inquiries where there are grounds for harming data subjects under the Privacy Protection Law, 5741-1981". When an individual lodges an inquiry with the PPA, it is authorized to exercise its various enforcement powers.

[1447] Article 15 PPL.

[1448] Pursuant to Article 4 PPL, an infringement of privacy constitutes a civil tort.

[1449] Article 15(d)(2) Basic Law: The Judiciary. Additionally, a class action may be filed against private operators.

[1450] Where a person has been convicted of a criminal offence under Article 5 PPL, the court can order the payment of compensation up to 50 000 NIS to the injured party, without the need for proof of damage, or a higher compensation if the damage is proven. The same applies in a trial for civil tort, see Article 29A PPL.

[1451] Article 29(a) PPL.

[1452] For instance, to name just a few, the PPA was involved in the legislation processes concerning the Credit Data Law, the Financial Information Services Law, 5782-2021, the Law regarding Powers of Collection and Analysis of Passenger Name Record (PNR) Data of Passengers travelling to or from Israel, 5783-2023, the Law on the Inclusion of Biometric Methods of Identification and Biometric Identification Data in Identification Documents and Databases, 5770-2009, and the Income Tax Regulations (Regulations Regarding Currency Service Providers (Temporary Provisions), 5779-2018.

immediately. In addition, it recommended that organizations and companies in all sectors of the economy that process personal data should appoint privacy protection officers.

Since the adoption of the adequacy decision, the PPA has also stepped up its enforcement activities[1453]. In terms of investigations, the PPA carried out a number of audits (resulting in specific corrective orders) in sectors that had been identified for a high risk of invasion of privacy (for instance retail companies, insurance funds, as well as the health sector). Its annual reports for instance show that the PPA conducted 244 audits across seven sectors in 2020, 224 audits across four sectors in 2021 and 400 audits across seven sectors in 2022. For example, the PPA investigated the trading of sensitive health data of patients by health care service providers, and investigated a breach of the Population Registry Database. In recent years, the PPA imposed administrative fines on various controllers and processors[1454]. In addition, the PPA carried out important criminal investigations that were followed by criminal proceedings, resulting in significant fines as well as imprisonment for certain individuals involved. In particular, the PPA opened six criminal investigations in 2020 and eight in 2022. For instance, following a joint criminal investigation by the Israel Police and the PPA, the mayor of a medium-sized Israeli city was, among other, charged under Article 5 PPL for the use of personal data from municipal databases for political purposes[1455]. Each year, the PPA handles a high number of security breach reports, as well as a significant number of public inquiries (e.g., 1470 public inquiries in 2020, 1670 in 2021 and 1935 in 2022)[1456].

Finally, the PPA carries out various outreach activities, including by sending a periodic newsletter to a large number of subscribers, by regularly organising information sessions and events and by managing a forum for privacy awareness and training for the private and government sectors.

2. ACCESS TO AND USE OF PERSONAL DATA TRANSFERRED FROM THE EUROPEAN UNION BY PUBLIC AUTHORITIES IN ISRAEL

2.1. General legal framework

The limitations and safeguards that apply to the collection and subsequent use of personal data by Israeli public authorities for purposes of criminal law enforcement and national security follow from Israel's overarching constitutional framework, the rules that apply to the processing of personal data, as well as specific laws regulating access to data.

Access to and processing of personal information by Israeli public authorities is first of all governed by general principles that follow from the constitutional framework, i.e., Basic Law:

[1453] See the annual reports of the PPA available at https://www.gov.il/he/departments/publications/?OfficeId=4aadba43-3d71-4e7c-a4fe-5bf47b723d4e&skip=30&limit=40.

[1454] For example, the PPA imposed administrative fines in a case concerning the misuse of personal data by a political party and on an employee of the Israeli Tax Authority for repeated unauthorized use of personal data from the database of the Tax Authority. Further information is available at: https://www.gov.il/he/departments/news/fine95k.

[1455] The criminal proceedings are still ongoing under reference number CrimeC 58743-03-23.

[1456] See the PPA's annual reports for 2021, available at https://www.gov.il/BlobFolder/reports/annual_report_2021/he/report_2021.pdf, and for 2019-2020, available at: https://www.gov.il/BlobFolder/reports/report_2019-2020/he/anual%20report%202019-2020.pdf.

Human Dignity and Liberty adopted in 1992[1457]. In particular, Article 7 of the Basic Law provides that all persons have the right to privacy and to intimacy, that there shall be no entry into the private premises of a person who has not consented thereto, that no search shall be conducted on the private premises of a person, nor in the body or personal effects, and that there shall be no violation of the confidentiality of conversation, or of the writings or records of a person[1458]. This article has been interpreted by Israel's Supreme Court as providing a comprehensive protection of the right to privacy for any individual and as including the right to the protection of personal data[1459]. Moreover, case law has confirmed the particular importance of the protection of the right to privacy in the Israeli legal order, as an essential precondition for a democratic regime[1460].

While the right to privacy is not absolute, any interference with this right by a public authority must be provided for in law or on the basis of a law through an explicit authorisation therein. A law providing for a lawful interference with the rights laid down in the Basic Law must be consistent with the values of the State of Israel, pursue an appropriate purpose and fulfil the principle of proportionality[1461]. As regards the principle of proportionality, the Supreme Court has clarified that any limitation of a right (such as through e.g., the processing, including the collection, of personal data by public authorities) must meet three cumulative elements. First, it must be suitable for the appropriate purpose that it is intended to achieve. Second, it must be the least harmful/intrusive measure to achieve that purpose (i.e., a limitation may not be imposed if the purpose can be achieved by another, less harmful measure). Third, there must be a proper balance between the benefits that would be achieved by the limitation and the harm that would be caused to the individual[1462].

In addition, the processing of personal information by Israeli public authorities (including criminal law enforcement authorities and national security authorities) is subject to the PPL and the Regulations adopted on the basis of the PPL[1463]. The PPL and the Regulations

[1457] In the Israeli legal system, Basic Laws enjoy a constitutional character. The superiority of Basic Laws over other laws has been upheld by Israeli courts in several instances. An overview of the relevant jurisprudence is available at: https://main.knesset.gov.il/EN/activity/Pages/BasicLaws.aspx.

[1458] Article 7 Basic Law: Human Dignity and Liberty. Pursuant to Article 11 of the Basic Law, all governmental authorities are bound to respect the rights established by this Basic Law.

[1459] On the inclusion of the right to personal data protection under the scope of Article 7, see the Supreme Court's ruling in HCJ 8070/98 ACRI v. Minister of Interior 58(4) PD 842 (2004), in which the practice of providing financial entities and other bodies with personal data listed in the Population Registry was deemed unlawful.

[1460] See e.g., HCJ 2109/20 Adv. Shachar Ben-Meir v. Prime Minister (26.4.2020), section 36 in the judgment of President Chayut.

[1461] Article 8 of the Basic Law.

[1462] See e.g., CA 6821/93 Bank Mizrachi Meuchad v. Migdal Cooperative Village 49(4) PD 221 (1995); HCJ 2605/05 The Human Rights Division, Academic Center of Law and Business v. Minister of Finance 63(2) PD 545 (2009). Ad. Cr.H. 1062/21 Urich v. The State of Israel (11.01.2022), (Urich) sections 73 and 75 in the judgment of President Chayut; Cr.Ap 1302/92 State of Israel v. Nachmias et al**.** P.D 49(3) 309, 353 (1995) (Nachmias), sections 10, 13 in the judgment of Justice Bach; Telecommunication Data Law HCJ, sections 16 and 26 of President (ret.) Beinisch; HCJ 2109/20 Adv. Shachar Ben-Meir v. Prime Minister (26.4.2020) (First ISA Authorization HCJ), sections 38-39, 43-45 in the judgment of President Chayut; Population Registry HCJ, section 7 in the judgment of Justice (ret.) Dorner; HCJ 6732/20 Association for Civil Rights in Israel v. the Knesset (2021) (Second ISA Authorization HCJ), section 7 in the judgment of Justice Hendel, section 18 in the judgment of President Chayut.

[1463] See in particular the Data Security Regulations, Transfer Regulations, and Privacy Protection Regulations. The Privacy Protection Regulations apply to data that is in a database in Israel that has been transferred from the European Economic Area, unless the data has been transferred directly from an authority in the EEA responsible

adopted on its basis, as interpreted by the PPA and case law of Israeli courts, reflect the principles of lawfulness[1464], purpose limitation[1465], accuracy[1466], transparency[1467], storage limitation[1468] and security[1469], and provide individuals with the right of access to their personal information[1470], the right to correction[1471] and the right to deletion[1472]. Finally, the Transfer Regulations contain specific provisions on international transfers of personal data[1473]. In addition to the PPL, criminal law enforcement and national security authorities are also subject to specific laws and regulations, which provide for limitations and safeguards concerning the collection and use of personal data reflecting the general principles following from the Basic Law: Human Dignity and Liberty, as further described below.

These general limitations and safeguards can be invoked by individuals before the PPA and courts to obtain redress (see sections 2.2.4 and 2.3.4).

In addition, the Attorney General has issued a binding legal opinion further clarifying the application of the constitutional principles of lawfulness, necessity and proportionality to the processing of personal data by public bodies in Israel[1474]. The opinion confirms that any public authority in Israel, including law enforcement and national security authorities, may only take a measure that interferes with the right to privacy of individuals if such measure is provided for or authorised by law, pursues an appropriate purpose (i.e., a purpose that is legitimate and in accordance with legal authority laid down in law), is suitable to achieve that purpose, constitutes the least intrusive measure (compared to other available measures) and is

---

for national security or criminal law enforcement to a Security Agency in Israel. In addition, their application to the use of data for the protection of national security or criminal law enforcement may be restricted, but only to the extent necessary and proportionate for these purposes, see Regulation 2(b)(2) of the Privacy Protection Regulations.

[1464] Chapter A PPL prohibits infringements of privacy without the individual's consent and thus recognises that consent can be a legitimate ground for the processing of personal data. It follows from Article 35 PPL and case law that the collection and processing of personal data can also be based on an authorization by a law. The Israeli Supreme Court has clarified with respect to public authorities that according to the principle of 'legality of authority' each administrative authority must act solely within the powers vested in it by law. When an administrative act may lead to an infringement of individual rights, there must be a clear and explicit legal authority in primary legislation allowing this act, and the legislative authority must comply with the Basic law: Human Dignity and Liberty. See PCA 2558/16 Jane Doe v. Compensation Officer - Ministry of Defence (5 November 2017).

[1465] Articles 2(9) and 8(b) PPL.

[1466] Article 14 PPL and Regulation 5 of the Privacy Protection Regulations.

[1467] Articles 11-12 PPL and Regulation 6 of the Privacy Protection Regulations.

[1468] Regulation 4 of the Privacy Protection Regulations and Regulation 2(c) of the Data Security Regulations.

[1469] Articles 16, 17, 17A and 17B PPL and Data Security Regulations.

[1470] Article 13(a) PPL.

[1471] Article 14 PPL and Regulation 5 of the Privacy Protection Regulations.

[1472] Regulation 3 of the Privacy Protection Regulations.

[1473] Articles 1, 2 and 3 of the Transfer Regulations.

[1474] See the legal opinion of the Attorney General addressed to the Director of the ISA "Re: Constitutional principles in processing personal data in public bodies and in the Israel Security Agency in particular" (AG Opinion), available at https://www.gov.il/he/Departments/DynamicCollectors/legal-opinions-attorney-general?skip=0&Title=%D7%A2%D7%A7%D7%A8%D7%95%D7%A0%D7%95%D7%AA%20%D7%97%D7%95%D7%A7%D7%AA%D7%99%D7%99%D7%9D. In the Israeli legal system, pursuant to case law of the Supreme Court, the legal opinion of the Attorney General on the interpretation of the law is binding for the entire executive branch. See e.g., HCJ 4723/96 Atiyah v. Attorney General P.D. 56(3) 714, 731 (1997); HCJ 4267/93 Amitai – Citizens for Sound Administration and Moral Integrity – Prime Minister of Israel, P.D. 47(5) 441, 473 (1993); HCJ 5124/18 Tnuva Central Coop. for the Marketing of Agricultural Products in Israel Ltd. v. Minister of Finance, (4.3.2019); HCJ 158/21 Physicians for Human Rights v. Minister of Public Security, (31.1.2021); see also: Attorney General Guideline no. 1.0000 on the subject "Roles of the Attorney General."

proportionate (which requires balancing the benefits that would be achieved by the measure against the harm that would be caused to the individual)[1475].

2.2. Access and use by Israeli public authorities for criminal law enforcement purposes

The Israel Police is the main law enforcement authority in Israel. Its functions and mandate are defined in the Police Order [New Version], 5731 – 1971, whereas the rules regulating the collection and processing of personal data by the Israel Police are enshrined in laws implementing the Police's general mandate and duties. Israeli law imposes a number of safeguards and limitations on how the Police has access to and uses personal data for criminal law enforcement purposes, and it also provides oversight and redress mechanisms in this area. The conditions under which access to personal data can take place and the safeguards applicable to the use of these powers are assessed in the following sections.

2.2.1. Legal bases and applicable limitations/safeguards

Personal data transferred under the adequacy decision and processed by organisations in Israel may be obtained by Israeli criminal law enforcement authorities mainly by means of investigative measures under the Criminal Procedure Ordinance (Arrest and Search) [New Version], 5729–1969 (Criminal Procedure Ordinance), the Criminal Procedure Law (Enforcement Powers – Communication Data), 5768 – 2007 (Communication Data Law), and the Wiretapping Law, 5739-1979. When collecting information on the basis of these laws, criminal law enforcement authorities also have to comply with the Constitutional requirements of necessity and proportionality, as developed in case law and reflected in the AG opinion (see also section 3.2.1.).

The Criminal Procedure Ordinance provides the Israel police with a legal basis for accessing personal data held by commercial operators through searches and seizures. It lays down detailed rules on the scope and application of these measures, aimed at ensuring that the interference with the rights of individuals will be limited to what is necessary for a specific criminal investigation and proportionate to the pursued purpose. Searches may only take place on the basis of a court-issued search warrant[1476] and the issuing of such warrant is subject to specific procedural and substantive requirements.

More specifically, a judge may issue a search warrant only if (1) the search is necessary in order to assure presentation of an object for purposes of any investigation, trial or other proceeding; (2) the judge has reason to believe that the place is used for the storage or sale of a stolen object (or that it contains an object with which or in respect of which an offense was committed, or which was used or is intended to be used for an illegal purpose); or (3) the

[1475] Article 8 of the Basic Law, as well as case law, see e.g., CA 6821/93 Bank Mizrachi Meuchad v. Migdal Cooperative Village 49(4) PD 221 (1995); HCJ 2605/05 The Human Rights Division, Academic Center of Law and Business v. Minister of Finance 63(2) PD 545 (2009).

[1476] See Articles 23 and 24 Criminal Procedure Ordinance. Pursuant to Article 25 Criminal Procedure Ordinance, warrantless searches may only take place in exceptional circumstances A policeman may search a premise if (1) he has reasonable grounds to assume that a felony is being committed there or that a felony was committed there recently; (2) the person in possession of the house or place asks for help from the police; (3) a person who is there asks for the help of the police and there are grounds to assume that an offense is being committed there; and (4) if the policeman chases a person who evades arrest or escapes from lawful custody.

judge has reason to believe that that an offense was committed or is intended to be committed against a person in that place[1477]. Moreover, access to computer data, irrespective of the kind of hardware on which it is stored (e.g., including smartphones etc.) is permitted only subject to a Court order which "details the objectives of the search and its conditions, that will be determined in a manner that will not harm the privacy of a person in an excessive manner."[1478] Any search, including the search of computers, must be carried out in the presence of two witnesses that are not policemen[1479] and the occupant of the house or place or the person whose computer material is being searched is entitled to be present during the search. On the basis of a search warrant, a policeman may seize any object described in the search warrant[1480], or any other object if he has reasonable grounds to assume that an offense was or is about to be committed with it or that it is likely to serve as evidence in a judicial proceeding for an offense[1481]. A list of objects seized is to be drawn up by the person who conducts the search and the occupant of the house or place or the person whose computer material is being searched shall be given a copy of the list of the objects seized[1482].

The Communication Data Law allows the Israel Police and other investigating authorities[1483] to obtain communication data, i.e., metadata[1484], from telecommunications companies. Such data may be collected from telecommunication providers on the basis of a detailed request[1485] by an investigating authority approved by the Magistrates Court[1486], and only for the purposes of saving or protecting the life of a person, investigating or preventing offences of the felony or misdemeanour class[1487], determining the identity of offenders and bringing legal action

[1477] Article 23 Criminal Procedure Ordinance.
[1478] Article 23A of the Criminal Procedure Ordinance.
[1479] Article 26 Criminal Procedure Ordinance. The presence of witnesses is not compulsory where the search cannot be performed in that manner under the circumstances of the case and because of the urgency of the matter, where a judge permitted the search to be conducted in the absence of witnesses or where the person in possession of the house or place where the search is conducted asks the search to be conducted in the absence of witnesses, see Article 26(1)-(3) Criminal Procedure Ordinance.
[1480] Article 24 Criminal Procedure Ordinance.
[1481] Article 32 Criminal Procedure Ordinance.
[1482] Articles 27 and 28 Criminal Procedure Ordinance.
[1483] Pursuant to Article 1 Communication Data Law, other investigative agencies are the following: Investigating Military Police, Internal Investigations Unit of the Military Police Corps, Policemen Investigation Division in the Ministry of Justice, Israeli Securities Authority, Antitrust Authority, Israel Tax Authority.
[1484] In Article 1 Communication Data Law, 'communication data' is defined as including 'subscriber' data, location data and communication traffic data. 'Subscriber' is defined as the recipient of telecommunication services or owner of a telecommunications device (or facility), whereas the definition of 'subscriber data' encompasses data on the type of telecommunication service provided to the subscriber, the subscriber's name, address, ID and payment means, the address of installation of the telecommunication facility used by the subscriber and the identifying data of the telecommunication facility in the subscriber's possession. The content of communications is explicitly excluded by the scope of 'communication data'.
[1485] Pursuant to Article 3(d) Communication Data Law, the application must be filed in writing and must contain a number of elements, including a summary of the facts, the purposes for which the communication data is required, the identification details of the subscriber or telecommunication facility for which communication data is sought, if known in advance, and the timeframe for which communication data is sought.
[1486] In addition, Article 6 Communication Data Law allows the Head of the Investigations and Intelligence Division in the Israel Police to request a limited number of basic categories of personal data from telecom companies in Israel. As this provision only allows the collection of identification data (defined in Article 1 Communication Data Law as including name, ID or corporation ID, address and phone number) from subscribers of a telecom service in Israel, it concerns exclusively data from Israeli subscribers and does not affect data received in Israel from controllers or processors abroad.
[1487] Article 1 Communication Data Law. Pursuant to the Penal Law, 5737 - 1977, 'felony' refers to an offence punishable by a prison term of more than 3 years. A 'misdemeanour' refers to an offence punishable by a prison term of 3 months to 3 years.

against them, as well as for the purpose of confiscation of assets according to law (for instance in order to gather evidence of the beneficial ownership of an asset)[1488]. The Court may only grant access to such data by means of an order if the conditions provided in the law are met, i.e., on condition that granting the authority access to the data does not harm the privacy of the data subject in an excessive manner, and that the collection of data is carried out only for one of the purposes specified in the law[1489]. When deciding on the application, the Court will consider, among others, the need to achieve the purposes specified in the law, the type of communication data sought, the extent of the infringement of privacy, and the severity of the offense. In the order, the Court sets out a timeframe during which communication data may be obtained, which cannot exceed 30 days from the date when the order is issued[1490].

In a situation where data is urgently needed, so that there is no time to submit an application to the Court pursuant to the above-described procedure, for the purpose of preventing a felony class offense or discovering its perpetrator, or for saving human life, a member of the Israel Police or Military Police may request access to communication data for a period of maximum 24 hours without a Court order[1491]. In this case, the request for this special permit is submitted to the relevant authorised officer[1492]. The authorised officer will grant such permit only upon condition that there is an urgent need to obtain communication data for the abovementioned purposes, and that there is no time to obtain a Court order. After having issued such a permit, the authorised officer is required to report in writing to a higher-ranking member of their respective police corps the reasons for issuing the permit[1493].

Importantly, all the above-mentioned provisions for the collection and use of communication data have been examined and further clarified by the Israeli Supreme Court in the case of *The Association for Civil Rights in Israel*[1494], where the Supreme Court assessed the constitutionality of some of the provisions of the Communication Data Law. It held that, in order to ensure the correct balance between the purpose of the law and the protection of the right to privacy, the legal arrangements for accessing personal data provided by the law would need to be interpreted narrowly and applied in a proportionate manner. In particular, the law should be interpreted as allowing the authorities to access data solely for the purpose of

[1488] Article 3 Communication Data Law.
[1489] Article 3(a) Communication Data Law.
[1490] Article 3(g) Communication Data Law. Under Article 3(b) Communication Data Law, if the subscriber with respect to whom the application for communication data is filed is subject to professional privilege by virtue of any applicable law (including case law), the Court will not allow receiving such communication data, unless it is convinced, based on clear elaboration in the application, that there are grounds to suspect that the professional is involved in the offense regarding which the application was filed. In such a case, the application must indicate that the subscriber is a person subject to professional privilege and, in the event that the Court decides to issue an order in relation to the communication data of that person, the Court shall detail in the reasons for issuing the order despite the circumstance of the professional privilege.
[1491] Article 4 Communication Data Law
[1492] Under Article 1 of the Communication Data Law, an authorised officer is one of the following: a police officer from the investigations or intelligence apparatus of the Israel Police with a rank of commander and above or a police officer who serves as commander of a national or district centre of the Police, authorized for that purpose by the Commissioner or (2) an officer with a rank of lieutenant colonel in the Investigating Military Police authorized by the Chief of Staff for the purpose.
[1493] See Article 4(a) and (d) Communication Data Law. Moreover, the Head of Investigation and Intelligence Department is required to submit a report to the Attorney General once per three months concerning permits issued on the basis of Article 4 Communication Data Law.
[1494] HCJ 3809/08 The Association for Civil Rights in Israel v. the Israel Police (May 28, 2012).

investigating or preventing specific offenses or offenders, and not for general intelligence activity purposes relating to offenses or offenders.

The Israel Police may also access personal data transferred from the EU on the basis of the Wiretapping Law. Wiretapping is defined as listening to a conversation without the consent of any of the parties, whereas "conversation" is defined to include oral conversations, but also conversations by means of telecommunication, including (inter alia) between computers[1495]. The Wiretapping Law thus regulates the collection of the content of communications. Wiretapping is prohibited and subject to imprisonment, except if explicitly authorised by law[1496]. The collection of the content of communications or the use of such information in violation of the Wiretapping Law is also subject to imprisonment. Communications that are intercepted in violation of the Wiretapping Law are inadmissible as evidence in judicial proceedings, except in limited circumstances, e.g., if the proceedings concern a violation of the Wiretapping Law subject to criminal sanctions[1497].

In the area of criminal law enforcement, the Wiretapping Law allows, in relation to offences of the felony class (i.e., offenses that are punishable by a prison term of more than three years), wiretapping for the purposes of detecting, preventing or investigating offences, of identifying or capturing offenders, and for the investigation of a forfeiture of property related to an offence[1498]. In these cases, wiretapping has to be authorised in an order by the Chief Justice of a District Court or a Deputy Chief Justice of a District Court authorised by the Chief Justice for this purpose. The order can be issued only following a request by an authorised police officer and only if the Judge is convinced, after having considered the extent of the violation of privacy, that such measure is required to achieve the purposes listed in the Law[1499].

If known in advance, the order needs to describe the identity of the person for whose conversation wiretap was approved, or the identity of the line or facility used or intended for use for reception, transfer or transmission of telecommunications and for which wiretap was approved, as well as the location or type of conversation. Moreover, the order needs to detail the manners of wiretapping that are permitted[1500]. The validity of the order is limited to three months, but it may be renewed subject to the same conditions as the initial order[1501].

Exceptionally, the Israeli Police General Commissioner can permit in writing wiretapping for a maximum period of 48 hours, if he is convinced that for preventing a felony or identifying its perpetrators there is need for immediate wiretapping and no time to obtain a Court order through the abovementioned procedure[1502]. The Police Commissioner is required to notify

[1495] Article 1 Wiretapping Law.
[1496] Article 2 Wiretapping Law.
[1497] Article 13 Wiretapping Law.
[1498] Article 6 Wiretapping Law.
[1499] Article 6(a) of the Wiretapping Law. The interception of privileged communications (i.e. of an attorney, physician, psychologist, social worker or clergyman) may only take place upon written request from the Police, if authorised by a District Court President or Deputy President if the latter is convinced that there are grounds to suspect that the concerned individual is involved in murder, manslaughter, an offense that poses danger to national security or a drug transaction offense (Article 9A(a)(2) Wiretapping Law.
[1500] Article 6(d) of the Wiretapping Law.
[1501] Article 6(e) of the Wiretapping Law.
[1502] Article 7 Wiretapping Law.

immediately the Attorney General in writing of such permit, and the Attorney General is entitled to revoke the permit[1503]. The Court may authorise to prolong the wiretapping if the conditions for wiretapping are fulfilled[1504].

Finally, the Police may, in the performance of its functions, receive information, including personal data, from other public authorities that can provide such information subject to their discretion under the PPL where they are not prohibited from doing so by other laws[1505]. As a general requirement, public authorities can share personal data with other authorities (1) where doing so is within the scope of the mandate or functions of the entity providing the information and is required for a purpose of implementing a law or for the performance of tasks by the providing or receiving entity; or (2) where the receiving entity may, by law, obtain the information in any event from any other source[1506]. Any personal data transfer between public authorities is subject to the constitutional necessity and proportionality requirements, as described in the AG Opinion[1507].

2.2.2. Further use of the information collected

The further use of data collected by Israeli criminal law enforcement authorities on one of the grounds referred to in Section 2.2.1, as well as the sharing of such data with a different authority for purposes other than the ones for which it was originally collected (so-called 'onward sharing'), is subject to different safeguards and limitations.

First, the processing of personal data by law enforcement authorities in Israel is governed by the provisions of the PPL and the Regulations adopted on the basis of the PPL, as described in section 2.1. The PPL and the relevant Regulations set requirements on lawfulness[1508], purpose limitation[1509], accuracy[1510], transparency[1511], storage limitation[1512] and security[1513]. In addition, Chapter D of the PPL provides for specific rules on the sharing of information between public bodies (as described in the section 2.2.1). When law enforcement authorities in Israel intend to share personal data with law enforcement authorities of a third country, specific requirements set out in the Transfer Regulations apply[1514]. According to these

[1503] See Article 7(b) of the Wiretapping Law.
[1504] See Article 7(c) of the Wiretapping Law.
[1505] Article 23B(b) PPL.
[1506] Article 23C PPL.
[1507] HCJ 8070/98 ACRI v. Minister of Interior 58(4) PD 842 (2004).
[1508] Chapter A PPL prohibits infringements of privacy without the individual's consent and thus recognises that consent can be a legitimate ground for the processing of personal data. It follows from Article 35 PPL and case law that the collection and processing of personal data can also be based on an authorization by a law. The Israeli Supreme Court has clarified with respect to public authorities that according to the principle of 'legality of authority' each administrative authority must act solely within the powers vested in it by law. When an administrative act may lead to an infringement of individual rights, there must be a clear and explicit legal authority in primary or secondary legislation allowing this act, and the legislative authority must comply with the Basic law: Human Dignity and Liberty.
[1509] Articles 2(9) and 8(b) PPL.
[1510] Article 14 PPL and Regulation 5 of the Privacy Protection Regulations.
[1511] Article 11 PPL and Regulation 6 of the Privacy Protection Regulations.
[1512] Regulation 4 of the Privacy Protection Regulations and Regulation 2(c) of the Data Security Regulations.
[1513] Articles 16, 17, 17A and 17B PPL and Data Security Regulations.
[1514] In certain limited situations, which concern data generated in Israel or received from law enforcement authorities abroad and therefore normally do not affect personal data transferred from the EU to Israel on the basis of the adequacy decision, the conditions for the transfer of personal data abroad are set out in specific legislation. See e.g., Article 15 Criminal Information and Rehabilitation of Offenders Law, 5779-2019, which

Regulations, the transfer abroad of data from databases in Israel is prohibited, unless the law of the country to which the data is transferred ensures a level of protection that is not lower than the level of protection provided for by Israeli law, and provided that certain principles listed in the Regulations apply[1515]. In a limited number of situations listed exhaustively in the Regulations, data may be transferred abroad even if the law of the country to which the data is transferred does not ensure an equivalent level of protection. These are either situations in which the recipient of the data is bound by an agreement with the database owner in Israel to guarantee the protection of privacy after the transfer in a way that would comply with the conditions for data processing in Israel, or situations that are similar to the specific situations in which transfers to third countries are possible in the absence of an adequacy finding or appropriate safeguards under the GDPR. Transfers may notably take place if the data subject has consented to the transfer, if the consent of the data subject cannot be obtained and the transfer is vital to the protection of his health or physical wellbeing, the data was made available to the public or was opened for public inspection by legal authority, or if the transfer of data is vital to public safety or security[1516]. Finally, in any case of transfer of personal data abroad, the database controller must ensure that the recipient of the data undertakes in writing to apply adequate measures in order to protect the privacy of the data subjects and guarantee that the data shall be transferred to no other person, whether in the recipient's country or in another[1517]. In any event, as follows in particular from case law, reflected in the AG Opinion, any processing, including the use, retention or sharing, of personal data by public authorities has to comply with the principles of lawfulness, necessity and proportionality.

Second, the different laws that allow for data collection by criminal law enforcement authorities in Israel impose specific limitations and safeguards as to the use and further dissemination of the information obtained in exercising the powers they grant.

With respect to wiretapping, the Wiretapping Law requires that wiretap material which is not needed to prevent offences or identify offenders shall be deleted[1518]. Moreover, further rules on the retention and use of wiretap data are contained in the Wiretapping Regulations, 5746-1986 (Wiretapping Regulations). In terms of retention, the Wiretapping Regulations stipulate that where an order was received to delete the recording material, every possessor of such

---

allows the Israel police to transfer information from the criminal registry to a foreign country or to a body outside of Israel for the purpose of fulfilling its duties, provided that Israel has committed to do so in an agreement or treaty and subject to certain conditions, notably that the information will only be used for the purpose of fulfilling the duties of the body receiving the information and only for the purpose of maintaining public peace and security and the information will not be further shared within the receiving country/receiving organization or with another country or international organisation. See also Article 214B Tax Authority Ordinance, which allows tax authorities in Israel to transfer personal information to a tax authority in a foreign country in accordance with an international agreement, provided that the tax authority was entitled to process that information, that the third country authority requires the information to enforce its tax laws, that the international agreement provides for confidentiality and security requirements, and that the information is not used in the third country for any other purpose than for the enforcement of tax laws and is not further shared within the country or with other third countries.

[1515] Article 1 Transfer Regulations. The principles are the following: (1) data shall be gathered and processed in a legal and fair manner; (2) data shall be held, used and delivered only for the purpose for which it was received; (3) Data gathered shall be accurate and up to date; (4) the right of access and correction is reserved to the data subject; (5) The obligation to take adequate security measures to protect data in databases is mandatory.

[1516] Article 2 Transfer Regulations.

[1517] Article 3 Transfer Regulations.

[1518] Article 9B (c) Wiretapping Law. In this case, the data must be deleted within 10 days, see Article 7(a) of the Wiretapping Regulations.

material will delete it within ten days from the order receipt[1519]. Moreover, the Wiretapping Regulations requires that recorded material is kept safe and in a manner that ensures confidentiality[1520]. The Wiretapping Regulations provide that information obtained through wiretapping or recorded material may be shared with a competent authority[1521] different from the one that requested the wiretapping or with the Institute for Intelligence and Special Operations if it may serve for preventing harm to the State security[1522] or serve to prevent felony class offences or to identify the perpetrators of such offences[1523]. Such information sharing may only take place to the extent it is necessary for the receiving authority to conduct its functions. The receiving authority has to confirm in writing the receipt of the information and the extent to which it is necessary to perform its functions[1524].

2.2.3. Oversight

Different bodies carry out oversight of the activities of criminal law enforcement authorities in Israel.

Internally, the Data Security Unit within the Israeli police is responsible for supervising the classification of all data held by the police (including data collected pursuant to the Communication Data Law or the Wiretapping Law) and its proper use. The Unit can conduct investigations and inquiries to detect any irregularity, unlawful use of data or use of data without permission. Irregularities or violations detected by the Data Security Unit are dealt with through administrative, disciplinary or criminal proceedings.

In terms of independent oversight, the processing of personal data by competent authorities for criminal law enforcement purposes is first of all subject to the oversight of the PPA, which is responsible for supervising compliance with the provisions of the PPL and of the regulations adopted thereunder[1525]. In order to carry out its functions, the staff of the PPA can request relevant information and documents from any person involved, as well as enter, search and seize any object in any place for which there are reasonable grounds to believe that a database is operated therein[1526]. The PPA can act on the basis of individual complaints or on

[1519] Article 7 Wiretapping Regulations.
[1520] Article 5(a) Wiretapping Law.
[1521] Pursuant to Article 1 of the Wiretapping Regulations, a competent authority is the head of a security agency or an authorized police officer, as relevant. Article 1 of the Wiretapping Law defines authorized police officer as police officer with the rank of commander and above authorized by the Police Commissioner.
[1522] The term 'state security' has not been interpreted by Israeli courts in the context of the Wiretapping Law or the Wiretapping Regulations, but in other contexts. For example, the Supreme Court held that the term refers to "anything relating to the prevention of the risk of enemy invasion from outside the State; thwarting of any attempt of a violent coup against the existing regime by hostile entities from inside the State; maintaining of public order and in securing public security", HCJ 73/53 Kol Haam v. Minister of Interior, G 871 (1953). In another case, the Supreme Court noted that matters that would be considered as direct threats to state security include "(1) an attack by a force from outside the state; (2) acts of espionage, sabotage or guerrilla warfare that might assist an outside enemy in its attempts to undermine the foundations of the regime; (3) direct threats to the integrity of the state or its institutions by way of sedition, insurgence or terrorism; (4) subversive organisation whose purpose is to abet, at an opportune time, in the commission of each of the first three acts." HCJ 4374/15 The Movement for Quality Government in Israel v. Prime Minister of Israel (published in Nevo, 27.03.2016).
[1523] Article 9 Wiretapping Law.
[1524] See Article 9(a) and (b) of the Wiretapping Regulations.
[1525] Articles 10(a) and (c) PPL.
[1526] Article 10(e1) PPL. Pursuant to Article 10(e1)(2) PPL the procedures for entering a military facility or a facility of a security agency are prescribed by the Minister of Justice upon consultation with the Minister in charge of the security agency. Such regulations have not yet been enacted and therefore physical access by the

its own initiative. If a possessor or owner of a database has infringed any provision of the PPL or fails to comply with a demand from the PPA, the PPA may suspend or cancel the registration of a database, the result of which is that the database owner is not allowed to process data in this database[1527].

The PPA conducts oversight actions that concern the processing activities carried out by law enforcement authorities. For example, in January 2023, the PPA imposed a fine on an employee of the Israeli Tax Authority for unauthorised use and disclosure of personal data from the Authority's database[1528]. The annual reports of the PPA also show that it regularly engages with law enforcement authorities, including at an early stage when new technologies are being tested or rolled out[1529].

Second, independent oversight of the Police is carried out by the State Comptroller ([1530], who, as part of his auditing mandate, may examine the lawfulness of acts carried out by public authorities and any other matter he deems necessary in regard to such acts[1531]. In his/her audit reports, the State Comptroller details any infringements of any law, of the principles of economy and efficiency or of moral integrity, and matters that demand for rectification[1532]. The head of the audited authority is required to report to the Comptroller on the envisaged actions to rectify identified deficiencies and the timing for implementing them[1533]. The findings of the State Comptroller are also brought to the knowledge of the Minister concerned, the Prime Minister, the Israeli Parliament (Knesset), as well as, in the case of a suspicion of a criminal act, the Attorney General[1534]. The Prime Minister must submit to the State Comptroller a detailed response to each report within eight months, including on the steps taken to rectify any deficiencies[1535]. While reports of the State Comptroller are in general made public, they may be redacted or withheld where necessary for the protection of national security or to avoid damage to Israel's foreign relations or international trade relations[1536].

Finally, oversight over the activities of law enforcement authorities in Israel is carried out by the Attorney General and the Knesset.

PPA to facilities of security agencies or military for the purpose of an inspection or to carry out an investigation has to be arranged on an ad hoc basis.

[1527] Article 10(b2) and (f) PPL. According to Article 31A(a)(1), managing or processing data in a non-registered database is a criminal offense.

[1528] https://www.gov.il/he/departments/news/fine95k.

[1529] See e.g., https://moj.my.salesforce.com/sfc/dist/version/download/?oid=00D1t000000uX5h&ids=0683Y00000GxYkf&d=%2Fa%2F3Y000001VFUu%2FLSL4C3hfDNacZjKXm65jnxMBYJxrjTOjqGw_YgHg.4s&asPdf=false.

[1530] The State Comptroller is elected by the Knesset, upon nomination by Knesset members (Article 1(a) and 3 State Comptroller Law, 5718-1958). During his/her term of office, the State Comptroller may inter alia not be a member of the Knesset, the council of a local authority or an entity carrying business for profit, or hold any other office or engage, directly or indirectly in any business, trade ore profession (Article 7(a) State Comptroller Law). The State Comptroller may only be removed by the Knesset on grounds of behaviour unfitting his/her position on demand of at least twenty Knesset members and upon a proposal of the House Committee of the Knesset (Article 8A State Comptroller Law).

[1531] Article 2(b) Basic Law: State Comptroller and Article 10(a)(d) State Comptroller Law.

[1532] Article 14(a) State Comptroller Law.

[1533] Articles 21A-21B State Comptroller Law.

[1534] Article 14(a)-(c) State Comptroller Law.

[1535] Articles 16 and 21B(b) State Comptroller Law.

[1536] Article 17 State Comptroller Law.

Under the Communication Data Law, the Head of Investigation and Intelligence Department is required to submit a report to the Attorney General once every three months concerning permits issued[1537]. Under the Wiretapping Law, the Police Commissioner is similarly required to submit monthly reports to the Attorney General on wiretapping permits issued to prevent offenses and identify offenders, and the Minister of Police reports annually to the Joint Committee for the Constitution, Law and Justice and the National Security Committee of the Knesset, including on the number of applications filed and the number of permits issued, as well as on the number of persons, telecommunication lines and facilities for which wiretap was permitted[1538]. Both the Attorney General and the Knesset may ask for any further information they consider necessary for the performance of their oversight role[1539]. The Attorney General may determine that a particular activity was unlawful and should be terminated or require to review and/or change unlawful police procedures. The Knesset's Committees may organise debates, summon public officials and civil servants to provide information at their disposal on the activities of the body in which they serve, and issue recommendations.

In addition to its review of the abovementioned periodic reports, the Knesset is also authorised, as part of its constitutional role, to require from any governmental authority, including from security authorities, any information regarding their activities.

2.2.4. Redress

The Israeli system offers different avenues to obtain redress, including the possibility to obtain compensation for damages.

First, pursuant to the PPL and the Privacy Protection Regulations, individuals have the rights of access to[1540] and correction[1541] and deletion[1542] of their personal data held by public authorities, including public authorities in the areas of criminal law enforcement and national security. While the exercise of the right of access to personal data granted by the PPL may be restricted with respect to certain data[1543], the case law of Israeli courts on the right of access,

[1537] Article 4(e) Communication Data Law.
[1538] Article 6(f) and (g) Wiretapping Law.
[1539] Regarding the role and powers of the Knesset, see Article 42 Basic Law: The Government and Articles 123-127 of the Knesset's rules of procedure.
[1540] Article 13(a) PPL. While the exercise of the right of access to personal data granted by Articles 13 and 13A PPL may be restricted with respect to, among others, data held in databases of security agencies or in databases regarding investigation and law enforcement, the case law of Israeli courts, as confirmed by the PPA, has clarified that the relevant entities are required to examine on a case-by-case basis whether to apply the exemption, and to apply the exemption only to the extent necessary and proportionate, see above section 2.1.
[1541] Article 14 PPL and Regulation 6 of the Privacy Protection Regulations. The application of the Privacy Protection Regulations to the use of data for the protection of national security or criminal law enforcement may be restricted, but only to the extent necessary and proportionate for these purposes, see Regulation 2(b)(2) of the Privacy Protection Regulations.
[1542] Regulation 3 of the Privacy Protection Regulations. In addition, their application to the use of data for the protection of national security or criminal law enforcement may be restricted, but only to the extent necessary and proportionate for these purposes, see Regulation 2(b)(2) of the Privacy Protection Regulations.
[1543] The right of access may be restricted in particular with respect to data contained in a database of a security agency, Article 13(e)(1) PPL, with respect to databases regarding investigation and law enforcement, Article 13(e)(5) PPL, and where the State security, its foreign relations or the provisions of any law require that data of a person is not disclosed to him, Article 13(e)(3) PPL. 'Security agency' is defined in Article 19(c) PPL as the Israel Police, the Directorate of Military Intelligence and the Military Police, the Israel Security Agency, the Institute for Intelligence and Special Operations, and the Witness Protection Authority.

as confirmed by the PPA in an opinion on the individual right of access pursuant to the PPL[1544], has clarified that this restriction does not exempt the relevant entities "from examining, on a case-by-case basis, the justification for applying the exemption, with regard to the individual's access to data about him in databases of these entities" and that "[…] the exemption is to be applied only to the extent necessary and proportionate". More specifically, the Israeli Supreme Court has held that any limitation to the individual right of access should be done while striking a balance with the interests standing against it, in each and every case. The striking of such balance should be made while taking into consideration the nature of the case, its circumstances, the essence of the harm that the authority's decision will cause for the individual, and the question of the finality of the decision for which access is requested[1545]. If a request for the exercise of rights is refused, individuals have the possibility to file a complaint with the PPA or, if a request for access or rectification is refused, may apply directly to court[1546].

Second, any individual may lodge a complaint concerning the processing of personal data by an Israeli law enforcement authority with the PPA, who can make use of all of its investigative and enforcement powers described in section 1.2.

Third, any individual may file a complaint with the Ombudsman[1547] against an act or omission of a public authority, including any unlawful processing of personal data by the Police[1548]. In investigating a complaint, the Ombudsman has access to any relevant information and may hear the complainant, the entity against which the complaint is directed, as well as any other person[1549]. Where the Ombudsman finds that the complaint is justified, the complainant will be notified thereof, together with the reasons[1550]. The Ombudsman may indicate to the relevant public authority the need to rectify an issue revealed by the investigation (including for instance by paying a monetary compensation), as well as how and within what time period such rectification should be carried out[1551]. The concerned authority must inform, within the time frame set by the Ombudsman, of the steps that have been taken in response to the Ombudsman's decision regarding the complaint[1552]. If the Ombudsman is not satisfied with the information provided, (s)he may bring the matter to the knowledge of the concerned

[1544] PPA Opinion on Article 13 of the Privacy Protection Law: The Individual Right of Access, published on 6 August 2023, available at: https://www.gov.il/he/departments/publications/reports/right_to_access2023.
[1545] Israeli Supreme Court, HCJ 93/06 Kol Gader v. The Minister of Industry, Trade and Labor (published in Nevo 2 August 2011). This approach was also confirmed with regard to access to criminal investigation files, both by the data subject itself and by third parties, in State Attorney Guideline No. 14.8 "Request from different entities to access data from investigation files" (last updated on 7 April 2021), available at: https://www.gov.il/BlobFolder/dynamiccollectorresultitem/14-008-00/he/s-a-guidelines_014.8.pdf.
[1546] Article 15 PPL.
[1547] In accordance with Article 4 Basic Law: State Comptroller and chapter 7 of State Comptroller Law, the State Comptroller of Israel also functions as the Israeli Ombudsman.
[1548] Articles 33, 36 and 37 State Comptroller Law. The Ombudsman does not investigate complaints that can be resolved through other avenues or that are submitted more than one year later than the date of the act to which they relate or the data on which the act became known to the complainant (whichever is later). See Article 39 State Comptroller Law.
[1549] Article 41(c)-(d) State Comptroller Law.
[1550] Article 43(a) State Comptroller Law.
[1551] Article 43(a) State Comptroller Law.
[1552] Article 43(b) State Comptroller Law.

Minister or the relevant Knesset Committee. Any complaint which raises the suspicion of a criminal act having occurred is forwarded to the Attorney General by the Ombudsman[1553].

Fourth, individuals can make use of the different judicial avenues described in section 1.2, including to obtain compensation for damages for violations of the PPL, submit a criminal complaint pursuant to Article 68 of the Israeli Criminal Procedure Law where unlawful processing of personal data constitutes a criminal offence (e.g., under the PPL).

Importantly, an individual seeking to challenge the collection of his or her personal data for the purposes of criminal law enforcement has the possibility to file a petition for judicial review to the Israeli Supreme Court[1554]. In accordance with Article 15(d) of the Basic Law: The Judiciary, the Supreme Court, sitting as High Court of Justice is empowered to hear and adjudicate petitions against state authorities or other bodies fulfilling by law public functions in the state, and thus exercises judicial review of the activities of government authorities. More specifically, a petition may be filed by an individual, including a non-Israeli national or resident, against any act or omission of any of the state authorities, including the Israel Police, which in the opinion of the petitioner violate the laws. The Supreme Court has a wide discretion in deciding whether to hear petition brought before them, so that even citizens and bodies not directly affected by the actions of the state can petition against it[1555].

The Supreme Court, sitting as High Court of Justice, is empowered to grant equitable relief, to order State and local authorities and the officials and bodies thereof, and other persons carrying out public functions under the law, to do or refrain from doing any act in the lawful exercise of their functions; to order courts, tribunals and bodies and persons having judicial or quasi-judicial powers under law, to hear, refrain from hearing, or continue hearing a particular matter or to void a proceeding improperly taken or a decision improperly given. It is also empowered to issue any order it sees fit towards any public body or any body exercising public authority. In case of a violation of privacy or data protection, this includes the power to order the deletion of personal data held by the relevant authority. Furthermore, the Supreme Court, sitting as a court of appeal, is empowered to order remedies in accordance with other laws, such as the PPL, including by ordering alternative relief (whereby the petitioner may for instance turn to a civil court to demand compensation)[1556].

2.3. Access and use by Israeli public authorities for national security purposes

[1553] Article 43(d) State Comptroller Law.

[1554] The Supreme Court is the highest court of judicial review for public matters, including administrative matters which relate to disputes between a citizen and an authority exercising governmental powers. As such, it is authorized to hear any matter in which it deems necessary to provide relief for the sake of justice (notably cases that are particularly sensitive, have wide implications or raise fundamental issues) or which is not within the jurisdiction of another court or tribunal, see Article 15(c) Basic Law: The Judiciary. The Supreme Court can also elect at its own discretion to hear a particular matter itself, even if it is under the jurisdiction of another court, for instance if that matter raises fundamental questions and/or has particularly wide or sensitive implications.

[1555] This was for example the case in the Association or Civil Rights in Israel case, in which the Supreme Court set important standards concerning data collection under the Telecommunication Data Law.

[1556] Article 15 of the Basic Law: The Judiciary.

In Israel, the main authority competent to collect personal data for national security purposes is the Israel Security Agency (ISA)[1557], whose powers are mainly governed by the Israel Security Agency Law, the Wiretapping Law and the PPL. Israeli law imposes a number of safeguards and limitations on how the ISA has access to and uses personal data for national security purposes and provides oversight and redress mechanisms in this area. The conditions under which access to personal data can take place and the safeguards applicable to the use of these powers are assessed in the following sections.

2.3.1. Legal bases and applicable limitations/safeguards

The ISA's functions and mandate are defined in the ISA Law, which provides that it is in charge of the "protection of State security and the order and institutions of the democratic regime against threats of terrorism, sabotage, subversion, espionage, and disclosure of State secrets, and to safeguard and promote other State interests vital for national State security"[1558]. The ISA may exercise different functions and powers, including protecting individuals, information and places determined by the Government; conducting intelligence research, as well as collecting and receiving information to safeguard and promote the abovementioned interests[1559]. In doing so, the ISA may access personal data transferred from the EU to Israel (including while in transit), subject to specific limitations and safeguards.

The ISA may intercept the content of communications on the basis of the Wiretapping Law, may collect communications data (i.e., metadata, excluding the content of communications) on the basis of the ISA Law and may, on the basis of the PPL, receive personal data from other Israeli public authorities. In addition to the limitations and safeguards that follow from these laws (as described below), the Attorney General has issued a binding legal opinion further clarifying the application of the constitutional principles of lawfulness, necessity and proportionality to the activities of public bodies in Israel and the ISA in particular.

As any other public authority, the ISA may only take a measure that interferes with the right to data protection of individuals if such measure is provided for or authorised by law, pursues an appropriate purpose, is suitable to achieve that purpose, constitutes the least intrusive measure (compared to other available measures) and is proportionate (which requires balancing the benefits that would be achieved by the measure against the harm that would be caused to the individual)[1560].

Accordingly, and as further specified in the legal opinion issued by the Attorney General, the ISA may only process personal data on the basis of the ISA Law and the Wiretapping Law, and in accordance with the PPL if the following conditions are met[1561]. First, there must be a legitimate purpose for the processing[1562]. The specific purposes for which the ISA may collect

[1557] On the basis of the Wiretapping Law, the Intelligence Branch of the Israel Defence Forces may also collect information for national security purposes, subject to the same conditions and legal requirements described for the ISA below. See Article 1 of the Wiretapping Law, where it defines 'security authority'.
[1558] Article 7(a) ISA Law.
[1559] Article 7(b) ISA Law. See also Articles 8-10 ISA Law.
[1560] Article 8 of the Basic Law, as well as case law, see e.g., CA 6821/93 Bank Mizrachi Meuchad v. Migdal Cooperative Village 49(4) PD 221 (1995); HCJ 2605-05 The Human Rights Division, Academic Center of Law and Business v. Minister of Finance 63(2) PD 545 (2009).
[1561] P. 4 of the AG Opinion.
[1562] Population Registry HCJ, sections 1 and 6 in the judgment of Justice (ret.) Dorner.

and process data follow from specific legislation (e.g., the ISA Law)[1563], as described below. Second, the processing must be necessary to attain the legitimate purpose. In this respect, the ISA must examine whether there are less intrusive means to achieve the same purpose and ensure that only the minimum data required for the legitimate purpose is processed[1564]. Finally, in assessing the proportionality of a surveillance measure, the ISA must take several factors into account, such as the nature and sensitivity of the data processed, the amount/scope of data processed, the duration of the processing (including how long it would be stored), the transparency of the processing towards concerned individuals, the number of employees that will have access to the data and the severity of the threat to national security[1565]. These requirements, which follow from the Basic Law and case law and are confirmed in the binding legal opinion of the Attorney General, apply to any processing of personal data by the ISA (e.g., to the collection, use, storage and sharing of personal data)[1566]. They constitute the standard against which bodies that authorise surveillance measures (see below), as well as oversight bodies and courts, have to assess the lawfulness of the collection and further processing of personal data for national security purposes[1567].

In terms of specific powers that have to be exercised in compliance with above legal requirements, the ISA may, on the basis of the Wiretapping Law, collect the content of communications. Procedurally, such collection must, upon request from the ISA, be authorised in writing by the Prime Minister[1568], if (s)he is satisfied that the collection is necessary (as interpreted in line with the principles set out above) for the protection of national security, after considering the level of interference with the rights of individuals (i.e., if the abovementioned requirement of proportionality is met)[1569]. The authorisation issued by the Prime Minister must, if known in advance, indicate the identity of the concerned individual or of the line or facility used, as well as the location and duration of the wiretap and manner in which it will be carried out[1570]. A wiretap authorisation is valid for a maximum period of three months, renewable under the same conditions[1571]. The Prime Minister must

---

[1563] P. 2 of the AG Opinion.

[1564] Nachmias, section 13 in the judgment of Justice Bach; Population Registry HCJ, sections 6-7 in the judgment of Justice (ret.) Dorner.]

[1565] Urich, sections 73 and 75 in the judgment of President Chayut; Nachmias, sections 10, 13 in the judgment of Justice Bach; Telecommunication Data Law HCJ, sections 16 and 26 of President (ret.) Beinisch; First ISA Authorization HCJ, sections 38-39, 43-45 in the judgment of President Chayut; Population Registry HCJ, section 7 in the judgment of Justice (ret.) Dorner; Second ISA Authorization HCJ, section 7 in the judgment of Justice Hendel, section 18 in the judgment of President Chayut.

[1566] See e.g., HCJ 3809/08 Association for Civil Rights in Israel v. Israel Police (May 28, 2012), (Telecommunications Data Law HCJ), sections 5-7 in the judgment of President (ret.) Beinisch; Nachmias, section 10 in the judgment of Justice Bach; First ISA Authorization HCJ, sections 18 and 38 in the judgment of President Chayut; Second ISA Authorization HCJ, section seven in the judgment of Justice Hendel, section 12 in the judgment of Justice Barak-Erez; HCJ 8070/98 Association for Civil Rights in Israel v. Ministry of Interior 58(4) PD 842 (2004) (Population Registry HCJ), section 7 in the judgment of Justice (ret.) Dorner. See also p. 13 of the AG letter.

[1567] P. 4-5 and 9-10 of the AG Opinion.

[1568] Or the Minister of Defence, as regards the Israel Defence Forces.

[1569] Article 4(a) Wiretapping Law. See also p. 5 of the AG Opinion. A specific procedure applies to the interception of communications of privileged communications. Such a wiretap may be requested by the ISA in writing with respect to an offense that endangers national security, where required for the protection of national security. The interception may be authorised by a District Court President or Deputy President if there are grounds to suspect that an attorney, physician, psychologist, social worker or clergyman is involved in the offence (Article 9A(a)(1) Wiretapping Law).

[1570] Article 4(b) Wiretapping Law.

[1571] Article 4(c) Wiretapping Law.

notify the Attorney General every three months about authorisations issued[1572]. In urgent cases, i.e., if the head of the ISA concludes that the protection of national security requires an immediate wiretap and there is no time to obtain authorisation, the head of the ISA may issue a written authorisation containing the same elements as described above[1573]. Such an authorisation is only valid for 48 hours and must be reported immediately to the Prime Minister, who may revoke it[1574].

Pursuant to the ISA Law, the ISA may also collect communications data (i.e., metadata, excluding the content of a conversation, which can only be intercepted on the basis of the Wiretapping Law) from telecommunication operators (i.e., companies licensed in Israel to offer communication services)[1575]. In particular, the ISA may request metadata where necessary for the performance of its duties, i.e., for the protection of national security and the order and institutions of the democratic regime against threats of terrorism, sabotage, subversion, espionage and disclosure of State secrets, as well as for safeguarding and promoting other State interests vital for national security[1576]. Any such request may only be issued by the ISA if it complies with the requirements of necessity and proportionality, as confirmed by the binding legal opinion of the Attorney General. With respect to the possibility to access data obtained in response to a request of the ISA, the ISA Law imposes additional safeguards. In particular, any employee of the ISA may only access such data for the performance of his/her official duties if specifically authorised to do so by the head of the ISA[1577].

Finally, the ISA may, under the same conditions as described in section 2.2.2 with respect to the Police, receive information, including personal data, from other public authorities providing such information on a voluntary basis[1578].

2.3.2. Further use of the information collected

The processing of personal data obtained by the ISA for national security purposes is governed by the provisions of the PPL and of the Regulations adopted on its basis, as described in section 2.1[1579]. As regards the sharing of information obtained through wiretapping with other Israeli authorities, the same requirements of the Wiretapping Regulations as the ones described in section 2.2.2 apply.

Additional requirements for the retention, deletion and further sharing of the content of communications and communications data follow from specific classified rules issued by the

[1572] Article 4(d) Wiretapping Law.
[1573] Article 5(a) Wiretapping Law.
[1574] Article 5(a)-(b) Wiretapping Law. In case of a wiretap of a privileged conversation (of an attorney, physician, psychologist, social worker or clergyman), the ISA must notify the Attorney General, who in turn may revoke the authorisation (Article 5(c) Wiretapping Law).
[1575] See Article 11(a) ISA Law. The ISA Law does not provide the ISA with a legal basis to demand information from other types of companies, such as internet and technology companies, or cloud service providers.
[1576] See the ISA's tasks described in Article 7(a) ISA Law.
[1577] Article 11(c) ISA Law.
[1578] Article 23B(b) PPL.
[1579] The PPL applies to the processing of personal data by a competent authority, including for the purpose of safeguarding against or preventing threats to national security.

Prime Minister under the Wiretapping Law and ISA Law[1580]. At the same time, as indicated in section 2.3.1 and as follows in particular from case law, reflected in the binding legal opinion of the Attorney General, any such processing, including the use, retention or sharing, of personal data by the ISA has to comply with the principles of lawfulness, necessity and proportionality.

2.3.3. Oversight

The access of personal data by Israeli security agencies for purposes of national security is subject to similar oversight mechanisms as already outlined with respect to criminal law enforcement.

Internally, the ISA Comptroller is responsible for internal audits, including with respect to the ISA's processing of personal data for national security purposes[1581]. The Comptroller has access to all relevant information and reports annually to the Head of the ISA, the Ministerial Committee on ISA Affairs and the Knesset Committee on ISA Affairs[1582]. If the comptroller finds a violation of the law, such findings must be included in the periodic reports[1583].

In terms of independent oversight, the PPA oversees the processing of personal data by national security authorities in light of the PPL and the relevant Regulations. The PPA can request relevant information and documents from any person involved in the processing of personal data for national security purposes. If a possessor or owner of a database has infringed any provision of the PPL, the PPA has the power to suspend or cancel the registration of a database, and thus suspend or prohibit the database owner from processing or managing this database.

In addition, the State Comptroller is competent to oversee the activities of the ISA, in the same way as described in section 2.2.3.

In terms of governmental and parliamentary oversight, Article 11(d) of the ISA Law requires the Head of the ISA to report every three months to the Prime Minister and to the Attorney general on the permits issued to use communication data that has been transmitted to the ISA pursuant to Article 11(b) of the ISA Law, and on the mode of use of such data under Article 11(c) of the Law. The reports include information on the number of permits issued by virtue of Article 11, the ways in which the information was used. The same type of report is submitted to the Knesset Service Affairs Committee, i.e., the Sub-Committee for Intelligence and Secret Services of the Foreign Affairs and Defence Committee of the Knesset, on an annual basis. Moreover, the Head of the ISA reports every three months to the Ministerial

[1580] Rules promulgated under the ISA Law are subject to approval by the Ministerial Committee on ISA affairs and the Knesset Committee on ISA affairs. Rules on retention and deletion of information collected under Article 11, require in addition the consent of the Minister of Justice (See Article 11(e) and Article 21(a) ISA Law). Rules promulgated under the Wiretapping Law on deletion of wiretap material and the retention of material for security purposes require the consent of the Minister of Justice and the approval of a joint committee of the Constitution Justice and Law Committee and Foreign Affairs and Security Committee of the Knesset (see Article 9B Wiretapping Law).

[1581] See Article 13(c) ISA Law. The Comptroller is appointed by the Prime Minister, in consultation with the head of the ISA, for one term of five years. Upon expiration of this term, the Comptroller cannot serve in any other position in the ISA. See Article 13(a)-(b) ISA Law.

[1582] Article 13(e)(2) and (5) ISA Law.

[1583] Article 13(e)(5) ISA Law.

Committee (i.e., a committee appointed by the Israeli government for Security Agency affairs, which for these matters operates in the name of the government) and the Knesset Service Affairs Committee on the general activities of the agency. Both the Ministerial Committee and the Knesset Service Affairs Committee may also request special reports from the Head of the ISA[1584]. Both the Attorney General and the Knesset may ask for any further information they consider necessary for the performance of their oversight role. The Attorney General may determine that a particular activity was unlawful and should be terminated or require to review and/or change unlawful procedures. The Knesset's Committees may organise debates, summon public officials and civil servants to provide information and issue recommendations.

As regards the Wiretapping Law, under Article 4(d) any issuing or renewal of a wiretap permit for the purposes of State Security has to be immediately notified to the Prime Minister, if the Minister of Defence issued it. Moreover, the Minister of Defence notifies the Attorney General once every three months of wiretap permits issued for the purposes of State Security[1585]. The Attorney General, together with the ISA, examines specific issues in order to ensure that data is used in a limited and proportionate manner, and solely for the purposes of state security set out in the Law. The issues discussed during these examinations may concern specific cases or broader trends and can lead to changes of internal procedures.

Finally, the Minister also reports on an annual basis the number of permits issued in this area to a joint committee of the Knesset Constitution, Law and Justice Committee and the Foreign Affairs and Security Committee[1586].

2.3.4. Redress

The Israeli system offers different avenues to obtain redress, including compensation for damages.

First, individuals can exercise their rights of access, correction and deletion with respect to data held by the ISA under the PPL, under the same conditions as described in section 2.2.4[1587]. If a request is refused, any individual has the possibility to lodge a complaint with the PPA, that can make use of all of its investigative and enforcement powers.

Second, any individual, can file complaints with the PPA about the processing of their personal data by the ISA. The PPA is bound to review every complaint it receives and to notify the applicant of its decision in that regard[1588].

Third, any individual can lodge a complaint before the Ombudsman concerning the handling of their data by the ISA, in the same way as described in section 2.2.4.

[1584] See Article 12(a) and (b) of the ISA Law.
[1585] Article 4(d) of the Wiretapping Law
[1586] See Article 4(e) of the Wiretapping Law.
[1587] See for example the Supreme Court ruling in HCJ 3098/20 Vinter v. Israel Police (17 November 2020), in which the Court, sitting as High Court of Justice, ruled on a request for access to investigative material, including personal data, held, among other, by the ISA and the Israel Police.
[1588] In addition, the PPA is required to handle public inquiries where there are grounds for harming data subjects under the PPL, see Article 2(D) of Government Resolution No. 1890.

Finally, the same judicial avenues as the ones described in section 2.2.4 (e.g., to obtain compensation for damages for violations of the PPL, to submit a criminal complaint, or to file a petition to the Israeli Supreme Court) are also available against the ISA.

VIII. JERSEY

1. RULES APPLYING TO THE PROCESSING OF PERSONAL DATA

1.1. Relevant developments in the data protection framework of Jersey

On 8 May 2008 the European Commission adopted a decision in which Jersey was considered as providing an adequate level of protection for personal data[1589]. The Article 29 Working Party had adopted a positive opinion on the level of protection of personal data in Jersey on 9 October 2007[1590]. At the time, data protection in Jersey was governed by the Data Protection (Jersey) Law 2005 (Data Protection Law 2005). The Data Protection Law 2005 was substantially identical to the UK's Data Protection Act 1998, which implemented Directive 95/46/EC (Data Protection Directive)[1591]. It also established the independent office of the Information Commissioner, which regulated compliance with the law.

Since the adoption of the Commission's adequacy decision, Jersey has significantly modernised its data protection framework, in particular by adopting the Data Protection (Jersey) Law 2018 (Data Protection Law), which repeals the previous 2005 Law. Along with the Data Protection Authority (Jersey) Law 2018 (Data Protection Authority Law), it was drafted to ensure a level of protection in line with Regulation (EU) 2016/679 (GDPR)[1592]. It entered into force in May 2018.

With the adoption and full entry into force of the Data Protection Law, the Jersey data protection regime has been significantly strengthened. As set out in more detail below, the Data Protection Law mirrors the provisions of the GPDR with respect to all of its key aspects. In particular, in areas where the GDPR has enhanced the protection of personal data when compared to the protection offered by its predecessor, the Data Protection Directive, the Data Protection Law of Jersey has been strengthened as well.

Like the Data Protection Law 2005, the new Data Protection Law has a broad scope of application, applying to both private operators and public authorities[1593]. While the definitions of 'personal data'[1594], 'controller'[1595], 'processor'[1596], 'data subject'[1597] and 'processing'[1598]

[1589] Commission Decision 2008/393/EC of 8 May 2008 on the adequate protection of personal data in Jersey, OJ L 128, 28.5.2008, p. 21-23.

[1590] Opinion 8/2007 on the level of protection of personal data in Jersey (WP141), available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp141_en.pdf.

[1591] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[1592] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[1593] The Jersey data protection regime applies to the processing of personal data in the context of a controller or processor established in Jersey, see Article 4(2)(a) Data Protection Law. The Law does not apply to the processing of personal data by natural persons in the course of a purely personal or household activity, see Article 4(1) Data Protection Law.

[1594] 'Personal data' is defined in Article 2(1) Data Protection Law as "any data relating to a data subject", while 'data subject' is defined in Article 2(2) of the Data Protection Law as "an identified or identifiable, natural, living person who can be identified, directly or indirectly, by reference to (but not limited to) an identifier such as (1) a name, an identification number or location data; (2) an online identifier; or (3) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the person."

[1595] Pursuant to Article 1(1) Data Protection Law, 'controller' means "the natural or legal person, public authority, agency or other body that, whether alone or jointly with others, determines the purposes and means of

(which are identical to those used in the GDPR) have not changed, the Data Protection Law has brought even more convergence with the GDPR, e.g., by introducing a definition of 'pseudonymisation'[1599]. Moreover, the recent reform further aligned the notion of personal data with the GDPR by clarifying when a person is "identifiable"[1600]. Also the territorial scope of the Law has been extended to cover the processing of personal data by controllers or processors not established in Jersey, subject to the same conditions that are set out in Article 3 of the GDPR[1601]. This confirms the intention of the Jersey legislator to strengthen the effectiveness of Jersey's data protection regime.

The main data protection principles (i.e., the principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality) were already present in the Data Protection Law 2005 and are present also in the modernised Law[1602]. Some of them have been further strengthened, e.g., the principle of lawfulness of processing, the transparency obligations, the security principle and the principle of accountability.

In particular, as regards the principle of lawfulness, the requirements for valid consent have been reinforced, by making clear that, in addition to being freely given, specific and informed, consent must be unambiguous and expressed by a clear affirmative action[1603]. Similarly, the Data Protection Law has strengthened the existing transparency obligations by requiring that additional information is provided to the individual (e.g., the contact details of the data protection officer, the fact that the controller intends to transfer the data to a third country, the retention period, the right to withdraw consent, the existence of automated decision-making, etc.) when data is collected directly from the individual or from third parties[1604] and when it is further processed[1605].

---

the processing of personal data, and where those purposes and means are determined by the relevant law, the controller or the specific criteria for its nomination may be provided for by such law."

[1596] Pursuant to Article 1(1) Data Protection Law, 'processor' means "a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller but does not include an employee of the controller."

[1597] See footnote 4.

[1598] 'Processing' is defined in Article 1(1) Data Protection Law as "any operation or set of operations that is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.".

[1599] Article 3 Data Protection Law.

[1600] Pursuant to Article 2(3) Data Protection Law, in deciding whether the person is identified or identifiable, one must take into account the means reasonably likely to be used by the controller or another person to identify the person, taking into account factors such as the cost and amount of time required for identification in the light of the available technology at the time of processing and technological factors; and whether the personal data, despite pseudonymization, is capable of being attributed to that person by the use of information other than that kept separately for the purposes of pseudonymisation.

[1601] Article 4(2)(b) and (c) Data Protection Law.

[1602] Article 8 Data Protection Law.

[1603] Article 11 Data Protection Law.

[1604] Article 12 Data Protection Law. This obligation is subject to several exceptions, which are similar to the exceptions listed in Article 14(5) GDPR. Where an exception applies, the controller must take appropriate measures to protect individual rights, including by making the information publicly available (see Article 13(6) and (7) Data Protection Law).

[1605] Article 13(3) Data Protection Law.

With respect to the principle of data security, the Data Protection Law has introduced the obligation to notify data breaches[1606], which was previously not present in the Jersey regime. As also required by the GDPR, in case of a personal data breach, the controller must, as soon as practicable, and in any event, within 72 hours after becoming aware of the breach (unless the latter is not practicable), notify the personal data breach in writing to the Authority. If a personal data breach is likely to pose a high risk to the significant interests of a data subject, written notice must be provided also to the data subject.

In terms of accountability, the obligations have been fully aligned with the GDPR and requirements that were previously not present in the Jersey law have been introduced: The Data Protection Law contains the obligations to implement principles of data protection by design and by default[1607], to keep records of processing[1608], to designate a data protection officer[1609], and to conduct impact assessments[1610]. Like the GDPR, the Data Protection Law follows a risk-based approach, and the scope of the obligations is tailored to the risks for the rights and freedoms of natural persons.

In addition to the strengthening of data protection principles and obligations, the protections for special categories of personal data have been reinforced since the adoption of the adequacy decision. The Data Protection Law 2005 already offered additional protection for information about the racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, about membership in a trade union or other labour organisation, about physical or mental health and the commission or alleged commission of an offence[1611]. The Data Protection Law extends this protection to biometric and genetic data, as well as to data concerning a natural person's sexual orientation[1612]. As regards the safeguards that apply to the processing of special categories of data, the Data Protection Law allows the processing of special categories of data only in specific circumstances[1613], as was already the case under the Data Protection Law 2005[1614]. Moreover, controllers and processors that process special categories of data may be subject to specific accountability requirements, such as the keeping of records[1615], the appointment of a data protection officer[1616], and the carrying out of impact assessments[1617].

[1606] Articles 6(1)(g) and 20 Data Protection Law.
[1607] Articles 6(1)(d) and 15 Data Protection Law.
[1608] Articles 6(1)I and 14 Data Protection Law.
[1609] Articles 6(1)(h) and 24 Data Protection Law.
[1610] Article 16 Data Protection Law.
[1611] Article 2 Data Protection Law 2005.
[1612] Article 1(1) Data Protection Law.
[1613] Part 2 of Schedule 2 to the Data Protection Law. For example, similarly to the GDPR, the Data Protection Law allows the processing of special categories of data where the data subject has given explicit consent, where processing is necessary for compliance with a legal obligation or where processing is necessary to protect the vital interest of the data subject. Article 26 of Schedule 2 provides that other regulations may set further requirements for the processing of special category data, including by excluding the application of Schedule 2 or modifying its application. To date there is no regulations in force which modifies the requirements for the processing of special category data (laid down in Part 2 of Schedule 2) pursuant to Article 26 of Schedule 2.
[1614] Article 4 and Schedule 3 to the Data Protection Law 2005.
[1615] Article 6(3)I and Article 22(2)I Data Protection Law.
[1616] Where the core activities consist of processing special categories of data on a large scale, see Article 24(1)I Data Protection Law.
[1617] Where special categories of data are processed on a large scale, see Article 16(5) Data Protection Law.

In terms of rights, Part 6 of the Data Protection Law provides individuals with all of the key data protection rights, i.e., the rights of access[1618] rectification[1619], and erasure[1620], and it also provides for a right to restriction[1621] and objection[1622]. The exercise of these rights is subject to conditions that are very similar to those of the GDPR. Moreover, when compared to the previous legislation, the Data Protection Law has strengthened the rights of individuals in several ways, further aligning them with the GDPR. The right of access not only requires controllers to provide individuals with information about the processing of their data (as was already the case under the Data Protection Law 2005[1623]), but also to give access to personal data, including by providing a copy[1624]. Moreover, additional grounds to object to processing have been added[1625]. For instance, individuals have a right to object to the processing of their personal where such processing is based exclusively on grounds of public interest or on the legitimate interest of the controller[1626]. In addition, the data subject no longer has to apply to a court to order the rectification and erasure of his or her personal data, as was required under the Data Protection Law 2005, but instead can make a request directly to the controller[1627]. Finally, the rights in relation to automated decision-making[1628] have been further strengthened and aligned with the GDPR through the introduction of a right for individuals not to be subject to a decision that is based solely on automated processing and that produces legal effects or similarly significantly affects the individual[1629]. Such automated decision-making may only take place under certain conditions (e.g., only where authorised by law or based on the data subject's explicit consent) and subject to suitable safeguards, including the possibility to obtain human intervention[1630]. In addition, the Data Protection Law introduced a right to data portability that corresponds to the same right available under the GDPR[1631].

As it is the case in the GDPR, transparency requirements and data subject rights in Jersey are subject to certain restrictions intended to allow the balancing of the data protection interests of individuals with objectives of general public interest and with the fundamental rights and freedoms of others.

These restrictions are set out in Part 7 of the Data Protection Law. Some of them are based on the nature of the personal data being processed and apply automatically whenever one of the listed categories of personal data is being processed. These categories cover a narrowly construed set of situations, such as information that the controller is obliged under any

[1618] Article 28 Data Protection Law.
[1619] Article 31 Data Protection Law.
[1620] Article 32 Data Protection Law.
[1621] Article 33 Data Protection Law.
[1622] Articles 35 to 37 Data Protection Law. The Jersey Data Protection Laws grants a right to object in three situations: where processing takes place in the public interest, for direct marketing purposes, and for historical or scientific purposes.
[1623] Article 7 Data Protection Law 2005.
[1624] Article 28(3)(a) Data Protection Law.
[1625] Pursuant to Articles 10 and 11 Data Protection Law 2005, the data subject was entitled to request from the controller to cease or not to begin any processing that would be likely to cause unwarranted damage or distress to him or to another, and any processing for purposes of direct marketing.
[1626] Article 35 Data Protection Law.
[1627] Article 31 Data Protection Law.
[1628] Article 12 Data Protection Law 2005.
[1629] Article 38 Data Protection Law.
[1630] Article 38(2) and (3) Data Protection Law.
[1631] Article 34 Data Protection Law.

enactment to make available to the public[1632], personal data processed for purposes of assessing a person's suitability for judicial appointments or appointments by the Crown[1633], the provision of references in confidence by the controller in the context of the education, employment or appointment of the data subject[1634], or personal data recorded by a candidate during an academic, professional or other examination[1635]. These categories are not only very limited in scope, but also do not typically cover situations where personal data is transferred to Jersey from the EU.

In the majority of cases, the restrictions are based on a prejudice standard. Namely, they can be invoked only if - and to the extent that - the application of the provisions "would be likely to prejudice" the legitimate aim pursued. For example, controllers can restrict data subject rights if their application would be likely to prejudice the combat effectiveness of the armed forces of the Crown[1636], or where personal data is processed for the purposes of the prevention, detection, or investigation of a crime or the assessment or collection of any tax or duty, and the application of the requirements or rights would be likely to prejudice that purpose[1637].

The Jersey Office of the Information Commissioner (JOIC) has issued interpretative guidance that clearly frames the application of the exemptions It further clarifies the scope of the different exemptions, which helps to prevent them from being understood and applied in an overly broad manner, and explains how the requirements of necessity and proportionality should be applied with respect to a specific exemption[1638].

With respect to international transfers of personal data, i.e., concerning the potential onward transfer of personal data that has been transferred from the EU, Jersey has reorganised and clarified its transfer regime. It has put in place a system that is very similar to the rules on international transfers set out in Chapter V of the GDPR in terms of structure and requirements. Article 66 of the Data Protection Law lays down the general principle for cross-border data transfers, permitting them only if the third country or international organisation provides an adequate level of protection. The level of protection is considered adequate if the

[1632] Article 51 Data Protection Law.
[1633] Article 55 Data Protection Law.
[1634] Article 53 Data Protection Law.
[1635] Article 54 Data Protection Law.
[1636] Article 56 Data Protection Law.
[1637] Article 45(1)(a) and (c) Data Protection Law.
[1638] Jersey Office of the Information Commissioner, Guidance note on exemptions of November 2021, available at: https://jerseyoic.org/media/44kldaym/joic-29a-exemptions-nov21-4.pdf. First, the guidance clarifies that controllers "must consider each exemption on a case-by-case basis because the exemptions only permit […] to depart from the [Data Protection Law's] general requirements to the minimum extent necessary to protect the particular functions or activities the exemptions concern." Second, the JOIC makes clear that controllers have to assess whether it is necessary and proportionate to invoke an exemption in relation to the specific data subject right and the specific set of personal data in question: Controllers "should not routinely rely on exemptions or apply them in a blanket fashion – it must be appropriate in the circumstances of the particular request that has been made […]. Similarly, any exemption should only be applied in reference to the specific […] right, the exercise of which would prejudice the interest in question (i.e., a controller's interests in respect of (for example) management forecasting could be prejudiced by the release of information in response to a subject access request but may not be prejudiced in respect of a request for rectification)." Third, with respect to the prejudice test, the JOIC explains that in order to rely on the restriction, "the harm must also be "likely" to prejudice that is to say, it must be more than a theoretical risk and the controller must be able to evidence why this is likely the case. […] There must be more than a mere assertion or belief that disclosure would lead to prejudice." Instead, the prejudice test is a high threshold, requiring a "very significant and weighty chance of prejudice".

European Commission has adopted an adequacy decision pursuant to Article 45 of the GDPR[1639], if appropriate safeguards as described in Article 67 have been put in place, or if the transfer falls within the scope of one of the exceptions listed in Schedule 3 of the Data Protection Law[1640].

Article 67 sets out the conditions for putting in place appropriate safeguards, requiring in particular that enforceable data subject rights and effective legal remedies for data subjects comparable to those under the Data Protection Law must be available in the third country or organization. The instruments that can be used to provide appropriate safeguards are similar to those provided in Article 46 of the GDPR: (1) a legally binding and enforceable agreement between public authorities, (2) binding corporate rules[1641], (3) standard data protection clauses[1642], (4) a code of conduct approved by another authority under the GDPR, and (5) a certification mechanism either approved by Regulations under the Data Protection Law or approved by another authority under the GDPR[1643].

Moreover, under the conditions laid down in Article 67(3), personal data can be transferred subject to the specific authorisation of the JOIC[1644]. Article 67(4) explicitly requires the JOIC to take into account any opinions or decisions of the EDPB in determining whether to authorise a transfer. In this area, Jersey has thus ensured that beyond the alignment of the law itself, also the interpretation of the law remains in line with the interpretation within the EU.

Finally, Schedule 3 of the Data Protection Law provides an exhaustive list of narrowly defined exceptions to the conditions for cross-border transfers laid down in Articles 66 and 67[1645]. These exceptions overlap to a large extent with the derogations for specific situations listed in Article 49 of the GDPR, and their interpretation by the JOIC is also aligned with the EU. In its guidance on international transfers, the JOIC confirms that the exceptions are for

[1639] While the Jersey Data Protection Law does not explicitly require that such adequacy finding is still in force, Jersey is in practice taking into account whether an adequacy decision adopted by the Commission is valid or not. After the EU-U.S. Privacy Shield was invalidated by the Court of Justice of the European Union, the JOIC alerted organisations in Jersey that they could no longer rely on the Privacy Shield for their transfers of personal data. See press release of 22 July 2020, available at: https://jerseyoic.org/blogs/eu-us-privacy-shield-invalidation/.

[1640] Article 66(1) and (2) Data Protection Law.

[1641] Binding corporate rules can be approved by the JOIC if they fulfil the requirements set by Schedule 4 of the Data Protection Law or can be approved by one of the authorities in the EU on the basis of the GDPR. So far, the JOIC has not approved any binding corporate rules.

[1642] While the JOIC has not yet approved any such clauses, data exporters in Jersey can rely on the Standard Contractual Clauses adopted by the European Commission, see also the JOIC's guidance note on international transfers of January 2021, p. 4, available at: https://jerseyoic.org/media/nsajlxvj/joic-international-transfers-guidance-21-01-2021.pdf.

[1643] An approved code of conduct or an approved certification mechanisms have to be each combined with binding and enforceable commitments of the recipient to apply the relevant safeguards in the mechanism, including as regards data subject rights.

[1644] A specific authorisation can be granted if appropriate safeguards are ensured by contractual clauses or by administrative arrangements between public authorities, and there is a mechanism in place for data subjects to enforce their data subject rights and obtain effective legal remedies against the recipient, see Article 67(3)(a) and (b) Data Protection Law.

[1645] Pursuant to Schedule 3 of the Data Protection Law, personal data may be transferred for instance where required by an order or a judgment of a court or tribunal having the force of law in Jersey, where required by a decision of a Jersey public authority based on an international agreement imposing an international obligation on Jersey, where explicit consent of the individual has been obtained, where necessary for the performance of a contract with or in the interest of a data subject, where the transfer is necessary for reasons of substantial public interest or where necessary to protect the vital interests of the data subject or of another individual and explicit consent cannot be obtained from the data subject.

specific situations, should only be used if it is not possible to rely on an adequacy decision or to put in place appropriate safeguards, and that organisations should take into account the EDPB's guidance on derogations[1646].

1.2. Oversight, enforcement and redress

Jersey has also reformed its system of oversight and enforcement of the Data Protection Law, strengthening both the independence and the powers of the oversight body.

Under the Data Protection Authority Law, oversight and enforcement is carried out by the Data Protection Authority (the Authority)[1647], which replaces the Commissioner under the Data Protection Law 2005[1648]. The Authority is composed of a chairperson, three to eight other voting members (the Members), and a commissioner (an ex officio and non-voting member)[1649]. Importantly, a statutory guarantee of the Authority's independence has been introduced in the Data Protection Authority Law, which requires it to act independently and in a manner free from direct or indirect external influence[1650]. In addition, the Authority now enjoys the status of a legal person separate from its members[1651].

The Authority's Members are appointed by the Chief Minister, who must present, at least two weeks prior to the appointment, to the States Assembly (i.e., the Jersey Parliament) a reasoned report about his intention to appoint[1652]. It is required by Law that the Minister must have particular regard to the need to ensure that Members have the qualifications, experience and skills necessary to exercise and perform the functions of a Member, in particular relating to the protection of personal data, as well as a strong sense of integrity and the ability to maintain confidentiality[1653]. The appointments are overseen by the Jersey Appointments Commission[1654].

[1646] Jersey Office of the Information Commissioner, Guidance note on international transfers, January 2021, available at: https://jerseyoic.org/media/nsajlxvj/joic-international-transfers-guidance-21-01-2021.pdf.

[1647] The Authority is established by Article 2 of the Data Protection Authority Law 2018. Its general functions include oversight and enforcement of the Data Protection Law, promoting awareness (among the public, controllers and processors), as well as issuing opinions, guidance and public statements. In addition, the Authority may engage in international co-operation, including by developing international cooperation mechanisms and providing international mutual assistance. See Articles 11 and 13 to 16 Data Protection Authority Law.

[1648] Prior to 2018, the Office of the Information Commissioner was a non-ministerial department of the Government of Jersey and subject to Government oversight, see Annual Report of the Jersey Data Protection Authority 2018, p. 10, available at: https://jerseyoic.org/media/g4ahgcwh/joic-annual-report-2018.pdf. The powers and duties of the Commissioner were set out in Part 6 Data Protection Law 2005.

[1649] Article 3(1) Data Protection Authority Law. At present, the Authority is composed of a chairperson and five voting members.

[1650] Article 12 Data Protection Authority Law. Also, the Authority's Corporate Governance Protocol, adopted in 2019, notes that it is important that the Authority is, in appearance and reality, an independent regulator capable of holding both the States and Government of Jersey to account. The Protocol is available at: https://jerseyoic.org/media/u1tgkgmb/jersey-data-protection-authority-governance-protocol-2019.pdf.

[1651] According to Article 2(2) Data Protection Authority Law, the Authority is established as a body corporate. This means that the Authority can directly employ staff, where in the past it relied on the government to do so and could only employ civil servants, and that it can separate its banking arrangements and internal audits from the government. See the Authority's Corporate Governance Protocol 2019, p. 5, and Annual Report 2018 of the Office of the Data Protection Authority, p. 13.

[1652] Article 3 Data Protection Authority Law. See for instance the Chief Minister's report on the appointment of the Authority's Chairman, available at: https://statesassembly.gov.je/assemblyreports/2018/r.38-2018.pdf.

[1653] Article 3(2) Data Protection Authority Law. An individual is ineligible to be a voting member if the individual is, or has at any time during the preceding 12 months been, a member of the States of Jersey, or if

The Commissioner is the Chief Executive of the Authority, in charge of its day-to-day operations and responsible for managing other employees. The role of the Commissioner is in principle incompatible with any other employment, business or occupation. The Commissioner is appointed by the Members of the Authority and holds office for a (renewable) term of 5 years[1655].

Members can be removed from office by the Chief Minister, but only if the specific conditions for dismissal that are listed exhaustively in the Law are met and if the States are informed at least two weeks in advance of the intended removal[1656]. The conditions for the dismissal of the Commissioner by the Authority are equally set out in the Law[1657].

Compared to the previous regime - regarding which the Article 29 Working Party had raised some questions concerning the extent of the Commissioner's investigatory and enforcement powers[1658] - the Data Protection Authority Law has significantly strengthened the Authority's powers that are now very similar to those foreseen in the GDPR. In particular, the Authority can conduct audits[1659], investigate individual complaints[1660] and carry out general inquiries on its own initiative[1661]. In carrying out its functions, the Authority has access to all relevant information, including the power to enter and search premises, to seize devices and information, to inspect etc.[1662]. Upon finding of a violation of the Data Protection Law, the authority can impose various sanctions, ranging from warnings and reprimands to binding

she/he is a States' employee or is otherwise under the direction and control of the States, or otherwise engaged in any employment, occupation (whether or not remunerated) or business, or receives any benefits, that is incompatible with the functions of a member of the Authority, see Article 3(6) Data Protection Authority Law.

1654 The Jersey Appointments Commission is an independent body that oversees the recruitment of States' employees and appointees to States supported or related bodies. On its involvement in the appointment of Members of the Jersey Data Protection Authority, see for instance the Jersey Appointments Commission annual report 2018, p. 7, available at: https://www.gov.je/Government/Departments/OfficeChiefExecutive/OfficeChiefExecutivesSections/JerseyAppointmentsCommission/Pages/AnnualReports.aspx

1655 Articles 5 and 6 Data Protection Authority Law.

1656 Members can only be dismissed on grounds of serious misconduct, conviction of a criminal offence, bankruptcy, incapacity because of physical or mental illness, other inability to perform their duties, or ineligibility, see Article 4(1) Data Protection Authority Law. A member can only be removed from office on the basis of serious misconduct if a panel consisting of three or more individuals appointed by the Authority and other than a member of the Authority, of the States or the Minister determines the Member to be guilty of a serious misconduct, see Article 4(1)(a) Data Protection Authority Law.

1657 Article 5 Data Protection Authority Law. The Commissioner can only be removed on grounds of serious misconduct, conviction of a criminal offence, bankruptcy, physical or mental illness, or if otherwise unable or unfit to perform the Commissioner's duties. Again, he or she can only be removed on the basis of serious misconduct if a panel consisting of three or more individuals appointed by the Authority and other than a member of the Authority or the Minister determines the Commissioner to be guilty of a serious misconduct, see Article 5(1)(a) Data Protection Authority Law.

1658 Opinion 8/2007 on the level of protection of personal data in Jersey (WP141), see footnote 2, p. 10. In particular, the Working Party was concerned that the Commissioner's powers were more limited than those set out in the Data Protection Directive, and that the Commissioner needed a warrant by a judicial authority to gain access to premises and gather information.

1659 Paragraph 7 of Schedule 1 to the Data Protection Authority Law.

1660 Article 20 Data Protection Authority Law.

1661 Article 21 Data Protection Authority Law.

1662 Paragraphs 1 and 2 of Schedule 1 to the Data Protection Authority Law.

orders (for instance to discontinue processing, bring processing into compliance with the Law, rectify, erase or restrict processing or suspend the transfer of personal data)[1663].

Moreover, the Authority can impose administrative fines for certain violations of the Law[1664]. The fines must be effective, proportionate and have a deterrent effect[1665]. As regards the amount of fines, the Authority has to take into account the same factors as those listed in Article 83(2) GDPR, i.e., the intentional or negligent character of the infringement, any action taken by the controller or processor to mitigate the damage suffered by data subjects, duration of the infringement etc.[1666]. In addition, several violations of the Data Protection Law continue to constitute offences and may therefore be subject to criminal sanctions[1667].

As regards possibilities for individuals to obtain redress, the Jersey system continues to offer various avenues, including the possibility to lodge a complaint with the Authority for any possible breach of the Data Protection Law[1668], to obtain judicial redress directly against controllers with respect to any alleged or potential violation of the transparency and subject rights provisions of the Jersey Data Protection Law[1669] and to obtain compensation for damages[1670]. In addition, individuals can obtain judicial redress against decisions of the Authority[1671].

Despite its relatively small size, the Authority plays an active role. Each year it handles a number of files, including enquiries, complaints, investigations and data breach notifications. In 2019, the Authority received 89 enquiries and 145 complaints. With respect to those complaints that required further action, the organisations concerned either took measures to resolve the complaint on their own account and those measures were deemed satisfactory, organisations were required to implement measures recommended by the Authority, or the complaints could be resolved through the provision of information to the Authority. In several cases the Authority issued warnings, informing organisations that any further breach of the

[1663] Article 25 Data Protection Authority Law. Failure to comply with an order from the Authority is an offence under the Law, see Article 25(8) of the Law.
[1664] These violations are (1) failure to make reasonable efforts to verify that a person giving consent to the processing of the personal data of a child as required by Article 11(4) Data Protection Law is a person duly authorized to give consent to that processing in accordance with that provision; (2) breach of any duty or obligation imposed by Article 7 of, and any provision of Parts 3, 4 or 5 of, the Data Protection Law; (3) processing personal data in breach of any other provision of Part 2 or 6 of the Data Protection Law; or (4) transfer of personal data to a person in a third country or international organisation in contravention of Article 66 or 67 Data Protection Law (Article 26(1) Data Protection Authority Law).
[1665] Article 26(3) Data Protection Authority Law. Article 27(2) Data Protection Authority Law sets the threshold for administrative fines at £300 000 or 10% of the organisation's total global annual turnover or total gross income in the preceding financial year, whichever is the higher. In addition, for violations of Articles 26(1)(a) and (b), the fine cannot exceed £5 000 000, while for violations of Article 26(1) (c) and (d) it cannot exceed £10 000 000, see Article 27(1) Data Protection Authority Law.
[1666] Article 26(2) Data Protection Authority Law.
[1667] This for example applies to processing personal data without being registered with the Authority as controller or processor (Article 17(3) Data Protection Authority Law), failing to comply with an order of the Authority (Article 25(8) Data Protection Authority Law), knowingly or recklessly obtaining or disclosing personal data without the consent of the relevant controller (Article 71(2) Data Protection Law) providing false or misleading information to the Authority (Article 73(1) Data Protection Law), and obstructing an Authority official (Article 74(3) Data Protection Law).
[1668] Article 19 Data Protection Authority Law.
[1669] Article 68 Data Protection Law.
[1670] Article 69 Data Protection Law.
[1671] Article 31 Data Protection Authority Law.

law may be subject to formal sanctions[1672]. In 2020, the Authority handled 106 enquiries and 140 complaints. In 60 cases, the Authority's investigation revealed contraventions of the Data Protection Law, which were remedied further to recommendations given by the Authority. Two cases were considered serious enough to warrant the issuing of public statements[1673]. In terms of outreach, the Authority organises a "Data Protection Week" each year in which it provides information and advice to a large audience, covering topics such as requests for access to data, surveillance in the workplace and data transfers[1674]. It also engages in outreach activities on an ongoing basis, such as presentations and courses for instance on data security for small businesses, on issues relating to the collection of employee data or on how to handle data breaches[1675]. Finally, the Authority provides a significant amount of information online, including toolkits and practical advice, addressing typical questions that organisations and individuals may face.

2. ACCESS TO AND USE OF PERSONAL DATA TRANSFERRED FROM THE EUROPEAN UNION BY PUBLIC AUTHORITIES IN JERSEY

2.1. General legal framework

The limitations and safeguards that apply to the collection and subsequent use of personal data for purposes of criminal law enforcement and national security follow from Jersey's international obligations in the area of fundamental rights and personal data protection, from the rules that apply to the processing of personal data by the public sector, as well as from specific laws regulating access to data by Jersey public authorities.

First, as an exercise of power by a public authority, government access in Jersey must be carried out in full respect of the law. The ratification of the European Convention of Human Rights by the United Kingdom has been extended to Jersey since 1953[1676]. The right to respect for private and family life (and the right to data protection as part of that right) is protected by the Human Rights (Bailiwick of Jersey) Law 2000, which incorporates the majority of rights under the European Convention on Human Rights into Jersey law[1677]. Article 8 of the Convention provides that any interference with privacy must be in accordance with the law, in the interests of one of the aims set out in Article 8(2) and proportionate in light of that aim. Article 8 also requires that the interference is "foreseeable", i.e., have a clear, accessible basis in law, and that the law contains appropriate safeguards to prevent abuse.

[1672] See Annual report 2019, available at: https://jerseyoic.org/media/jydftlzx/joic-annualreport-2019.pdf.
[1673] See Annual report 2020, available at: https://jerseyoic.org/media/f0gfxnkx/joic-annualreport-2020-final.pdf.
[1674] For more information on the Data Protection Weeks in 2019 and 2020, see Annual report 2019, p. 40, and Annual report 2020, p. 41.
[1675] For recent courses and presentations, see for example the events set out on the website of the Authority, available at: https://jerseyoic.org/events/.
[1676] See Declaration contained in a letter from the United Kingdom's Permanent Representative to the Council of Europe, dated 23 October 1953, registered at the Secretariat General on 23 October 1953 – available at: https://www.coe.int/en/web/conventions/full-list2?module=declarations-by-treaty&numSte=005&codeNature=0.
[1677] Article 1(1) and 2(1) Human Rights (Bailiwick of Jersey) Law 2000.

In addition, in its case law[1678], the European Court of Human Rights has specified that any interference with the right to privacy and data protection should be subject to an effective, independent and impartial oversight system that must be provided for either by a judge or by another independent body[1679] (e.g., an administrative authority or a parliamentary body).

Moreover, individuals must be provided with an effective remedy, and the European Court of Human Rights has clarified that the remedy must be offered by an independent and impartial body which has adopted its own rules of procedure, consisting of members that must hold or have held high judicial office or be experienced lawyers, and that there must be no evidential burden to be overcome in order to lodge an application with it. In undertaking its examination of complaints by individuals, the independent and impartial body should have access to all relevant information, including closed materials. Finally, it should have the powers to remedy non-compliance[1680].

Second, the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) also applies in Jersey[1681]. Article 9 of Convention 108 provides that derogations from the general data protection principles, the rules governing special categories of data and data subject rights are only permissible when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences, or for protecting the data subject or the rights and freedoms of others.

Therefore, through adherence to the European Convention of Human Rights and to Convention 108, Jersey is subject to a number of obligations, enshrined in international law and that frame its system of government access on the basis of principles, safeguards and individual rights similar to those guaranteed under EU law and applicable to the Member States. Furthermore, as far as the ECHR is concerned, compliance with these obligations is subject to the judicial control of the European Court of Human Rights.

Third, the Jersey Parliament has adopted specific provisions for the processing of personal data in the law enforcement context, i.e., the Data Protection (Jersey) Law 2018, as modified by Schedule 1 to the Law[1682]. The material scope of the Data Protection Law is similar to the

[1678] According to Article 2(1)(a) Human Rights (Bailiwick of Jersey) Law 2000, a court or tribunal in Jersey that is determining a question which has arisen in connection with a Convention right must take into account any judgment, decision, declaration or advisory opinion of the European Court of Human Rights.
[1679] European Court of Human Rights, Klass and others v. Germany, Application no. 5029/71, paragraphs 17-51.
[1680] European Court of Human Rights, Kennedy v. the United Kingdom, Application no. 26839/05, (Kennedy), paragraphs 167 and 190.
[1681] Declaration contained in a letter from the Permanent Representative of the United Kingdom to the Council of Europe, dated 26 August 1987, handed to the Secretary General at the time of deposit of the instrument of ratification, on 26 August 1987, available at: https://www.coe.int/en/web/conventions/full-list?module=declarations-by-treaty&numSte=108&codeNature=0.
[1682] Pursuant to Article 4(5) Data Protection Law, Schedule 1 modifies the Data Protection Law where processing is carried out by a competent authority and for a law enforcement purpose. The modifications reflect the differences between obligations set out in the GDPR and the Law Enforcement Directive. Competent authorities in Jersey are listed non-exhaustively in Paragraph1 of Schedule 1 to the Data Protection Law and include the Jersey Police, Health and Social Services, Social Services Department, Department for Infrastructure, Social Security Department, Health & Safety Inspectorate, Income Tax Department, Jersey Customs & Immigration Service Jersey Financial Services Commission, Jersey Fire and Rescue Service, Jersey Gambling Commission, Jersey Police Complaints Authority, Jersey Probation Service, Judicial Greffe, The Law Officers'

one of the GDPR. It applies to the processing of personal data by both commercial and public entities[1683]. Furthermore, the data protection principles of lawfulness and fairness[1684], purpose limitation[1685], data minimisation[1686], accuracy[1687], storage limitation[1688] and security[1689] are retained in the Data Protection Law, as modified by Schedule 1, in similar terms as in the Law Enforcement Directive. In essence, the processing of personal data by a competent authority for a law enforcement purpose is permitted only if it is authorised by law and either the data subject has given its consent, or the processing is necessary for the performance of a task carried out by the controller for a law enforcement purpose[1690]. In addition, the Data Protection Law as modified by Schedule 1 imposes specific transparency obligations[1691] and recognises the same data subject rights as the LED[1692]. In particular, individuals enjoy a right of access[1693], correction[1694] and deletion[1695] and have the right not to be subject to automated

---

Department, the Ports of Jersey etc. Pursuant to Article 1(1) Data Protection Law, a law enforcement purpose covers the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against, and the prevention of, threats to public security.

[1683] The Jersey data protection regime applies to the processing of personal data in the context of a controller or processor established in Jersey, see Article 4(2)(a) Data Protection Law. The Law does not apply to the processing of personal data by natural persons in the course of a purely personal or household activity, see Article 4(1) Data Protection Law.

[1684] Article 8(1)(a) Data Protection Law. The processing of personal data by a competent authority for a law enforcement purpose is permitted only to the extent it is permitted by law and (1) the data subject has given consent, (2) the processing is necessary for the performance of a task carried out by a controller for a law enforcement purpose, see Article 9 Data Protection Law as modified by paragraph 4 of Schedule 1 to the Data Protection Law.

[1685] Article 8(1)(b) Data Protection Law. Article 13 of the Data Protection Law, as modified by paragraph 7 of Schedule 1, allows for further processing of data for criminal law enforcement purposes only if the controller is authorised by law to process the data for the other purpose and the processing is necessary and proportionate to that other purpose.

[1686] Article 8(1)I Data Protection Law.

[1687] Article 8(1)(d) Data Protection Law. In addition, as required also by the Law Enforcement Directive, competent authorities must make a clear distinction between personal data relating to different categories of data subjects, such as persons suspected of having committed an offence, persons convicted of a criminal offence, persons who are victims of a criminal offence and witnesses, see Article 13(3) Data Protection Law, as modified by paragraph 7 of Schedule 1 to the Data Protection Law.

[1688] Article 8(1)I Data Protection Law.

[1689] Article 8(1)(f) Data Protection Law.

[1690] Article 9(1) Data Protection Law, as modified by paragraph 4 of Schedule 1 to the Data Protection Law. Pursuant to Article 9(2) Data Protection Law, as modified by paragraph 4 of Schedule 1, stricter conditions apply to the processing of special category data. The processing of such data is only lawful if and to the extent that it is permitted by law and (1) is strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject; (2) serves to protect the vital interests of the data subject or another individual; or (3) the processing relates to data that are manifestly made public by the data subject.

[1691] Article 12 Data Protection Law, as substituted by paragraph 6 of Schedule 1 requires that data subjects are provided with information on the identity and contact details of the controller/controller's representative and the data protection officer, the purposes for processing, the recipients or categories of recipients of personal data, where applicable the intention to transfer data to a third country, the period for which personal data will be stored, data subject rights, the right to lodge a complaint with the Data Protection Authority, etc.

[1692] Similarly to Article 12 Law Enforcement Directive, Article 27 Data Protection Law, as modified by paragraph 12 of Schedule 1 to the Data Protection Law, further specifies the modalities for exercising these rights, allowing competent authorities to refuse to comply with a request from an individual or to charge a reasonable fee for complying with the request if the request is manifestly unfounded, frivolous, vexatious, unnecessarily repetitive or otherwise excessive.

[1693] Article 28 Data Protection Law, as modified by paragraph 13 of Schedule 1 to the Data Protection Law. In addition, Article 28 provides individuals with a right to obtain a confirmation as to whether or not personal data relating to the individual is being processed, as well as to access that data and obtain information relating to its processing (e.g., on the purpose, categories of personal data concerned, the source of the personal data, the recipients, etc.).

[1694] Article 31 Data Protection Law, as modified by paragraph 14 of Schedule 1 to the Data Protection Law.

[1695] Article 32 Data Protection Law, as modified by paragraph 15 of Schedule 1 to the Data Protection Law.

decision-making[1696]. Competent authorities are also required to implement data protection by design and default[1697], to keep records of processing activities[1698], and, in certain situations, to carry out data protection impact assessments and to pre-consult the Data Protection Authority[1699]. Moreover, they are required to put in place appropriate measures to ensure security of processing[1700] and are subject to specific obligations in case of a data breach, including notification of such breaches to the Authority and data subjects[1701]. Like in the Law Enforcement Directive, there is also a requirement for a controller (unless it is a court or other judicial authority acting in a judicial capacity) to designate a data protection officer who assists the controller in complying with its obligations as well as monitoring that compliance[1702]. Finally, the Data Protection Law, as modified by Schedule 1, contains specific provisions on international transfers of personal data[1703]. The provisions substantially echo those in the Law Enforcement Directive. Essentially, transfers to a third country or an international organisation are prohibited unless they are necessary for a law enforcement purpose and based either on an adequacy decision adopted by the European Commission in accordance with Article 37 Law Enforcement Directive or on appropriate safeguards[1704]. In the absence of an adequacy decision and appropriate safeguards, transfers to unauthorised jurisdictions are only possible in specific circumstances that are listed in the law in an exhaustive manner and correspond to the 'derogations' set forth in the Law Enforcement Directive[1705].

Under similar conditions as under the Law Enforcement Directive, Schedule 1 to the Data Protection Law specifies that certain specific provisions of the Data Protection Law[1706] may be restricted to the extent that and for as long as the restriction is a necessary and

[1696] Article 38 Data Protection Law, as modified by paragraph 18 of Schedule 1 to the Data Protection Law.
[1697] Article 15 Data Protection Law, as modified by paragraph 8 of Schedule 1 to the Data Protection Law.
[1698] Article 14 Data Protection Law.
[1699] Articles 16 and 17 Data Protection Law, as modified by paragraph 9 of Schedule 1 to the Data Protection Law.
[1700] Article 21 Data Protection Law, as modified by paragraph 11 of Schedule 1 to the Data Protection Law. This includes additional requirements in relation to automated decision making and requiring logs of processing operations to be kept, as required by the Law Enforcement Directive.
[1701] Article 20 Data Protection Law, as modified by paragraph 10 of Schedule 1 to the Data Protection Law.
[1702] Article 24 Data Protection Law.
[1703] Articles 66 to 67C Data Protection Law, as substituted by paragraph 19 of Schedule 1 to the Data Protection Law.
[1704] Article 66(2) in conjunction with Article 67A Data Protection Law, as substituted by Article 19 of Schedule 1. Appropriate safeguards are in place where provided by a legal instrument binding the intended recipient, such as a legally binding and enforceable agreement between the controller and the recipient, or where the controller, having assessed all the circumstances surrounding the transfer, concludes that appropriate safeguards exist to protect the data. The controller is required to keep detailed written records of any transfer relying on appropriate safeguards, and when relying on appropriate safeguards on the basis of the circumstances surrounding the transfer, the controller must notify the Authority of the categories of data transferred on that basis.
[1705] Article 67B Data Protection Law as substituted by paragraph 19 of Schedule 1 sets out the special circumstances in which international transfers can take place in the absence of appropriate safeguards, i.e. for the protection of vital interests of individuals, to safeguard legitimate interests of the data subject, to prevent immediate and serious threats to the public security of any country, in individual cases for a law enforcement purpose, and in individual cases for a legal purpose.
[1706] The provisions that may be restricted are those that concern: the notification of data breaches (Article 20 Data Protection Law as modified by paragraph 10 of Schedule 1); the right of access (Article 28 Data Protection Law as modified by paragraph 13 of Schedule 1); the right to rectification (Article 31 Data Protection Law, as modified by paragraph 14 of Schedule 1, permits the controller to refrain from informing the data subject about a refusal of rectification in certain circumstances); and the right to erasure and the right to restriction (Articles 32 and 33 Data Protection Law as modified by paragraphs 15 and 16 of Schedule 1 permit the controller to refrain from informing the data subject about a refusal of erasure or restriction in certain circumstances).

proportionate measure for one of the purposes listed in the law, having regard to the fundamental rights and legitimate interests of the data subject concerned[1707].

Moreover, Part 7 of the Data Protection Law imposes restrictions to specific provisions of the Law[1708]. First, Part 7 allows the restriction of individual rights based on the nature of the personal data being processed. These restrictions apply automatically whenever one of the listed categories of personal data is being processed. These categories are listed in an exhaustive manner and cover a very limited, narrowly construed set of situations, which are to a large extent irrelevant in a law enforcement context. In addition, they do not typically cover situations where personal data is transferred to Jersey from the EU[1709]. Second, Part 7 sets out restrictions on grounds of prejudice. They can be invoked only when and to the extent that the application of the provisions "would be likely to prejudice" the legitimate aim pursued. For example, controllers can restrict data subject rights to the extent that their application would be likely to prejudice the combat effectiveness of the armed forces of the Crown[1710], or would be likely to prejudice the prevention, detection, or investigation of crime[1711]. As explained in section 1.1., the JOIC has issued interpretative guidance that clearly frames the application of the restrictions. It clarifies the scope of the different restrictions, including by means of examples, which helps to prevent them from being misunderstood and applied in an overly broad manner. It also explains how the requirements of necessity and proportionality should be applied with respect to these specific restrictions[1712].

The processing of personal data for national security purposes in Jersey is subject to the provisions of the Data Protection Law. As explained above, the Data Protection Law applies to the processing of personal data by both private entities and by public authorities, including for the purpose of safeguarding against or preventing threats to national security. While the Law provides for an exemption from specified provisions[1713] for national security purposes,

[1707] These purposes are to avoid obstructing official or legal inquiries, investigations or procedures; to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties; to protect public security; to protect national security; or to protect the significant interests of others. In case of restriction, the controller must provide the data subject as soon as practicable with a statement informing about the restriction, along with the reasons and the possible redress avenue.
[1708] Most exemptions allow the restriction of data subject rights and transparency provisions.
[1709] The exemptions apply automatically to personal data covered by legal professional privilege, see Article 57 Data Protection Law.
[1710] Article 56 Data Protection Law.
[1711] Article 45 Data Protection Law.
[1712] Jersey Office of the Information Commissioner, Guidance note on exemptions of November 2021, available at: https://jerseyoic.org/media/44kldaym/joic-29a-exemptions-nov21-4.pdf. First, the guidance clarifies that controllers "must consider each exemption on a case-by-case basis because the exemptions only permit you [i.e., as a data controller] to depart from the Data Protection Law's general requirements to the minimum extent necessary to protect the particular functions or activities the exemptions concern." Second, the JOIC makes clear that controllers have to assess whether it is necessary and proportionate to invoke an exemption in relation to the specific data subject right and the specific set of personal data in question: Controllers "should not routinely rely on exemptions or apply them in a blanket fashion – it must be appropriate in the circumstances of the particular request that has been made […]. Similarly, any exemption should only be applied in reference to the specific […] right, the exercise of which would prejudice the interest in question" Third, with respect to the prejudice test, the JOIC explains that in order to rely on the restriction, "the harm must also be "likely" to prejudice that is to say, it must be more than a theoretical risk and the controller must be able to evidence why this is likely the case. […] There must be more than a mere assertion or belief that disclosure would lead to prejudice." Instead, the prejudice test is a high threshold, requiring a "very significant and weighty chance of prejudice".
[1713] Pursuant to Article 41 Data Protection Law, the processing of personal data necessary for the purpose of safeguarding national security can in particular be exempt from the data protection principles and provisions on transparency and data subject rights and from certain parts of the Data Protection Authority Law.

these provisions may only be restricted to the extent it is necessary to safeguard national security. In addition, the application of these exemptions has been clarified through detailed guidance. As recalled above for restrictions applicable in the field of criminal law enforcement, in particular, relying on the exemption is only allowed to the minimum extent necessary to protect the particular functions or activities the exemptions concern. The exemption cannot be invoked in a blanket manner but can be relied upon only on the basis of a case-by-case analysis and considering the actual consequences of applying the relevant provision. All decisions to rely on an exemption have to be documented and controllers must be prepared to share that documentation with the Data Protection Authority[1714].

Moreover, according to Article 41(2) of the Data Protection Law, a certificate signed by the Minister for Home Affairs can confirm the legality of the reliance on the national security restriction[1715]. That means that the certificate serves as conclusive evidence of the fact that a restriction from one or more provision specified in the certificate is required for the purposes of national security. It is important to note that the national security certificate does not provide for an additional ground for restricting data protection rights and obligations for national security reasons. In other words, the controller or processor can only rely on a certificate when it has concluded that it is necessary to rely on the national security restriction which, as explained above, must be applied on a case-by-case basis[1716]. Even if a national security certificate applies to the matter in question, the Jersey Data Protection Authority can investigate whether or not reliance on the national security restriction was justified in a specific case[1717]. Moreover, any person directly affected by the issuing of a certificate may appeal to the Royal Court. The Royal Court will review the decision to issue a certificate and decide whether there were reasonable grounds for issuing it. As a result, the Court can quash the certificate or determine that the certificate does not apply to specific personal data which is the subject of the appeal[1718].

It follows from the above that limitations and conditions are in place under the applicable Jersey legal provisions, as interpreted by the Jersey Data Protection Authority, to ensure that these exemptions and restrictions remain within the boundaries of what is necessary and proportionate to protect criminal law enforcement and national security.

2.2. Access and use by Jersey public authorities for criminal law enforcement purposes

In Jersey, criminal law enforcement functions are primarily carried out by the States of Jersey Police, which is headed by the Chief Officer. Jersey law imposes a number of limitations on how law enforcement authorities have access to and use personal data for criminal law enforcement purposes, and it also provides oversight and redress mechanisms in this area. The

[1714] See the Jersey Office of the Information Commissioner Guidance note on exemptions of November 2021, p. 4, available at: https://jerseyoic.org/media/44kldaym/joic-29a-exemptions-nov21-4.pdf.
[1715] To date, no such certificate has been issued under Jersey's data protection framework.
[1716] See the JOIC's guidance note on exemptions, available at: https://jerseyoic.org/resource-room/guidance-on-exemptions/.
[1717] Article 6(1)(a) Data Protection Law requires the controller to be in a position to demonstrate that it has complied with the law. This implies that any data controller would need to demonstrate to the Data Protection Authority that when relying on the restriction, it has considered the specific circumstances of the case.
[1718] Article 41(4) and (5) Data Protection Law.

conditions under which access to personal data can take place and the safeguards applicable to the use of these powers are assessed in the following sections.

2.2.1. Legal bases and applicable limitations/safeguards

Personal data transferred under the adequacy decision and processed by organisations in Jersey may be obtained by Jersey criminal law enforcement authorities notably by means of investigative measures under the Police Procedures and Criminal evidence (Jersey) Law 2003 (PPCE), on the basis of the Regulation of Investigatory Powers (Jersey) Law 2005, or in the context of anti-money laundering legislation[1719].

The PPCE provides the Jersey police with a legal basis for accessing personal data held by commercial operators through searches and seizures, and production orders. The PPCE lays down detailed rules on the scope and application of these measures, aimed at ensuring that the interference with the rights of individuals will be limited to what is necessary for a specific criminal investigation and proportionate to the pursued purpose. With limited exceptions, searches and seizures may only take place on the basis of a court-issued search warrant[1720] and the issuing of such warrant is subject to specific procedural and substantive requirements. An application for a production order requiring a person to provide the police with access to information must also be made to a court and will also be subject to specific procedural and substantive requirements[1721].

More specifically, a police officer may apply for a search warrant to the Bailiff or a Jurat[1722]. An application for a warrant must state the ground on which it is made and specify the premises to be searched, as well as the articles and persons to be sought[1723].

A search warrant may be issued only if the Bailiff or Jurat is satisfied that there are reasonable grounds to believe[1724] that (1) a serious offence[1725] has been committed of which there is

[1719] In addition, under Jersey law, UK public authorities can lawfully operate in Jersey to access personal data for criminal law enforcement purposes where that is specifically authorised by legislation in force in Jersey (e.g., under the RIPL). The extent to which UK authorities can process law enforcement data that is collected in Jersey on the basis of UK legislation is covered in the Commission Implementing Decision of 28.6.2021 pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data by the United Kingdom, available at: https://commission.europa.eu/system/files/2021-06/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_en.pdf.-

[1720] Pursuant to Articles 19 and 20 PPCE, warrantless searches may only take place in exceptional circumstances that do not appear relevant in the context of data transfers covered by an adequacy decision adopted under the GDPR. In particular, a police officer may search a premise for the purpose of (1) arresting a person whom the officer has reasonable cause to suspect has committed an offence or where the officer has reasonable cause to suspect that any offence is in progress on the premises or is about to be or has been committed on the premises; (2) where the officer has reasonable cause to suspect that any person is committing, is about to commit or has committed an offence on the premises; or (3) for the purpose of saving life or limb or preventing serious damage to property. In addition, a warrantless search may take place on a premise occupied or controller by a person under arrest for a serious offence, if the police have reasonable grounds to suspect that there is evidence on the premise that relates to that offence, or a connected/similar offence.

[1721] Article 16 and Schedule 2 to PPCE.

[1722] A Bailiff is the senior judge of Jersey's Royal Court and Jurats are elected lay judges.

[1723] Article 17(2) PPCE.

[1724] The test of 'reasonable grounds to believe' is an objective one. It is not necessary that there should be proof that a criminal offence has been committed, but it requires some evidence which suggests that the crime may have been committed. See Ashbolt v Revenue and Customs Commissioners [2020] EWHC 1588, at para 14 which has been cited with approval by the Royal Court in Jersey.

evidence on the premises specified in the application[1726] or (2) that there are goods on premises specified in the application which have been unlawfully obtained[1727].

In terms of formal requirements, the warrant must specify the identity of the person who applied for it, the date of issuance, the enactment under which it is issued, the premise to be searched and, in as far as practicable, the articles or persons to be sought[1728]. The police officer carrying out the search must provide the occupier of the searched premise with the warrant, or in case the latter is not present, leave a copy of the warrant[1729].

A police officer may seize and retain anything for which a search was authorised[1730]. A police officer who is lawfully on any premises may furthermore seize anything at the premise if he/she believes on reasonable grounds that the item has been obtained as a result of committing a crime and it is necessary to seize it in order to prevent it from being concealed, lost, tampered with or destroyed[1731]. Moreover, the police officer may require information stored in electronic form to be produced in a form in which it can be taken away if he/she has reasonable grounds to believe that it is evidence or has been obtained as a result of the commission of an offence and it is necessary to do so to prevent it from being concealed, lost, tampered with or destroyed[1732].

In addition to the powers of search and seizure described above, Article 101 PPCE allows the Attorney General to authorise the taking of any action as the Attorney General may specify, in respect of any property or wireless telegraphy. Such authorisation can be issued by the Attorney General only if (s)he believes that such action is necessary for detecting or

---

[1725] Schedule 1 to the PPCE sets out which offences qualify as 'serious offences', covering for instance treason, murder, manslaughter, rape, kidnapping etc.

[1726] The evidence must be likely to be of substantial value to the investigation of the offence, must be likely to be relevant, and must not consist of or include items subject to legal privilege, excluded material or special procedure material, see Article 15(2) PPCE. 'Items subject to legal privilege' are communications between a professional legal adviser and the advisor's client made in connection with the giving of legal advice to the client or in connection with legal proceedings and items enclosed with or referred to in such communications. Items held with the intention of furthering a criminal purpose are not items subject to legal privilege, see Article 5 PPCE. 'Excluded material' means (1) personal records which a person has acquired or created in the course of any trade, business or other occupation or for the purposes of any paid or unpaid office and which the person holds in confidence; (2) human tissue or tissue fluid which has been taken for the purposes of diagnosis or medical treatment and which a person holds in confidence; (3) journalistic material which a person holds in confidence and which consists of documents, or of records other than documents, see Article 6(1) PPCE. 'Special procedure material' is material in the possession of a person who (1) acquired or created it in the course of any trade, business or other occupation or for the purpose of any paid or unpaid office; and (2) holds it subject to an express or implied undertaking to hold it in confidence or journalistic material, other than excluded material, see Article 6(4-5) PPCE.

[1727] Article 15(1)(b) PPCE. In addition, one of the following conditions must be met: (1) it is not practicable to communicate with any person entitled to grant entry to the premises; (2) it is practicable to communicate with a person entitled to grant entry to the premises but it is not practicable to communicate with any person entitled to grant access to the evidence; (3) entry to the premises will not be granted unless a warrant is produced; (4) the purpose of a search may be frustrated or seriously prejudiced unless a police officer arriving at the premises can secure immediate entry to them. See Article 15(3) PPCE.

[1728] Article 17(6) PPCE.

[1729] Article 18(5)-(7) PPCE.

[1730] Article 15(2) PPCE.

[1731] Article 21(2) PPCE. The same applies if the police officer has reasonable grounds to believe that the item to be seized is evidence in relation to an offence or it is necessary to seize it in order to prevent the evidence from being concealed, lost, tampered with or destroyed, see Article 21(3) PPCE.

[1732] Article 21(4) PPCE.

preventing serious crime[1733] or in the interests of the security of Jersey and the action is proportionate to what it seeks to achieve[1734]. In considering whether this is the case, the Attorney General must take into account whether what it is thought necessary to achieve by the authorised action could reasonably be achieved by other means[1735]. An authorisation must be in writing and ceases to have effect after three months[1736].

Specific limitations and safeguards also apply to the use of investigatory powers by public authorities in Jersey. The use of investigatory powers to obtain information on communications is governed by the Regulation of Investigatory Powers (Bailiwick of Jersey) Law 2003 (RIPL)[1737]. The RIPL regulates notably the interception of communications, the acquisition and disclosure of communications data (i.e., metadata stored by the service providers), and the use of surveillance (such as covert investigations).

Article 5 RIPL introduces a general principle of confidentiality of communications by providing that it is an offence to intercept communications in the course of their transmission by means of a public postal service or a public or private telecommunication system without lawful authority. Article 7 RIPL further clarifies that to be lawful, any interception of communications must be authorised by an interception warrant[1738] issued by the Attorney General[1739].

[1733] Pursuant to Article 101(4) PPCE, 'serious crime' for the purposes of such authorisation, is defined as conduct which constitutes an offence which involves the use of violence, or results in substantial financial gain, or is committed by a large number of persons in pursuit of a common purpose, or any other offence for which a person over 21 with no previous convictions could reasonably be expected to be sentenced to imprisonment for three years or more.

[1734] Article 101(2) PPCE.

[1735] Article 101(3) PPCE.

[1736] Article 102(1)-(2) PPCE. In urgent cases, authorisation may be given orally and ceases to have effect after 72 hours. An authorisation may be renewed in writing for another period of three months and must be cancelled if the Attorney General is satisfied that the action is no longer necessary.

[1737] The RIPL is supplemented by the Regulation of Investigatory Powers (Codes of Practice) (Jersey) Order 2006 (the Codes). The Codes provide guidance on the procedures that must be followed before the interception of communications, the acquisition and disclosure of communications data or surveillance can take place under the provisions of the RIPL. The Codes are legally binding to the extent provided by Article 52 of the RIPL. Pursuant to Article 52(3) RIPL, they are admissible in civil and criminal proceedings. If any provision of the Codes appears relevant to proceedings before any court or tribunal, including the Tribunal established under the RIPL, or to the Commissioner responsible for overseeing the use of these powers (see section 2.2.3), it must be taken into account, see Article 52(4) RIPL.

[1738] Interception without warrant is only lawful in specific limited circumstances set out exhaustively in Articles 8 and 9 RIPL, for instance if the sender and the intended recipient of the communication have consented to the interception, if the sender or the intended recipient has consented to the interception and surveillance by means of that interception has been authorized under Part 3 RIPL, if the interception is carried out by a provider of postal or telecommunication services and connected to the purpose of providing that service, if it is related to the granting of wireless telegraphy licenses or the prevention and detection of interference with wireless telegraphy, or if it is carried out for the purpose of obtaining information about the communications of a person who is or is reasonably believed to be in a country or territory outside of Jersey, the interception relates to the use of a telecommunications service provided to persons in that country and the law of that country or territory requires the provider of that service to carry out, secure or facilitate the interception in question. Any interception conducted by public authorities under Articles 8 and 9 RIPL must be done in accordance with the Human Rights Law 2000 (in particular Article 8 of the European Convention of Human Rights incorporated by that Law) and with the Data Protection Law.

[1739] The Attorney General is independent of the Government. Pursuant to Article 2(1) of the Departments of the Judiciary and the Legislature (Jersey) Law 1965, he/she is appointed by Her Majesty and his/her independence is guaranteed by the provisions of that Law.

An interception warrant can be issued on application by certain persons specifically listed in the law[1740] only if the Attorney General believes that it is necessary for one of the purposes listed in Article 10(3) RIPL. These include the purpose of preventing or detecting serious crime[1741]. Importantly, the law explicitly requires that the conduct that would be authorised must be proportionate to what is sought to be achieved by that conduct[1742]. In considering the necessity and proportionality of the measure, the Attorney General must take into account whether any alternative means could be reasonably used to obtain the information[1743]. In addition, paragraph 2.5 of the Code of Practice on the Interception of Communications Data further clarifies that this requires a balance of the intrusiveness of the interference against the need for it in operational terms. The interception of communications will not be proportionate if it is excessive in the circumstances of the case. In addition, any interception should be carefully managed to meet the objective in question and must not be arbitrary or unfair[1744].

In accordance with Article 12 RIPL, the warrant must either name or describe one person as the interception subject or specify a single set of premises as the premise in relation to which the interception is to take place. The warrant must also describe the communications for which interception is authorised, including the addresses, numbers, apparatus or other factors used to identify the communications[1745]. An interception warrant in principle ceases to have effect after 3 months beginning with the day of the warrant's issue, unless it is renewed. A renewal may be authorised by the Attorney General only where (s)he believes that the warrant continues to be necessary for the purposes described in Article 10(3) RIPL[1746].

The RIPL also regulates the acquisition and disclosure of communications data. The acquisition and disclosure of communications data is not aimed at obtaining the content of a communication, but aimed at obtaining information such as traffic data, information about the use of a postal service or telecommunications service, and any other information held or obtained by a postal service/telecommunication service in relation to persons to whom the service is provided[1747].

Persons designated with respect to a specific public authority[1748] may obtain communications data by giving notices to a postal or telecommunications operator, requiring the operator to

---

[1740] Pursuant to Article 11(1) RIPL, these are the Chief Officer, the Agent of the Impôts, the Chief Immigration Officer, the Director General of the Security Service, the Chief of the Secret Intelligence Service, the Director of GCHQ, the Chief of Defence Intelligence of the Ministry of Defence of the Government of the United Kingdom and a person who, for the purposes of any international mutual assistance agreement, is the competent authority of a country or territory outside Jersey.

[1741] Article 1(1) RIPL defines 'serious crime' as conduct which constitutes one or more offences which involve the use of violence, results in substantial financial gain or is conducted by a large number of persons in pursuit of a common purpose; and for which a person who has attained the age of 21 and has no previous convictions could reasonably be expected to be sentenced to imprisonment for 3 years or more.

[1742] Article 10(2)(b) RIPL.

[1743] Article 10(4) RIPL.

[1744] Schedule 1, paragraph 2.5, Regulation of Investigatory Powers (Codes of Practice) (Jersey) Order 2006.

[1745] Article 12(3) RIPL. Under Articles 12(4) and (5) RIPL, these specifications are not required for the interception of communications sent or received outside Jersey where the Attorney General has issued a certificate certifying that the examination of certain described intercepted material is necessary. In that case, specific additional safeguards set out in Article 20 RIPL apply.

[1746] Article 13 RIPL.

[1747] 'Communications data' is defined in Article 24 RIPL.

[1748] In accordance with Article 29(1) RIPL and Schedule 1 to the RIPL, the designated persons are the Chief Officer (for the Jersey Police Force), the Agent of the Impôts (for Customs and Excise), the Chief Immigration

obtain and/or disclose relevant data[1749]. The designated person may also grant an authorisation for persons holding relevant offices, ranks or positions in that public authority to obtain communications data[1750]. A notice or authorisation may only be issued if the designated person believes that it is necessary to obtain communications data for one of the specific purposes listed exhaustively in the law, including for the purpose of preventing or detecting crime or of preventing disorder[1751].

Importantly, the notice or authorisation may only be granted if the designated person believes that obtaining the data in question is proportionate to what is sought to be achieved[1752]. According to the Code of Practice on Accessing Communications Data, this means that even if an action that interferes with a Convention right is directed at pursuing a legitimate aim, this will not justify the interference if the means used to achieve the aim are excessive in the circumstances. Any interference with a Convention right must be carefully designed to meet the objective in question and must not be arbitrary or unfair. Even taking all these considerations into account, in a specific case interference may still not be justified because the impact on the individual or group is too severe[1753].

The notice must be issued in writing and specify the communications data to be obtained, the grounds on which it is necessary to obtain the data, the office, rank or position held by the person issuing the notice, and the manner in which any disclosure required by the notice is to be carried out[1754]. The effect of a notice is limited and unless it is renewed, it ceases to require that data be obtained one month after the date on which the notice is given[1755]. A notice may be renewed before the end of the period of one month under the same conditions as described above[1756].

In Jersey, criminal law enforcement authorities can also obtain personal data from business organisations in the context of investigations into whether a person has engaged in or benefited from criminal conduct, or into the whereabouts of the proceeds of criminal conduct. These powers are governed by the Proceeds of Crime (Jersey) Law 1999 (POCL).

In accordance with the POCL, the Bailiff can, on an application of a police officer, make orders to produce or give access to material, issue search warrants to obtain that material

---

Officer (for the Immigration and Nationality Department) and the Attorney General (for the Income Tax Department, the Social Security Department, any of the Parishes and any of the intelligence services).

[1749] Article 26(4) RIPL.

[1750] Article 26(3) RIPL.

[1751] Pursuant to Article 26(2) RIPL, the notice or authorisation can also be issued if it is in the interests of national security, in the interests of the economic well-being of Jersey (as specified in Schedule 3, paragraph 4.2 of the Code of Practice, only to the extent relevant in the interest of national security), in the interests of public safety, for the purpose of protecting public health, for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department, for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health, or for any other purpose which is specified by Regulations made by the States.

[1752] Article 26(5) RIPL.

[1753] Schedule 3, paragraph 4.4 of the Regulation of Investigatory Powers (Codes of Practice) (Jersey) Order 2006.

[1754] Article 27(1)-(2) RIPL.

[1755] Article 27(4) RIPL.

[1756] Article 27(5) RIPL. If the person who has given the notice is satisfied that it is no longer necessary on these grounds or no longer proportionate to what is ought to be achieved, the person shall cancel the notice, pursuant to Article 27(8) RIPL.

where a production order is not appropriate or not complied with, make customer information orders and account monitoring orders.

Each type of order is subject to strict formal and substantial requirements. In essence, the scope of such orders is always limited to one individual or one set of premises, they must contain specific mandatory information, and they may only be issued for limited purposes.

For instance, under the POCL, the Bailiff can make an order to make material available if there are reasonable grounds for suspecting that a specified person has engaged in or benefited from criminal conduct, there are reasonable grounds for suspecting that the material is likely to be of substantial value to the investigation, and does not consist of or include items subject to legal professional privilege, and there are reasonable grounds for believing that it is in the public interest that the material should be produced or that access to it should be given[1757].

The Bailiff can issue a search warrant under the POCL authorising a police officer to enter and search specific premises, provided that the same conditions as described above are met and an order to make material available has not been complied with, or it would not be appropriate to make such an order[1758]. Where a police officer has entered premises in the execution of a search warrant, he or she may seize and retain any material, other than items subject to legal professional privilege, which is likely to be of value to the investigation for the purposes of which the warrant was issued[1759].

A customer information order is an order made by the Bailiff with the consent of the Attorney General[1760] on application by a police officer which requires a financial services business[1761] to provide any customer information[1762] that the institution has relating to a person specified in the application for the order[1763], in such manner, and within such time as specified in the application[1764]. An account monitoring order requires the financial services business specified in the application to provide account information specified in the order to an appropriate

[1757] Article 40 POCL. In relation to any material that consists of information contained in a computer, such an order requires to produce the material in a form in which it can be taken away and in which it is visible and legible, or to give access to the material in a form in which it is visible and legible, see Article 40(8) POCL.
[1758] Article 41 POCL.
[1759] Article 41(5) POCL.
[1760] Paragraphs 3 and 4, Part 1 of Schedule 3 to the POCL.
[1761] Financial services businesses are defined in Schedule 2 to the POCL and include for instance lending, financial leasing, operating a money service business, currency exchange and cheque cashing, facilitating or transmitting money or value through an informal money or value transfer system or network, issuing, redeeming, managing or administering means of payment, including credit, charge and debit cards, cheques, travellers' cheques, money orders and bankers' drafts and electronic money, providing financial guarantees or commitments, trading in money market instruments, foreign exchange, exchange, interest rate or index instruments, and commodity futures, transferable securities or other negotiable instruments or financial assets, participating in securities issues and the provision of financial services related to such issues, etc.
[1762] Customer information is defined in Paragraph 6, Part 1 of Schedule 3 to the POCL and covers information about whether a business relationship exists or existed between a person carrying on a financial services business and a particular person (a 'customer'), a customer's account number, full name, date of birth, address or former address, the date on which a business relationship between a financial services business and a customer begins or ends, any evidence of a customer's identity obtained by a financial services business in pursuance of or for the purposes of any legislation relating to money laundering, and the identity of a person sharing an account with a customer.
[1763] Paragraph 5(b), Part 1 of Schedule 3 to the POCL.
[1764] Paragraph 1(3), Part 1 of Schedule 3 to the POCL.

officer, for the period[1765], in a manner, and by the time stated in the order[1766]. The conditions for issuing these orders are identical to the ones described above[1767].

Importantly, any disclosure of personal data obtained on the basis of the abovementioned provisions has to comply with the Data Protection Law, and the further processing by criminal law enforcement authorities of personal data obtained through such disclosures is subject to the provisions of the Data Protection Law, as modified by Schedule 1 to the Law.

2.2.2. Further use of the information collected

The further use of data collected by Jersey criminal law enforcement authorities on one of the grounds referred to in Section 2.2, as well as the sharing of such data with a different authority for purposes other than the ones for which it was originally collected (so-called 'onward sharing'), is subject to safeguards and limitations.

First, the processing of personal data by law enforcement authorities in Jersey is governed by the provisions of the Data Protection Law, as modified by Schedule 1 to the Law (see section 2.1. above) With respect to onward sharing, Article 13 of the Data Protection Law as modified by Schedule 1, like the LED, allows that personal data collected for a law enforcement purpose may be further processed (whether by the original controller or by another controller) for any other (secondary) law enforcement purpose provided that the controller is authorised by law to process the data for the other purpose and the processing is necessary and proportionate to that other purpose. In this case, all the safeguards provided by the Data Protection Law (referred to in section 2.1) apply to the processing carried out by the receiving authority. The Law explicitly prohibits personal data collected for a law enforcement purpose from being processed for a purpose that is not a law enforcement purpose, unless that processing is authorised by law[1768].

When law enforcement authorities in Jersey intend to share personal data processed under the Data Protection Law with law enforcement authorities of a third country, specific requirements apply[1769]. These requirements are very similar to those set out by the Law Enforcement Directive. Essentially, transfers of personal data to a third country or an international organisation are prohibited, unless the intended recipient is a law enforcement authority[1770], the transfers are necessary for a law enforcement purpose, and they are based on

[1765] The period stated in an account monitoring order must not exceed the period of 90 days beginning with the day on which the order is made (Paragraph 1(6), Part 2 of Schedule 3 to the POCL).
[1766] Paragraph 1(5), Part 2 of Schedule 3 to the POCL.
[1767] See Paragraph 5, Part 1 of Schedule 3 to the POCL, and Paragraph 1(1), Part 2 of Schedule 3 to the POCL.
[1768] Article 13(2) Data Protection Law, as modified by paragraph 13 of Schedule 1 to the Data Protection Law.
[1769] Part 8 Data Protection Law, as modified by paragraph 19 of Schedule 1 to the Data Protection Law.
[1770] Pursuant to Article 66(2)(b)(ii) in conjunction with Article 67C Data Protection Law, as modified by paragraph 19 of Schedule 1 to the Data Protection Law, personal data can be transferred to any other person only subject to specific conditions and safeguards: the transfer must be strictly necessary in a specific case for the performance of a task of the transferring controller as provided by law for any of the law enforcement purposes, and the transferring controller has determined that there are no fundamental rights and freedoms of the data subject concerned that override the public interest necessitating the transfer, considers that the transfer of the personal data to a relevant authority in the third country would be ineffective or inappropriate (for example, where the transfer could not be made in sufficient time to enable its purpose to be fulfilled), and informs the intended recipient of the specific purpose or purposes for which the personal data may, so far as necessary, be processed. Where personal data are transferred to a person in a third country other than a relevant authority, the transferring controller must inform a relevant authority in that third country without undue delay of the transfer,

an adequacy decision adopted by the European Commission pursuant to Article 36 Law Enforcement Directive or on appropriate safeguards[1771]. In the absence of an adequacy decision or appropriate safeguards, transfers are only possible in specific circumstances that are listed in the law in an exhaustive manner, e.g., for the protection of vital interests of individuals, to safeguard legitimate interests of the data subject, to prevent immediate and serious threats to the public security of any country, and in individual cases for a law enforcement purpose or a legal purpose, provided that there are no fundamental rights and freedoms of the data subject overriding the public interest in the transfer[1772].

Second, the different laws that allow for data collection by law enforcement authorities in Jersey impose specific limitations and safeguards as to the use and further dissemination of the information obtained in exercising the powers they grant.

As regards the powers of search and seizure under the PPCE, the police officer who seizes anything must, if requested by the occupier of premises, provide in reasonable time that person with a record of what he has seized. The police officer must also grant access to or supply a photograph or a copy of the seized or retained item at the request of the person who had custody of the item before it was seized[1773]. Importantly, anything that has been seized by the police may not be retained longer than necessary in the circumstances[1774].

With respect to the interception of communications, Article 19 RIPL sets out the safeguards that need to be applied to material intercepted on the basis of a warrant. In particular, the Attorney General must make arrangements to ensure that the dissemination of the intercepted material (i.e., the number of people who can access it, the extent to which the material is disclosed or copied, the number of copies[1775], etc.) is limited to the minimum necessary for the authorised purposes. Each copy made of any of the materials must be destroyed as soon as there are no longer any grounds for retaining it as necessary for any of the authorised purposes[1776]. If intercepted material is shared with authorities of a country or territory outside

---

unless this would be ineffective or inappropriate. The transferring controller must document any transfer to a recipient in a third country other than a relevant authority; and inform the Authority of the transfer.

[1771] Article 66 Data Protection Law, as modified by paragraph 19 of Schedule 1 to the Data Protection Law. In addition, in a case where the personal data was originally transmitted or otherwise made available to the controller or another competent authority by a Member State of the European Union, that Member State, or any person based in that Member State that is a competent authority for the purposes of the Law Enforcement Directive, has authorized the transfer in accordance with the law of the Member State. Appropriate safeguards are in place where provided by a legal instrument binding the intended recipient, or where the controller, having assessed all the circumstances surrounding the transfer, concludes that appropriate safeguards exist to protect the data. The controller is required to keep detailed written records of any transfer relying on appropriate safeguards, and when relying on appropriate safeguards on the basis of the circumstances surrounding the transfer, the controller must notify the Authority of the categories of data transferred on that basis.

[1772] Article 67B Data Protection Law, as modified by paragraph 19 of Schedule 1 to the Data Protection Law.

[1773] Article 23 PPCE.

[1774] Article 24 PPCE.

[1775] 'Copy' is defined in Article 19(7) RIPL as (1) any copy, extract or summary of the material or data which identifies itself as the product of an interception; and (2) any record referring to an interception which is a record of the identities of the persons to or by whom the intercepted material was sent, or to whom the communications data relates, and "copied" shall be construed accordingly.

[1776] Pursuant to Article 19(4) RIPL, something is considered necessary for the authorised purposes if (1) it continues to be, or is likely to become, necessary as mentioned in Article 10(3), (2) it is necessary for facilitating the carrying out of any of the functions of the Attorney General in relation to the interception of communications, (3) it is necessary for facilitating the carrying out of any functions of the Commissioner or of the Tribunal in relation to the interception of communications, or (4) it is necessary to ensure that a person

of Jersey, the Attorney General is required to make arrangements that ensure corresponding limitations, to the extent that the Attorney General seems fit, and that prevent any disclosure that would not be lawful within Jersey[1777].

These safeguards are further specified in the Codes of Practice. In particular, the Code of Practice on the Interception of Communications requires all intercepted material to be handled in accordance with the arrangements made by the Attorney General, the details of which must be made available to the Investigatory Powers Commissioner (see section 2.2.3 below). The Attorney General must ensure that the safeguards are in force before any interception can begin. The Commissioner is required to review the adequacy of the safeguards[1778]. All intercepting agencies are required to keep detailed records of interception warrants for which they have applied[1779]. The Code further requires intercepted material, as well as copies and summaries of the material, to be handled and stored securely to minimise the risk of loss or theft. In particular, it must be inaccessible to persons without the required level of security clearance, and this requirement for secure storage also applies to communications service providers. It also requires intercepted material to be securely destroyed as soon as it is no longer needed for any of the authorised purposes and retained material to be reviewed at appropriate intervals to confirm that its retention is justified and valid[1780].

Concerning the acquisition and disclosure of Communications Data, the Code of Practice on Accessing Communications Data provides that applications and notices for communications data must be retained by the relevant public authority until they have been audited by the Investigatory Powers Commissioner. The public authority should also keep a record of the dates on which an authorisation or notice is started and cancelled. The Code furthermore provides that communications data, as well as all copies, extracts and summaries of it, must be handled and stored securely[1781].

2.2.3. Oversight

Different bodies carry out oversight of the activities of criminal law enforcement authorities.

First, the processing of personal data by competent authorities for criminal law enforcement purposes is subject to the oversight of the JOIC, whose independence is enshrined in law[1782]. The tasks and powers of the JOIC mirror those set out in Article 46 and 47 of the LED[1783]. To perform those tasks, the JOIC may investigate complaints, conduct inquiries into the processing of personal data by criminal law enforcement authorities[1784], issue recommendations, make a determination of a violation of the Law and impose sanctions[1785]. These sanctions can include reprimands, warnings or corrective orders (e.g., requiring the

conducting a criminal prosecution has the information needed to determine what is required of that person by his or her duty to secure the fairness of the prosecution.

[1777] Article 19(6)(b) RIPL.

[1778] Schedule 1, paragraph 6.1-6.3, Regulation of Investigatory Powers (Codes of Practice) (Jersey) Order 2006.

[1779] Schedule 1, paragraph 5.15, Regulation of Investigatory Powers (Codes of Practice) (Jersey) Order 2006.

[1780] Schedule 1, paragraph 6.4 to 6.9, Regulation of Investigatory Powers (Codes of Practice) (Jersey) Order 2006.

[1781] Schedule 3, paragraph 7, Regulation of Investigatory Powers (Codes of Practice) (Jersey) Order 2006.

[1782] Article 12 Data Protection Authority Law.

[1783] Article 11 Data Protection Authority Law.

[1784] Article 21 Data Protection Authority Law.

[1785] Article 24 Data Protection Authority Law.

authority to bring processing in compliance with the Law, rectify or erase data, cease the processing, etc.)[1786]. In addition, the JOIC may issue a public statement concerning data breaches, violations of the Data Protection Law or imposed corrective orders/sanctions, where it considers that it would be in the public interest to do so given the gravity of the matter or other exceptional circumstances[1787]. In determining which order to impose, the JOIC must have regard to different factors, such as the nature, gravity and duration of the violation, whether the violation was intentional or negligent, the degree of cooperation with the JOIC to remedy the breach, any other action taken to mitigate any damage suffered by data subjects etc.[1788]. Since the entry into force of the Data Protection Law, the JOIC has engaged with law enforcement authorities by providing guidance and advice on the application of the Data Protection Law[1789]. The JOIC and SOJP have also worked together on joint initiatives such as a Fraud Prevention Forum and CCTV awareness.

Second, the activities of the Attorney General under the PPCE, i.e., the authorisation of interference with property or wireless telegraphy pursuant to Article 101 PPCE, are subject to the oversight of a commissioner appointed by the Bailiff among one of the ordinary judges of the Court of Appeal[1790]. The role of the Commissioner is to keep under review the carrying out by the Attorney General of his functions. To that end, the Attorney General is required to notify the Commissioner of any authorisations given, renewed or cancelled at least every 12 months[1791]. The Commissioner has a duty to make a report to the Bailiff on the carrying out of the Attorney General's functions under the PPCE as soon as practicable after the end of each year. The Bailiff in turn is required to submit a copy of that report to the States[1792].

Third, the use of investigatory powers under the RIPL is overseen by the Investigatory Powers Commissioner. Under Part IV of the RIPL, the Bailiff must appoint a judge of the Court of Appeal (of Jersey) as the Investigatory Powers Commissioner. The Commissioner is responsible for reviewing the activities under the RIPL, including the issuing of interception warrants, and the issuing of authorisations and notices for the collection and disclosure of communications data[1793]. All persons involved in the use of investigatory powers are required to disclose or provide to the Commissioner all documents and information that the Commissioner may require for the purpose of enabling him to carry out his functions[1794]. The Commissioner is in turn required to prepare an annual report on the use of investigatory powers for submission to the Bailiff of Jersey[1795]. The Bailiff must lay before States a copy of every annual report made by the Commissioner[1796]. The Commissioner's report is also made

[1786] Article 25 Data Protection Authority Law. The JOIC cannot impose administrative fines on competent authorities processing personal data for criminal law enforcement purposes, see Article 26(9) Data Protection Authority Law.
[1787] Article 14 Data Protection Authority Law.
[1788] Article 26(2) Data Protection Authority Law.
[1789] There have been complaints relating to the handling of data subject access requests and compliance with data protection principles against the States of Jersey Police and Honorary Police. The States of Jersey Police has also reported data breaches to the JOIC. These matters have been investigated by the JOIC but have not been found to require regulatory sanctions.
[1790] Article 104 PPCE.
[1791] Article 103 PPCE.
[1792] Article 104(3) and (4) PPCE.
[1793] Article 43 RIPL.
[1794] Article 44 RIPL.
[1795] Article 44(4) RIPL.
[1796] Article 44(6) RIPL.

public. If it appears to the Commissioner that there has been a contravention of the RIPL or insufficient safeguards have been put in place for intercepted communications, he/she must report that to the Bailiff[1797].

As described in the Commissioner's recent annual reports, the overwhelming majority of warrants requested and granted in Jersey are in support of law enforcement activities, notably for the purpose of detecting and preventing large-scale commercial drug trafficking and associated money laundering. In his annual reports, the Commissioner found that warrants had been issued for properly identified statutory purposes, in respect of the principles of necessity and proportionality and in compliance with procedural requirements. He also noted that the safeguards required by Article 19 RIPL had been implemented in a satisfactory manner[1798].

2.2.4. Redress

As regards the processing of personal data by law enforcement authorities in Jersey, redress mechanisms are available under the data protection legislation, under the Human Rights Law 2000 and under the RIPL. This series of mechanisms provide data subjects with effective administrative and judicial means of redress, enabling them in particular to ensure their rights, including the right to have access to their personal data, or to obtain the rectification or erasure of such data.

First, data subjects have the right to lodge a complaint with the JOIC concerning the processing of their personal data by criminal law enforcement authorities[1799]. The JOIC has the power to determine breaches of the Data Protection Law and impose necessary sanctions. It also has the power, on request by a data subject or on its own initiative, to bring proceedings before a court in respect of any breach or anticipated breach of the Law. Following such complaint, the court can make any order, relief and remedy it considers just under the circumstances, including an award of compensation to any person who suffers damage as a result of the breach, an injunction or interim injunction to restrain any actual or anticipated breach of an operative provision, and a declaration that a breach was committed[1800].

Second, individuals can obtain judicial redress against decisions of the JOIC. This includes the possibility to challenge an action or inaction of the JOIC before a court, e.g., decisions not to investigate a complaint, or decisions finding that there has been no violation of the Law.

[1797] Article 44(2) and (3) RIPL.
[1798] Recent reports of the Investigatory Powers Commissioner are available at: https://statesassembly.gov.je/assemblyreports/2022/r.98-2022.pdf, https://statesassembly.gov.je/assemblyreports/2022/r.4-2022.pdf, https://statesassembly.gov.je/assemblyreports/2019/r.112-2019.pdf. In 2021, the Commissioner noted that in two cases the Attorney General had declined to authorise an interception warrant because the 'serious crime' threshold had not been satisfied. The Commissioner considered these instances as indicative for the care with which the Attorney General performed his statutory functions. In 2018, the Commissioner identified some areas in the applications for interception warrants in which further detail could have been beneficial, and others in which quality could be improved. In addition, the Commissioner noted a limited number of exceptional cases in which 'human error' had led to data being acquired from a wrong telephone number. He explained that to prevent such errors from happening in the future, additional procedural safeguards has been put in place.
[1799] Article 19 Data Protection Authority Law.
[1800] Article 30 Data Protection Authority Law.

Moreover, an individual can appeal to the court against any failure of the JOIC to provide written notice that a complaint is either being investigated or not being investigated, within the time period specified in the Law, or if the complaint is being investigated, written notice of the progress and, where applicable, the outcome of the investigation within the time period specified in the Law. If a determination of the Authority is appealed, the court has the power to confirm or annul the determination of the JOIC and remit the matter back to the JOIC for reconsideration and make any other order it considers just[1801].

Third, under Articles 68 and 69 of the Data Protection Law, individuals can also obtain judicial redress against criminal law enforcement authorities directly before the courts. In particular, if there is a breach of the operative provisions of the Law and the breach causes damage to another person, it is actionable in court by that person[1802].

Fourth, as far as any person considers that their rights, including rights to privacy and data protection, have been violated by public authorities, individuals can obtain redress before the Jersey courts under the Human Rights Law 2000. Under Article 7(1) of the Human Rights Law, it is unlawful for a public authority to act in a way which is incompatible with rights provided in the law[1803]. A person who claims that a public authority has acted (or proposes to act) in a way which is unlawful under Article 7(1) can bring proceedings against the authority under this Law in the appropriate court or tribunal, when he or she is (or would be) a victim of the unlawful act[1804]. If the court finds any act of a public authority to be unlawful, it can grant such relief or remedy, or make such order, within its powers as it considers just and appropriate[1805].

Finally, any individual may obtain judicial redress before the European Court of Human Rights against the unlawful collection of his/her data by criminal law enforcement authorities, provided that all available domestic remedies have been exhausted.

For violations of the RIPL or the PPCE, individuals can also obtain redress before the Interception of Communications Tribunal. This redress avenue is described in section 2.3.4 below.

2.3. Access and use by Jersey public authorities for national security purposes

[1801] Articles 31 and 32 Data Protection Authority Law.
[1802] For instance, in Alwitry-v-The States Employment Board and Minister for H&SS 25-Feb-2016 (jerseylaw.je), a data subject challenged the content of disclosures made in response to a data subject access request.
[1803] However, the act of the public authority is not unlawful if as the result of one or more provisions of primary legislation, the authority could not have acted differently or in the case of one or more provisions of, or made under, primary legislation which cannot be read or given effect in a way which is compatible with the Convention rights, the authority was acting so as to give effect to or enforce those provisions, see Article 7(6) of the Human Rights Law.
[1804] Article 8(1) Human Rights Law. According to Article 8(5) Human Rights Law a person is a victim of an unlawful act only if he would be a victim for the purposes of Article 34 of the Convention if proceedings were brought in the European Court of Human Rights in respect of that act.
[1805] Article 9(1) Human Rights Law.

In Jersey, access to information transferred under the adequacy decision for purposes of national security can take place in the form of the interception of communications and the acquisition and disclosure of communications data on the basis of the RIPL[1806].

2.3.1. Legal bases and applicable limitations/safeguards

The interception of communications and acquisition and disclosure of communications data may not only take place in the context of criminal investigations, but also when necessary in the interests of national security or to safeguard the economic well-being of the Bailiwick[1807]. The use of these powers for those purposes is subject to the same substantive and procedural limitations and safeguards as described in section 2.2.1 in the context of criminal law enforcement, notably the need for independent authorisation, requirements of necessity and proportionality and limitation to specific communications or information[1808].

Moreover, although the notion of "economic well-being" may appear broad, Article 10 RIPL sets out that an interception warrant can only be considered necessary for the purpose of safeguarding the economic well-being of Jersey if the purpose is to obtain information relating to the acts or intentions of persons outside Jersey[1809]. In addition, the Code of Practice on the Interception of Communications further specifies that the Attorney General can only issue an interception warrant for the purpose of safeguarding the economic well-being of Jersey if he considers, on the basis of the facts of each case, that there is a direct link between the economic well-being of the Bailiwick and national security[1810]. Similarly, the Code of Practice on Accessing Communications Data sets out that communications data can only be obtained for the purpose of the economic well-being of Jersey if, on the basis of the facts of each case, the economic well-being is directly related to national security[1811].

2.3.2. Further use of the information collected

The further use of personal data obtained in the interests of national security is governed by the provisions the Data Protection Law, as described in section 2.1[1812]. Pursuant to Article

[1806] The safeguards under the RIPL apply to any Jersey or UK public authorities making use of powers under the RIPL, notably the requirements for the issuing and implementation of interception warrants, restrictions on the use and disclosure of intercepted material, and the right of complaint to the Tribunal. The Human Rights Law and the Data Protection Law also apply. Where UK intelligence services process information collected in Jersey there are also limitations and safeguards provided by UK law, see the Commission Implementing Decision of 28.6.2021 pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data by the United Kingdom, available at: https://commission.europa.eu/system/files/2021-06/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_en.pdf.

[1807] Articles 10(3)(a) and (c) and 26(2)(a) and (c) RIPL.

[1808] Differently from what is described in Section 2.2.1, when relating to the interception of communications in the interest of national security or the safeguarding of Jersey's economic well-being, a warrant can be renewed for up to six months, see Article 13(3)(a) RIPL.

[1809] Article 10(5) RIPL.

[1810] Schedule 1, paragraph 4.4, Regulation of Investigatory Powers (Codes of Practice) (Jersey) Order 2006. An example of a situation where it might be possible to rely on this ground to authorise an interception would be a threat to Jersey's critical national infrastructure that would impact Jersey's economic interests (e.g., through an attack on Jersey's essential communications infrastructure).

[1811] Schedule 3, paragraph 4.4 Regulation of Investigatory Powers (Codes of Practice) (Jersey) Order 2006.

[1812] The Data Protection Law applies to the processing of personal data by a competent authority, including for the purpose of safeguarding against or preventing threats to national security. While the Data Protection Law provides for an exemption from specified provisions for national security purposes, these provisions may only be

8(1)(a) and (b) of the Data Protection Law, data processing must be lawful, and data must not be further processed in a manner that is incompatible with the purpose for which it was collected[1813].

Moreover, specific requirements apply when personal data is shared with authorities outside of Jersey[1814]. As described in more detail in sections 1.1 and 2.1, these requirements are very similar to those set out by the EU's data protection framework. Transfers of personal data to a third country or an international organisation are prohibited, unless they are based on an adequacy decision adopted by the European Commission pursuant to either Article 45 GDPR or Article 36 of the Law Enforcement Directive, or on appropriate safeguards[1815]. In the absence of an adequacy decision or appropriate safeguards, transfers are only possible in specific circumstances that are listed in the law in an exhaustive manner[1816].

In addition, the RIPL, complemented by the relevant Codes of Practice, sets out specific safeguards for the further use and sharing of data obtained on the basis of its provisions. These involve particular arrangements to ensure that the dissemination of material obtained is limited to the minimum necessary for the purposes pursued with the authorisation. Material must be handled and stored securely to minimise the risk of loss or theft and must be destroyed as soon as there are no longer any grounds for retaining it as necessary for any of the authorised purposes. Retained material must be reviewed at appropriate intervals to confirm that its retention is justified and valid. All agencies exercising powers on the basis of the RIPL are required to keep detailed records of warrants or authorisations for which they have applied[1817]. Intercepted material may be shared with authorities of a country or territory outside of Jersey only if arrangements are in place to ensure corresponding limitations and to prevent any disclosure that would not be lawful within Jersey[1818].

2.3.3. Oversight

Government access for national security purposes in Jersey is overseen by different bodies. The Data Protection Authority oversees the processing of personal data in light of the Data Protection Law, while specific oversight on the use of the investigatory powers under the RIPL is provided by the Investigatory Powers Commissioner.

---

restricted if necessary and proportionate and to the extent that their application would be likely to prejudice national security.

[1813] Pursuant to Article 13(2) Data Protection Law, the controller must assess whether that processing is compatible with the purposes for which the personal data were collected by taking into account factors that include any link between the purposes for which the data have been collected and the purposes of the intended further processing, the context in which the data have been collected, in particular regarding the relationship between data subjects and the controller, the nature of the data, in particular whether it is special category data, the possible consequences of the intended further processing for data subjects, and the existence of appropriate safeguards.

[1814] Part 8 Data Protection Law, as modified by paragraph 19 of Schedule 1 to that Law where the processing is by a competent authority for a law enforcement purpose.

[1815] Article 66 Data Protection Law.

[1816] Article 66(2)I Data Protection Law in conjunction with Schedule 3 to the Data Protection Law.

[1817] Article 19 RIPL, Schedule 1, paragraphs 5.15, 6.1-6.3 and 6.4-6.9 Regulation of Investigatory Powers (Codes of Practice) (Jersey) Order 2006; Schedule 3, paragraph 7, Regulation of Investigatory Powers (Codes of Practice) (Jersey) Order 2006.

[1818] Article 19(6)(b) RIPL, see also section 2.2.2 above.

The processing of personal data carried out for national security purposes is governed either by the provisions of the Data Protection Law. The general functions and powers of the JOIC are laid down in Article 11 *et seq.* of the Data Protection Authority Law. The tasks include, but are not limited to, monitoring and enforcement, promoting public awareness, advising the Jersey parliament and government and other institutions on legislative and administrative measures, promote the awareness of controllers and processors of their obligations, provide information to a data subject concerning the exercise of the data subject's rights, handle complaints, conduct investigations, issue guidance etc. The JOIC has the powers to notify controllers of an alleged infringement and to issue warnings that a processing is likely to infringe the rules, issue reprimands, ban processing or order the controller to take certain actions[1819]. While the Data Protection Law[1820] allows exemptions from certain provisions, including from those that concern the JOIC, for national security purposes, these provisions may only be restricted on a case-by-case basis to the extent that their application would be likely to prejudice national security and if necessary and proportionate (as explained in section 2.1).

Furthermore, as described in section 2.2.3 above in the context of criminal law enforcement, the Investigatory Powers Commissioner oversees the application of the RIPL i.e., the interception of communications and the acquisition and disclosure of communications data. In his recent annual reports, the Commissioner noted that the overwhelming majority of warrants in Jersey were requested and granted in a law enforcement context, in particular for the purposes of detection and prevention of drug trafficking and associated money laundering[1821].

2.3.4. Redress

Individuals can obtain redress for violations of the RIPL or the PPCE before the independent Investigatory Powers Tribunal established by Article 46 RIPL[1822].

The Tribunal is the appropriate forum for any complaint by a person, including any individual in the EU, who believes[1823] that conduct under the RIPL or under the PPCE[1824] has taken

[1819] Part 4 Data Protection Authority Law.
[1820] Pursuant to Article 41 Data Protection Law, the processing of personal data necessary for the purpose of safeguarding national security can be exempt from certain parts of the Data Protection Authority Law, provided that the applicable conditions are fulfilled.
[1821] Recent reports of the Investigatory Powers Commissioner are available at:
https://statesassembly.gov.je/assemblyreports/2022/r.98-2022.pdf,
https://statesassembly.gov.je/assemblyreports/2022/r.4-2022.pdf,
https://statesassembly.gov.je/assemblyreports/2019/r.112-2019.pdf.
[1822] In accordance with Article 46(1) RIPL, the Tribunal consists of three members appointed by the by the Superior Number of the Royal Court of Jersey, of whom one shall be an ordinary judge of the Court of Appeal, who shall be the president of the Tribunal, and two shall be Jurats. Pursuant to Schedule 3 to the RIPL, the members are appointed for a term of 5 years and can be reappointed. A member of the Tribunal may be removed from office by the Royal Court at the member's own request.
[1823] On the standard of the 'belief' test, in the absence of relevant case law in Jersey, UK case law is likely to be persuasive. In Human Rights Watch v Secretary of State [2016] UKIPTrib15_165-CH, paragraph 41, the Investigatory Powers Tribunal, by referring to the European Court of Human Rights case law, held that the appropriate test is whether in respect of the asserted belief that any conduct falling within Subsection 68(5) of RIPA 2000 has been carried out by or on behalf of any of the intelligence services, there is any basis for such belief, such that the individual may claim to be a victim of a violation occasioned by the mere existence of secret measures or legislation permitting secret measures, only if he is able to show that due to his personal situation, he is potentially at risk of being subjected to such measures.

place in relation to him, his property or his communications or in relation to that person's use of any postal service, telecommunications service or telecommunication system[1825]. In addition, the complainant is required to believe that the conduct has taken place either in "challengeable circumstances"[1826] or has been carried out by or on behalf of the intelligence services[1827].

When considering a complaint, it is the duty of the Tribunal to investigate whether surveillance has taken place in relation to the complainant, as well as the authority for such surveillance, if any[1828]. The Tribunal determines whether any errors of law, errors of fact or procedural errors have been committed, or whether there has been any other irregularity, such as a lack of proportionality[1829]. All persons involved in the exercise of powers under the RIPL are required to provide to the Tribunal all such documents and information that the Tribunal may need to carry out its functions[1830]. The Tribunal also has the power to require the Investigatory Powers Commissioner to provide the Tribunal with all such assistance (including the Commissioner's opinion as to any issue to be determined by the Tribunal) as the Tribunal think fit[1831]. The Commissioner must be kept informed about the proceedings and any determination, award, order, or other decision made in relation to those proceedings[1832].

If the Tribunal makes a determination in favour of the complainant, the Tribunal must provide the complainant with a summary of that determination including any findings of fact. The tribunal must also give notice to the complainant if no determination has been made in his/her favour[1833]. The Tribunal has the power to issue interim orders and to provide any such award of compensation or other order as it thinks fit. This may include an order quashing or cancelling any warrant or authorisation and an order requiring the destruction of any records of information obtained in exercise of any power conferred by a warrant or authorisation, or otherwise held by any public authority in relation to any person[1834].

Further, an individual who believes that his or her rights under the Data Protection Law have been (or are about to be) breached can make a complaint to the JOIC, (as described in section 2.3.3 above). Redress mechanisms under the Data Protection Law include breach

[1824] Pursuant to Article 46(6) RIPL, conduct is subject to the jurisdiction of the Tribunal if it is carried out by or on behalf of any of the intelligence services, if it is in connection with the interception of communications in the course of their transmission by means of a postal service or telecommunication system, if it is conduct to which the rules on the acquisition and disclosure of communications data apply, conduct to which the rules on surveillance covert human intelligence sources apply, or if it is any entry on or interference with property or any interference with wireless telegraphy.
[1825] Article 46(5)(a) RIPL.
[1826] Pursuant to Article 46(8) RIPL, conduct has taken place in 'challengeable circumstances' if it has taken place with authority (e.g., on the basis of an interception warrant or an authorisation/notice for the acquisition and disclosure of communications data), or if the circumstances are such that it would not have been appropriate for the conduct to take place without authority, or at least without proper consideration having been given to whether such authority should be sought. Conduct does not take place in challengeable circumstances to the extent that it is authorized by, or takes place with the permission of, the Bailiff.
[1827] Article 46(5)(b) RIPL.
[1828] Article 48(3)(a) and (b) RIPL.
[1829] Article 48(3)(c) RIPL.
[1830] Article 49(6) and (7) RIPL.
[1831] Article 49(2) RIPL.
[1832] Article 49(3) RIPL.
[1833] Article 49(5) RIPL.
[1834] Article 48(7) RIPL.

determinations or sanctions issued by the JOIC, and civil proceedings before a court, in which a court can make any order, relief and remedy it considers just under the circumstances, including an award of compensation to any person who suffers damage as a result of the breach, an injunction or interim injunction to restrain any actual or anticipated breach of an operative provision, and a declaration that a breach was committed (as described in section 2.2.4 above).

Finally, as also described in section 2.2.4 above, as far as individuals consider that their rights, including rights to privacy and data protection, have been violated by public authorities, they can obtain redress before the Jersey courts under the Human Rights Law 2000. In addition, any individual may obtain judicial redress before the European Court of Human Rights against the unlawful collection of his/her data for national security purposes, provided that all available domestic remedies have been exhausted.

IX. NEW ZEALAND

1. RULES APPLYING TO THE PROCESSING OF PERSONAL DATA

1.1. Relevant developments in the data protection framework of New Zealand

The adequacy decision for New Zealand was adopted on 19 December 2012[1835], following the opinion of the Article 29 Working Party of 4 April 2011[1836]. At the time of the adoption of the decision, the protection of personal data in New Zealand was mainly governed by the Privacy Act of 17 May 1993[1837]. Since the adoption of the adequacy decision, the Privacy Act 1993 was amended several times: by the Privacy Amendment Act 2013, the Harmful Digital Communications Act 2015, the Intelligence and Security Act 2017 and the Enhancing Identity Verification and Border Processes Legislation Act 2017. Moreover, a comprehensive reform of the Privacy Act 1993 was launched in 2018 and concluded in 2020 with the adoption of the Privacy Act 2020, which entered into force in December 2020. In addition, further interpretations and clarifications have been provided by the courts and the data protection authority (the Office of the Privacy Commissioner, OPC).

Like its predecessor, the Privacy Act 2020 has a broad scope of application, applying to "agencies"[1838], i.e., private operators[1839] and the public sector[1840], regardless of where they

[1835] Commission Implementing Decision 2013/65/EU of 19 December 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by New Zealand, OJ L 28, 30.1.2013, p. 12.

[1836] Opinion No 11/2011 on the level of protection of personal data in New Zealand, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp182_en.pdf.

[1837] In addition, the OPC has the power to adopt legally binding Codes of Practice providing for specific data protection rules (that may amend corresponding provisions of the Privacy Act 2020) for certain sectors (Section 32 Privacy Act 2020). There are currently six codes of practice: the Civil Defence National Emergencies (Information Sharing) Code (which applies in relation to emergencies for which a state of national emergency is in force, e.g., a natural disaster or epidemic); the Credit Reporting Privacy Code (which applies to credit reporters); the Health Information Privacy Code (which applies to agencies providing health or disability services, institutions providing training of health professionals, health insurance agencies, etc. and, inter alia, provides for enhanced transparency requirements and specific grounds for data processing); the Justice Sector Unique Identifier Code; the Superannuation Schemes Unique Identifier Code and the Telecommunications Information Privacy Code (which applies to subscriber information, traffic information and telecommunications content held by telecommunications agencies). The Codes were amended several times to reflect corresponding changes introduced in the Privacy Act, most recently on the occasion of the 2020 reform.

[1838] Section 4, in conjunction with Section 7(1), 8 and 9 Privacy Act 2020. The Act does not apply to 'news entities', to the extent they carry out news activities (the gathering, preparing or compiling of any (observations on) news or current affairs for the purpose of publication, as well as the publication itself, Section 7(1) Privacy Act 2020). Case law has clarified that this is to be understood as "news activity which is conducted responsibly", i.e., ethically and in a manner consistent with the public interest in fair and accurate reporting. In particular, the exemption cannot be used to "shield a news medium from the Privacy Act where the agency fails to meet the standards of responsible news activity, including impartiality, accuracy and balance" (Director of Human Rights Proceedings v Slater [2019] NZHRRT 13, at 62.8, 80 and 92.5). The recent reform further limited this exception, by specifying that only news entities that are subject to oversight by a recognised independent body (e.g., the Broadcasting Standards Authority, BSA or New Zealand Media Council, NZMC) are able to rely on it (Section 7(1) Privacy Act 2020). When the exception applies, the balance between privacy and freedom of expression is ensured through other standards developed by these oversight bodies on fairness, ethical journalism, privacy and complaint handling, e.g., Standard 7 of the BSA and the Principles of the NZMC.

[1839] The Act does not apply to individuals that handle personal information solely for domestic affairs unless the processing is highly offensive to a reasonable person (Section 27 Privacy Act 2020). The OPC has explained that, to determine whether this is the case, different factors should be taken into account, such as the sensitivity of the information, the harm to the individual, whether the information was in the public domain, etc. (https://privacy.org.nz/further-resources/knowledge-base/view/232).

collect or hold personal information, and regardless of where the concerned individuals are located[1841]. While the definition of personal information in the Privacy Act 2020 itself (i.e., information about an identifiable individual[1842]) has not changed, decisions of the OPC have confirmed its broad interpretation, e.g., by clarifying that information will be considered personal information as long as "any person can link the information with other information to identify the individual or individuals to which it relates"[1843]. The territorial scope of the New Zealand data protection rules have been extended by the Privacy Act 2020, which also applies to overseas agencies that carry on business in New Zealand (which is understood broadly and does not necessarily imply a commercial operation, having a place of business in New Zealand, receiving any monetary payment for the supply of goods or services or intending to make a profit from the business in New Zealand)[1844].

The main data protection principles provided under the New Zealand data protection framework at the time of the adoption of the adequacy decision, which are mainly reflected in the Privacy Act's Information Privacy Principles (IPP), have remained in place. This is the case for the principles of lawfulness[1845], purpose limitation (IPP 1, 10 and 11), data minimisation (IPP 1)[1846], data accuracy (IPP 7(2) and 8), data retention (IPP 9), data security (IPP 5) and accountability[1847]. At the same time, several aspects of the legal framework have been further clarified and developed, either through legislative amendments or case law and/or guidance and decisions of the OPC.

In particular, several aspects of the requirements for lawfulness of processing have been strengthened. Whereas agencies were already only allowed to collect personal information for a lawful purpose connected with their function or activity[1848], the Privacy Act 2020 has further clarified that, even if there is such a purpose, but pursuing it does not require the collection of an individual's identifying information, the agency may not require such information[1849]. The Act also requires agencies to specifically take into account the situation

---

[1840] A few public authorities are excluded from the scope of application, such as the Sovereign, the House of Representatives, the Governor-General, courts in relation to their judicial functions and Ombudsmen (Section 8(b) Privacy Act 2020). The processing of personal information by those authorities is subject to other rules, such as the Parliamentary Practice in New Zealand (p. 86, 507 and 750; the Standing Orders for private and secret evidence; and Senior Courts (Access to Court Documents) Rules 2017. In addition, as explained in more detail in section 2.1, the processing of personal data by intelligence agencies is subject to (limited) exceptions.

[1841] Section 4(1)(a) and (2) Privacy Act 2020.

[1842] Section 7(1) Privacy Act 2020.

[1843] AO 1/2016 [2017] NZPrivCmr 1, at 11.

[1844] Section 4(1)(b) and (3) Privacy Act 2020. Factors the OPC considers to qualify as "carrying on business in New Zealand" include repetitive, systematic or continuing use of personal information in New Zealand, websites targeted at New Zealanders, the holding of trademarks and registered web domains in New Zealand, etc. (see e.g., the information provided under the decision tree at https://www.privacy.org.nz/responsibilities/your-obligations/disclosing-personal-information-outside-new-zealand/decision-tree-page/).

[1845] See IPP 1, 2 and 4 (collection of personal information), IPP 10 (use) and IPP 11 (disclosure).

[1846] See for example Case Note 87513 [2006] NZPrivCmr 11 and Case Note 229558 [2012] NZPrivCmr 1.

[1847] Section 201 of the Privacy Act 2020.

[1848] In particular, personal information may not be collected in contravention of the law (e.g., collection in violation of another statute, collection to carry out a criminal activity etc.) or if not relevant to and closely linked with an agency's activities or functions. Where personal information is received by a New Zealand agency on the basis of the adequacy decision, the purpose of collection will in principle be the purpose for which the information is transferred.

[1849] IPP 1 (2).

of children or young people when collecting personal information, to ensure that the way in which the information is collected is fair in the circumstances[1850].

In addition, since the adoption of the adequacy decision, certain legal bases for the use or disclosure of personal information have been further circumscribed[1851]. First, the possibility to use or disclose personal information whose source is publicly available has been limited through an amendment introduced by the Harmful Digital Communications Act 2015 that clarified that this ground cannot be relied upon if, in the circumstances of the case, it would be unfair or unreasonable to use/disclose the information[1852]. The OPC has clarified that different factors should be taken into account in this context, including how old the information is, how it was made public, the sensitivity of the information, the seriousness of the possible impact of it and the steps that have been taken by an agency to verify the information[1853]. Second, the Privacy Amendment Act 2013 clarified in which situations personal information may be used or disclosed to prevent or lessen a serious threat to public health or public safety, or the life or health of an individual[1854]. In particular, to determine whether there is a serious threat, regard has to be given to the likelihood of the threat being realised; the severity of the consequences if the threat is realised and the time at which the threat may be realised[1855].

With respect to public authorities, the Privacy Amendment Act 2013 introduced the possibility for the government to approve so-called information sharing agreements (AISAs)[1856], which allow different bodies or different parts/departments within one authority to share personal information to facilitate the provision of public services[1857]. AISAs are adopted after consulting the OPC, as well as any person or organisation representing the interests of the (classes of) individuals whose information would be shared[1858]. AISAs may provide for modifications to the IPPs, e.g., by establishing specific grounds to collect, use or disclose personal information and must specify the categories of information that may be shared, as well as the purposes for which and circumstances in which this may take place[1859]. There are currently 13 approved AISAs, including between Inland Revenue and the Department of Internal Affairs, between the Ministry of Social Development and the New Zealand Customs Service, as well as an AISA for improving public services to vulnerable

[1850] IPP 4 (b).
[1851] The Privacy Act 2020 allows the use and disclosure of personal information for a different purpose than for which it was collected in a limited number of situations, e.g., if the purpose of use/disclosure is directly related to the purpose for which the information was collected; the use/disclosure is authorised by the individual; the use/disclosure is necessary for the conduct of proceedings before a court or tribunal, etc. (IPP 10 and 11).
[1852] IPP 10(1)(d) and 11(1)(d).
[1853] Available at: https://privacy.org.nz/tools/knowledge-base/view/250?t=169619_237542.
[1854] IPP 10(1)(f) and 11(1)(f).
[1855] See the definition of serious threat in Section 7(1) Privacy Act 2020. The notion has also been further clarified in case law. For example, in R v R [2015] NZHC 713 at [71]-[73], the High Court found that the threshold was not reached, as the disclosure was made based on suspicion and there was not sufficient evidence to meet the test that the release of the information was necessary to prevent or lessen a serious threat. In another case, the OPC found that the threshold had been met in relation to a disclosure by the Police to an emergency mental health team about a woman who told Police that she was suicidal (Case Note 279251 [2017] NZPrivCmr 4). See also Te Pou Matakana Limited v Attorney-General (No 1) [2021] NZHC 2942 (WOCA 1) and Te Pou Matakana Limited v Attorney-General (No 2) [2021] NZHC 3319 (WOCA 2).
[1856] Section 145-146 Privacy Act 2020.
[1857] Section 136, in conjunction with Section 139 and 140 Privacy Act 2020. While private operators may also become party to an AISA, at least one of the agencies must be a public authority (Section 141 Privacy Act 2020).
[1858] Section 150 Privacy Act 2020.
[1859] Section 144 and 145(2) Privacy Act 2020.

children[1860]. Before recommending an AISA, a Minister must inter alia be satisfied that it will facilitate the provision of a public service, the type and quantity of personal information to be shared is no more than necessary to facilitate the provision of the public service and the AISA contains adequate safeguards to protect the privacy of concerned individuals[1861]. The handling of personal information under AISAs remains subject to the oversight of the OPC[1862].

As regards transparency, the Privacy Act 2020 generally requires agencies to provide certain information, including about their contact details, the purpose of collection and intended recipients (IPP 3), when they collect information directly from the individual. To further strengthen the level of transparency, the New Zealand government introduced in September 2023 a bill in the Parliament to amend the Privacy Act 2020 to extend these proactive notification requirements to also apply to situations where information is collected indirectly (i.e., where it is obtained from other entities and further used/disclosed)[1863].

Another area of the New Zealand data protection regime that has evolved since the adoption of the adequacy decision concerns the requirements with respect to security. Although until recently, New Zealand agencies would voluntarily report data breaches to the OPC, the Privacy Act 2020 introduced an obligation to notify both the OPC and concerned individuals[1864] as soon as practicable after becoming aware of notifiable privacy breaches (i.e., a privacy breach that it is reasonable to believe has caused serious harm to an affected individual or individuals or is likely to do so)[1865]. To assess whether a privacy breach has or is likely to cause serious harm, different factors should be taken into account, including any action taken by the agency to reduce the risk of harm following the breach; the sensitivity of the information; and the nature of the harm that may be caused to affected individuals[1866]. In limited situations, an agency is not required to inform individuals, e.g., where doing so would prejudice the security or defence of New Zealand or endanger the safety of a person, or may delay the notification (where and as long as providing the information may constitute a risk for the security of the information that outweighs the benefits of informing the individuals)[1867]. Failure to notify the OPC without a reasonable excuse is an offence subject to a fine[1868]. In this context, an agency may not use the fact that it has taken steps to address the breach as a defence[1869].

Whereas the accountability requirements under the Privacy Act 2020 have not changed, the OPC has developed several tools to assist agencies with their compliance efforts. For example, the OPC issued detailed guidance and a toolkit to carry out privacy impact

[1860] Available at: https://www.privacy.org.nz/privacy-act-2020/information-sharing/approved-information-sharing-agreements/.
[1861] Section 149 Privacy Act 2020.
[1862] The OPC can exercise its different enforcement powers (see below) and conduct specific reviews of the operation of the AISAs (Section 158 et seq. Privacy Act 2020).
[1863] https://bills.parliament.nz/v/6/56e3fbe7-1f3d-464e-b54d-08dbae8917ae?Tab=history.
[1864] Where it is not practicable to notify each individual separately, the agency must instead provide public notice (Section 115(2) Privacy Act 2020).
[1865] Sections 114 and 115, in conjunction with Section 112(1) Privacy Act 2020.
[1866] Section 113 Privacy Act 2020.
[1867] Section 116 Privacy Act 2020.
[1868] Section 118 Privacy Act 2020.
[1869] Section 118 Privacy Act 2020.

assessments[1870]. It also launched a "Privacy Trust Mark" in 2018, which may be issued for a specific product or service on the basis of an assessment of several criteria, including whether a privacy impact assessment has been carried out, whether the product/service demonstrates privacy by design and by default, how end-to-end security is demonstrated, etc. [1871]

As regards the processing of special categories of data, the New Zealand privacy framework considers information sensitive depending on the circumstances and context in which it is processed. The OPC has clarified through guidance that this will generally be the case when the inferences that can be drawn about the individual from information are potentially sensitive[1872]. This for example applies to information about a person's race, ethnicity, gender, sexual orientation, sex life, health, disability, age, membership of an advocacy group, trade union or political party and religious, cultural or political beliefs[1873]., i.e., categories of data that are also considered sensitive under EU data protection law. The sensitivity of personal information is a relevant factor to take into in the application of several requirements of the Privacy Act 2020, e.g., to determine which security safeguards to apply (IPP 5) and whether the means to collect personal information are fair and not unreasonably intrusive (IPP 4)[1874].

With respect to data subject rights, the New Zealand data protection framework continues to provide individuals with a right of access and correction[1875], which have been further and strengthened through legislative developments, as well as case law and OPC guidance. For example, recent case law has confirmed that the right of access extends to any information necessary to provide meaningful access, including for instance on the purpose of processing, the logic involved in the processing of personal information on the basis of algorithms, as well as third parties with whom information may be shared[1876]. In addition, the restrictions to

[1870] Available at: https://privacy.org.nz/publications/guidance-resources/privacy-impact-assessment/ and https://privacy.org.nz/responsibilities/privacy-impact-assessments/.

[1871] Available at: https://privacy.org.nz/resources-2/applying-for-a-privacy-trust-mark/ and https://www.privacy.org.nz/privacy-for-agencies/applying-for-a-privacy-trust-mark/privacy-trust-mark-criteria-and-considerations/.

[1872] Available at: https://www.privacy.org.nz/assets/New-order/Your-responsibilities/Privacy-resources-for-organisations/Sensitive-Personal-Information-and-the-Privacy-Act-2020.pdf

[1873] See also the guidance and case notes of the OPC with respect to health (e.g., https://privacy.org.nz/further-resources/knowledge-base/view/39?t=204565_283253, Case note 297084 [2019] NZPriv Cmr 11, Case note 269784 [2016] NZ PrivCmr 3), genetic (e.g., https://privacy.org.nz/blog/your-dna-is-only-a-click-away-home-dna-tests-and-privacy/) and biometric information (e.g., https://privacy.org.nz/further-resources/knowledge-base/view/277?t=204613_283308). Moreover, New Zealand recently signed the Agreement on the exchange of personal data between Europol and the designated authorities of New Zealand that contains a definition of sensitive data covering the same categories.

[1874] See also several cases of the OPC, e.g., Case Note 83994 [2008] NZPrivCmr 6 (August 2008, Case Note 270745 [2016] NZPrivCmr 10 (June 2016) and case law of the Human Rights Review Tribunal, e.g., Taylor v Orcon [2015] NZHRRT 15.

[1875] IPP 6 and Part 4, subpart 1 (access) and IPP 7 and Part 4, subpart 2 (correction) Privacy Act 2020. Whereas the Privacy Act 2020 does not contain separate provisions on direct marketing, other instruments continue to provide for specific protections when personal information is used for direct marketing purposes. This includes the Unsolicited Electronic Messages Act of 2007 (which imposes restrictions on address-harvesting and prohibits the sending of commercial electronic messages for marketing purposes without consent of the concerned individual), as well as specific provisions on the use of personal information for direct marketing purposes in the Credit Information Privacy Code (which prohibits credit reports from using/disclosing credit information for any purpose related to marketing or direct marketing, Rule 10(1B) and 11(3)(b) of the Code) and the Telecommunications Information Privacy Code (which e.g., requires telecommunication agencies to inform individuals of the right to withdraw their authorisation for the use of their information for direct marketing purposes, Rule 10(1)(b) of the Code). In addition, there is a Marketing Association voluntary Do Not Call/Mail registry (https://marketing.org.nz/do-not-call-do-not-mail).

[1876] Naidu v Royal Australasian College of Surgeons [2018] NZHRRT 23.

the right of access have further evolved. Like Regulation (EU) 2016/679 (GDPR)[1877], the New Zealand data protection regime provides agencies with the possibility to refuse to disclose personal information in response to a request for access from an individual in specific, limited circumstances[1878], e.g., if disclosure of the information would be likely to prejudice the security or defence of New Zealand; the prevention, investigation and detection of offences or would disclose a trade secret[1879]. The recent reform added limited additional grounds for refusal[1880], e.g., where disclosure would be likely to pose a serious threat to the life or health of an individual[1881], or to public health or public safety; or would create a significant likelihood of serious harassment of an individual[1882]. The Privacy Act 2020 also introduced the possibility to, instead of refusing access, impose conditions relating to the use and/or disclosure of the information by the applicant, where one of the exceptions laid down in the Act applies[1883]. Moreover, it provided the OPC with the power to issue a binding written notice directing agencies to grant individuals access to their personal information (see below).

Under NZ law, individuals can obtain erasure of their data in different circumstances, although not expressly formulated as a separated right under Privacy Act 2020. In particular, exercising the right of correction may lead to deletion[1884], i.e., where this is necessary to ensure that the information is accurate, up to date, complete and not misleading. In addition, agencies have to delete personal information that was collected unlawfully or can no longer be lawfully used (e.g., where the purpose has been obtained)[1885]. In those situations, individuals can obtain deletion before the OPC or the Human Rights Review Tribunal[1886] (HRRT, which may order deletion as one of the possible remedies, see below). Several cases handled by the OPC and the Tribunal demonstrate that erasure may for instance be obtained where information was collected without being necessary for a lawful purpose or by means that intruded to an unreasonable extent on the personal affairs of an individual (in violation of

[1877] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[1878] Case law, as well as guidance and decisions of the OPC clarify the scope of the different exceptions, including by means of concrete examples, and confirm that the exceptions may not be applied in a blanket manner, but that each piece of information must be assessed individually to determine whether a specific exception applies (see e.g., https://www.privacy.org.nz/tools/knowledge-base/view/520?t=218847_301679 and Kelsey v Minister of Trade [2016] 2 NZLR 218 (HC)). See https://www.privacy.org.nz/privacy-act-2020/privacy-principles/6/, including the guidance and cases cited there for each of the exceptions. For example, the 'likely to prejudice' test requires a "distinct or significant possibility, a serious or real or substantial risk that the prejudice might eventuate" (Commissioner of Police v Ombudsman [1988] 1 NZLR 385 (CA), whereas the test of 'significant likelihood' refers to a very likely outcome of releasing the information (https://www.privacy.org.nz/privacy-act-2020/privacy-principles/6/harassment/#_ftn2). Moreover, invoking certain exceptions (e.g., the protection of other individuals) requires a balancing of the different interests involved (https://www.privacy.org.nz/privacy-act-2020/privacy-principles/6/unwarranted-disclosure-of-another-persons-affairs/).

[1879] Sections 49-53 Privacy Act 2020.

[1880] Section 49(1)(a) Privacy Act 2020.

[1881] To rely on this exception, there must be some evidence to indicate that the threat in fact exists and the importance of protecting the health and safety of the person outweighs the benefits of providing access, see https://www.privacy.org.nz/privacy-act-2020/privacy-principles/6/serious-threat-to-life-health-or-safety/.

[1882] Harassment is repeated, unwanted contact in ways that fall short of posing physical danger but that seriously detracts from the quality of life (https://www.privacy.org.nz/privacy-act-2020/privacy-principles/6/harassment/).

[1883] Section 54 Privacy Act 2020.

[1884] See the definition of correction in Section 7(1) Privacy Act 2020.

[1885] IPP 9.

[1886] The Human Rights Review Tribunal is a specialised, easily accessible court that mainly deals with claims concerning human rights (including privacy) violations.

IPP 1 and 4)[1887], upon request of an individual to erase incorrect or misleading information[1888], and where information is disclosed unlawfully[1889]. Moreover, on the basis of the Harmful Digital Communications Act 2015, an individual that has suffered or will suffer serious emotional distress as a result of a digital communication[1890] may apply to a court that may order the deletion of such material[1891].

Finally, the rules on international transfers have been significantly strengthened since the adoption of the adequacy decision. The previous regime – by which the OPC could prohibit transfers to third countries if the personal information was received from another third country in certain situations[1892] – remains in place but has been complemented by a comprehensive set of rules that agencies have to comply with in order to disclose personal information outside New Zealand[1893]. First, such a transfer may only take place if the concerned individual authorises[1894] the transfer (after having been expressly informed that the recipient may not be required to protect the information in a way that provides comparable safeguards to the Privacy Act 2020). Alternatively, a transfer may take place if the transferring agency believes on reasonable grounds[1895] that (1) the recipient is subject to the Privacy Act 2020 (because it is carrying on business in New Zealand, see earlier); (2) the recipient is subject to privacy

[1887] Armfield v Naughton [2014] NZHRRT 48.
[1888] Case Note 9257 [1997] NZPrivCmr 4 (1 July 1997), case note 256329 [2016] NZ PrivCmr 1.
[1889] Hammond v NZCU Baywide [2015] NZHRRT 6 (2 March 2015), where the agency was also ordered to request all third parties to whom the information was disclosed to delete the information and seek written confirmation thereof.
[1890] This refers to any form of electronic communication, including text messages, writing, photographs, pictures, recordings, or other matters communicated electronically, (Section 4 Harmful Digital Communications Act).
[1891] Section 11 and 19(1)(a) Harmful Digital Communications Act.
[1892] I.e., where the information is likely to be transferred to a country where it will not be subject to a law providing comparable safeguards to the Privacy Act 2020 and the transfer would likely lead to a contravention of the basic principles of the national application of the Guidelines of the Organisation for Economic Cooperation and Development (as set out in Schedule 8 Privacy Act 2020, see Section 193 of the Act).
[1893] IPP 12, which applies when information is disclosed to other entities processing the information on their own behalf (i.e., 'controllers'). The sharing of personal information by a New Zealand agency with a third party for processing (i.e., a 'processor') on behalf of the first agency is not considered a disclosure within the meaning of the Privacy Act 2020. In particular, where an agency (including in a third country) holds personal information as an agent for another agency (e.g., for safe custody or processing) and does not use it for its own purposes, the information is considered to be held by the agency on whose behalf that information is held/processed (Section 11 Privacy Act 2020). Agencies therefore remain responsible for the activities of their processors (i.e., agents, service providers, etc.). For example, the New Zealand agency must do everything reasonably within its power to prevent unauthorised use or unauthorised disclosure of the information (IPP 5(b)). This may for example be achieved through a contract requiring a service provider to put in place sufficient security measures, or by providing appropriate training (see for example Case Note 2663 [1998] NZPrivCmr 6). In addition, individuals can exercise their rights with respect to the data that is held overseas vis-à-vis the New Zealand agency.
[1894] The notion of 'authorisation' requires positive, rather than passive consent by the individual. There must be a decision that conveys authority to the agency to undertake a particular action. In addition, an individual must understand what he/she is agreeing to, and the agency must believe on reasonable grounds that the individual has indeed provided authorisation. See e.g., Case Note 2976 [1996] NZPrivCmr 1, in which the OPC found that the failure by an individual to object to collection does not amount to authorisation, and Case Note 19740 [2002] NZPrivCmr 5 in which the OPC found that an individual does not implicitly authorise an agency to use his/her information because it has been given to the agency. See also https://www.privacy.org.nz/blog/click-to-consent-not-good-enough-anymore/.
[1895] The test of « reasonable belief » in the Privacy Act 2020 has a subjective and objective component. In particular, the agency must believe that the relevant exception applies (subjective) and there must be a reasonable basis for that belief (objective), see also Deeming v. Whangarei District Council (Discovery) (WDC) [2015] NZHRRT 37, at 201-203. The burden of proof lies with the agency that relied on a specific exception.

laws that, overall, provide comparable safeguards to those in New Zealand[1896]; (3) the recipient is a participant in a "prescribed binding scheme" or is located in a "prescribed country"[1897]; or (4) the recipient is otherwise required to protect the information in a way that, overall, provides comparable safeguards to those in the Privacy Act 2020 (in particular because it entered into an agreement with the New Zealand agency). In practice, the OPC recommends that agencies rely on contractual instruments providing for comparable data protection safeguards in order to transfer personal information overseas[1898]. To assist agencies in developing such instruments, the OPC has developed model contract clauses, which share a number of similarities with the standard contractual clauses adopted by the European Commission (e.g., with respect to data protection principles, individual rights, onward transfers, and redress)[1899].

The abovementioned requirements do not apply in limited circumstances, i.e., if the information is disclosed to the concerned individual; if the source of the information is a publicly available publication[1900] and it would not be unfair or unreasonable to provide the information in the circumstances of the case; if the disclosure is necessary to enable New Zealand's intelligence agencies to perform their functions; if the disclosure is necessary on important public interest grounds (e.g., to avoid prejudice to the maintenance of the law by a public sector agency, for the conduct of legal proceedings) and it is not reasonably practicable in the circumstances to comply with the general transfer requirements; or if the disclosure is necessary to prevent or lessen a serious threat to public health/safety or the life or health of an individual and it is not reasonably practicable in the circumstances to comply with the general transfer requirements [1901].

1.2. Oversight, enforcement and redress

The OPC is the independent authority in charge of the oversight and enforcement of the New Zealand data protection rules[1902]. Its tasks include engaging in awareness activities,

[1896] According to OPC guidance, the following elements should be taken into account in assessing whether a country's privacy laws offer comparable protections to the Privacy Act 2020: the scope of the privacy laws, the protections around personal information, rights of access and correction for individuals, accessibility and meaningfulness of their complaint processes, and independence of oversight and enforcement (see e.g., https://privacy.org.nz/responsibilities/your-obligations/disclosing-personal-information-outside-new-zealand/decision-tree-page/).

[1897] The Privacy Act 2020 provides the New Zealand government with the power to, after consulting the OPC, adopt regulations "prescribing" a binding scheme (i.e., an internationally recognised scheme in which the participants agree to be bound by specified measures to protect personal information and mechanisms to enforce compliance with those measures, see Section 7(1) Privacy Act 2020) or country, on which agencies could rely to transfer personal information. Such regulations may only be adopted if the government is satisfied that personal information will be protected in a way that provides comparable safeguards to the Privacy Act 2020 under the binding scheme or the country's privacy laws (Section 213 and 214 Privacy Act 2020). So far, the government has not made use of these powers.

[1898] https://privacy.org.nz/responsibilities/your-obligations/disclosing-personal-information-outside-new-zealand/.

[1899] See the model contract clauses for cross border transfer of personal information, available at: https://www.privacy.org.nz/responsibilities/your-obligations/disclosing-personal-information-outside-new-zealand/.

[1900] This refers to a publication (including a register, list or roll of data) in printed or electronic form that is, or will be, generally available to members of the public (see the definition in Section 7(1) Privacy Act 2020).

[1901] IPP 12(1) and (2) in conjunction with IPP 11(b), (d), I, (f) and (g).

[1902] The OPC is headed by the Privacy Commissioner, an Independent Crown Entity, appointed by the Governor-General on the recommendation of the Minister of Justice for a renewable term of 5 years (Section 13 Privacy Act 2020, in conjunction with Section 28(1)(b) and 32(1)(b) Crown Entities Act). Certain individuals, such as

conducting audits of agencies upon their request, carrying (general) inquiries, undertaking research, examining and advising on proposed legislation, etc.[1903].

In terms of powers, the OPC may carry out general inquiries into any matter (including any practice or procedure) if it appears that the privacy of individuals is being, or may be infringed[1904]; conduct an audit to ascertain whether personal information is handled in accordance with the IPPs, upon request of an agency[1905]; and initiate investigations (on the basis of a complaint or on its own initiative) concerning an interference with the privacy of an individual[1906]. In carrying out inquiries or investigations, the OPC has access to all relevant information[1907]. In principle, the OPC aims at reaching a settlement between the parties (in case the investigation was initiated on the basis of a complaint) or obtaining a satisfactory assurance against the repetition of the action that was investigated[1908]. Where the OPC is unable to secure a settlement or assurance, or an agency has acted against a previously reached settlement or provided assurance, it may refer the matter to the Director of Human Rights Proceedings[1909]. The Director (or the individual themselves) may in turn initiate proceedings before the HRRT[1910], which may grant appropriate remedies (e.g., a declaration that an action is an interference with privacy, a corrective order, damages, or other relief[1911]).

The Privacy Act 2020 significantly strengthened the powers of the OPC, by introducing the possibility to (1) adopt binding "access directions", i.e., decisions with respect to individuals' requests for access to their personal information ordering agencies to provide individuals with access in any manner the OPC considers appropriate[1912]; and (2) issue binding compliance notices if a breach of the Act (or a code of practice) has occurred, requiring the concerned agency to remedy the breach (including by identifying the specific steps the OPC considers needed)[1913]. The OPC can enforce a compliance notice before the HRRT if there is reason to

---

members of parliament or of local authorities cannot be appointed (Section 30(2) Crown Entities Act and Section 15(1) Privacy Act 2020). The Commissioner may only be removed for just cause (which includes misconduct, inability to perform the functions of office and neglect of duty) by the Governor-General, on the advice of the responsible Minister and after consultation with the Attorney-General (Section 39 and 40 Crown Entities Act). The Privacy Act 2020 (Section 20) expressly provides that the Commissioner has the duty to act independently in performing statutory duties and powers.

[1903] Section 17 Privacy Act 2020.

[1904] Section 17(1)(i), in conjunction with Section 203 Privacy Act 2020.

[1905] Section 17(1)(l) Privacy Act 2020.

[1906] Section 79 Privacy Act 2020. An action is an interference with privacy if (1) an agency has made a decision without proper basis with respect to the individual's request for access or correction (e.g., refusing to grant access); or (2) there has been a breach of an IPP or the requirements for notifying data breaches to individuals that has caused (or may cause) loss, detriment, damage or injury to an individual; has adversely affected, or may adversely affect, the rights, benefits, privileges, obligations, or interests of that individual; or has resulted in, or may result in, significant humiliation, loss of dignity or injury to the feelings of that individual (Section 69(2) Privacy Act 2020). See also https://privacy.org.nz/tools/knowledge-base/view/211.

[1907] See Sections 86-90, in conjunction with sections 202 and 203 Privacy Act 2020.

[1908] Section 77, 83, 91(3)-(4) and 94(2)-(3) Privacy Act 2020.

[1909] Section 78, 91(5)(b) and 94(4)(a) Privacy Act 2020. In addition, the Commissioner may report significant breaches of duty or misconduct to the competent authorities (Section 96 Privacy Act 2020). The Director is an independent institution that assists individuals in bringing their case before the HRRT, or represents individuals before the Tribunal, on referral by OPC.

[1910] Section 97 Privacy Act 2020.

[1911] Section 102 Privacy Act 2020.

[1912] Section 92 Privacy Act 2020.

[1913] Section 123 and 126 Privacy Act 2020. In deciding whether to issue a compliance notice, the OPC may take different factors into account, e.g., whether there is another means for dealing with the breach, the seriousness of the breach and likelihood of a repeat, and the number of affected individuals (Section 124 Privacy Act 2020).

believe that the agency has not remedied or will not remedy the violation, or the agency fails to report timely on the steps taken to remedy the violation[1914]. The Tribunal may order that the agency comply with the notice or perform any act specified in the order[1915]. Failure to comply with an order of the Tribunal constitutes an offence and may be subject to a fine. Fines are imposed by the District Court, which takes a number of factors into account in determining the level of the fine and may not exceed 10 000 NZD for each charge[1916]. The OPC may also publish information on compliance notices, including the identity of agencies to whom they have been issued, if it considers it in the public interest to do so[1917].

As regards the possibility for individuals to obtain redress, different avenues continue to be available in the New Zealand system. In particular, individuals may turn directly to agencies[1918], file a complaint with the OPC[1919] and obtain judicial redress (against agencies[1920] or against the findings of the OPC[1921]), which may lead to different types of remedies, including injunctive relief and compensation for damages[1922].

Its annual reports show that the OPC deals with a number of investigations and complaints on an annual basis. For example, between June 2018 – June 2019, the OPC closed 894 investigation files and referred two cases to the HRRT (while 23 individuals turned to the HRRT themselves), and between June 2019 – June 2020, the OPC closed 769 investigation files and referred three cases to the HRRT (23 individuals turned to the HRRT

[1914] Section 130(1) Privacy Act 2020.
[1915] Section 133(1) Privacy Act 2020.
[1916] Section 133(3) Privacy Act 2020. See also the Sentencing Act 2002 (Sections 7-9, 13-14, 40-41), according to which the court must inter alia take into account the gravity and seriousness of the offence, the deterrent effect of the fine, and possible aggravating (e.g., the vulnerability of the victim) and mitigating factors, when deciding on the level of the fine.
[1917] Section 129 Privacy Act 2020.
[1918] See e.g., Section 74(1)(a) Privacy Act 2020.
[1919] Section 70 Privacy Act 2020. A complaint may be filed by or on behalf of one or more individuals (Section 71 Privacy Act 2020).
[1920] Individuals may initiate proceedings against an agency before the HRRT in different situations, e.g., if the OPC decides not to investigate a complaint after using endeavours to settle it, investigates but does not take a decision on a complaint or does not refer it to the HRRT, or if the Director of Human Rights Proceedings decides not to launch proceedings before the HRRT (Section 98 Privacy Act 2020). Decisions of the HRRT may be appealed to the higher courts, see Section 111 Privacy Act 2020, in conjunction with Section 123-124 of the Human Rights Act 1993. The right of access can directly be enforced against public authorities before the ordinary courts (Section 31(2) Privacy Act 2020).
[1921] For example, individuals may challenge an access direction before the HRRT (Section 105 Privacy Act 2020). More generally, individuals may obtain judicial review of decisions of the OPC before the ordinary courts pursuant to the Judicial Review Procedure Act 2016, see also Mitchell v Privacy Commissioner [2017] NZAR 1706; Henderson v Privacy Commissioner [2010] NZHC 554. A court may overturn a decision on the basis that it is considered to be unlawful, irrational, unreasonable or unfair, depending on the circumstances.
[1922] With respect to complaints handled by the OPC, see earlier on access directions and compliance notices. As regards proceedings before the HRRT, the Tribunal may order a variety of remedies, including an order restraining the agency from continuing or repeating the violation, an order that the agency remedies the violation, damages and any other relief it considers appropriate (Section 102 Privacy Act 2020). In terms of damages, the HRRT may award compensation in respect of pecuniary loss, loss of any benefit (whether or not of a monetary kind), as well as humiliation, loss of dignity and injury to the feelings of the aggrieved individual (Section 103 Privacy Act 2020). Compensation for damages can also be obtained before the ordinary courts under the tort of invasion of privacy (which relies on two elements: the existence of facts in respect of which there was a reasonable expectation of privacy, and publicity given to those facts that would be considered highly offensive to an objective reasonable person, see e.g., Hosking v Runting [2005] 1 NZLR 1 (CA)) or intrusion upon seclusion (for which an plaintiff must show an intentional or unauthorised intrusion; into seclusion (namely intimate personal activity, space or affairs), involving infringement of a reasonable expectation of privacy that is highly offensive to a reasonable person, see e.g., C v Holland [2012] NZHC 2155, [2012] 3 NZLR 672).

themselves)[1923]. This for instance includes an inquiry into the unlawful sharing of data between credit companies[1924] and investigations into the unlawful disclosure of data to the police by a bank[1925] and the use of inaccurate debt records[1926]. In the same reporting periods, the OPC received a total of 427 voluntary notifications on data breaches. In addition, the OPC conducted several general inquiries, e.g., into the police's conduct relating to the photographing of members of the public, the use and disclosure of COVID-19 patient information by the Ministry of Health, and Trade Me's (New Zealand's largest online auction website) privacy policy and compliance with the Privacy Act 1993[1927].

According to the first annual report after the entry into force of the Privacy Act 2020, the OPC received 531 complaints (and closed 580 complaints) during June 2020 – June 2021, and received 544 data breach notifications (which have become mandatory after the reform)[1928]. In September 2021, the OPC issued its first compliance notice, addressed to the Reserve Bank in relation to its response to a cyber-attack[1929]. The notice was closed in September 2022, after the Reserve Bank introduced all the improvements requested by the OPC[1930].

The OPC has also issued guidance on various topics, including on health data, biometric data, privacy impact assessments, the use of data and analytics by government agencies, contact tracing and individual rights[1931]. Moreover, it developed several tools to assist agencies with training and compliance efforts (e.g., e-learning tools[1932], a privacy statement generator[1933] and a platform to report data breaches[1934]), as well as to help individuals with exercising their rights (e.g., through a dedicated online tool by which the right of access can be exercised)[1935].

Finally, the OPC regularly engages with stakeholders, through campaigns regional visits, presentations, livestreams (so-called PrivacyLive events), responding to public inquiries (including through a call centre) and podcasts[1936]. The OPC also advised the government and parliament on the protection of personal data in relation to bills and legislative reforms (including through public submissions), e.g., in the context of the response to the COVID-19

[1923] See the 2019 annual report (available at: https://www.privacy.org.nz/assets/New-order/Resources-/Publications/Corporate-reports/Privacy-Commissioner.pdf) and 2020 annual report (available at: https://www.privacy.org.nz/assets/New-order/Resources-/Publications/Corporate-reports/Privacy-Commissioner-Annual-Report-20.pdf).

[1924] Available at: 2020-09-11-illion-Inquiry-Report.pdf (privacy.org.nz).

[1925] Available at: https://privacy.org.nz/publications/statements-media-releases/privacy-commissioner-welcomes-westpac-privacy-breach-settlement/.

[1926] Available at: https://privacy.org.nz/publications/case-notes-and-court-decisions/case-note-312145/.

[1927] Available at: https://www.privacy.org.nz/publications/commissioner-inquiries/.

[1928] Available at: https://www.privacy.org.nz/assets/New-order/Resources-/Publications/Corporate-reports/Annual-Report-2021.pdf.

[1929] Available at: https://www.privacy.org.nz/publications/statements-media-releases/compliance-notice-issued-to-reserve-bank-of-new-zealand-following-cyber-attack/.

[1930] Available at: https://www.privacy.org.nz/publications/statements-media-releases/first-privacy-act-compliance-notice-successfully-closed/.

[1931] Available at: https://www.privacy.org.nz/publications/guidance-resources/.

[1932] See e.g., on reporting privacy breaches, health data, employment and privacy, etc., see https://www.privacy.org.nz/tools/online-privacy-training-free/.

[1933] Available at: https://www.privacy.org.nz/tools/privacy-statement-generator/.

[1934] Available at: https://www.privacy.org.nz/responsibilities/privacy-breaches/notify-us/.

[1935] Available at: https://www.privacy.org.nz/tools/aboutme-request-my-info-tool/.

[1936] See e.g., the annual reports of 2019, 2020 and 2021. For example, the OPC gave 112 presentations in 2019, 89 in 2020 151 in 2021; and handled 7947 public inquiries in 2019, 7734 in 2020 and 9165 in 2021. In 2020, the OPC launched a broad public campaign – "Privacy is Precious" – targeted specifically at certain groups, including small business and non-profit organisations (see the annual report 2021, p. 21.

pandemic, the use of DNA in criminal investigations, counterterrorism and tax administration[1937].

2. ACCESS TO AND USE OF PERSONAL DATA TRANSFERRED FROM THE EUROPEAN UNION BY PUBLIC AUTHORITIES IN NEW ZEALAND

2.1. General legal framework

The limitations and safeguards that apply to the collection and subsequent use of personal data by New Zealand public authorities for criminal law enforcement and national security purposes follow from the overarching constitutional framework, specific laws regulating data access, as well as the rules that apply to the processing of personal data.

New Zealand does not have a single written constitution, but a number of statutes are of particular constitutional importance. These statutes set out principles relating to fundamental rights and freedoms that must be taken into account when developing or proposing new legislation. These include the Bill of Rights Act 1990, the Human Rights Act 1993 and the Privacy Act 2020, which are relevant for the protection of personal data.

Section 21 of the New Zealand Bill of Rights Act of 1990 guarantees the right to be secure against unreasonable search or seizure, whether of the person, property, correspondence or otherwise. This right may be subject "only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society"[1938]. The New Zealand Supreme Court has held that Section 21 protects against unjustified intrusions on an individual's "reasonable expectation of privacy"[1939], which is directed at protecting "a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination by the state"[1940]. It applies to information that "tends to reveal intimate details of the lifestyle and personal choices of the individual"[1941].

To comply with the Bill of Rights Act, any search or seizure must be reasonable. In this regard, the Supreme Court of New Zealand has clarified that a search or seizure can be unreasonable either because it occurred at all or because of the unreasonable manner in which it is carried out[1942]. In particular, to determine whether a search is unreasonable, "it is necessary to look at the nature of the place or object which was being searched, the degree of intrusiveness into the privacy of the person or persons affected and the reason why the search

[1937] See https://www.privacy.org.nz/publications/reports-to-parliament-and-government/. With respect to data use and analytics by public authorities, see https://www.privacy.org.nz/news-and-publications/guidance-resources/principles-for-the-safe-and-effective-use-of-data-and-analytics-guidance/.
[1938] Section 5 of the Bill of Rights Act.
[1939] R v Alsford [2017] 1 NZLR 170. To determine whether there is a reasonable expectation of privacy, both subjective and objective elements should be taken into account: firstly, whether the individual had a subjective expectation of privacy in the circumstances (the subjective element); and, if so, whether that expectation is one that society is prepared to recognise as reasonable (the objective element), see Hamed v R [2011] NZSC 101 at [163]-[164].
[1940] R v Alsford [2017] NZSC 42 at [63].
[1941] R v Alsford [2017] 1 NZLR 170 at [56]. For example, whereas individuals generally do not have a reasonable expectation of privacy in basic electricity consumption data, there could be situations where electricity data could reveal intimate details about an individual (e.g., from smart meters), in which case a reasonable expectation of privacy may arise (R v Alsford [2017] 1 NZLR 170).
[1942] Hamed v R [2011] NZSC 101, Blanchard J, at [172].

was occurring"[1943]. This requires considering factors such as the nature of the information at issue, the nature of the relationships between the parties, the place where the information was obtained and the manner in which it was obtained[1944].

As described in more detail in sections 2.2.1 and 2.3.1, the general principles following from the Bill of Rights Act are reflected in specific laws that regulate the powers of law enforcement and national security authorities.

Moreover, the processing of personal information by New Zealand public authorities (including criminal law enforcement and national security authorities) is subject to the Privacy Act 2020. The Privacy Act 2020 lays down the conditions under which public authorities may use and disclose personal information; reflects the principles of purpose limitation, data accuracy, transparency and storage limitation; and provides individuals with a right to obtain access to or correction of their personal data (see section 1.1).

With respect to the activities of criminal law enforcement authorities, the Privacy Act 2020 applies in its entirety. In addition, following a reform that entered into force with the Intelligence and Security Act 2017, intelligence and security agencies are subject to the majority of the IPPs, including the Principles governing the use and disclosure of information (IPP 10 and 11), security (IPP 5), purpose limitation, data accuracy and limited data retention (IPP 1, 8 and 9) as well as the Principles providing for individual rights (IPP 6 and 7)[1945]. The only principles that do not apply to personal information collected by intelligence and security agencies are IPP 2 (i.e., the general requirement to collect information directly from the individual), IPP 3 (concerning transparency) and IPP 4(b)[1946] (concerning the manner of collection)[1947].

The general limitations and safeguards described in this section can be invoked by individuals before independent administrative bodies (e.g., the Independent Police Conduct Authority), the OPC and courts to obtain redress (see sections 2.2.4 and 2.3.4).

2.2. Access and use by New Zealand public authorities for criminal law enforcement purposes

New Zealand law imposes a number of limitations on the access and use of personal data for criminal law enforcement purposes and provides oversight and redress mechanisms. The conditions under which such access can take place and the safeguards applicable to the use of those powers are described in the following sections.

2.2.1. Legal bases and applicable limitations/safeguards

[1943] Hamed v R [2011] NZSC 101, Blanchard J, at [172].
[1944] R v Alsford [2017] 1 NZLR 170 at [63]. For example, contractual terms and conditions with customers may be relevant to whether there is a reasonable expectation of privacy, but these are not necessarily determinative (R v Alsford [2017] 1 NZLR 170 at [68]). Similarly, while in urgent circumstances a search by a voluntary request may be reasonable, a search may be unreasonable if there is time to obtain a production order or search warrant (R v Alsford [2017] 1 NZLR 170 at [64]).
[1945] Prior to this reform, intelligence agencies were largely exempt from the IPPs (since only the IPPs regarding individual's rights of access and correction applied).
[1946] However, IPP 4(a), according to which a collection must take pace by lawful means, still applies.
[1947] Section 28 Privacy Act 2020.

Personal data transferred under the adequacy decision and processed by New Zealand agencies may be obtained by criminal law enforcement authorities by means of investigative measures under the Search and Surveillance Act, on the basis of anti-money laundering and anti-terrorist financing legislation or through voluntary disclosures[1948].

The Search and Surveillance Act 2012 empowers law enforcement authorities to obtain evidential material (i.e., evidence of the offence, or any other item, tangible or intangible, of relevance to the investigation of the offence[1949]) in relation to an offence or a suspected offence through searches, production orders and surveillance device warrants. The information that may be collected can take different forms, such as phone call recordings, financial records and e-mails. The Act generally applies to the Police, but also governs certain activities of other law enforcement authorities, such as animal welfare inspectors, fisheries inspectors, product safety officers, food officers, forestry officers, gambling inspectors, immigration officers, etc.[1950].

The Search and Surveillance Act lays down clear and precise rules on the scope and application of these measures, thereby ensuring that the interference with the rights of individuals will be limited to what is necessary for a specific criminal investigation and proportionate to the pursued purpose. As explained in more detail below, prior judicial authorisation is in principle required in order to access personal information on the basis of the Search and Surveillance Act. It is only in exceptional cases that law enforcement authorities do not have to obtain a judicial warrant. These exceptions are specifically set out

[1948] In addition, the Privacy Act 2020 authorises certain specified public authorities to obtain personal information held by other specified public authorities. First, it allows one authority (the accessing agency) to verify the identity of an individual by obtaining information about that individual from another authority (holder agency), Part 7, Subpart 2 of the Privacy Act 2020. The information that can be accessed on this basis is 'identity information', which inter alia includes biographical details, biometric data, and photographs (Section 164 Privacy Act 2020). Schedule 3 of the Privacy Act 2020 lists, for each accessing agency, the purpose for which they may access the information and the holder agency from which they may request it. This list can only be amended by Order in Council following consultation by the Minister of Justice with the OPC. Before recommending an amendment, the responsible Minister must be satisfied that (1) the purpose for which the identity information is to be accessed relates to a specified function of the accessing agency and (2) the identity information to be accessed is no more than reasonably necessary to enable the accessing agency to achieve that purpose. (Section 168 Privacy Act 2020). Second, the Act authorises certain public authorities to access specified information held by other public authorities for law enforcement purposes (Part 7, Subpart 3 Privacy Act 2020). The authorities that may rely on these provisions are listed in Schedule 4 of the Privacy Act 2020 (e.g., the Ministry of Justice, the Serious Fraud Office, the Police, etc.). Only 'law enforcement information' (e.g., details of hearings, court document processing, offender identity, etc.) can be accessed on this basis (Section 171 Privacy Act 2020). For each type of law enforcement information, the public authority authorised to request access is specifically listed. The list can only be amended by Order in Council following consultation by the Minister of Justice with the OPC (Section 173 Privacy Act 2020). Thirdly, the Privacy Act 2020 provides for public authorities to obtain personal information for public service purposes under approved information sharing agreements (Part 7, subpart 1 Privacy Act 2020), as described in more detail in section 1.1.

[1949] Section 3 Search and Surveillance Act. The Search and Surveillance Act also foresees the possibility for law enforcement authorities to obtain a declaratory order, i.e., a statement by a judge that he/she is satisfied that the use of a device, technique or procedure, or the carrying out of an activity is, in the circumstances of the case, reasonable and lawful (Section 65 Search and Surveillance Act). Such an order is advisory in nature and does not affect the jurisdiction of any court to examine the lawfulness and reasonableness of the underlying activity. Authorities may apply for a declaratory order if (1) they wish to use a device, technique or procedure, or carry out an activity that is not specifically authorised by another statutory regime, and (2) the use of that device, technique or procedure, or the carrying out of the activity, may constitute an intrusion into the reasonable expectation of privacy of any person (Section 66 Search and Surveillance Act). A declaratory order must inter alia contain a description of the device, technique, procedure or activity, as well as details on the person, place, vehicle or other thing that will be subjected to the proposed activity.

[1950] Schedule to the Search and Surveillance Act.

in the Act. At the same time, even in those exceptional cases, case law has clarified that a warrant is to be preferred if it is possible to obtain one without prejudicing the purpose of the search[1951].

Searches or seizures to access a place, vehicle or other things (e.g., a computer or remote server) may only take place if (1) there are reasonable grounds to suspect that an offence punishable by imprisonment has been committed, is being committed or will be committed and (2) there are reasonable grounds to believe that the search will find evidential material in respect of the offence[1952]. In principle, a search warrant must be obtained from a court, which must specify the target, the period during which it may be used and the conditions for the search/seizure[1953]. Searches or seizures may be carried out without a warrant only under specific conditions set out by law, e.g., when effecting arrest[1954], in urgent circumstances[1955], in relation to certain serious offences (e.g., a terrorist act) if the evidential material would be destroyed, concealed, altered or damaged if the search would be delayed to obtain a warrant[1956]. In this case, a written report must be provided to the Commissioner of the Police as soon as practicable,[1957] with a summary of the circumstances surrounding the exercise of the power and the reasons why it was exercised, together with an explanation whether evidential material was obtained and whether criminal proceedings have been brought or are being considered[1958]. The Commissioner of the Police must in turn report on the use of warrantless powers in its public annual report[1959].

In case of a seizure (regardless of whether it took place on the basis of a warrant or not), the concerned individual must be provided with written notice and a copy of the warrant/legal authority at the time of the seizure or as soon as practicable afterwards, but no later than seven days[1960]. Notification of the individual may be deferred after applying to a judge for a postponement on the grounds that notification would endanger the safety of any person or

[1951] Hall v R [2018] NZCA 279, [2019] 2 NZLR 325; Moore v R [2022] NZCA 109 and Swain v R [2015] NZCA 216.
[1952] Section 6 Search and Surveillance Act. As regards the standards of 'reasonable grounds to believe' and 'reasonable grounds to suspect', case law has clarified that 'belief' means that "there has to be an objective and credible basis for thinking that a search will turn up the item(s) named in the warrant", whereas 'suspicion' means that "it is likely that a situation exists" ("the issuing officer must hold the view that the state of affairs the applicant officer is suggesting actually exists"), See R v Williams at [213].
[1953] Sections 3(1) and 6, in conjunction with Section 102-108 Search and Surveillance Act. The application for a search warrant itself must contain inter alia the grounds on which the application is made; a description of the place, vehicle or thing to be searched; a description of the information believed to be there; and the period for which the warrant is sought (Section 98 Search and Surveillance Act). Copies of the application for a warrant and/or the search warrant itself must be kept by the competent court and the applicant (Section 101 Search and Surveillance Act). After a search has been carried out, the court may require a report detailing, inter alia, whether the search warrant was executed, whether it resulted in the seizure of evidential material (and if so, whether that material was specified in the warrant) and whether any criminal proceedings were brought that relate to the seized material (Section 104 Search and Surveillance Act).
[1954] Section 7 and 8 Search and Surveillance Act.
[1955] I.e., if an offence is being committed or is about to be committed that would likely cause injury to any person or serious damage to any property, or there is risk to the life or safety of a person that requires an emergency response (Section 14 Search and Surveillance Act).
[1956] 15 - Search and Surveillance Act.
[1957] Section 169(1) and (2) Search and Surveillance Act.
[1958] Section 169(3) Search and Surveillance Act.
[1959] Section 170 Search and Surveillance Act.
[1960] Section 133 Search and Surveillance Act.

prejudice ongoing investigations[1961]. The postponement may not exceed 12 months and may be repeated only once, again for a maximum of 12 months[1962].

Specific limitations and safeguards apply to carrying out surveillance, i.e., to intercept private communications, use a tracking device, observe and record private activities, or use a surveillance device, which may in principle only take place on the basis of a judicial 'surveillance device warrant'[1963]. Moreover, trespass surveillance[1964] (other than by means of a tracking device) and interception devices (to intercept private communications)[1965] may only be deployed to obtain information in relation to offences punishable by a term of imprisonment of seven years or more, certain offences covered by the Arms Act of 1983 and certain offences laid down in the Psychoactive Substances Act of 2013[1966]. A surveillance device warrant may only be issued if there are reasonable grounds to suspect that an offence has been/is being/will be committed and there are reasonable grounds to believe that the proposed use of the surveillance device will obtain evidence in respect of the offence[1967].

Once the search has been carried out, the Search and Surveillance Act provides additional safeguards in the form of specific reporting and transparency requirements. Within one month after the expiry of the period specified in the warrant, the person carrying out the surveillance must report to the judge that issued the warrant[1968]. The report must specify whether the surveillance resulted in obtaining evidence, whether or not this evidence was specified in the warrant, the circumstances in which the surveillance was carried out, and whether criminal proceedings have been brought as a result[1969]. Upon receipt of the report, the issuing judge may give directions as to the destruction or retention of the obtained material, report to the chief executive of the relevant agency about breaches of the issued warrant, or order that the subject of surveillance is notified[1970].

Warrantless surveillance activities are only allowed in exceptional situations, for example for recording what an enforcement officers observes when being lawfully in private premises, when recording an oral communication with the consent of at least one of the persons

[1961] Section 134(1) Search and Surveillance Act.
[1962] Section134(3) Search and Surveillance Act. A second postponement may not be granted unless the thing seized is a copy of information or is an unlawful item (e.g., narcotics), Section 135 Search and Surveillance Act.
[1963] Section 46 Search and Surveillance Act.
[1964] I.e., surveillance involving trespass to land or goods, see Section 3(1) Search and Surveillance Act.
[1965] An interception device is defined as any electronic, mechanical, electromagnetic, optical or electro optical instrument, apparatus, equipment or other device that is used or can be used to intercept or record a private communication (including telecommunications). It does not include a hearing aid or similar device. See Section 3(1) Search and Surveillance Act.
[1966] Section 45 Search and Surveillance Act
[1967] Section 51(a) Search and Surveillance Act. The application for a surveillance device warrant must set out the grounds on which the application is made, the suspected offence, the type of surveillance device to be used, the name and address of the object of the proposed surveillance, a description of the evidential material sought and the period for which the warrant is sought (Section 49(1) Search and Surveillance Act).
[1968] Section 59(1) Search and Surveillance Act.
[1969] Section 59(2) Search and Surveillance Act. Similar reporting requirements apply for warrantless surveillance, see Section 60 Search and Surveillance Act.
[1970] Section 61(1) Search and Surveillance Act. A judge may not notify the subject of surveillance unless the warrant should not have been issued/there was a serious breach of the law or the conditions of the warrant, and the public interest in notification outweighs a potential prejudice to any law enforcement investigation, the safety of informants, international relations of the law enforcement agency, etc (Section 61(2) and (3) Search and Surveillance Act).

involved, or in emergency situations[1971]. In emergency situations, a surveillance device may only be used if obtaining a warrant would be impracticable in the circumstances, for a period not exceeding 48 hours[1972]. The enforcement officer must have reasonable grounds to suspect that certain specific crimes described in the Act have been, are being or are about to be committed[1973] and that the use of a surveillance device is necessary to prevent it. Within one month, the enforcement officer must report to a judge whether the surveillance resulted in obtaining evidence of the relevant offense, preventing the offense from being committed or averting the emergency, as well as the circumstances in which the device was used[1974]. A judge receiving such a report may give directions as to the destruction or retention of the obtained material, order that the individual is notified or report to the chief executive of the relevant agency if he/she considers that the use of the device was not lawful[1975].

Under the Search and Surveillance Act, a law enforcement authority may also obtain a production order to require another agency to produce documents, for instance financial records, call associated data and the content of communications that may be stored in the normal course of business[1976]. A production order may only be issued by a court if there are reasonable grounds to suspect that an offence has been committed, is being committed or will be committed and there are reasonable grounds to believe that the documents sought constitute evidential material in respect of the offense and are in the possession or under the control of the person against whom the order is sought (or will do so while the order is in force)[1977]. A production order must inter alia contain information on the grounds on which the order is made, the documents required to be given and the person to whom it is directed[1978]. Production orders are in force for a maximum of 30 days after the order is issued[1979].

In addition to disclosing information pursuant to coercive powers adopted under the Search and Surveillance Act, private operators may in certain circumstances provide information to public authorities on a voluntary basis to comply with an informal request. Depending on the nature of the information and whether there is a reasonable expectation of privacy in the specific circumstances of the case, requesting personal information by law enforcement authorities may constitute a 'search' within the meaning of Section 21 of the New Zealand Bill of Rights Act[1980], in which case a judicially authorised warrant is in principle required for the request to be lawful. When receiving information on the basis of voluntary requests,

[1971] See Section 47 and 48 Search and Surveillance Act. This is the case for example for recording what an enforcement officers observes when being lawfully in private premises, or when recording an oral communication with the consent of at least one of the persons involved. In addition, no warrant is required in certain emergency situations.
[1972] Section 48(1) Search and Surveillance Act.
[1973] I.e., crimes punishable by a term of imprisonment of at least 14 years, offences in relation to arms or against the Arms Act 1983, offences in relation to narcotics, where an offence would likely cause injury to any person or serious damage to or serious loss of a property (Section 48, in conjunction with Section 14(2), 18(2) and 81(2)(a) to (d) of the Search and Surveillance Act).
[1974] Section 60 Search and Surveillance Act.
[1975] Section 62 Search and Surveillance Act.
[1976] Section 70 Search and Surveillance Act.
[1977] Section 72 Search and Surveillance Act.
[1978] Section 73(2) Search and Surveillance Act. The application for a production order must set out, inter alia, the provision authorising an application for a search warrant, a description of the offence that is suspected of been committed, being committed or will be committed, the grounds for suspicion, and a description of the documents that are sought (Section 71 Search and Surveillance Act).
[1979] Section 76 Search and Surveillance Act.
[1980] R v Alsford [2017] NZSC 42.

criminal law enforcement authorities may only use or disclose it in accordance with the requirements described in section 2.2.2.

The conditions under which agencies are allowed to respond to informal requests are laid down in the Privacy Act 2020 and have been further clarified in guidance of the OPC[1981]. First, an agency may disclose personal information when it believes on reasonable grounds that it is necessary to avoid prejudice to the maintenance of the law, including the prevention, detection, investigation, prosecution and punishment of offences[1982]. As clarified by the OPC, this exception only covers situations where not providing the information would prejudice or be detrimental to enforcing the law, i.e., there must be a direct connection between the disclosure and the prejudice to the maintenance of the law that would otherwise arise[1983]. The OPC has also specified that the requesting law enforcement authority must provide sufficient information to allow an agency to form a view of whether there are indeed reasonable grounds to believe that the disclosure of information would be necessary. In particular, it must indicate a link between the offence being investigated and the relevance of the requested information. Moreover, when deciding whether or not to disclose, agencies must take the sensitivity or intimacy of the requested information into account. Second, an agency may disclose personal information when it believes on reasonable grounds that disclosure is necessary to prevent or lessen a serious threat to public health or public safety, or the life or health of the individual concerned or another individual[1984]. To determine whether a threat is "serious", an agency must take into account the likelihood of the threat being realised, the severity of the consequences if the threat is realised and the time at which the threat may be realised[1985]. The information may only be disclosed to an authority that will be able to do something to prevent or lessen the threat[1986].

Finally, criminal law enforcement authorities may also indirectly receive personal data from the Financial Intelligence Unit of the Commissioner of the Police[1987], to which certain New Zealand agencies (financial institutions, casinos, lawyers, conveyancers, accountants, real estate agents and the Racing Board) have to report financial transaction information. In particular, they must report on 'suspicious activities' (where there are reasonable grounds to suspect that a (proposed) transaction, (proposed) service or inquiry may be relevant to the investigation or prosecution of a money laundering offence or the enforcement of certain Acts, such as the Terrorism Suppression Act 2002 and the Proceeds of Crime Act 1991)[1988]

[1981] Available at: https://www.privacy.org.nz/assets/Files/Reports/October-2017-Final-Guidance-on-releasing-personal-information-to-Police-and-law-enforcement-agencies-Principle-11f-and-ei.pdf
[1982] IPP 11(e)(i).
[1983] Available at: https://www.privacy.org.nz/assets/Files/Reports/October-2017-Final-Guidance-on-releasing-personal-information-to-Police-and-law-enforcement-agencies-Principle-11f-and-ei.pdf.
[1984] IPP 11(f)(i).
[1985] Section 2 Privacy Act 2020.
[1986] Available at: https://www.privacy.org.nz/assets/Files/Reports/October-2017-Final-Guidance-on-releasing-personal-information-to-Police-and-law-enforcement-agencies-Principle-11f-and-ei.pdf.
[1987] The Financial Intelligence Unit was established to implement the international recommendations for combating money laundering and terrorist financing issued by the Financial Action Task Force.
[1988] Section 39A of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (AML/CFT Act). The information to be provided includes the date and time of transaction or service, the mode of transaction, the type of funds, the amount of the transaction, the name and contact details of the persons involved in the transaction, as well as the grounds on which the reporting entity holds the suspicion (See Schedule 1 of the Anti-Money Laundering and Countering Financing of Terrorism (Requirements and Compliance) Amendment Regulations 2017).

and ‘prescribed transactions’ (international wire transfers of at least 1 000 New Zealand dollars and domestic large cash transactions of at least 10 000 New Zealand dollars)[1989]. The Financial Intelligence Unit may in turn transmit information that indicates grounds for criminal investigation to the investigative branches of the New Zealand Police and other law enforcement authorities[1990]. Any information received and disclosed in this context must be processed in accordance with the Privacy Act 2020, see also below in section 2.2.2.

2.2.2. Further use of the information collected

The processing of personal data collected by New Zealand criminal law enforcement authorities is subject to all requirements of the Privacy Act 2020, including with respect to purpose limitation, lawfulness of use and provision to third parties, international transfers, proportionality/data minimisation and storage limitation (see section 1.1). In addition, more specific requirements follow from certain statutes.

For example, the Policing Act 2008 imposes specific conditions for the disclosure of personal information by the Police to overseas authorities with corresponding functions and for a corresponding purpose[1991]. Such a disclosure may only take place if it is reasonably necessary to enable the overseas authority to perform its policing function[1992]. Moreover, personal information may only be disclosed in accordance with an international disclosure instrument (such as an international agreement or agency-to-agency agreement that must be made publicly available) or on the basis of directions issued by the Police Commissioner and made publicly available[1993], which describe the circumstances in which personal information may be disclosed without a request from the corresponding overseas agency and set out any criteria for the disclosure[1994].

As regards raw surveillance data, the Search and Surveillance Act sets out a specific retention period, which generally lasts until the conclusion of criminal proceedings in relation to an offence in respect of which the data was collected, or for a maximum of three years if no criminal proceedings have commenced but the data is necessary for an ongoing investigation[1995]. Any information that may not be retained within this timeframe must be deleted[1996].

2.2.3. Oversight

The activities of New Zealand criminal law enforcement authorities are supervised by different bodies.

[1989] Section 5(1) of the AML/CTF Act. The reports must contain, inter alia, a description of the transaction, the amount of the transaction, the date on which it occurred and the parties of the transaction (Section 48B(1) of the AML/CFT Act).
[1990] Section 142(g) of the AML/CFT Act.
[1991] Section 95B(1) of the Policing Act.
[1992] Section 95B(2) of the Policing Act.
[1993] Section 95B(3) and 95E of the Policing Act. Before entering into agency-to-agency agreements, the Police Commissioner must consult the Privacy Commissioner, see Section 95D of the Policing Act.
[1994] Section 95C of the Policing Act.
[1995] Section 63(1) Search and Surveillance Act. This period may moreover be extended by judicial order, see para. 2 of the same Section.
[1996] Section 64 Search and Surveillance Act.

Within the public sector, the Government Chief Privacy Officer (GCPO) is the central entity for the management of personal information across the public sector. The GCPO is in charge with setting the vision for privacy in the public sector, developing guidance, capability building within public bodies, providing assurance to government and engagement with the Privacy Commissioner and other stakeholders[1997]. The GCPO has issued ten core expectations describing good practices for privacy management within the public sector, supported by a Privacy Maturity Assessment Framework to help agencies assess their own privacy capability and identify where and how they can make improvements[1998].

In addition, independent oversight is ensured through different bodies: the OPC oversees law enforcement agencies' compliance with the Privacy Act 2020, while the Independent Police Conduct Authority (IPCA) carries out general oversight of conduct, practices, policies and procedures of the New Zealand Police[1999]. The OPC and IPCA may also conduct joint reviews. For example, in 2022, the OPC and IPCA conducted a joint inquiry into the collection and use of photographs (biometric information) by the Police, which led to a number of recommendations and a compliance notice from the OPC[2000].

In carrying out its oversight of criminal law enforcement authorities, the OPC can make use of all of its powers provided under the Privacy Act 2020. This includes the possibility to conduct general inquiries, audits (upon request of the relevant authority) and investigations[2001] (on the basis of a complaint or on its own initiative)[2002] and to endeavour to secure a settlement or assurance, reach findings, make recommendations and/or determinations and issue binding access directions and compliance notices (that can be enforced before the HRRT), as described in more detail in section 1.2.

The IPCA[2003] may investigate Police conduct/policies/procedures on the basis of a complaint or on its own motion[2004]. After conducting an investigation, the IPCA forms an opinion on

---

[1997] See for example the guidance issued by the GCPO, which is available at: https://snapshot.ict.govt.nz/resources/digital-ict-archive/static/localhost_8000/guidance-and-resources/privacy/guidance-on-privacy-management-issued-by-the-government-chief-privacy-officer/index.html.

[1998] The Framework is available at; https://snapshot.ict.govt.nz/resources/digital-ict-archive/static/localhost_8000/assets/Guidance-and-Resources/Privacy-Framework-August-online.pdf.

[1999] Independent Police Conduct Authority Act 1988.

[2000] Available at: https://privacy.org.nz/publications/statements-media-releases/new-news-page-3/.

[2001] See e.g., the 2018 ex officio investigation where the OPC found that the police had unlawfully collected personal information at a checkpoint and recommended that the data would be deleted (https://privacy.org.nz/publications/statements-media-releases/operation-painter-findings-in-privacy-investigation/.).

[2002] The OPC in principle has access to all relevant information, with the exception that information may not be disclosed to the OPC where the Prime Minister certifies that the provision of the information might prejudice the security, defence or international relations of New Zealand; or the Attorney-General certifies that the provision of information might prejudice the prevention, investigation or detection of offences, or might involve the disclosure of proceedings of Cabinet relating to matters of a secret or confidential nature (and the disclosure would be injurious to the public interest), Section 88(3) Privacy Act 2020. However, this exceptional procedure has so far never been used.

[2003] The IPCA consists of up to five members appointed by the Governor-General on the recommendation of the House of Representatives and is chaired by a (retired) judge (Section 5 and 5A IPCA Act). It acts independently in performing its statutory functions and duties (Section 4AB IPCA Act). Members that are judges can only be removed under the general rules that apply to removals of judges from office or for a breach of collective duties of the Authority, only if all of the other members are being removed for the same breach at the same time (Section 6(1) IPCA Act and Section 42 of the Crown Entities Act 2004). Members that are not judges may only be removed for just cause by the Governor-General acting upon an address from the House of Representatives

whether or not any decision, recommendation, act, omission, conduct, policy, practice, or procedure which was the subject matter of the investigation was contrary to law, unreasonable, unjustified, unfair or undesirable[2005]. The IPCA may provide recommendations to the Commissioner of the Police, including a recommendation that disciplinary or criminal proceedings be considered or instituted[2006]. If no adequate and proportionate action is taken in response to its recommendations, the IPCA must send its opinion and recommendation to the Attorney-General and the Minister of Police and may provide the Attorney-General with a report to be presented to Parliament[2007].

2.2.4. Redress

The New Zealand system offers different avenues to obtain redress, including compensation for damages.

First, individuals have a right to obtain access to and correction of their data held by public authorities under the Privacy Act 2020 (IPP 6 and 7). In limited and specific circumstances, a law enforcement authority may refuse to grant access or correction[2008], in particular where the disclosure of the information would be likely to pose a serious threat to the life, health, or safety of any individual, or to public health or public safety; would be likely to prejudice the safe custody or the rehabilitation of the individual concerned; would be likely to prejudice the maintenance of the law, including the right to a fair trial and the prevention, investigation, and detection of offences; or would be likely to prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand[2009]. In those cases, a law enforcement authority may also provide a reply that neither confirms nor denies that it holds any personal information about the individual, if it is satisfied that the interest protected by one of the exceptions would likely to be prejudiced by confirming whether or not information is held about the individual[2010].

The restrictions to the right of access and correction foreseen by the Privacy Act 2020 cannot be invoked in a blanket manner (e.g., with respect to all information processed by the Police)[2011], but must always be applied on a case by case basis, to determine whether reasons

---

(Section 6(3) IPCA Act). Just cause includes misconduct, inability to perform the functions of office, neglect of duty and breach of any of the collective duties of the Authority or the individual duties of members (Section 40 of the Crown Entities Act).

[2004] Section 12(1)(a)-(b) IPCA Act.

[2005] Section 27(1) IPCA Act. The IPCA in principle has full access to all relevant information (Section 24 IPCA Act) unless the Attorney-General or Prime Minister produces a specific certification (which has so far never happened). The Attorney-General may certify that the provision of information might prejudice the prevention, investigation or detection of offence, or might involve the disclosure of proceedings of Cabinet relating to matters of a secret or confidential nature (and the disclosure would be injurious to the public interest), Section 26(1)(b) IPCA Act. Similarly, the Prime Minister may certify that the provision of the information might prejudice the security, defence or international relations of New Zealand (Section 26(1)(a) IPCA Act). In practice, these exceptions would only be relevant when there is a covert investigation and the early disclosure of information to the IPCA (and potentially other witnesses) might prejudice the successful conclusion of the operation.

[2006] Section 27 of the IPCA Act.

[2007] Section 29 IPCA Act.

[2008] Section 44(2)(c) Privacy Act 2020.

[2009] Sections 49-53 Privacy Act 2020.

[2010] Section 47 Privacy Act 2020.

[2011] DHRP v. Police [2007] HRRT 34/05, para. 52.

for refusing access outweigh the interests of the person seeking to have access[2012]. In particular, "due consideration must be given to the competing concerns, and in the end the outcome depends on the facts at work in the particular case"[2013]. Instead of refusing access, a public authority may also decide to grant access, but impose conditions regarding the use of the information or its disclosure to any other person[2014]. Moreover, a public authority may make documents available to the largest extent possible in redacted form, or make the requested information available in alternative ways, e.g., by giving the individual the opportunity to inspect the information[2015].

If a request to obtain access or correction to data is refused, any individual has the possibility to lodge a complaint with the OPC, who can take different measures, including binding "access directions" (i.e., decisions ordering agencies to provide individuals with access in any manner the OPC considers appropriate[2016]), which can be challenged before the HRRT (whose decisions can in turn be appealed before the High Court, with the Court of Appeal as a last resort)[2017]. Moreover, individuals can also enforce their right of access directly against public authorities before the ordinary courts[2018].

Second, any individual may lodge a complaint concerning an interference with privacy by a criminal law enforcement authority with the OPC, who can endeavour to secure a settlement or assurance, reach findings, make recommendations and/or determinations and issue a binding access direction or compliance notice (see section 1.2 and 2.2.4). The OPC has dealt with several complaints against criminal law enforcement authorities, which have in certain cases led to findings of violations of the Privacy Act, e.g., as regards the collection of information without a warrant[2019] and the unlawful disclosure of information by the Police[2020]. Individuals may obtain judicial review of decisions of the OPC before the ordinary courts pursuant to the Judicial Review Procedure Act 2016 (see also below)[2021]. A court may overturn a decision on the basis that it is considered to be unlawful, irrational, unreasonable or unfair, depending on the circumstances[2022]. Individuals may also initiate proceedings against a law enforcement authority before the HRRT in different situations, e.g., if the OPC decides not to investigate a complaint following unsuccessful settlement endeavours, does not take a decision on a complaint during or following an investigation or does not refer it to the HRRT, or if the Director of Human Rights Proceedings decides not to launch proceedings before the HRRT[2023]. The HRRT may order a variety of remedies, including an order restraining the agency from continuing or repeating the violation, an order that the agency remedies the

[2012] DHRP v. Police [2007] HRRT 34/05, para. 48.
[2013] DHRP v. Police [2007] HRRT 34/05, para. 55.
[2014] Section 54 Privacy Act 2020.
[2015] Section 55-56 Privacy Act 2020.
[2016] Section 92 Privacy Act 2020.
[2017] Section 105 Privacy Act 2020.
[2018] Section 31(2) Privacy Act 2020.
[2019] Available at: https://www.privacy.org.nz/publications/statements-media-releases/statement/.
[2020] Privacy Commissioner case note 209484 [2010].
[2021] See also Mitchell v Privacy Commissioner [2017] NZAR 1706; Henderson v Privacy Commissioner [2010] NZHC 554.
[2022] See Section 16 of the Judicial Review Procedure Act.
[2023] Section 98 Privacy Act 2020.

violation, damages and any other relief it considers appropriate[2024]. Decisions of the HRRT may be appealed to the higher courts[2025].

Third, any individual may lodge a complaint with the IPCA alleging any misconduct or neglect of duty by any Police employee, or concerning any practice, policy or procedure of the Policy affecting the person in a personal capacity[2026]. Upon receiving a complaint, the IPCA may investigate the complaint itself, refer the complaint to the Police for investigation, oversee the investigation by the Police, or defer action until receipt of the report on the investigation of the Police or on a criminal or disciplinary investigation[2027]. The IPCA may obtain information from such persons as it thinks fit and may hold a hearing.[2028] When concluding an investigation, the IPCA may take the measures described earlier in section 2.2.3. For example, procedures before the IPCA initiated by complaints have led the Police to correct information held on a complainant[2029], provide additional training to its staff[2030] and conduct disciplinary procedures[2031].

Fourth, individuals can apply to the High Court to seek judicial review of actions of a law enforcement agency (e.g., a decision, the exercise of statutory power, requiring a person to do something, make an investigation or inquiry, etc.)[2032]. For example, an individual can challenge the validity of a search warrant (e.g., because it was overly broad and did not adequately describe the offences for which it was issued, or the items to be searched for[2033]). To bring a claim for judicial review, an individual must either have personal standing (i.e., their personal rights and interests are affected by the decision/action under challenge) or public interest standing (i.e., there is a public interest that the claim is heard because it is important for the court to rule on the lawfulness of the decision/action)[2034]. Case law of the New Zealand courts has confirmed that the requirement of standing in judicial review proceedings is "significantly relaxed" and that a request will only be dismissed for lack of standing if the claims to both personal standing and public interest standing are "so untenable that the court must be certain they cannot possibly succeed"[2035]. Standing is usually considered in the course of a substantive procedure, which allows it to be assessed in light of

[2024] Section 102 Privacy Act 2020. In terms of damages, the HRRT may award compensation in respect of pecuniary loss, loss of any benefit (whether or not of a monetary kind), as well as humiliation, loss of dignity and injury to the feelings of the aggrieved individual (Section 103 Privacy Act 2020).
[2025] See Section 111 Privacy Act 2020, in conjunction with Section 123-124 of the Human Rights Act 1993.
[2026] Section 12(1) of the IPCA Act.
[2027] Section 17(1) IPCA Act. The IPCA may decide not to act upon a complaint in a limited number of circumstances, i.e., if the complaint relates to a matter that was known for more than 12 months before the complaint was made, or if the subject matter of the complaint is minor, the complaint is frivolous, vexatious, or not made in good faith. The same applies if the complainant does not desire that action be taken, if the identity of the complainant is unknown and the investigation would therefore be substantially impeded, or an adequate remedy or appeal is available (Section 18(1) of the IPCA Act).
[2028] Section 23(3) of the IPCA Act.
[2029] https://www.ipca.govt.nz/Site/Outcomes/2021-summaries-of-facilitated-resolutions/2021-apr-20-counties-manukau-police-update-records.aspx
[2030] https://www.ipca.govt.nz/Site/Outcomes/2018-19-summaries-of-police-investigations/2019-oct-29-allegation-unlawful-search-wellington-police.aspx
[2031] https://www.ipca.govt.nz/Site/Outcomes/2018-19-summaries-of-police-investigations/2019-nov-11-police-officer-sanctioned-policy-breach.aspx
[2032] Judicial Review Procedure Act 2016.
[2033] See e.g., Dotcom v Attorney-General [2014] NZSC 199; Hager v Attorney-General [2015] NZHC 3628.
[2034] See e.g., Smith (Phillip) v Attorney-General (Department of Corrections) [2017] NZHC 1647 [2].
[2035] Smith (Phillip) v Attorney-General (Department of Corrections) [2017] NZHC 1647 [2].

the merits of the case, which may show the public interest at issue[2036]. In a judicial review procedure, the court may find that the decision/action was unlawful (e.g., in violation of a statute, exceeding the discretion provided to the public authority, etc.), unreasonable (e.g., because it is arbitrary) or procedurally improper[2037]. The court may order different remedies, e.g., referring the decision back to the relevant authority, prohibiting future actions, setting the decision/action aside, declaring the action/decision unlawful or issuing an injunction[2038].

Fifth, depending on the type of remedies sought, individuals may invoke a violation of Section 21 of the Bill of Rights Act in different procedures to obtain redress. For example, individuals can invoke Section 21 of the Bill of Rights Act in the course of judicial review proceedings to have a decision/action (e.g., a warrant) quashed. In addition, individuals may bring a civil claim for public law damages, alleging a violation of Section 21 of the Bill of Rights Act[2039]. To determine whether such compensation is an effective and proportionate remedy, the court must examine the nature of the right and the nature of the breach. In addition, any awarded sum must reflect any relevant intention behind the conduct, the duration of the breach and the ways in which the state has acknowledged the wrongdoing[2040]. Moreover, if criminal proceedings are instituted against the individual, Section 21 of the Bill of Rights Act can be invoked to challenge the admissibility of evidence if it was unlawfully obtained[2041].

Finally, under certain conditions, individuals could claim compensation for damages under the tort of publication of private facts (i.e., if a public authority publishes facts for which the individual had a reasonable expectation of privacy, and the publication is highly offensive to a reasonable person[2042]) and intrusion into seclusion (i.e., in case of an intentional and unauthorised intrusion into an intimate personal activity or space, involving infringement of a reasonable expectation of privacy, in circumstances which are highly offensive to a reasonable person[2043]).

2.3. Access and use by New Zealand public authorities for national security purposes

There are two intelligence and security agencies in New Zealand, the Government Communications Security Bureau (GCSB) and the New Zealand Security Intelligence Service (NZSIS). The GCSB specialises in signals intelligence, information assurance and cybersecurity[2044], whereas the NZSIS specialises in human intelligence activities[2045]. Both agencies may access personal information on the basis of the Intelligence and Security Act of 2017 (I&S Act), subject to specific limitations and safeguards. The objective of the I&S Act, which was the result of a significant reform in 2017 of the rules applicable to intelligence activities, is inter alia to ensure that the functions of the intelligence and security agencies are

[2036] Ibid.
[2037] See e.g., Stevenson v Office of Police Commissioner [2015] NZHC 1408 at [6].
[2038] Section 16 of the Judicial Review Procedure Act.
[2039] Simpson v Attorney General [1994] 3 NZLR 667 (NZCA).
[2040] Taunoa v Attorney General [2008] 1 NZLE 429 (NZ Supreme Court).
[2041] See Section 30 of the Evidence Act 2006. See also R v Hamed [2011] NZSC 101; R v Reti and Wood [2020] NZSC 16; Griffith v R [2016] NZCA 390.
[2042] Hosking v Runting [2005] 1 NZLR 1 (CA).
[2043] C v Holland [2012] NZHC 2155 [2012] 3 NZLR 672.
[2044] Section 8 I&S Act.
[2045] Section 7 I&S Act.

performed in accordance with New Zealand law and human rights and in a manner that facilitates effective democratic and institutional oversight[2046]).

2.3.1. Legal bases and applicable limitations/safeguards

As a general principle, the I&S Act stipulates that, when performing their functions, the intelligence agencies must act (1) in accordance with New Zealand law and all human rights obligations recognised by New Zealand; (2) independently and impartially in the performance of their operational functions; (3) with integrity and professionalism and (4) in a manner that facilitates effective democratic oversight[2047]. The Directors-General of the two intelligence and security agencies must take all reasonable steps to ensure that the agencies' activities are limited to those that are relevant to the performance of their functions, kept free from any influence or consideration that is not relevant to the performance of their functions and politically neutral[2048]. Moreover, any cooperation with foreign jurisdictions and international organisations must take place in accordance with New Zealand law, including human rights obligations[2049].

In June 2023 (after a previous version in 2021), 14 national security priorities were approved by the government, which direct the intelligence and security agencies' collection of information[2050]. These priorities include, for instance, foreign interference and espionage, malicious cyber activity, national security implications of climate change, national security implications of disinformation, terrorism and violent extremism, transnational serious and organised crime, and economic security. On the basis of the I&S Act, the two intelligence and security agencies may make use of different powers to collect personal information to pursue these priorities.

First, an 'intelligence warrant' may authorise different activities, such as human intelligence, surveillance[2051], the interception of private communications[2052] and searches and seizures[2053]. The I&S Act foresees a 'Type 1' warrant issued by the responsible Minister and the Chief Commissioner of Intelligence Warrants[2054] (for the collection of information on New Zealand citizens or permanent residents) and a 'Type 2' warrant issued by the responsible Minister (for the collection of information on non-New Zealand nationals or residents) intelligence

[2046] Section 3 of the I&S Act. As described in section 2.1, one of the reforms brought by the Intelligence and Security Act was the amendment of the Privacy Act to expand the IPPs that apply to the intelligence and security agencies.
[2047] Section 17 I&S Act.
[2048] Section 18(a) I&S Act.
[2049] Section 18(b) I&S Act.
[2050] Available at: https://www.dpmc.govt.nz/our-programmes/national-security/national-security-intelligence-priorities#:~:text=that%20could%20impact-,New%20Zealand's%20national%20security%20interests.,that%20affect%20our%20national%20interest.
[2051] This includes both visual surveillance and electronic tracking of one or more (classes of) persons, places or things (Section 47 I&S Act).
[2052] Interception includes "to hear, listen to, record, monitor, acquire or receive the communication, or acquire its substance, meaning or sense, while it is taking place or in the course of transmission" (Section 47 I&S Act). 'Communication' is broadly defined and covers signs, signals, writing, images, sounds, information, etc. (Section 47 I&S Act).
[2053] Section 67 I&S Act.
[2054] Pursuant to the I&S Act, the Governor-General must, on the recommendation of the Prime Minister after consultation of the leader of the opposition, appoint up to three persons as Commissioners of Intelligence Warrants. A person may only be appointed a commissioner if (s)he has previously held office as a Judge of the High Court. See Sections 112-113 I&S Act.

warrant[2055]. An application for an intelligence warrant (Type 1 and Type 2) must be made in writing by the Director-General of the relevant agency and set out, inter alia, the details of the activity proposed to be carried out and the grounds on which the application is made (including the reasons why the legal requirements for issuing the warrant are believed to be satisfied)[2056].

A Type 1 intelligence warrant may be issued if it will enable the intelligence and security agency to carry out an activity that (1) is necessary to contribute to the protection of national security and identifies, enables the assessment of, or protects against certain harms listed in the I&S Act (e.g., terrorism or violent extremism, espionage, proliferation of weapons of mass destruction), or (2) will contribute to he international relations and well-being of New Zealand, or the economic well-being of New Zealand and there are reasonable grounds to suspect that the targeted individual is acting on behalf of a foreign person, organisation or terrorist entity[2057]. A Type 2 intelligence warrant may only be issued if the authorising Minister is satisfied that the warrant will enable the intelligence agency to carry out an activity that is necessary to contribute to the protection of national security; or will contribute to the international relations and well-being of New Zealand, or the economic well-being of New Zealand (i.e., an activity that is necessary to pursue the government's national security priorities, as described above)[2058].

In addition to the abovementioned criteria, Type 1 and Type 2 warrants may only be issued if (1) the activity is "necessary to enable the agency to carry out its functions"; (2) the activity is "proportionate to the purpose for which it is to be carried out"; (3) the purpose of the warrant "cannot be reasonably be achieved by less intrusive means" and (4) arrangements are in place to ensure that nothing will be done in reliance on the warrant beyond what is necessary and reasonable to perform the agency's function, all reasonably practicable steps will be taken to minimise the impact on any members of the public and any information obtained in reliance on the warrant will be retained, used and disclosed only in accordance with the law[2059]. According to the Inspector General of Intelligence and Security, the key concepts in this assessment are the principles of 'necessity' (i.e., "more than useful, reasonable or desirable, although not necessarily indispensable" – requiring a law enforcement authority "to make a compelling case" for the use of its powers) and 'proportionality' (which requires weighing different factors, such as the gravity of any adverse effects, the importance of the purpose, the anticipated benefits to be gained, the likelihood of success, any alternative ways to achieve the result sought, and any measures that can be taken to mitigate adverse effects)[2060].

Type 1 and Type 2 warrants must specify, among other information, the objective and purpose of the warrant, as well as the person or class of persons (e.g., a terrorist cell) that will be subject to the activity[2061]. The validity of an intelligence warrant may not exceed 12

[2055] Sections 52-55 I&S Act.
[2056] Section 55 I&S Act.
[2057] Sections 58-59 I&S Act.
[2058] Section 60 I&S Act.
[2059] Section 61 I&S Act.
[2060] See the report of the Inspector General of Intelligence and Security of December 2018 on "Warrants issued under the Intelligence and Security Act 2017", paras. 39-41.
[2061] Section 66 I&S Act. As specified by the Inspector General, "a warrant can authorise activities against a named person or persons, or against a defined class of persons. The same applies to places, things and

months and may at any time be revoked by the responsible Minister, who may in that case require that all information collected under that warrant is destroyed[2062].

In situations of urgency, the authorising Minister (and, for Type 1 warrants, a Commissioner of Intelligence Warrants) may allow the application for a warrant to be done orally and issue the warrant subsequently in accordance with the abovementioned criteria[2063]. Such a warrant is revoked by law 48 hours after its issue unless, before the expiry of that period, the applicant applies in writing for a warrant in accordance with the previously described procedure[2064]. Upon receiving such an application, the responsible Minister (and, for Type 1 warrants, a Commissioner for Intelligence Warrants) may either confirm or revoke the warrant[2065]. If revoked, all information obtained under that warrant must be destroyed as soon as practicable[2066]. In addition, in very urgent situations – i.e., only if the delay in making an application for an urgent issue of a warrant would defeat the purpose of obtaining the warrant – the Director-General of an intelligence agency may authorise an activity on the basis of the abovementioned criteria[2067]. In this case, the relevant Minister (and, for Type 1 warrants, the Chief Commissioner of Intelligence Warrants) must be notified and an application for a warrant must be filed within 24 hours after the authorisation is given (otherwise the warrant is revoked, and all collected information must be destroyed)[2068]. Moreover, the reasons for the urgent issue of a warrant must be recorded and all urgent warrants must be sent to the Inspector-General of Intelligence and Security for review[2069].

More generally, any unauthorised information that has been collected must be destroyed immediately after it is obtained, unless an application for a warrant is made as soon as practicable and a warrant is issued[2070]. Incidentally obtained information may only be retained for the purpose of disclosing it to the Police, the New Zealand Defence Force or another public authority (in New Zealand or overseas) if there are reasonable grounds to believe that such a disclosure may assist in (1) preventing or detecting serious crime; (2) preventing or responding to threats to the life of any person; (3) identifying, preventing or responding to threats or potential threats to security or defence or (4) preventing the death of any person who is outside the territorial jurisdiction of any country[2071]. In addition, the Director General of an intelligence and security agency must keep a register of intelligence warrants that were issued to them, which may be accessed at any time by the responsible Minister as well as the Inspector-General of Intelligence and Security (see below), and the Chief Commissioner of

---

communications, which can be specified individually (e.g., searching a particular place) or as classes (e.g., searching any place owned, used or occupied by a targeted person)", see para. 23 of the report "Warrants issued under the Intelligence and Security Act 2017".

[2062] Section 64-65, Section 84(2) I&S Act.

[2063] Section 72 I&S Act. For Type 1 warrants, the authorising Minister may, if it is necessary to do so without the involvement of a Commissioner of Intelligence Warrants, alone allow an oral application and urgently issue the warrant. In this case, the Chief Commissioner of Intelligence Warrants must immediately be notified and may, at any time, revoke the warrant. See Section 71 I&S Act.

[2064] Section 74(1) and 75(1) I&S Act.

[2065] Article 74(2) and 75(2) I&S Act.

[2066] Section 76 I&S Act.

[2067] Section 78(1), (2)(b), (4) I&S Act.

[2068] Section 79, 80 and 81 I&S Act.

[2069] Sections 73, 77 and 82 I&S Act.

[2070] Section 102(2) I&S Act.

[2071] Section 104 I&S Act.

Intelligence Warrants, in relation to Type 1 intelligence warrants [2072]. Violations of several requirements with respect to intelligence warrants (e.g., failure to destroy information, unlawful use or disclosure of collected information, providing false or misleading information when applying for a warrant) are subject to criminal sanctions[2073].

Second, the intelligence and security agencies may have access to business records of telecommunication network operators[2074] and financial service providers[2075], after obtaining approval[2076] from the responsible Minister and the Chief Commissioner of Intelligence Warrants[2077]. Such approval is only granted if the Minister and Commissioner are satisfied that (1) obtaining business records is necessary to enable the carrying out of a function of the intelligence agency; (2) the privacy impact does not outweigh the importance of performing that function; (3) it would not be more appropriate to apply for an intelligence warrant; (4) there are satisfactory arrangements in place to ensure that nothing will be done beyond what is necessary and reasonable for the proper performance of a function of the agency and (5) there are satisfactory arrangements in place to ensure that obtained information will be retained, used and disclosed only in accordance with the law[2078]. The approval must state, inter alia, the circumstances in which the business records may be accessed, the business records that may be accessed, and any restrictions or conditions[2079]. An approval expires 6 months after the date on which it is granted and may be extended upon application for a subsequent approval[2080]. The Director-General of an intelligence and security agency must keep a register of all business records directions that received the approval referred to above[2081]. All business records obtained under a business records direction must be destroyed as soon as practicable

[2072] Section 83 I&S Act.
[2073] Sections 106-111 I&S Act.
[2074] With respect to telecommunication network operators, the notion of 'business records' includes customer and subscriber information, bank account number details, credit card number details, IP addresses, call associated data, device-related information, details of mobile data usage, information on linked accounts, and details of any persons communicating with the network operator (Section 144 I&S Act). It does not include the content of telecommunications and web browsing history (Section 144 I&S Act). It also does not cover personal information about the network operator's employees and directors, as well as any information relating to the business operations of the operator and the content of any other communications or files held by the operator in providing any service to a customer (e.g., cloud storage servers or insurance).
[2075] In relation to financial service providers, 'business records' include customer information, bank account number details, credit card number details, statement and account information, transaction information and other information related to a specific account (Section 144 I&S Act). It does not include the content of communications, personal information about the provider's employees and directors, information relating to the business operations of the provider or the content of any other communications or files held by the provider in providing any service to a customer.
[2076] Approval must be requested by the Director-General of an intelligence and security agency, through a written application to the responsible Minister and the Chief Commissioner of Intelligence Warrants that includes the circumstances giving rise to the need for the application, the business records or class of business records sought, the function that the intelligence and security agency would be performing and an explanation as to why applying for an intelligence warrant is likely to be impractical or otherwise inappropriate in the circumstance in the case (Section 145(3) I&S Act). The function of the intelligence agency must be either intelligence collection and analysis (Section 10 I&S Act), protective security services, advice and assistance (Section 11 I&S Act) or cooperation with other entities to respond to imminent threat (Section 14 I&S Act).
[2077] Section 145 I&S Act. Under Part 4, Subpart 6 I&S Act, the Governor-General must, on the recommendation of the Prime Minister, appoint up to three Commissioners of Intelligence Warrants. A person may be appointed as Commissioner only if he/she has previously held office as a Judge of the High Court.
[2078] Section 147(2) I&S Act.
[2079] Section 147(3) I&S Act.
[2080] Section 148 I&S Act.
[2081] Section 153 I&S Act.

if they are not required or are no longer required for the performance of the agency's functions[2082].

Third, intelligence agencies may have access to specific categories of information (e.g., birth information, citizenship information) held in certain government databases[2083], in accordance with a written agreement between the responsible Ministers[2084]. Such a 'direct access agreement' may only be concluded if the relevant Ministers are satisfied that (1) direct access is necessary to enable the intelligence agency to perform its duties; (2) there are adequate safeguards to protect the privacy of individuals (existing agreements e.g., contain provisions on data security, access controls, data retention and data sharing); and (3) the agreement will include appropriate procedures for direct access, use, disclosure and retention of the information[2085]. Both the OPC and the Inspector-General (see below) must be consulted before concluding an agreement and the relevant Ministers have to take into account any comments received in this respect[2086]. A direct access agreement must specify, inter alia, the database and particular information that may be accessed, the function/duty/power to be exercised by the intelligence agency, the safeguards to be applied to particular categories of information (e.g., commercially sensitive information), requirements relating to storage, retention and disposal of information, etc.[2087] All agreements must be published on the website of both the intelligence agency and the public authority holding the database[2088]. Finally, the relevant Ministers must review the agreement every three years, in consultation with the OPC and Inspector-General[2089]. So far, two direct access agreements have been concluded: between the Minister responsible for the NZSIS and the Minister of Customs and between the Minister responsible for the NZSIS and the Minister of Immigration[2090].

[2082] Section 152 I&S Act.

[2083] In addition, the I&S Act provides the intelligence agencies with a legal basis to collect four types of so-called 'restricted information', i.e. (1) information maintained by Inland Revenue under the Tax Administration Act 1994; (2) information relating to a national student number to students enrolled with a tertiary education provider; (3) information relating to an adoption held by the Registrar-General; and (4) photographic images used for driver licences (Sections 135 and 136 I&S Act). To access such information in relation to a non-New Zealand citizen or permanent resident, the Director-General of an intelligence agency must obtain permission from the responsible Minister (Section 136(1) and (2)(b) I&S Act). Permission may be granted if the Minister is satisfied that (1) access to the information is necessary to contribute to the protection of national security or will contribute to the international relations and well-being of New Zealand; or the economic well-being of New Zealand; (2) the access is necessary for the purpose of enabling the intelligence agency to perform its functions (i.e. intelligence collection and analysis and protective security services, advice and assistance, (3) the privacy impact is proportionate to that purpose and the information cannot be collected by any other means (Section 138 and 139 I&S Act in conjunction with ss 10 and 11). The Ministerial permission must specify the information that may be accessed and the agencies holding the restricted information are required to comply with the permission and provide access (Section 140 and 141 I&S Act).

[2084] Section 125 I&S Act. The intelligence agencies that may access the database on the basis of such agreements, the information that may be accessed, as well as the authority in charge of the database are specified in the Intelligence and Security Act (Schedule 2 I&S Act).

[2085] Section 126 I&S Act.

[2086] Section 127 I&S Act.

[2087] Section 129 I&S Act.

[2088] Section 131(1)-(2) I&S Act.

[2089] Section 131(3) I&S Act.

[2090] Available at: https://www.nzsis.govt.nz/assets/NZSIS-Documents/DAA/Direct-Access-Agreement-Customs-NZSIS.pdf and https://www.nzsis.govt.nz/assets/NZSIS-Documents/DAA/Direct-Access-Agreement-NZSIS-DIA-BDM-database.pdf.

Finally, the NZSIS and GCSB may obtain personal information from any public or private sector agency on a voluntary basis[2091]. In particular, the Privacy Act 2020 allows the disclosure of information (either upon request or on their own initiative) if a private entity or public authority believes on reasonable grounds that the disclosure of the information is necessary to enable an intelligence and security agency to perform any of its functions[2092]. The Director-General of an intelligence and security agency may request information if he/she believes on reasonable grounds that the information is necessary to enable the agency to perform any of its functions[2093]. Such a request must provide the details of the requested information and confirm that it is necessary for the agency to carry out its functions[2094]. To enable agencies to decide whether or not to disclose information upon request, the Director-General of an intelligence and security agency may certify that he or she believes that the relevant requirements are met[2095]. A Ministerial Policy Statement provides further guidance as to the elements to be taken into account by intelligence and security agencies when making requests for voluntary disclosure. In particular, they must consider the legality, necessity and proportionality of each request, must take reasonable steps to mitigate the impact on privacy, consider less intrusive means and, in, general, ensure that they make use of the most appropriate statutory mechanism to access personal information[2096]. Intelligence agencies must keep registers of all certificates they have issued, which may be accessed any time by the responsible Minister, as well as the Inspector-General[2097].

2.3.2. Further use of the information collected

The processing of personal data by the two intelligence and security agencies is subject to most provisions of the Privacy Act 2020, including the Principles governing the use and disclosure of information, security, purpose limitation, data accuracy and limited data retention[2098].

With respect to the further sharing of data with other entities, the I&S Act also imposes specific limitations. In particular, it only allows the intelligence and security agencies to share collected information with the Chief Executive of the Department of the Prime Minister and Cabinet, or other persons (whether in New Zealand or overseas) when authorised to do so by the responsible Minister[2099]. The Minister may only authorise a disclosure if he/she is satisfied that it would take place in accordance with New Zealand law and human rights obligations[2100]. A Ministerial Policy Statement on Cooperation with Overseas Public Authorities provides further guidance to intelligence agencies in this respect. For example, it requires them to comply with the following principles: legality, compliance with human rights obligations, necessity, reasonableness and proportionality, information management, and

[2091] Subpart 1 of Part 5 I&S Act.
[2092] IPP 11(1)(g) Privacy Act 2020. See also Sections 120(b) and 122 I&S Act.
[2093] Section 121(1) I&S Act.
[2094] Section 121(2) I&S Act.
[2095] Section 122(3) I&S Act.
[2096] See https://www.nzic.govt.nz/assets/assets/mpss/Ministerial-Policy-Statement-Requesting-information-under-section-121.pdf.
[2097] Section 123 I&S Act.
[2098] Section 28 Privacy Act 2020.
[2099] Section 10(1)(b) I&S Act.
[2100] Section 10(3) I&S Act.

oversight[2101]. In accordance with the I&S Act, all intelligence and security agency employees are required to have regard to any relevant Ministerial Policy Statement in making any decision or taking any action[2102].

2.3.3. Oversight

The activities of the NZSIS and GCSB are supervised by different bodies.

First, the OPC independently oversees compliance of data processing by the NZSIS and GCSB with the Privacy Act 2020. In doing so, the OPC may make use of different powers, including to conduct general inquiries, audits (upon request) and investigations (see also section 2.2.3)[2103]. If, after completing an investigation, the OPC concludes that an action of an intelligence and security agency is an interference with the privacy of an individual, the OPC must issue a report setting out its opinions and reasons for that opinion. [2104] The report may include any recommendations the OPC considers appropriate and may request the intelligence and security agency to notify the OPC within a specified time of any steps the agency proposes to take in response[2105]. If the intelligence and security agency does not take steps in response to a report that the OPC considers to be adequate and appropriate within a reasonable time, the OPC may send a copy of the report to the Prime Minister, who in turn may present the report to the Parliament[2106]. In addition, the OPC may issue a binding compliance notice[2107], which may be enforced before the HRRT in accordance with the procedure described above (see section 1.2 and 2.2.3).

Second, independent oversight is also provided by the Inspector-General of Intelligence and Security[2108]. The Inspector-General carries out regular reviews (at least every 12 months) of procedures and compliance systems of each intelligence and agency and conducts inquiries into specific activities upon request from other authorities (e.g., the responsible Minister or the Prime Minister) or on its own initiative[2109]. For example, in 2021[2110], the Inspector-General initiated reviews of the NZSIS information sharing with the Police and the GCSB's raw data sharing with partner agencies, and in 2020[2111], of the GCSB's access to information infrastructures. In carrying out its oversight activities, the Inspector-General may require any person to provide any information the Inspector-General considers may be relevant to an inquiry.[2112]. On the completion of an inquiry, the Inspector-General must prepare a written

---

[2101] See https://www.nzic.govt.nz/assets/assets/mpss/Ministerial-Policy-Statement-Cooperation-with-overseas-public-authorities.pdf.
[2102] Section 209 I&S Act
[2103] The OPC in principle has access to all relevant information, with the exception that information may not be disclosed to the OPC where the Prime Minister certifies that the provision of the information might prejudice the security, defence or international relations of New Zealand (Section 88(3) Privacy Act 2020). However, this exceptional procedure has so far never been used.
[2104] Section 95(2) Privacy Act 2020.
[2105] Section 95(3)-(4) Privacy Act 2020.
[2106] Section 95(5)-(6) Privacy Act 2020.
[2107] Subpart 2 of Part 6 of the Privacy Act 2020.
[2108] Subpart 1 of Part 6 I&S Act. The Inspector-General is appointed by the Governor-General on the recommendation of the House of Representatives and after consulting the Intelligence and Security Committee (Section 157 I&S Act).
[2109] Section 158(1) I&S Act.
[2110] Available at: https://igis.govt.nz/assets/Annual-Reports/Annual-Report-2021-2022.pdf.
[2111] Available at: https://igis.govt.nz/assets/ANNUAL-REPORT-2020-2021.pdf.
[2112] Section 179 I&S Act.

report containing his or her conclusions and recommendations[2113]. Reports by the Inspector-General must be sent to the responsible Minister and Director-General of the intelligence and security agency to which the inquiry relates, as well as to either the Prime Minister or the Intelligence and Security Committee if the inquiry was requested by either of the latter. If the inquiry was carried out at the request of a Minister or the Prime Minister, or on the Inspector-General's own initiative, the Inspector-General may send the report to the Intelligence and Security Committee if the responsible Minister/the Prime Minister agrees[2114]. In addition, the Inspector-General must make reports publicly available[2115]. The responsible Minister must respond to a report of the Inspector-General as soon as practicable after receiving a report[2116].

Finally, the Intelligence and Security Committee of the New Zealand Parliament examines the policy, administration and expenditure of each intelligence and security agency, considers their annual reports and conducts annual reviews on that basis, and considers any Bill, petition or other matter relating to the intelligence and security agencies referred to the Committee by the House of Representatives[2117]. The Committee consists of the Prime Minister, the Leader of the Opposition, members of the House of Representatives nominated by the Prime Minister as well as members nominated by the Leader of the Opposition with the agreement of the Prime Minister[2118]. While the Committee does not itself have the power to inquire into matters falling within the jurisdiction of the Inspector-General, it may request the Inspector-General to conduct an inquiry into any matter relating to intelligence and security agencies' compliance with New Zealand law (including human rights law) and the propriety of particular activities of an intelligence and security agency[2119]. The Committee itself does not have the function to inquire into any matter within the jurisdiction of the Inspector-General, into any information that is operationally sensitive or into complaints from individuals[2120].

2.3.4. Redress

The New Zealand system offers different avenues to obtain redress, including compensation for damages.

First, individuals have a right to obtain access to and correction of their data held by the NZSIS and GCSB under the Privacy Act 2020, under the same conditions as described under section 2.2.4. If a request to obtain access or correction to data is refused, any individual has the possibility to lodge a complaint with the OPC[2121], that can issue a report with

[2113] Section 185(1) I&S Act.
[2114] Section 185 I&S Act.
[2115] Section 188 I&S Act. At the same time, the public report may not contain information that, if publicly disclosed, would be likely to prejudice the entrusting of information to the Government of New Zealand on a confidential basis by a third country or international organisation. The same applies to information that would be likely to endanger the safety of any person, would prejudice the continued performance of functions of an intelligence agency or the security, defence or international relations of New Zealand, or reveal the identity of officers or employees of intelligence agencies, see Section 188(2) I&S Act.
[2116] Section 187 I&S Act.
[2117] Section 193 I&S Act.
[2118] Section 194(2) I&S Act.
[2119] Section 193(1)(e) I&S Act.
[2120] Section 193(2) I&S Act.
[2121] For example, in one case, the OPC investigated a refusal to grant access by the NZSIS and the GCSB, which had argued that responding to the request would likely prejudice the security or defence of New Zealand. In this case, the OPC accepted that both the NZSIS and the GCSB did have reasons to neither confirm nor deny the existence or non-existence of the information. See Case note 284416 [2017] NZ PrivCmr 5.

recommendations, that may also contain a request to notify the OPC within a specified time of any steps the intelligence agency proposes to take in response to the recommendations[2122]. If an intelligence agency does not take steps that the OPC considers to be adequate and appropriate in response to a report of the OPC within a reasonable time, the OPC can send a copy of the report to the Prime Minister, who may in turn present the report to the House of Representatives[2123]. Moreover, individuals can also enforce their right of access directly against public authorities before the ordinary courts[2124].

Second, any individual may lodge a complaint concerning an interference with privacy by an intelligence agency with the OPC, who can issue recommendations[2125] and binding compliance notices which may be enforced before the HRRT in accordance with the procedure described above (see section 1.2 and 2.2.4).

Finally, the same judicial avenues as the ones described in section 2.2.4 (i.e., to obtain judicial review of decisions/actions of intelligence agencies, exclude illegally obtained evidence from judicial proceedings and/or obtain compensation for damages, including by invoking a violation of Section 21 of the New Zealand Bill of Rights Act) are also available against the NZSIS and GCSB[2126].

[2122] Section 95(2)-(4) Privacy Act 2020.
[2123] Section 95(5)(6) Privacy Act 2020.
[2124] Section 31(2) Privacy Act 2020. See also Dotcom v USA and District Court of North Shore [2014] NZHC 2550 [56], [69], [84].
[2125] If the intelligence agency does not take steps that the OPC considers to be adequate and appropriate in response to a report of the OPC within a reasonable time, the OPC can send a copy of the report to the Prime Minister, who may in turn present the report to the House of Representatives (Section 95(5)(6) Privacy Act 2020).
[2126] See e.g., Dotcom v. Attorney-General [2012] NZHC 3268, and Attorney-General v Dotcom [2013] NZCA 43,
in which an individual sought damages for breach of the New Zealand Bill of Rights Act, in respect of GCSB's unlawful interception of that individual's communications. In that case, GCSB admitted liability and the High Court entered judgment against it: see Dotcom v Attorney-General [2019] NZCA 412 at [3].

X. SWITZERLAND

1. RULES APPLYING TO THE PROCESSING OF PERSONAL DATA

1.1. Relevant developments in the data protection framework of Switzerland

On 26 July 2000, the Commission adopted the adequacy decision[2127] for Switzerland, following an opinion of the Article 29 Working Party of 7 June 1999[2128]. At the time of the adoption of the adequacy decision, the protection of personal data in Switzerland was mainly governed by the Federal Act on Data Protection of 19 June 1992 (FADP 1992)[2129] and its implementing Data Protection Ordinance of 14 June 1993 (DPO 1993)[2130].

Since then, there have been a number of significant developments in the Swiss data protection framework that created a higher level of convergence with the EU one. More specifically, in order to implement the data protection requirements of Convention 108 of the Council of Europe[2131] and the Schengen acquis, the FADP was subject to revisions in 2006[2132] and 2010[2133]. On 25 September 2020, the Federal Assembly adopted a new Federal Act on Data Protection (FADP 2020) to replace the Act from 1992[2134]. The FADP entered into force on 1 September 2023. It takes into account the revised Convention 108 of the Council of Europe (Convention 108+), ratified by Switzerland on 7 September 2023, and Regulation (EU) 2016/679 (GDPR)[2135]. The FADP 2020 also incorporates the content of the previous Swiss Schengen Data Protection Act[2136], thereby implementing Directive (EU) 2016/680 (Law Enforcement Directive)[2137] with respect to data processing in the context of Schengen cooperation in criminal matters. The FADP 2020 is complemented by a new Data Protection Ordinance (DPO 2022), which was adopted by the Federal Council on 31 August 2022 and

[2127] Commission Decision 2000/518/EC of 26 July 2000 on the adequate protection of personal data provided in Switzerland, OJ L 215, 25/08/2000 p. 1.
[2128] Opinion No 5/99 on the level of protection of personal data in Switzerland, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1999/wp22_en.pdf.
[2129] Federal Act on Data Protection of 19 June 1992 .
[2130] Ordinance to the Federal Act on Data Protection of 14 June 1993.
[2131] Switzerland ratified Convention 108 on 2 October 1997, and its Additional Protocol 181 on 20 December 2007.
[2132] Federal Act of 24 March 2006 (Official Compilation 2007 4983). As part of this amendment, the FADP was strengthened in several ways. For example, the requirements for valid consent were updated, by making clear that consent must be a free expression of the individual's will concerning one or more processing activities after having been duly informed (Article 4(5) FADP 1992); a general principle of transparency and obligations to proactively inform individuals about the processing of their data in certain situations were introduced (Articles 4, 14 and 18 FADP 1992); a specific obligation for controllers to adopt measures to ensure that inaccurate or incomplete data is corrected was added (Article 5(1) FDAP 1992); a modernised regime for international data transfers was put in place (Article 6 FADP 1992); and specific rules governing the relationship between controllers and service providers were included (Article 10a FADP 1992).
[2133] Federal Acts of 19 March 2010 (Official Compilation 2010 33387). This amendment in particular updated the transparency requirements and the right of individuals to obtain access to their data, as well as the possible restrictions to those provisions (Article 9 FADP 1992).
[2134] Federal Act on Data Protection of 25 September 2020.
[2135] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[2136] Schengen Data Protection Act of 28 September 2018.
[2137] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

also entered into force on 1 September 2023. As explained in more detailed below, the FADP 2020 has strengthened the Swiss data protection framework in several areas.

The FADP 2020, like the previous legal framework, has a broad scope of application[2138], applying to all private operators and federal public authorities. Cantonal and communal public bodies are subject to cantonal data protection rules, which must meet Federal Constitutional requirements[2139] and Switzerland's international commitments in the area of data protection. In particular, according to Article 35 of the Federal Constitution, fundamental rights (including the right to privacy and data protection) are directly applicable in the entire Swiss legal system and have to be respected by all state organs and public bodies, at federal, cantonal and communal level. In line with Articles 13 and 36 of the Federal Constitution, any restriction to the fundamental right to privacy must have a legal basis, must be justified by a public interest or the protection of the fundamental rights of others and must be proportionate, while the essence of the right is inviolable. In addition, cantonal law must be in line with international conventions or treaties concluded by Switzerland, including Convention 108, its additional Protocol 181, and, in the future, Convention 108+, which are directly binding for the cantons[2140]. Individuals can appeal up to the Federal Supreme Court if they consider cantonal law to infringe federal constitutional or international rules[2141]. Reflecting these principles, all 26 cantons have data protection laws providing general data protection principles, rights for individuals and oversight by independent cantonal supervisory authorities. Several cantons recently enacted data protection reforms similar to the 2020 reform at federal level[2142].

[2138] Article 2 FADP 2020. The law does not apply to personal data processed by a natural person exclusively for personal use, the deliberations of the Federal Assembly, court proceedings, and personal data processed by institutional beneficiaries to whom the immunity of jurisdiction in Switzerland applies. Public registers for private legal transactions (the electronic civil status register, the Central Business Name Index, the aircraft register of the Federal Office of Civil Aviation and the registers of the Swiss Federal Institute of Intellectual Property), and in particular access to such registers and data subject rights, are regulated by specific laws (see e.g., Article 43a of the Swiss Civil Code and the Ordinance on the Civil Status, which lays down specific modalities for individuals to obtain access to their data in the register, and contains specific provisions on data security). To the extent that such laws do not contain data protection provisions, the FADP 2020 continues to apply. .

[2139] See Articles 49-51 Federal Constitution, which provide that federal law takes precedence over any contrary law of a canton and requires cantons to adopt their own democratic constitutions that must be compatible with federal law. See also the case law of the Federal Supreme Court regarding the 'principle of supremacy of federal law' (e.g., ATF 143 I 272, 276 seq., ATF 131 I 394, 396 seq.).

[2140] See Article 54 Federal Constitution, which establishes the exclusive powers of the Confederation in foreign affairs. Consequently, international treaties concluded by the Confederation are also binding for the cantons which must implement them in their areas of competence.

[2141] For example, in a recent case about facial recognition by the police the Swiss Federal Supreme Court judged that the cantonal legal basis for a system of automated vehicle search and monitoring traffic surveillance using facial recognition by the police was not sufficiently precise in light of Article 13 of the Federal Constitution. According to the Court, the purpose of processing, the extent of processing, as well as the duration of conservation and the erasure must be sufficiently determined in the law (ATF 146 I 116B_908/2018).

[2142] The data protection reforms at cantonal level aim at implementing the relevant international obligations in the field of data protection (Convention 108+ and the Law Enforcement Directive) and at taking into account the FADP 2020. As of November 2023, 14 cantons have new or revised data protection laws (AG, AI, BL, GL, JU, LU, NE, SG, SH, SZ, ZG, ZH, BS); one canton (GR) declares the provisions of the FADP 2020 applicable for cantonal authorities (while it is in parallel developing a new cantonal data protection law); in the other cantons drafts of revised data protection laws are either currently deliberated in parliament or have been submitted to public consultation.

While the core definitions (e.g., of 'personal data' and 'processing') have remained the same, the FADP 2020 brought further convergence with the GDPR, e.g., by aligning the notion of 'controller' and introducing new definitions that are very similar or identical to the ones used in the GDPR (e.g., of 'processor'[2143], 'profiling' and 'data breach')[2144]. The FADP 2020 codifies the territorial scope of the Swiss data protection rules[2145], making clear that they apply to events producing effects in Switzerland, even if they take place abroad[2146].

The main data protection principles provided under the Swiss data protection framework that were in place at the time of the adoption of the adequacy decision have remained in place without substantial changes. This is the case for the principles of lawfulness[2147], purpose limitation[2148], proportionality[2149], data accuracy[2150], data security[2151], and accountability. At the same time, case law and the recent reforms have further strengthened a number of principles (e.g., the principles of data minimisation and storage limitation) and introduced new obligations (e.g., with respect to transparency, data breach notification and accountability).

As regards the principle of fairness of data processing, the Federal Administrative Court confirmed in 2009 that, to ensure fairness of processing, personal data may not be collected or otherwise processed in a way that the data subject would not expect and would not agree to[2152]. Similarly, the Federal Administrative Court has also further explained the legal implications of the principle of purpose limitation, by clarifying that personal data may be processed for purposes compatible with the original purpose[2153]. The FADP 2020 codified this

[2143] Like the FADP 1992, the FADP 2020 contains specific obligations when controllers engage a processor (Article 9 FADP 2020), including that the relationship between both parties must be regulated by a contract or law, the controller must ensure that the processor guarantees data security, and the data is only processed by the processor in the same way as the controller would be allowed to do so. The FADP 2020 adds a further requirement, only allowing the processor to engage a sub-processor with the prior authorisation of the controller (Article 9(3) FADP 2020).
[2144] Article 5 FADP 2020.
[2145] The FADP 1992 was already applied broadly to situations with international aspects, including in public law, under the effects theory. For example, the Federal Court held that images taken in Switzerland and published in such a way that they can be accessed in Switzerland also have an overriding connection with Switzerland, even if the images are processed abroad and are not posted directly from Switzerland (ATF 138 II 346 ["Google Street View"]).
[2146] Article 3 FADP 2020. See also Articles 14 and 15 FADP 2020 on the obligations for controllers established outside of Switzerland to, under certain conditions, appoint a representative in Switzerland.
[2147] See the general principle of lawfulness in Article 6(1)-(2) FADP 2020, as well as Articles 30-31 FADP 2020 (for private operators, making clear that any processing may not unlawfully interfere with the rights of data subjects), and Article 34 FADP 2020 (for federal public authorities, in general only allowing data processing if there is a statutory basis, or exceptionally and in a particular case, for instance on the basis of consent of the individual or where the processing is necessary to protect the life or physical integrity of an individual). See also Article 36 FADP 2020 with respect to the legal bases for disclosure of personal data by federal public authorities.
[2148] Article 6(3) FADP 2020.
[2149] Article 6(2) FADP 2020.
[2150] Article 6(5) FADP 2020.
[2151] Article 8 FADP 2020.
[2152] Decision of the Federal Administrative Court A-3144/2008 of 27 May 2009. Article 4 FADP set out the general principle that personal data may only be processed lawfully. It also refers to the principle of good faith ('*bonne foi*', '*Treu und Glauben*'). The principle of good faith, equivalent to the principle of fairness in the GDPR, obliges data controller to a loyal, trustworthy and transparent processing of personal data (the term '*Treu und Glauben*' in the FADP is also used in the German version of the GDPR to translate the term 'fairness').
[2153]Decision of the Federal Administrative Court A-3144/2008 of 27. May 2009 (c. 10.3.1 and 10.3.2) ; ATF 146 I 11 (c. 3.3.2). See also: Philippe Meier, Protection des données: fondements, principes généraux et droit privé,

case law by enshrining that personal data may be collected only for specified purposes that are recognisable to the data subject and must be further processed in a manner compatible with those purposes[2154].

Similarly, the principle of data minimisation has further developed through case law and the FADP 2020. The principle of proportionality (i.e., requiring that the processing of personal data must be carried out in good faith and in a proportionate manner[2155]) has been further clarified in case law as requiring that data must be limited to what is actually and objectively necessary for the defined purposes of processing[2156]. The FADP 2020 consolidated the principle of proportionality[2157] (as interpreted in case law) and complements it with the principle of data protection by design and by default[2158], explicitly requiring data controllers to ensure (prior to the processing) that the processing of personal data is limited to the minimum necessary to achieve the intended purpose.

The FADP 2020 also strengthened the requirement of storage limitation, by introducing a clear obligation to destroy or anonymise data as soon as it is no longer needed for the purpose of processing[2159]. While the principle of proportionality under the FADP 1992 already implied that personal data can be stored only as long as needed for the purpose of the processing[2160], the FADP 2020 has provided a more explicit requirement of limited data retention, in the same way as the GDPR.

Another area that has been further strengthened by the FADP 2020 concerns transparency of data processing. The FADP 1992 already contained a general principle of transparency (by requiring the controller to ensure that the collection of personal data and the purpose of its processing are evident to the data subject) and obligations to proactively inform individuals about the processing of their data in certain situations (e.g., when the processing was carried out by federal public authorities or sensitive data is processed by private operators)[2161]. The FADP 2020 now requires any controller (i.e., private operators and federal public authorities) to proactively inform the individual[2162]. Where data is collected from the data subject, the data controller must at the time when data are obtained, provide the data subject at least with information on the identity and contact details of the controller, the purpose of the processing and, where applicable, the recipients or categories of recipients to whom personal data are transmitted. Where data has not been obtained from the data subject, the controller must provide the data subject with the aforementioned (and additional) information within one month or at the latest when the personal data are first disclosed to another recipient. This

---

Stämpfli, Bern 2011, p. 281. See also Despatch of the federal Council of 23 March 1988 to the FADP (Federal Gazette 1988 II 451) explaining that the goal of Article 4 is to prohibit any unauthorised change of purpose when further processing takes place.

[2154] Article 6(3) FADP 2020.

[2155] Article 4(2) FADP.

[2156] Decision A-3144/2008 of 27 May 2009 of the Federal Administrative Court. See also the Despatch of the Federal Council of 15 September 2017 (FF 2017 6644) in its comments to Article 6, par. 2 of the FADP 2020: "les principes d'évitement et de minimisation en constituent deux expressions [du principe de proportionnalité]".

[2157] Article 6(2) FADP 2020.

[2158] Article 7 FADP 2020.

[2159] Article 6(4) FADP 2020.

[2160] Limited data retention stems from 'temporal proportionality'. See: PHILIPPE MEIER, Protection des données: fondements, principes généraux et droit privé, Stämpfli, Bern 2011, p. 270.

[2161] See Article 4(4), Article 14(1) and Article 18a(1) FADP.

[2162] Article 19 FADP 2020.

obligation concerns both federal administration and private entities processing personal data. Where data are transferred abroad, data subjects must be informed about the country of destination and the safeguards that are put in place.

With respect to data security, the DPO 2022 has extended previous obligations, by requiring controllers and processors to put in place technical and organisational measures appropriate to the risks in order to ensure security of data, taking into account several factors (e.g., the type of data processed, the purpose of the processing, the risks for the rights of individuals)[2163]. The DPO 2022 also specifies the types of measures that controllers and processors must have in place (e.g., storage control, recovery, transport control, data integrity) and requires them to keep records of such measures. In addition, the FADP 2020 introduced a requirement for controllers to notify data breaches as soon as possible: (1) to the federal data protection authority (Federal Data Protection and Information Commissioner, FDPIC), where they are likely to result in a high risk to the data subject's personality or fundamental rights; and, (2) to the data subject, where necessary for his or her protection or when required by the FDPIC[2164].

Moreover, the FADP 2020 and the DPO 2022[2165] have modernised previously existing accountability requirements (e.g., to maintain a record of processing, issue a privacy policy and register certain types of processing with the FDPIC, e.g., in case of large-scale processing of sensitive data[2166]), including by moving away from prior registration requirements[2167]. The FADP 2020 requires controllers to implement the principles of data protection by design and by default[2168], keep an inventory of processing activities[2169], conduct a data protection impact assessment for data processing likely to result in a high risk to the data subject's personality or fundamental rights[2170], and, in certain circumstances, consult the FDPIC prior to data processing (e.g., if an impact assessment shows that the processing would involve high risks for the concerned individuals)[2171]. Moreover, the FADP 2020 foresees the appointment of data protection officers (as possibility for private operators and as obligation for federal public authorities)[2172], and provides for the possibility to adhere to sectoral codes of conduct[2173] and participate in certification schemes[2174].

In addition to the strengthening of data protection principles and obligations, the protections for special categories of data have been reinforced since the adoption of the adequacy decision. The FADP 1992 already offered additional protection for personal data on religious, ideological, political or trade union-related views or activities, health data, data related to

[2163] Articles 1-6 DPO 2020.
[2164] Article 24 FADP 2022.
[2165] See Articles 1-6 and 42 DPO 2022.
[2166] See Articles 7, 10a and 11a FADP 1992, as well as Articles 3-4, 8-11, 16, 18, 20-21 and 28 DPO 1993.
[2167] Article 11a of the FADP 1992 required all federal public bodies and certain private operators (i.e., that regularly process sensitive personal data or personality profiles, or regularly disclose personal data to third parties) to register their data processing with the FDPIC. Under the FADP 2020, this obligation only applies to federal public bodies.
[2168] Article 7 FADP 2020.
[2169] Article 12 FADP 2020.
[2170] Article 22 FADP 2020.
[2171] Article 23 FADP 2020.
[2172] Article 10 FADP 2020.
[2173] Article 11 FADP 2020.
[2174] Article 13 FADP 2020 (see also Article 11 of the FADP 1992).

intimate sphere[2175], racial origin, social aid measures and administrative and criminal proceedings and sanctions. The FAPD 2020, similarly to the EU data protection framework, has added to the list also data on ethnic origin, genetic data and biometric data which uniquely identifies a natural person[2176].

With respect to the rights of data subjects, the Swiss data protection framework continues to provide for a right of access, correction and erasure[2177], as well as a right to object[2178]. At the same time, the FADP 2020 has reinforced and modernised several rights.

This is particularly the case for the right of access[2179]. Under the FADP 1992, any individual could request information from a private controller or federal public authority as to whether data concerning him or her is being processed. The data controller was in turn required to inform the data subject of all data collected on him or her and provide additional information, including the source of the data and the purpose of the processing. Under the FADP 2020, controllers are required to provide additional information in response to an access request (including the identity and contact details of the controller, the retention period and the recipients or categories of recipients to whom personal data are disclosed), as well as any information necessary to enable them to assert their rights and to ensure the transparency of the processing[2180]. With respect to the right of correction, the FADP 2020 limits the possibility for controllers to refuse to rectify inaccurate data to situations where a statutory obligation prohibits the rectification, or the personal data is processed for archiving purposes in the public interest[2181].

Moreover, the FADP 2020 has introduced new rights. This includes rules for automated individual decision-making, in particular a duty to inform the data subject about decisions taken exclusively on the basis of automated processing that produce legal effects or similarly significantly affect the individual[2182], to give the individual the opportunity to make known his or her views upon request and to ensure review by a natural person upon request of the data subject. In addition, the FADP 2020 provides for a right to data portability, i.e., a right to receive a copy of personal data processed by automated means in a commonly used format, or to have such personal data transferred to another controller[2183].

[2175] The notion of 'intimate sphere' includes any information that the data subject would not share with others or only with a restricted circle of close persons, such as sexual life and sexual orientation, see ATF 137 I 167 (c. 9.1.1), 118 IV 41 (c. 4).
[2176] Article 5(c) FADP 2020.
[2177] Article 32(2)(c) (for private operators) and Article 41(1) FADP 2020.
[2178] Article 32(2)(a)-(b) and 41(1)(a) FADP 2020, according to which personal data may not be processed where an individual has expressly objected to it, unless there is an overriding public or private interest to continue processing the data. This right also applies in case personal data is processed for direct marketing purposes. With respect to public authorities, the FADP 2020 (Article 37) provide individuals with an additional specific right to object to the disclosure of their data.
[2179] Like the GDPR, the Swiss legal framework also provides for the possibility to refuse, restrict or defer the exercise of the right of access in specific circumstances, e.g., where providing the information would jeopardise the outcome of a criminal investigation, or to protect the overriding interests of third parties (Article 26-27 FADP 2020). Similar restrictions/limitations apply to the right of the data subject to obtain information in accordance with the transparency principle (Article 20 FADP 2020).
[2180] Article 25 of the FADP 2020. The relevant information must be provided free of charge and, in principle, within 30 days of the request.
[2181] Article 32(1) FADP 2020.
[2182] Article 21 FADP 2020.
[2183] Article 28 FADP 2020 and Articles 20-22 DPO 2022.

Finally, the rules on international transfers of personal data have been reinforced. As a general rule, personal data may only be transferred if the data is subject to adequate protections in the country of destination[2184]. Under the FADP 1992, the FDPIC had developed an indicative list of countries that provide an adequate level of data protection, but it remained the responsibility of the data exporter to assess whether and ensure that data will be adequately protected in a third country. With the FADP 2020, the Federal Council is in charge of deciding whether a State or international organisation offers an adequate level of protection, on which data exporters can rely to transfer data without the need to carry out their own assessment or put in place specific safeguards[2185]. The criteria to be taken into account for the evaluation of the adequacy of the level of protection are listed in Article 8 of the DPO 2022, referring inter alia to the international obligations of the country/organisation, the rule of law and respect for human rights, applicable data protection legislation and its implementation, the effective functioning of one or more independent authorities responsible for data protection, etc. A list of States, territories, specific sectors in a State and international organisations adequately protecting personal data, published in Annex 1 to the DPO 2022, includes members of the European Economic Area and most countries that have received an adequacy decision from the EU[2186].

If a third country is not recognised as providing an adequate level of data protection, personal data may only be transferred to that country if sufficient safeguards are put in place by the data exporter and importer to ensure an adequate level of protection (e.g., by means of contractual clauses or binding corporate rules[2187]) or on the basis of specific statutory grounds (e.g., if the individual has consented to the transfer, the transfer is necessary in a specific case to safeguard an overriding public interest, the transfer is necessary in a specific case to protect the life of the data subject, etc.[2188]). The FDPIC has recognised the modernised standard contractual clauses adopted by the European Commission in June 2021[2189] (with some modifications to adapt it to the domestic legal framework) as an instrument that can be used by Swiss data exporters for data transfers to countries without an adequate level of data protection[2190].

1.2. Oversight, enforcement and redress

[2184] Article 16(1) FADP 2020.
[2185] Article 16(1) FADP 2020.
[2186] Annex 1 to the DPO 2022 lists the following countries and territories as adequately protecting personal data: Andorra, Argentina, Austria, Belgium, Bulgaria, Canada (commercial organisations), Croatia, Cyprus, Czech Republic, Denmark, Estonia, Faroe Islands, Finland, France, Germany, Gibraltar, Greece, Guernsey, Hungary, Iceland, Ireland, Isle of Man, Israel, Italy, Jersey, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, Netherlands, New Zealand, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom, Uruguay.
[2187] See Article 16(b) and (e) FADP 2020. In June 2021, in the context of the *Schrems II* judgement, the FDPIC published a "Guide to checking the admissibility of direct and indirect data transfers to third countries", available at: https://www.edoeb.admin.ch/edoeb/en/home/data-protection/handel-und-wirtschaft/transborder-data-flows.html.
[2188] See Article 17 FADP 2020.
[2189] Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.
[2190] See the announcement at: https://www.edoeb.admin.ch/dam/edoeb/en/dokumente/datenschutz/Paper%20SCC%20def.en%2024082021%20(2).pdf.download.pdf/Paper%20SCC%20def.en%2024082021%20(2).pdf.

The independent body in charge of overseeing compliance with the data protection rules by private operators and federal public authorities is the FDPIC[2191]. Whereas, in the past, the head of the FDPIC was appointed by the Federal Council, after which the appointment had to be approved by the Federal Assembly, the FADP 2020 requires that the head is elected directly by the Federal Assembly[2192]. Similarly, under the FADP 2020, (s)he may only be dismissed by the Federal Assembly[2193]. The FDPIC's tasks include advising and assisting controllers on data protection matters, providing opinions on draft legislation that is relevant to data protection, cooperating with domestic and foreign data protection authorities and raising public awareness on data protection[2194]. It is also involved in analysing the impact of quickly developing technologies, such as Artificial Intelligence, on the protection of personal data.[2195] The supervision of data processing by cantonal and communal public authorities is carried out by independent cantonal data protection authorities[2196].

In terms of powers, the FADP 2020 provides that the FDPIC may initiate an investigation on its own initiative or upon request of a third party with respect to both private operators and public authorities[2197]. In carrying out its investigations, the FDPIC has access to any relevant information[2198]. If the data subject has filed a report, the FDPIC shall inform him or her about the steps taken in response and the result of any investigation[2199]. The FDPIC's investigatory and enforcement powers have been strengthened by the FADP 2020. In the past, the FDPIC could issue recommendations and, if such recommendations were not followed, refer the matter to the federal courts (in cases concerning private operators) or the Federal Chancellery/competent Federal Department (in cases concerning federal public bodies) whose decisions could in turn be appealed by the FDPIC before the courts[2200]. Under the FDAP 2020, the FDPIC has the power to compel access to premises and documents[2201] and adopt binding decisions with respect to both private operators and public authorities, including to modify, suspend or terminate processing or destroy personal data[2202]. It will be important that the FDPIC makes full use of these new powers in the future, as they constitute essential aspect of the overall effectiveness of the system.

[2191] The FDPIC is appointed for a term of four years, which may be renewed twice (Article 44(1) FADP 2020). The FADP 2020 provides that the FDPIC exercises its duties independently, does not receive instructions from any authority or third party, has its own budget and appoints its own staff (Article 43(4)-(5) FADP 2020). The FDPIC may not have any other occupation, unless specifically authorised by the Federal Assembly, provided such other occupation does not compromise his/her independence and standing (Articles 46-47 FADP 2020).
[2192] Article 26(1) FADP and Article 43(1) FADP 2020.
[2193] This may only occur in case of serious violations of the duties of office committed wilfully or through gross negligence, or if (s)he is permanently unable to fulfil the duties of office (Article 44(3) FADP 2020).
[2194] See Article 58 FADP 2020.
[2195] 09.11.2023 - Current data protection legislation is directly applicable to AI (admin.ch)
[2196] The cantons have to meet the same requirements in terms of independence as the FDPIC. As explained above, they have to meet the requirements of the Convention 108+ and with respect to data processing in relation to the Schengen cooperation in criminal matters, of the Law Enforcement Directive. All cantonal data protection laws prescribe the creation of independent data protection authorities and provide that these authorities shall be independent in their position and in the performance of their duties.
[2197] Article 49 FADP 2020.
[2198] Article 49(3) and 50(1)(a) FADP 2020.
[2199] Article 49(4) FADP 2020.
[2200] Article 27(4)-(6) (for public authorities) and Article 29(3)-(4) FADP 1992.
[2201] Article 50 FADP 2020.
[2202] Article 51 FADP 2020.

In addition, the Swiss legal framework imposes criminal sanctions (fines) for certain violations of the data protection rules by private operators. The FADP 2020 expanded the list of violations for which fines can be imposed (adding inter alia intentional infringements of the obligations to inform data subjects and cooperate with the FDPIC[2203], violating the duty of care[2204], and failing to comply with a decision of the FDPIC[2205]) and has imposed a maximum amount of CHF 250 000. While such fines are in principle imposed on individuals, the FADP 2020 also foresees the possibility of fining a company, where determining who in the organisation is responsible for the infringement would require disproportionate investigative efforts[2206]. Other Swiss laws, including the Swiss Criminal Code contain further criminal sanctions (custodial sentences or monetary penalties) for violations of the privacy of individuals as well (e.g., obtaining personal data without authorisation)[2207].

As regards the possibility for individuals to obtain redress, different avenues continue to be available in the Swiss system. In particular, individuals can obtain judicial redress before the civil courts (against private operators) and under the Administrative Procedure Act (against public authorities), including by directly enforcing their individual rights[2208], obtaining the termination of unlawful processing[2209], or claiming compensation for damages[2210].

The FDPIC regularly engages "upstream" with data controllers and data processors by advising on data protection matters while projects and IT systems are being developed. This includes working with private operators (e.g., through impact assessments) as well as federal public bodies (e.g., in the context of digitalisation within the federal administration, the use of cloud services and digital projects, such as contact tracing applications, related to the COVID-19 pandemic)[2211]. The FDPIC also plays an active role by advising on data protection issues during the legislative process (e.g., in the context of the recent reform of the FADP).

Since the adoption of the adequacy decision, the FDPIC has also carried out a number of investigations (e.g., into a data breach at a telecommunications provider[2212], the use of GPS data by a music streaming service[2213], the processing of data by a dating application[2214], data practices of insurance companies and financial institutions[2215], etc.). Whereas in some cases, the identified issues were resolved during the investigation, other investigations led to the

[2203] Article 60 FADP 2020.
[2204] Article 61 FADP 2020 lists the relevant breaches of duties of care: a transfer of personal data to third countries in breach of Article 16 FADP 2020 or without meeting the requirements of Article 17 FADP 2020; entrusting a processor with the data processing without meeting the requirements of Article 9 FADP 2020; and non-compliance with the minimum data security requirements adopted by the Federal Council based on Article 8(3) FADP 2020.
[2205] Article 63 FADP 2020.
[2206] Article 64 FADP 2020.
[2207] See e.g., Articles 143, 179[ter] and 179[novies] of the Criminal Code.
[2208] See Article 32 (with respect to private operators) and 41 (with respect to federal public authorities) FADP 2020.
[2209] E.g., pursuant to Article 28a of the Swiss Civil Code.
[2210] Pursuant to Article 41 and 49 of the Swiss Code of Obligations and the Federal Act on the Liability of the Confederation, Members of its Authorities and Officials.
[2211] See e.g., the annual report of the FDPIC of 2020-2021, available at; https://edb.reader.epaper.guru/de-CH/viewer/0d88373a-c278-44f7-9e4c-c80e4d5f1438.
[2212] See FDPIC's 27th Activity Report 2019/20: p. 20.
[2213] See FDPIC's 27th Activity Report 2019/20, p 22.
[2214] See FDPIC's 28th Activity Report 2020/21: p. 20 and 29th Activity Report 2021/22 p. 17.
[2215] https://www.edoeb.admin.ch/dam/edoeb/Empfehlungen-DS/Empfehlung%20Helsana.pdf.download.pdf/Empfehlung%20Helsana.pdf.

adoption of formal recommendations, which were generally followed by the concerned controllers (e.g., in the transportation sector, retail and banking). The FDPIC also referred several cases to the courts where its recommendations had not been followed, e.g., in a case against the Federal Tax Administration[2216].

Finally, the FDPIC has issued a number of guidance documents (e.g., on data subject rights[2217], cross-border data flows[2218], the processing of biometric data[2219], the processing of data for marketing purposes[2220] and technical and organisational measures[2221]). The FDPIC also provides assistance to individuals by answering queries, running a phone helpline and offering model letters which can be used by data subjects to exercise their rights[2222].

2. ACCESS TO AND USE OF PERSONAL DATA TRANSFERRED FROM THE EUROPEAN UNION BY PUBLIC AUTHORITIES IN SWITZERLAND

2.1. General legal framework

The limitations and safeguards that apply to the collection and subsequent use of personal data by Swiss public authorities for criminal law enforcement and national security purposes follow from the overarching constitutional framework, specific laws regulating data access, as well as rules that apply to the processing of personal data.

The Swiss Federal Constitution recognises privacy and the protection of personal data as fundamental rights. Any restrictions of these rights must have a legal basis, must be justified in the public interest or for the protection of the fundamental rights of others, must be proportionate and respect the essence of fundamental rights[2223]. Similar rights and restrictions apply under cantonal constitutions. Pursuant to the Federal Constitution, cantonal constitutions must be compatible with federal law and the latter prevails in case of conflict[2224]. While cantonal constitutions may provide additional protections, they must at least provide for the same rights (and conditions for restrictions) as the Federal Constitution, either by directly referring to the provisions of the Federal Constitution (as is for instance done in Article 10 of the Constitution of the Canton of Zurich) or by providing for their own constitutional guarantees (see e.g., Articles 21 and 43 of the Constitution of the Canton of Geneva). Moreover, all fundamental rights guaranteed by the Federal Constitution apply directly in the entire Swiss legal system and must be respected by all state organs and public bodies at federal, cantonal and communal level[2225].

[2216] See the annual report of the FDPIC 2019-2020.
[2217] https://www.edoeb.admin.ch/edoeb/en/home/datenschutz/grundlagen/auskunftsrecht.html.
[2218]https://www.edoeb.admin.ch/dam/edoeb/en/dokumente/datenschutz/Anleitung%20f%C3%BCr%20die%20Pr%C3%BCfung%20von%20Daten%C3%BCbermittlungen%20mit%20Auslandbezug%20EN.pdf.download.pdf/Anleitung%20f%C3%BCr%20die%20Pr%C3%BCfung%20von%20Daten%C3%BCbermittlungen%20mit%20Auslandbezug%20EN.pdf.
[2219] https://www.edoeb.admin.ch/edoeb/en/home/deredoeb/infothek/infothek-ds.html.
[2220] https://www.edoeb.admin.ch/edoeb/en/home/datenschutz/arbeit_wirtschaft/werbung_marketing.html.
[2221] https://www.edoeb.admin.ch/edoeb/en/home/datenschutz/internet_technologie.html.
[2222] https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/dokumentation/lettres-type/comment-proceder-lorsque-vous-souhaitez-soumettre-une-demande-de.html. For example, according to information received from the FDPIC, it received around 1680 requests in 2021.
[2223] Articles 13 and 36 of the Federal Constitution.
[2224] Article 49 and 51 of the Federal Constitution.
[2225] Article 35 of the Federal Constitution.

In addition, Switzerland is a party to the European Convention on Human Rights (ECHR), which protects the right to respect for private and family life (and the right to the protection of personal data as part of it). According to settled case law in Switzerland, obligations under international law, in particular agreements such as the ECHR that deal with human rights, take precedence over federal legislation in case of a conflict[2226]. Pursuant to Article 8 of the ECHR, a public authority may only interfere with the right to privacy in accordance with the law, in the interests of one of the aims set out in Article 8(2), and if proportionate in light of that aim. Article 8 also requires that the interference is "foreseeable", i.e., has a clear, accessible basis in law, and that the law contains appropriate safeguards to prevent abuse.

Moreover, in its case law, the European Court of Human Rights has specified that any interference with the right to privacy and data protection should be subject to an effective, independent and impartial oversight system that must be provided for either by a judge or by another independent body (e.g., an administrative authority or a parliamentary body)[2227]. Moreover, individuals must be provided with an effective remedy, and the European Court of Human Rights has clarified that the remedy must be offered by an independent and impartial body which has adopted its own rules of procedure, consisting of members that must hold or have held high judicial office or be experienced lawyers, and that there must be no evidential burden to be overcome in order to lodge an application with it. In undertaking its examination of complaints by individuals, the independent and impartial body should have access to all relevant information, including closed materials. Finally, it should have the powers to remedy non-compliance[2228].

Therefore, through its adherence to the European Convention on Human Rights, as well as its submission to the jurisdiction of the European Court of Human Rights, Switzerland is subject to a number of obligations, enshrined in international law, that frame its system of government access on the basis of principles, safeguards and individual rights similar to those guaranteed under EU law and applicable to the Member States.

As described in more detail in sections 2.2.1 and 2.3.1, these general principles are reflected in specific laws that regulate the access and use of personal data for criminal law enforcement and national security purposes.

Moreover, the processing of personal data by Swiss public authorities (including criminal law enforcement and the national security authority) is subject to specific data protection rules.

Federal criminal law enforcement authorities are first of all subject to the FADP 2020, which lays down the conditions under which public authorities may use and disclose personal information; reflects the principles of purpose limitation, data accuracy, transparency and storage limitation; and provides individuals with several rights (see section 1.1 and below). The substantive provisions of the FADP 2020 do not apply to court proceedings or the processing of personal data in pending civil, criminal (including preliminary investigations of

[2226] AFT 125 II 417 E. 4d, AFT 144 I 126.
[2227] European Court of Human Rights, Klass and others v. Germany, Application no. 5029/71, paragraphs 17-51.
[2228] European Court of Human Rights, Kennedy v. the United Kingdom, Application no. 26839/05, (Kennedy), paragraphs 167 and 190.

specific offences by the police and the prosecution)[2229] and international mutual legal assistance proceedings[2230]. In those cases, the processing of personal data and the rights of data subjects are regulated by other statutes, in particular the Civil Procedure Code, Criminal Procedure Code (CrimPC), Criminal Code, International Mutual Assistance in Criminal Matters Act and Administrative Procedure Act[2231]. However, the FDPIC in principle remains competent to supervise compliance by law enforcement authorities with data protection requirements either following from the FADP 2020 (i.e., outside of judicial proceedings) or from those other statutes (i.e., in the context of judicial proceedings)[2232]. The only exceptions (i.e., activities/entities for which the FDPIC is not competent) are the federal courts, the Office of the Attorney General in relation to data processing as part of criminal proceedings[2233] and courts or federal authorities in relation to proceedings for international mutual assistance in criminal matters. In those cases, compliance with applicable data protection requirements is subject to the supervision of courts[2234].

Similarly, the processing of personal data by criminal law enforcement authorities at the cantonal and communal level is subject to cantonal data protection laws and/or the CrimPC , which, as explained in section 1.1, contain key data protection principles, obligations and individual rights, and ensure supervision by an independent data protection authority or, in the context of judicial proceedings, by courts.

The processing of personal data by national security authorities is subject to specific data protection requirements in the Intelligence Service Act and accompanying Ordinances, as well as the FADP 2020, which applies to the extent no specific provisions are foreseen under the Intelligence Service Act. These different legal instruments impose key data protection principles (principles of purpose limitation, data minimisation, accuracy, security), provide individuals with data protection rights and subject the processing of personal data by intelligence agencies to independent oversight.

These safeguards, including corresponding limitations applicable to the criminal law enforcement and national security areas can be invoked by individuals before independent administrative bodies (e.g., the FDPIC, cantonal data protection authorities) and courts to obtain redress (see sections 2.2.4 and 2.3.4).

2.2. Access and use by Swiss public authorities for criminal law enforcement purposes

[2229] Conversely, the processing of personal data in the context of preventive investigations by the police (i.e., prior to an imminent danger or crime) remains fully subject to the FADP 2020, see Ruling A-4186/2015 of the Federal Administrative Court of 28 January 2016.
[2230] Article 2(3) FADP 2020. See also Articles 299-300 of the CrimPC.
[2231] Administrative proceedings at first instance are fully subject to the FADP 2020 (see Article 2(3) FADP 2020).
[2232] Article 4(2) FADP 2020.
[2233] The Office of the Attorney General is excluded from the supervision of the FDPIC in this case because it is considered an independent judicial authority carrying out judicial tasks. As is the case for courts acting in their judicial capacity, subjecting the Office to the supervision of the FDPIC would affect the separation of powers and independence of the judiciary. Since 1 September 2023, the supervision over data processing by the federal courts is guaranteed by the Administrative Commission of the Federal Supreme Court, and with support by the Federal Supreme Court's data protection officer (Supervisory Regulations of the Federal Supreme Court of 12 June 2023).
[2234] At federal level, the Federal Criminal Court is responsible for such oversight, see Article 37(1) Federal Act on the Organisation of Federal Criminal Authorities.

In Switzerland, criminal law enforcement functions are mainly carried out by cantonal and communal authorities, whereas the Federal Office of Police investigates offences falling under federal jurisdiction, such as inter-cantonal or international organised crime (e.g., terrorism and terrorist financing), corruption and money laundering[2235]. Swiss law imposes a number of limitations on the access and use of personal information for criminal law enforcement purposes by each of these authorities and provides oversight and redress mechanisms. The conditions under which such access can take place and the safeguards applicable to the use of those powers are described in the following sections.

2.2.1. Legal bases and applicable limitations/safeguards

Personal data transferred under the adequacy decision and processed by Swiss controllers and processors may be obtained by Swiss criminal law enforcement authorities at federal level by means of investigative measures under the Criminal Procedure Code (CrimPC), or on the basis of anti-money laundering and anti-terrorist financing legislation. At cantonal/communal level, access by Swiss public authorities to personal data transferred under the adequacy decision is, since 2011, also governed by the CrimPC[2236].

The CrimPC provides Swiss criminal law enforcement authorities with a legal basis to access personal data through searches, seizures, surveillance of (the content of and/or the current metadata of) post and telecommunications, and surveillance of financial transactions. It lays down clear and precise rules on the scope and application of these measures, thereby ensuring that the interference with the rights of individuals will be limited to what is necessary for a specific criminal investigation and proportionate to the pursued purpose. Moreover, to exercise these powers, judicial authorisation is in principle required (except for instance in emergencies, as described in more detail below).

As a general requirement, the CrimPC provides that criminal law enforcement authorities must comply with the principle of good faith, may not abuse the rights of others and are prohibited from using methods that violate human dignity when obtaining evidence[2237]. In addition, the use of coercion, threats, promises, deception and methods that may compromise the ability of the persons concerned to decide freely are prohibited, also if the person consents to their use[2238].

In accordance with the CrimPC, as an overarching requirement, any compulsory measure (including a search, seizure or surveillance of post and telecommunications) may only be taken if (1) it is permitted by law, (2) there is a reasonable suspicion that an offence has been committed, (3) the aims cannot be achieved by less stringent measures and (4) the seriousness of the offence justifies the compulsory measure[2239].

A search of a house, dwelling or other not generally accessible premise may only be searched with the consent of the owner, or if it is suspected that there are wanted persons, that there is

[2235] Article 23-24 CrimPC.
[2236] Article 1(1) CimPC. Whereas prior to the enactment of the CimPC, each canton established its own criminal procedure rules, the CrimPC provides for the legal framework at federal, cantonal and communal level (i.e., there are no longer separate criminal procedural rules at cantonal or communal level).
[2237] Article 3(2) CrimPC.
[2238] Article 140 CrimPC.
[2239] Article 197 CrimPC.

forensic evidence or assets that must be seized, or offences are being committed[2240]. A document, recording (audio, video or other), data carrier or equipment for processing and storing information (e.g., a computer) may be searched if it is suspected that it contains information that is liable to seizure (see below, e.g., if it is expected that the information will be used as evidence)[2241]. Procedurally, a search must be authorised by a warrant issued by a public prosecutor or a court[2242]. In case of urgency, a search may be authorised orally, but such authorisation must be confirmed subsequently in writing[2243]. In principle, the proprietor must be present during the search and, as regards searches of documents, recordings, data carriers or processing equipment, has the possibility to comment on the content of the information[2244].

The seizure of items belonging to an accused or a third party may take place if it is expected that the items will be used as evidence; will be used as security for procedural costs, monetary penalties, fines or damages; will have to be returned to persons suffering harm or will have to be forfeited[2245]. Certain items that could be used as evidence may nevertheless not be seized, such as personal records and correspondence belonging to the accused, if the interest in protecting their privacy outweighs the interest in prosecution[2246]. A seizure must be authorised by a warrant issued by a public prosecutor or a court that sets out the grounds for the seizure[2247]. In urgent cases, a seizure may also be ordered orally, in which case the authorisation must be confirmed in writing afterwards[2248]. Where there is a risk in any delay, the police may provisionally seize items on behalf of the public prosecutor or the courts[2249].

Specific substantive and procedural limitations apply to the use of covert surveillance measures (i.e., monitoring/interception of post and telecommunications, including e-mails, communications via the internet, etc.)[2250]. Covert surveillance may only be ordered by the public prosecutor (1) if there is a strong suspicion that certain specific offences (e.g., murder, serious assault, fraud, extortion, human trafficking, crimes related to narcotics, nuclear energy or weapons, etc.[2251]) have been committed, (2) the seriousness of the offence justifies the surveillance and (3) other investigative activities have been unsuccessful, or the investigation

[2240] Article 244 CrimPC.
[2241] Article 246 CrimPC.
[2242] Articles 198(1) and 241(1) CrimPC. The warrant must indicate the premises, property or records to be searched; the purpose of the measure and the authorities or persons authorised to conduct the search (Article 241(2) CrimPC).
[2243] Article 241 CrimPC.
[2244] Article 245(2) and 247(1) CrimPC.
[2245] Article 263(1) CrimPC.
[2246] Article 264 CrimPC.
[2247] Articles 198(1) and 263(2) CrimPC.
[2248] Article 263(2) CrimPC.
[2249] Article 263(3) CrimPC.
[2250] Criminal law enforcement authorities may also, upon request, obtain subscriber information (e.g., the name, date of birth and address of the subscriber, as well as the type of services to which (s)he subscribed, see Article 21 SPTA) from the Post and Telecommunications Surveillance Service (see below) for the purpose of carrying out their tasks (Article 15 SPTA). The same applies if it is suspected that a criminal offence has been committed via the internet, in which case telecommunication providers are required to provide the Service with information necessary to identify the perpetrator (which may in turn be obtained by criminal law enforcement authorities), see Article 22 SPTA.
[2251] See the list in Article 269(2) CrimPC, read in conjunction with the Criminal Code.

would otherwise have no prospect of success or would be made unreasonably complicated[2252]. Only the communications of the accused may be monitored, or of a third party if there is reason to believe based on specific information that the accused uses the communication service of the third party or the latter receives/transmits communications on behalf of the accused[2253]. A public prosecutor may also request metadata relating to telecommunications[2254] (1) if there is a strong suspicion that a felony or misdemeanour has been committed, (2) the seriousness of the offence justifies the request and (3) other investigative activities have been unsuccessful, or the investigation would otherwise have no prospect of success or would be made unreasonably complicated[2255]. Metadata may be requested for the six months prior to the date of the request[2256].

Procedurally, the use of covert surveillance or the collection of metadata relating to telecommunications must first be ordered by a public prosecutor and must subsequently be authorised by a court (the Compulsory Measures Court)[2257]. In particular, within 24 hours of ordering the surveillance or release of information, the public prosecutor must inform the Compulsory Measures Court of the order and the reasons therefor (and provide relevant documentation)[2258]. The court must decide within 5 days to grant or refuse the authorisation, and may impose a time limit or other conditions, or request further information or investigations[2259]. An authorisation may be issued for a maximum of three months, with a possibility to extend for periods of three months at a time, again upon authorisation of the Court[2260]. The public prosecutor must stop surveillance immediately if the abovementioned requirements are no longer fulfilled or the authorisation or its extension is refused[2261]. Documents and data carriers obtained through unauthorised surveillance activities must be

[2252] Article 269 CrimPC. If these requirements are met and previous surveillance measures have been unsuccessful or would be futile or disproportionately difficult, the public prosecutor may also order the use of special technical devices (to listen to or record conversations, identify a person/property or determine their location), see Article 268bis CrimPC. Similarly, under the same conditions and for the investigation of specific offences listed in Article 286(2) CrimPC, the public prosecutor may order the introduction of special software into a data processing system to intercept and recover the content of communications and telecommunications metadata (Article 269ter CrimPC). In this case, the order of the public prosecutor must specify the desired data types and the non-public spaces that may have to be entered to introduce the software system. Any data collected using such software that does not meet the abovementioned conditions must be destroyed immediately. See Article 269ter CrimPC.

[2252] I.e., the data that indicates with whom, when, for how long, and from where the person under surveillance is or has been communicating, as well as the technical characteristics of the communication concerned (secondary telecommunications data), see Article 273(1) CrimPC in conjunction with Article 8(b) Federal Act on the Surveillance of Post and Telecommunications (SPTA).

[2253] Article 270 CrimPC.

[2254] I.e., the data that indicates with whom, when, for how long, and from where the person under surveillance is or has been communicating, as well as the technical characteristics of the communication concerned (secondary telecommunications data), see Article 273(1) CrimPC in conjunction with Article 8(b) SPTA.

[2255] Article 273(1) CrimPC.

[2256] Article 273(3) CrimPC.

[2257] Article 272(1) and Article 273(2) CrimPC.

[2258] Article 274(1) CrimPC.

[2259] Article 274(2) CrimPC. The decision of the court must contain a brief statement of the reasons. If enquiries reveal that the person under surveillance is changing his or her telecommunications connection regularly, the Compulsory Measures Court may, by way of exception, authorise the surveillance of all identified connections used by the person under surveillance so that the authorisation is not required in each individual case (general authorisation), see Article 272(2) CrimPC.

[2260] Article 274(5) CrimPC.

[2261] Article 275(1) CrimPC.

destroyed immediately and the results of unauthorised surveillance operations may not be used[2262].

The surveillance of post and telecommunications is carried out with the assistance of the Post and Telecommunications Surveillance Service (PTSS), which is administratively assigned to the Federal Department of Justice and Police but performs its tasks autonomously[2263]. The PTSS operates a processing system in which it receives data requested by law enforcement authorities (in accordance with the abovementioned procedure) from telecommunication providers and makes it available to the relevant authorities[2264]. The PTSS must keep documentation on inter alia the requests it has received, related authorisations, confirmations from the providers required to cooperate about the surveillance carried out, etc.[2265]. In addition, it is required to publish annual statistics about surveillance carried out, including the measures that were used, the type of offences that were being investigated, the authorities requesting the surveillance, the duration of the surveillance and the nature of the information that was collected[2266].

Individuals subject to surveillance must be notified thereof (as well as of the reason for, type of and duration of the surveillance) by the public prosecutor at the latest when the preliminary proceedings (i.e., the police inquiry and the investigation by the prosecutor[2267]) are concluded[2268]. This notification may only be deferred or dispensed with upon the authorisation of the Compulsory Measures Court, if the findings are not used as evidence in court proceedings and deferring or dispensing with notice is necessary to protect overriding public or private interests[2269].

Pursuant to the CrimPC, the Compulsory Measures Court may also, at the request of the public prosecutor, order the surveillance of banking transactions[2270], in order to investigate felonies or misdemeanours. The account holder must in this case be notified under the same conditions as described above for the surveillance of communications[2271].

Finally, criminal law enforcement authorities may also indirectly receive personal data from the Swiss Money Laundering Reporting Office, under the Anti-Money Laundering Act (AMLA)[2272]. The AMLA requires financial intermediaries (e.g., banks, investment

[2262] Article 277 CrimPC. This has been confirmed in decisions of the Federal Supreme Court, e.g., ATF 144 IV 254 and ATF 145 IV 42.
[2263] Article 3 SPTA.
[2264] Article 7 SPTA. The system inter alia contains the content of communications of individuals under surveillance, as well as data indicating with whom, when, for how long and from where individuals under surveillance have been communicating. It is made available to law enforcement authorities by granting them access to the data in the system, or by transmitted it securely to them. See Article 8-9 SPTA.
[2265] Article 9 Ordinance on the Surveillance of Post and Telecommunications (SPTO).
[2266] Article 12 and 13 SPTO
[2267] Article 299(1) CrimPC.
[2268] Article 279(1) CrimPC.
[2269] Article 279(2) CrimPC. The CrimPC does not define the meaning of "overriding public or private interests". According to legal doctrine, overriding public interests exist when it is necessary to postpone or waive the notification for internal or external security or to combat organised crime. Overriding private interests exist in particular if the notification would expose a third party to a serious risk. However, the omission of the notification must be a rare exception (JEAN-RICHARD-DIT-BRESSEL MARC, in: NIGGLI/HEER/WIPRÄCHTIGER (Hrsg.), Basler Kommentar, Strafprozessordnung, 2. Aufl. 2014, N 8 zu Article 279 StPO).
[2270] Article 284 CrimPC.
[2271] Article 284(3) CrimPC.
[2272] Federal Act on Combating Money Laundering and Terrorist Financing of 10 October 1997 (SR 955.0).

companies, insurance institutions, securities firms, payment systems, etc.[2273]) as well as dealers (natural/legal persons that deal in goods commercially and in doing so accept cash)[2274] to report assets or cash payments for which there are reasonable grounds to suspect that they are connected to money laundering or terrorist financing to the Money Laundering Reporting Office[2275]. Similarly, authorities that are charged with the supervision of financial intermediaries (e.g., the Financial Market Supervisory Authority, the Federal Gaming Board) are also required to report to the Reporting Office if they have reasonable grounds to suspect that a money laundering or terrorist financing offence has been committed[2276]. The Reporting Office is located in the Federal Office of Police and acts as a relay point between financial intermediaries and law enforcement authorities. It must immediately notify the responsible prosecution authority if it has reasonable doubts that an offence relating to money laundering or terrorist financing has been/is being committed[2277]. The information received from the Reporting Office can only be processed by a criminal law enforcement authority in accordance with the requirements described below in section 2.2.2.

2.2.2. Further use of the information collected

The processing of personal data by federal and cantonal criminal law enforcement authorities in the context of criminal investigations/proceedings is subject to specific data protection rules laid down in the CrimPC and Criminal Code. As a general requirement, the CrimPC provides that personal data must be obtained from the individual concerned or with their knowledge, unless the proceedings would otherwise be prejudiced, or unreasonable inconvenience or expense would be incurred[2278]. If personal data is obtained without the knowledge of the individual, (s)he must be notified immediately, although such notification may be dispensed with or postponed where necessary for overriding public or private interests. When processing personal data, law enforcement authorities must distinguish between different categories of data subjects and between personal data based on facts and personal data based on personal assessments[2279].

The CrimPC also imposes the principle of data accuracy[2280], as well as limitations on the further use and disclosure of data in pending criminal proceedings[2281]. In particular, personal data from pending criminal proceedings may in principle only be disclosed for use in other pending proceedings if there are grounds for assuming that the data will make a significant contribution to the clarification of the facts[2282]. In some cases however, criminal law enforcement authorities are obliged to disclose such personal data on the basis of other statutes[2283], i.e., to the Federal Intelligence Service (in order for the Service to carry out its

[2273] Article 2(2) AMLA.
[2274] Article 2(1) AMLA.
[2275] Article 9 AMLA. The Reporting Office may require additional information from financial intermediaries to analyse their reports (Article 11a AMLA).
[2276] Article 16(
[2277] Article 23(4) AMLA.
[2278] Article 95 CrimPC.
[2279] Article 95a CrimPC.
[2280] Article 98 CrimPC.
[2281] Article 96 CrimPC.
[2282] Article 96(1) CrimPc. Data should therefore neither be requested nor transmitted if it is not necessary for the clarification of the facts, e.g., preventive data collection, see Basler Kommentar zur Strafprozessordnung, 2. Aufl. 2014, Bd. 2, N 21.
[2283] Article 96(2) CrimPc.

tasks, see below section 2.3.1); in response to requests from individuals exercising their right of access with respect to different police information systems (e.g., the Schengen Information System); and to criminal police central offices (in charge of the fight against organised international crime) upon their request. In terms of data retention, the CrimPC provides that, after the conclusion of proceedings, case documents must be preserved at least until conclusion of the time limits for prosecution and for the execution of the sentence have expired[2284].

In the context of administrative assistance on police matters or mutual legal assistance cooperation, the sharing of personal data with third country (i.e., non-Schengen) law enforcement authorities or international organisations is subject to specific limitations. In particular, such sharing may not take place if this would seriously endanger the privacy of individuals, in particular due to a lack of adequate protection[2285]. Adequate protection may be ensured by the legislation of a third country (if the country benefits from an adequacy decision adopted by the European Commission), an international treaty or specific guarantees[2286]. Exceptionally[2287], personal data may also be disclosed if necessary in a particular case (1) to protect the life or physical integrity of an individual, (2) to prevent imminent serious danger threatening the public security of a Schengen or a third country, (3) to prevent, detect or prosecute a criminal offence, provided that disclosure does not conflict with the overriding legitimate interests of the individual, or (4) to exercise or enforce legal claims against a criminal law enforcement authority, provided that disclosure does not conflict with the overriding legitimate interests of the individual[2288].

The processing of personal data by criminal law enforcement authorities outside of criminal proceedings (e.g., in the context of a preventative investigation or once criminal proceedings are concluded) is subject to the FADP 2020 (for federal law enforcement authorities) and cantonal data protection laws (for cantonal law enforcement authorities)[2289]. For federal criminal law enforcement authorities, the FADP 2020 contains requirements on inter alia purpose limitation, data accuracy, transparency, storage limitation and data security, as

[2284] Article 99(2), in conjunction with Article 103 CrimPC. Specific data retention requirements also apply to data processed by the PTSS in its processing system. Different retention periods apply depending on the type of investigation (e.g., request for mutual legal assistance, search for a missing person) and type of data collected (e.g., data collected in the context of mobile phone localisation), see Article 11 SPTA.
[2285] Article 349c(1) Criminal Code and Article 11f(1) International Mutual Assistance in Criminal Matters Act.
[2286] Article 349c(2) Criminal Code and Article 11f(2) International Mutual Assistance in Criminal Matters Act. In the context of administrative police cooperation, federal authorities are moreover required to inform the FDPIC of the categories of disclosures made on the basis of specific guarantees (Article 349c(3) Criminal Code).
[2287] In the context of administrative assistance, a Swiss authority may exceptionally also disclose data to another recipient than a law enforcement authority in a third country where, in particular cases of emergency, it is not possible to disclose personal data to the competent authority of a third country through the normal channels of police cooperation, if the disclosure is essential to fulfil its statutory task and no overriding interests of the data subject worthy of protection stand in the way of disclosure (Article 349e(1) Criminal Code). In this case, the Swiss authority is obliged to inform the recipient that the data may only be used for the purposes specified by the authority and to inform the competent authority of the third country (Article 349e(2)-(4) Criminal Code). Federal criminal law enforcement authorities are again required to inform the FDPIC of such disclosures without delay and to document each disclosure of personal data (Article 349*e*(5) Criminal Code).
[2288] Article 349c(4) Criminal Code and Article 11f(3) International Mutual Assistance in Criminal Matters Act. Pursuant to Article 349c(5) Criminal Code, federal criminal law enforcement authorities are again required to inform the FDPIC when relying on these grounds for international data sharing in the context of administrative cooperation.
[2289] See also Article 99(1) CrimPC.

described in more detail in section 1.1 As regards the sharing of personal data with third countries, the requirements for international transfers of personal data of the FADP 2020 apply. As explained in section 1.1, ssimilar obligations apply under cantonal data protection laws.

2.2.3. Oversight

The activities of Swiss criminal law enforcement authorities are supervised by different bodies.

The FDPIC supervises compliance by the federal police with the FADP 2020 and other federal data protection regulations[2290]. In particular, whereas in the past, the supervisory powers of the FDPIC only covered the processing of personal data by the federal police outside pending criminal proceedings, the FADP 2020 has extended them to all data processing by the federal police (whether before, during or after criminal proceedings). Depending on the stage of the investigation/proceedings, the FDPIC will oversee compliance with the FADP 2020 (e.g., in preventative investigations or once criminal proceedings have ended) or with the data protection provisions of the CrimPC and Criminal Code (e.g., during the criminal investigation, court proceedings and in the context of international mutual legal assistance cooperation). In exercising its supervisory role, the FDPIC can make use of all of its investigatory and remedial powers, as described in section 1.2. Compliance of the processing of personal data by the federal public prosecutor with the FADP 2020 (outside of pending criminal proceedings) and the data protection requirements of the CrimPC and Criminal Code (during criminal proceedings) is supervised by the FDPIC and the Federal Criminal Court respectively[2291]. Compliance of data processing by cantonal police and prosecutors with cantonal data protection laws (for data processing outside of criminal proceedings) and the CrimPC and Criminal Code (during criminal proceedings) is supervised by cantonal data protection authorities and courts respectively.

The activities of the federal public prosecutor are subject to independent oversight by a Supervisory Authority that may issue general instructions to the public prosecutor on the performance of its duties and monitor compliance with those instructions[2292]. It may carry out inspections and obtain information from the public prosecutor[2293]. If the Supervisory Authority finds that the public prosecutor or a deputy has breached official duties, it may take disciplinary measures (warnings, reprimands, wage reductions) and, if it considers that conditions for impeachment are met, submit a request for removal from office to the Federal

[2290] Article 4(1) FADP 2020.
[2291] Article 4(2d) FADP 2020 and Article 37(1) Federal Act on the Organisation of Federal Criminal Authorities.
[2292] The Supervisory Authority consists of seven members elected by the Federal Assembly (one judge of the Federal Supreme Court, one judge of the Federal Criminal Court, two lawyers registered at cantonal level and three professionals that do not belong to one of the other categories), see Article 23 Federal Law on the Organisation of Federal Criminal Authorities. The members may not be members of the Federal Assembly or Federal Council and may not be employed by the government (Article 24 Federal Law on the Organisation of Federal Criminal Authorities-. They are appointed for four years and may only be dismissed by the Federal Assembly in case of intentional or grossly negligent serious breach of official duty, or permanent loss of the ability to exercise the office (Article 26 Federal Law on the Organisation of Federal Criminal Authorities).
[2293] Article 29-30 Federal Law on the Organisation of Federal Criminal Authorities.

Assembly[2294]. Similar oversight bodies that supervise the activities of cantonal public prosecutors exist at cantonal level.

Finally, activities of federal law enforcement authorities related to state security are subject to parliamentary oversight by the Control Delegation (CDel) of the Federal Assembly, which consists of three members of the House of Representatives (National Council) and three members of the Senate (Council of States) [2295]. The CDel oversees the legality, expediency and effectiveness of such activities[2296]. In carrying out its oversight tasks, the CDel has unrestricted access to information, including secret intelligence information[2297]. According to the "Action principles of the Control Delegation" developed by the CDel itself[2298], it may request reports, carry out regular inspections/investigations and on-site visit, etc. As a result of an investigation, the CDel can issue recommendations[2299].

2.2.4. Redress

The Swiss system offers different avenues to obtain redress, including compensation for damages.

First, individuals can exercise different rights against criminal law enforcement authorities.

While criminal proceedings are pending, individuals have, in accordance with their right to inspect case documents, the right to information on personal data relating to them that has been processed[2300]. This applies to parties to the proceedings, as well as third parties adversely affected by procedural acts[2301]. The provision of information can only be restricted if there is a justified suspicion that the individual is abusing his or her rights or if necessary to safeguard public or private interests in preserving confidentiality[2302]. In this case, the information must be granted retrospectively and in a suitable form, as soon as the reason for the restriction no longer exists[2303].

After the conclusion of criminal proceedings, individuals can exercise their rights under the FADP 2020 and cantonal data protection laws[2304]. Under the FADP 2020, individuals have a right of access, correction, erasure, as well as a right to object, including vis-à-vis criminal

---

[2294] Article 31 Federal Law on the Organisation of Federal Criminal Authorities, as well as Article 16, 17 and 19 Ordinance of the Federal Assembly on the organisation and tasks of the supervisory authority over the Office of the Attorney General of Switzerland.
[2295] Article 81 IntelSA and Article 53 Act on the Federal Assembly.
[2296] Article 52(2) Act on the Federal Assembly.
[2297] See Article 169(2) of the Federal Constitution, which provides that secrecy rules do not apply to special delegations of supervisory committees established by law.
[2298] Principes d'action de la Délégation des Commissions de gestion, avalable at: https://www.parlament.ch/centers/documents/fr/gpdel-handlungsgrundsaetze-f.pdf.
[2299] Article 158 Act on the Federal Assembly.
[2300] Article 97 CrimPC and Article 10 SPTA. Parties to the case may always inspect documents relating to the proceedings, whereas third parties may do so if they have an academic or other legitimate interest in doing so and inspection is not contrary to any overriding public or private interests (Article 101 CrimPC).
[2301] Article 105(1f) CrimPC. This right is not granted to third parties whose personal data appears in the files. However, based on Article 95(2) CrimPC these persons must as a rule be actively informed about the acquisition of their personal data.
[2302] Article 108(1) CrimPC.
[2303] Article 108(5) CrimPC.
[2304] Article 99(1) CrimPC.

law enforcement authorities[2305]. A request for access to data may be refused, restricted or delayed if (1) this is necessary to satisfy overriding public interests, in particular Switzerland's internal or external security, or (2) providing the information may compromise an enquiry, an investigation or administrative or judicial proceedings[2306]. Case law has clarified that whether such a limitation to the right of access can be applied must be assessed on a case-by-case basis, on the basis of the concrete circumstances of a case[2307]. A refusal to provide information must be limited to what is absolutely necessary and restrictions must be subject to a balancing of interests (i.e., the existence of a public interest cannot in itself justify a restriction)[2308]. Moreover, the reasons for applying a restriction must be provided in reply to the individual by the relevant public authority, which carries the burden of proof that a restriction is justified[2309]. In response to a request for deletion, a federal law enforcement authority may, instead of deleting the data, restrict its processing if this is necessary for an overriding public interest (in particular Swiss internal or external security) or deleting the data may jeopardise an enquiry,

If an individual is not satisfied with the response to his/her request, (s)he can lodge a complaint before the FDPIC, which can make use of its different enforcement powers as described in section 1.2. Moreover, the reply from a federal criminal law enforcement authority to a request to exercise individual rights constitutes a ”ruling” that can be appealed before the Federal Administrative Court in accordance with the Administrative Procedure Act (APA)[2310]. In particular, an individual may for instance argue that their discretionary powers have been exceeded or abused, that the decision is inadequate, or that there has been an incorrect/incomplete determination of the legally relevant facts of the case[2311]. The Federal Administrative Court may amend the contested decision if it violates federal law or is based on an incorrect or incomplete determination of the facts of the case[2312].

With respect to personal data processed in police information systems or in the context of international administrative assistance on police matters (within the framework of the application of the Schengen acquis), individuals are also provided with an indirect avenue to exercise their rights (introduced in the Swiss legal framework as a result of the implementation of the Law Enforcement Directive). In particular, while the police may defer providing access to information processed in police information systems if there are overriding interests related to criminal prosecution that require maintaining secrecy[2313], it must notify the individual about his or her right to request the FDPIC to check whether any data relating to him or her is being processed lawfully and whether overriding interests in

[2305] Articles 25, 37 and 41 FADP 2020
[2306] Article 26(2)(b) FADP 2020.
[2307] Decision of the Federal Supreme Court 4A_125/2020 of 10 December 2020, cons. 3.4.4 and decision of the Federal Administrative Court A-4725/2020 of 1 February 2023, cons. 8.4.2
[2308] See e.g., decision of the Federal Supreme Court ATF 147 II 408, cons. 2.3 and decisions of the Federal Administrative Court A-4806/2023 of 2 June 2023, cons. 4.2 and decision A-7307/2008 of 14 April 2009, cons. 6.3; decision of the Federal Court ATF 141 III 119, cons. 7.1.1 and decision of the Federal Administrative Court A-4725/2020 of 1 February 2023, cons. 7.4.1 and 8.4.
[2309] See e.g., decision of the Federal Administrative Court A-4715/2020 of 23 November 2022, cons. 5.3.3; decisions A-4277/2021 of 1 February 2023, cons. 5.9 and A-4806/2021 of 2 June 2023, cons. 6.3.
[2310] Article 5 APA.
[2311] Article 49 APA.
[2312] Article 62 APA.
[2313] Article 8(1)(b) Federal Law on the Federal Police Information Systems.

secrecy justify the postponement[2314]. Following an audit, the FDPIC informs the individual (through a standard reply) that either no data about him or her is being processed unlawfully or that, in the event of errors in the processing of personal data, an investigation under the FADP 2020 will be opened[2315]. If the individual demonstrates that it is likely that the postponement of the response will seriously and irreparably harm him/her, the FDPIC can order the police to immediately and exceptionally provide the information requested, provided that this does not constitute a threat to internal or external security[2316].

Similarly, an individual may request the FDPIC to check whether any data relating to the data subject is being processed lawfully by competent law enforcement authorities in Switzerland in the context of administrative assistance on police matters[2317] (i.e., with other Schengen countries or with non-Schengen countries) if his/her request to obtain access, correction or deletion is restricted, deferred or refused[2318]. After carrying out an audit, the FDPIC informs the individual (using a standard formulation) that either no data about him or her is being processed unlawfully or that an investigation under the FADP 2020 has been opened[2319]. In the context of an investigation, the FDPIC can make use of all of its enforcement powers provided by the FADP 2020.

In addition, individuals are granted rights of access, correction, deletion and objection against cantonal and communal criminal law enforcement authorities under cantonal data protection laws, which can be enforced before cantonal data protection authorities and courts.

Second, individuals can lodge complaints before different bodies concerning the processing of their data by criminal law enforcement authorities under the FADP 2020. Anyone that has a legitimate interest (i.e., whose data is being processed[2320]) may request a criminal law enforcement authority to (1) stop unlawful processing of personal data, (2) redress the consequences of the unlawful processing or (3) declare the processing to be unlawful[2321]. The response from a public authority to such a request can be challenged by the individual (e.g., arguing that the decision is inadequate or that discretionary powers have been abused) before the Federal Administrative Court[2322], which may may amend the contested decision if it violates federal law or is based on an incorrect or incomplete determination of the facts of the case[2323]. Moreover, any individual may lodge a complaint before the FDPIC or cantonal data protection authorities about compliance with the FADP 2020, data protection provisions in criminal (procedural) rules (e.g., the Criminal Code, CrimPC), and/or cantonal data protection rules. The FDPIC and cantonal data protection authorities may make use of all of their various investigatory and enforcement power, as described in section 1.2. Any decision of the FDPIC

[2314] Article 8(2) Federal Law on the Federal Police Information Systems.
[2315] Article 8(3) Federal Law on the Federal Police Information Systems.
[2316] Article 8(7) Federal Law on the Federal Police Information Systems.
[2317] For instance, if personal data is exchanged in the context of searches of persons or missing objects. Personal data obtained through other compulsory measures, such as surveillance of communications, is not exchanged in the context of administrative assistance but under mutual legal assistance legislation/agreements.
[2318] Article 349g(1) Criminal Code.
[2319] Article 349g(3) Criminal Code. This notification may not be contested by the individual (Article 349g(5) Criminal Code).
[2320] See the case law of the Federal Supreme Court, e.g., TF, 1C_377/2019.
[2321] Article 41 FADP 2020.
[2322] Article 25a(2), in conjunction with Article 5 and 49 APA.
[2323] Article 62 APA.

can be challenged before the Federal Administrative Court, whose decisions can in turn be challenged before the Federal Supreme Court.

Third, in the context of criminal proceedings, individuals may file an objection before an "objections authority"[2324] against any "ruling" by the federal police, the public prosecutor, federal courts of first instance and the Compulsory Measures Court (e.g., on the authorisation of a search, seizure or collection of communications)[2325]. An objection may for instance concern an infringement of the law (e.g., an unlawful disclosure of personal data, or a rejection to a request for access to information), including exceeding and abusing discretionary powers, or a decision that is inequitable[2326]. In response to an objection, a court may inter alia issue a new decision, quash the contested decision, or award reasonable compensation and reparation (if compulsory measures were applied unlawfully)[2327].

Fourth, any individual that has an interest worthy of protection may request an injunction from a federal public authority that is responsible for acts based on federal law that affect rights or obligations (including a criminal law enforcement authority), i.e., that it (1) refrains from, discontinues or revokes unlawful acts, (2) rectifies the consequences of unlawful acts or (3) confirms the illegality of such acts[2328]. The response from a public authority to such a request is considered a "ruling" that can be challenged by the individual (e.g., arguing that the ruling/decision is inadequate or that discretionary powers have been abused) before the Federal Administrative Court[2329], which may may amend the contested decision if it violates federal law or is based on an incorrect or incomplete determination of the facts of the case[2330].

Fifth, any individual may obtain compensation for damage caused by federal public authorities (including criminal law enforcement authorities) on the basis of the Federal Act on the Liability of the Confederation, Members of its Authorities and Officials[2331]. The state will be held liable for damage caused by an unlawful activity by a civil servant in the performance of his/her duties, regardless of the culpability of that civil servant[2332]. All cantons have enacted similar laws on state liability[2333].

Finally, after exhausting domestic remedies, any individual may obtain judicial redress before the European Court of Human Rights concerning the collection and use of their data by Swiss criminal law enforcement authorities.

2.3. Access and use by Swiss public authorities for national security purposes

[2324] Article 20 CrimPC. At federal level, this is the Federal Criminal Court (Article 37(1)) Federal Act on the Organisation of Federal Criminal Authorities). Each canton similarly assigns this role to a court at cantonal level.
[2325] Article 393(1) CrimPC. This possibility is also explicitly provided for in the CrimPC with respect to the collection of communications, see Article 279(3) CrimPC. In this case, the CrimPC provides that the time limit for filing an objection (in principle 10 days) only starts to run once the individual is notified of the measure.
[2326] Article 393(2) CrimPC.
[2327] Article 397 and 431(1) CrimPC.
[2328] Article 25a APA.
[2329] Article 25a(2), in conjunction with Article 5 and 49 APA.
[2330] Article 62 APA.
[2331] Article 3 Federal Act on the Liability of the Confederation, Members of its Authorities and Officials.
[2332] Article 3(1) Federal Act on the Liability of the Confederation, Members of its Authorities and Officials.
[2333] See e.g., BS, Law on the Liability of the State and its Personnel of 17 November 1999 or GR, State Liability Act of 5.12.2006 or FR, Loi sur la responsabilité civile des collectivités publiques et de leurs agents of 16.09.1986).

In Switzerland, the main authority competent to collect personal data for national security purposes is the Federal Intelligence Service (FIS)[2334]. There are no intelligence agencies at cantonal level, but each canton must designate an authority to work with the FIS, which may issue assignments to such an authority[2335]. The legal framework in which the FIS and cantonal authorities carrying out national security assignments[2336] operate is laid down in the Intelligence Service Act (IntelSA), complemented by three Ordinances: the Ordinance on the Federal Intelligence Service (FISO), the Ordinance on the FIS Information and Storage Systems (ISSO-FIS) and the Ordinance on the Supervision of Intelligence Activities (OSIA).

2.3.1. Legal bases and applicable limitations/safeguards

On the basis of the IntelSA, the FIS may access personal data transferred from the EU to Switzerland (including while in transit) as part of different activities, subject to specific limitations and safeguards.

The FIS may collect information (including personal data) for the following purposes: (1) the early recognition and prevention of threats to internal or external security resulting from certain activities (terrorism; espionage; the proliferation of nuclear, biological or chemical weapons; violent extremism and attacks on critical infrastructures[2337]); (2) to identify, observe and assess events outside Switzerland that are of security-policy significance; (3) to safeguard Switzerland's capacity to act; and (4) to safeguard other important national interests (i.e., the basis constitutional order in Switzerland; Swiss foreign policy; or Switzerland as a location for employment, business and finance[2338]) in the event of a serious and immediate threat, where the Federal Council has issued a specific mandate to do so[2339]. The FIS may not gather or process any information relating to political activities or the exercises of freedom of speech, assembly or association in Switzerland except if there are specific indications that a

[2334] In addition, the Swiss army has an intelligence service – the Army Intelligence Service (AIS) – that may search for and evaluate information about foreign countries that is of importance to the army, in particular from the perspective of national defence, peace promotion and foreign support (e.g., providing humanitarian aid), see Article 99(1) Army Act. The AIS may process personal data necessary for an engagement of the army for specific purposes, i.e., to protect military personnel, infrastructure and sources from activities that pose a threat to security; to verify access to information necessary for the performance of its tasks; or to recognise events abroad that are important for Switzerland's security policy (Article 8 Ordinance on the Army Intelligence Service). To carry out its mission, the AIS may use radio exploration, in accordance with the Intelligence Service Act and its accompanying Ordinances (Article 99(1bis) Army Act), see in more detail below. The AIS does not carry out cable intelligence. The activities of the AIS are subject to oversight by the same bodies as those that supervise the FIS (see below).

[2335] Article 9 IntelSA. Such assignments are issued in writing. To carry out an assignment, the cantons may collect personal data to be shared with the FIS but may not establish their own databases to process data under the IntelSA (Article 46 and 85 IntelSA). The FIS is responsible for ensuring proper internal oversight within the cantons when they carry out tasks under the IntelSA (Article 75 IntelSA). When carrying out tasks under the IntelSA, cantonal authorities are also subject to independent oversight by specialised federal administrative and parliamentary bodies, see in more detail section 2.3.3. In addition, the cantons may establish their own supervisory authorities competent to oversee compliance with the IntelSA (Article 82 IntelSA).

[2336] Further references to the FIS in this section also include cantonal authorities carrying out an assignment for the FIS.

[2337] I.e., information, communication, energy, transport and other infrastructures that are essential for the proper functioning of society, the economy and the state (Article 6(1)(a)(4) IntelSA).

[2338] See Article 6(1)(d) in conjunction with Article 3 IntelSA.

[2339] Article 6(1) IntelSA.

person is exercising these rights in order to prepare for or carry out terrorist, espionage or violent activities[2340].

As a general principle applicable to all FIS collection activities, the IntelSA provides that, in each case, the FIS must choose the measure that (1) is most suitable and necessary for achieving a specific information gathering objective and (2) causes the least interference with the fundamental rights of the persons concerned[2341].

The FIS may collect information (including personal data) in Switzerland without specific external authorisation when gathering it from public sources, carrying out observations in public and generally accessible places, or when using human sources as well as in cases of issuing alerts regarding individuals and property[2342]. By contrast, the following information gathering measures require prior authorisation: surveillance of post and telecommunications[2343]; the use of special technical devices to monitor telecommunications, record transmissions or identify a person/object or ascertain their location (which may only be carried out if other surveillance techniques have been unsuccessful, would be without prospect of success or would be unreasonably difficult); the use of localisation devices; the use of monitoring devices to listen to and record conversations in non-public places; the intrusion into computer systems and networks; and the search of premises, vehicles or storage facilities[2344].

Such measures may only be carried out if there is a specific threat to the internal or external security of Switzerland[2345], the seriousness of the threat justifies the measure, and intelligence investigations so far have been unsuccessful or would be without prospect of success or unreasonably difficult[2346]. In terms of procedural safeguards, the FIS must first obtain authorisation of the Federal Administrative Court and, subsequently, clearance of the Head of the Federal Department of Defence, Civil Protection and Sport (DDPS)[2347]. An authorisation of the Court is valid for a maximum of three months and can be extended by a further Federal

[2340] Article 5(5)-(6) IntelSA.
[2341] Article 5(2) IntelSA.
[2342] Articles 13-16 IntelSA. See also Annual Report 2022 of the Independent Oversight Authority for Intelligence Activities OA-IA, p. 12
[2343] Article 26 IntelSA. For the surveillance of post and telecommunications, the FIS also relies on the assistance of the PTSS, as is the case for criminal law enforcement authorities (see section 2.2.1).
[2344] Article 26(1) IntelSA.
[2345] I.e., if a significant legal interest such as the life and limb or the liberty of persons or the existence and functioning of the state is affected and the threat comes from terrorism, espionage, anti-bribery and corruption proliferation or the illegal trade in radioactive substances, ware material and other armaments, or an attack on critical infrastructure. In addition, in the event of a serious and immediate threat, this may, when mandated by the Federal Council, include the protection of the basis constitutional order in Switzerland, the support of Swiss foreign policy or the protection of Switzerland as a location for employment, business and finance. See Article 27(1)(a), in conjunction with Article 19(2)(a)-(d) and 3 IntelSA.
[2346] Article 27(1) IntelSA. These measures may be used against a third party if there is reason to believe that the person from whom the information will be gathered is using premises, vehicles or storage facilities belonging to the third party or is using the third party's postal addresses, telecommunication connection points, computer systems or computer networks in order to transmit, receive or store information (Article 28(1) IntelSA).
[2347] Article 27(2) IntelSA. An application for an authorisation from the Federal Administrative Court must inter alia contain a reasoning on why the abovementioned standard is considered to be met; details of the persons that will be affected; a precise description of the measure; and information on the timeframe for carrying out the measure (Article 29(1) IntelSA). The authorisation issued by the Federal Administrative Court must contain a brief statement of reasons and may impose further conditions (Article 29(2) IntelSA).

Administrative Court authorisation[2348]. Once a measure has been authorised by the Court, the Head of the DDPS, after consulting in writing with the Head of the Federal Department of Foreign Affairs (FDFA) and the Head of the Federal Justice and Police Department (FDJP) decides on the clearance for the measure to be carried out[2349].

In cases of urgency, the FIS may order the immediate use of information gathering measures requiring authorisation but must immediately inform the Federal Administrative Court and the DDPS, both of which may terminate the measure with immediate effect[2350]. An application for authorisation must in this case be filed before the Court within 24 hours and must include an explanation of the reasons for the urgency[2351]. If the measure is authorised by the Court, the DDPS, after consulting the FDFA and the FDJP, decides on clearance for the measure to be continued[2352]. Any information gathering measure requiring authorisation must immediately be terminated if the authorisation period expires, the requirements for the measure are no longer fulfilled, or authorisation/clearance is not granted[2353]. In case of the use of urgency measures, the FIS is required to ensure immediate destruction of the collected information if an application for a measure is rejected by the Federal Administrative Court or the Head of the DDPS terminates the measure or refuses clearance for continuation[2354].

In terms of additional safeguards, the IntelSA requires the FIS to notify the individual whose information was collected within one month after the conclusion of the intelligence operation of the reason for, nature and duration of the measure[2355]. Such notification may be postponed or dispensed with if necessary to avoid jeopardising an ongoing information gathering measure or ongoing legal proceedings; if necessary due to another overriding public interest to safeguard internal or external security or Swiss or foreign relations; if the notification could cause serious danger to third parties; or if the concerned individual cannot be contacted[2356]. However, such a postponing or dispensing with notification must be authorised by the Federal Administrative Court and cleared by the DDPS in accordance with the abovementioned procedure[2357]. More generally, the FIS is required to keep written documentation on each information gathering measure, which must inter alia contain information on the authorisation and clearance, when the measure ended, as well as the notification (and/or postponing of/dispensing with such notification)[2358].

The IntelSA also provides the FIS with a legal basis to collect information about events outside of Switzerland[2359]. In this case, the FIS must ensure that the risk following from the

[2348] Article 29(6)-(7) IntelSA.
[2349] Article 30 IntelSA.
[2350] Article 31(1) IntelSA.
[2351] Article 31(2) IntelSA.
[2352] Article 31(4) IntelSA.
[2353] Section 32(1) IntelSA.
[2354] Article 32(2) IntelSA.
[2355] Article 33(1) IntelSA.
[2356] Article 33(2) IntelSA.
[2357] Article 33(3) IntelSA.
[2358] Article 22 FISO.
[2359] Article 36(1) IntelSA. Pursuant to Article 37 IntelSA, the FIS may also intrude into computer systems and networks located outside of Switzerland (to disrupt, prevent or slow down access to information) where those are used to carry out attacks on critical infrastructures in Switzerland. In addition, the FIS may intrude into such systems/networks to gather information about events outside Switzerland that is available there or that has been transmitted from there. Such measures must be authorised by the Head of the DDPS (after consulting the Heads

information gathering is not disproportionate to the expected benefit and that interference with the fundamental rights of the persons concerned can be limited to what is necessary[2360].

The FIS may obtain cable communication intelligence (e.g., internet traffic transmitted by international telecommunications cables, such as emails, internet telephony, etc.) in order to gather information about events outside Switzerland that are of significance to security and, in the event of a serious and immediate threat and in accordance with a mandate issued by the Federal Council, to safeguard important national interests (the protection of the basic constitutional order in Switzerland, supporting Swiss foreign policy and the protection of Switzerland as a location for employment, business and finance)[2361]. The purposes for which such collection may take place are further specified in the FISO, which clarifies that the collection of cable communications may be carried out in specific fields: terrorism (e.g., to identify activities, lines and structures of terrorist groups), proliferation (e.g., to identify weapons of mass destruction programmes), counter-espionage (to identify activities and structures of foreign state or non-state actors), foreign actions and motives directed against Switzerland and foreign acts or conflicts affecting Switzerland (e.g., to assess the security situation or stability of the concerned foreign regimes), and cyber threat exploration and critical infrastructure protection[2362].

The recording of cross-border signals from cable-based networks is done by the Centre for Electronic Operations (CEO) of the Swiss Armed Forces[2363], upon a mandate issued by the FIS. To issue a mandate for cable communications intelligence, the FIS must obtain authorisation from the Federal Administrative Court, as well as a clearance from the Head of the DDPS (who must in turn consult in writing the Heads of the FDFA and FDJP)[2364]. An authorisation from the Court is valid for a maximum of six months and may be extended by another Court authorisation for a maximum of three months[2365]. In cases of urgency, the same procedure as the one described above for issuing/authorising urgent information gathering measures in Switzerland applies[2366]. The CEO may only pass recorded signals on to the FIS if the content corresponds to the search parameters defined for the operation, which must be defined in such a way that their application causes as little interference as possible in the private life of persons[2367]. Search terms may for instance be the names of legal or natural

---

of the FDFA and FDJP). A request for authorisation must be in writing and inter alia set out the type of information sought through the measure, the period during which the measure would take place, as well as the necessity, proportionality and risks of the measure, see Article 24(1) FISO. The FIS must document the implementation, results and termination of an authorised measure (Article 24(4) FISO).

[2360] Article 36(3) IntelSA.

[2361] Article 39(1) IntelSA, in conjunction with Article 6(1)(b) and Article 3 IntelSA.

[2362] Article 25 FISO.

[2363] Article 26 FISO.

[2364] Article 40 IntelSA, Article 41(2) IntelSA, in conjunction with Article 30 IntelSA. The application for an authorisation from the Court must inter alia contain the reasons why the operation is necessary, details of the categories of search parameters, and details of the operators of cable-based networks and telecommunication services providers that must supply the information (Article 41(1) IntelSA). The Court issues an authorisation with a brief statement of reasons and may impose additional conditions (Article 41(2), in conjunction with Article 29(3) and (5) IntelSA).

[2365] Article 41(3) IntelSA.

[2366] See Article 41(2) IntelSA, in conjunction with Article 31 IntelSA.

[2367] Article 39(3) IntelSA. Details of Swiss natural or legal persons are not permitted as search parameters.

persons, telephone numbers, IP addresses, etc.[2368]. The CEO receives signals from operators of cable-based networks and telecommunication service providers, who are obliged to provide the relevant information[2369], converts them into data and assesses on the basis of the content which data meets a search parameter and therefore has to be passed on to the FIS[2370]. If the data contains information about events in Switzerland or abroad that provides evidence of a specific threat to internal security (e.g., terrorism, espionage, the proliferation of weapons of mass destruction), the data is passed unchanged to the FIS[2371]. The CEO must destroy data that does not contain any relevant information as quickly as possible[2372].

In addition to conducting cable communication intelligence, the FIS may carry out radio communication intelligence (i.e., recording electro-magnetic emissions from telecommunication systems located abroad, in practice relating primarily to telecommunication satellites and shortwave transmitters[2373])[2374]. This type of collection may be used to gather information about events outside Switzerland that are of significance to security or in the event of a serious and immediate threat and in accordance with a mandate issued by the Federal Council, to safeguard important national interests (the protection of the basic constitutional order in Switzerland, supporting Swiss foreign policy and the protection of Switzerland as a location for employment, business and finance)[2375]. The purposes for which such collection may take place are further specified in the Ordinance on Electronic Warfare and Radio Exploration, which clarifies that radio exploration may be carried out in specific fields: terrorism (e.g., to identify activities, lines and structures of terrorist groups), proliferation (e.g., to identify weapons of mass destruction programmes), counter-espionage (to identify activities and structures of foreign state or non-state actors), foreign conflicts affecting Switzerland (e.g., to assess the security the security situation or stability of regimes), army and armaments (e.g., to recognise actual or potential military conflicts), the engagement of the Swiss Armed Forces[2376].

While the use of these measures does not require prior authorisation by a court, each mandate[2377] for radio communication intelligence must be reported to an independent oversight body, the Independent Control Authority for Radio and Cable Communications Intelligence, which verifies the legality of radio communication intelligence mandates on an annual basis[2378]. The Authority may carry out audits, issue recommendations, and request the

[2368] See the Explanatory Report on the revision of the IntelSA, available at: https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/dl/proj/2022/15/cons_1/doc_4/de/pdf-a/fedlex-data-admin-ch-eli-dl-proj-2022-15-cons_1-doc_4-de-pdf-a.pdf.
[2369] Article 43 IntelSA.
[2370] Article 42(1) IntelSA.
[2371] Article 42(3) IntelSA, in conjunction with Article 6(1)(a) IntelSA.
[2372] Article 42(4) IntelSA.
[2373] See the FIS' annual report 2023 ("Switzerland's security 2023"), p. 83, available at: https://www.newsd.admin.ch/newsd/message/attachments/80146.pdf.
[2374] The Armed Forces Intelligence Service may also carry out radio communication intelligence, under the same conditions as the FIS (i.e., following from the IntelSA, Ordinance on Electronic Warfare and Radio Exploration and OSIA) and subject to the same oversight by the Independent Control Authority. See Article 99(1bis) Army Act.
[2375] Article 38(2) IntelSA.
[2376] Article 3 Ordinance on Electronic Warfare and Radio Exploration.
[2377] A mandate to carry out radio exploration must be issued in writing, define the purpose of the exploration and the results to be obtained (Article 3(4) Ordinance on Electronic Warfare and Radio Exploration).
[2378] Article 10(2) OSIA.

termination of radio communication intelligence as well as the deletion of collected information[2379]. More information on the Authority and its oversight powers is provided in section 2.3.3.

According to its annual report 2023, the FIS used 92 information gathering measures (affecting 26 individuals in total), issued three cable communication intelligence orders, and issued 30 radio communication intelligence orders, in 2022[2380].

Finally, the FIS may obtain data from other public authorities (at federal and cantonal level), which are either, under certain conditions, obliged to disclose information to the FIS upon its request, or are allowed to voluntarily share information, again under specific conditions. Such authorities are obliged to respond to a justified request[2381] from the FIS with information required to identify or repel a specific threat to internal or external security[2382] or to safeguard other important national interests[2383]. With some exceptions, public authorities may (but are not required to) share information with the FIS on their own initiative if the same conditions are met[2384]. Some authorities (e.g., courts, prosecution authorities, customs authorities, authorities responsible for diplomatic and consular matters, authorities receiving reports of money laundering and terrorist financing) are obliged to proactively report to the FIS if they identify a specific and serious threat to internal or external security[2385].

2.3.2. Further use of the information collected

The processing of personal data by intelligence agencies is first of all subject to specific data protection obligations following from the IntelSA and its accompanying ordinances[2386].

The FIS operates different information systems (e.g., for information about violent extremism, information that only initiates administrative processes, data from publicly accessible sources, etc.)[2387] and the IntelSA establishes for each of those systems how collected data may be used.

[2379] Article 79(3) IntelSA, Article 9(1) OSIA.

[2380] See Switzerland's Security 2023 – Situation. Report of the Federal Intelligence Service 2023, p. 82.

[2381] In particular, the request must explain the concrete threat or the important national interest to be protected, see Article 20(1) FISO.

[2382] Such a threat exists if a significant legal interest such as the life and limb or the liberty of persons or the existence and functioning of the state is affected and the threat results from, inter alia, terrorist activities, espionage, an attack on critical infrastructure or violent extremism (Article 19(2) IntelSA).

[2383] I.e., the basic constitutional order in Switzerland; Swiss foreign policy; or Switzerland as a location for employment, business and finance, where this is determined by the Federal Council (Article 19(1) in conjunction with Article 3 IntelSA).

[2384] Article 19(4) IntelSA.

[2385] Article 20 IntelSA.

[2386] The processing of personal data by other authorities that are required to assist the FIS in the collection of information, i.e. the PTSS (for the surveillance of telecommunications) and the CEO (for radio and cable exploration), is also subject to the FADP 2020, as well as specific data protection rules (e.g., data retention periods laid down in Article 28 FISO, Article 11 SPTA and Article 4 Ordinance on Electronic Warfare and Radio Exploration). As regards the processing of personal data by the Army Intelligence Service, specific data protection requirements follow from the Army Act and the Ordinance on the Army Intelligence Service. These instruments for instance lay down the specific purposes for which the AIS may process personal data and regulate the sharing of data with other entities (the AIS may communicate personal data to federal and cantonal services, as well as foreign authorities, if such communication is required for the execution of a lawful mandate or if the processing of the data falls within the legal competence of the receiving service (Article 10 Ordinance on the Army Intelligence Service)). In addition, the FADP 2020 applies, see the information provided in section 2.2.2).

[2387] Article 48 IntelSA.

In particular, it provides for each system which information must be recorded[2388], for which purposes and which employees/entities can access and search the information[2389]. In accordance with the IntelSA, the FIS must assess the relevance and accuracy of personal data before recording it in its information systems and destroy any data that is not necessary to fulfil its tasks as set out in the Act[2390]. The FIS must correct or delete any incorrect data and periodically check whether personal data recorded in its information systems is still required to carry out its tasks (and if not delete such data)[2391]. In addition, the FIS is required to, inter alia, verify by random sample the legality, expediency, effectiveness and accuracy of the data processing in all of the FIS' information systems[2392]. Moreover, the ISSO-FIS imposes the principle of data security, including by referring to obligations under the FADP 2020[2393].

Data collected through information gathering measures that require court authorisation (e.g., the content of communications collected through interception) must initially be stored separately from other information systems[2394]. Only FIS employees that have the task of carrying out the information gathering measure and evaluating the results have access to such data[2395]. Any personal data obtained through such measures that is not related to the specific threat situation for which the measure was taken may not be used and must be destroyed at the latest 30 days after conclusion of the measure[2396]. Personal data related to specific threat situations that is not used in legal proceedings or an ongoing intelligence operation must be deleted (1) within six months after the notification of the measure to the data subject concerned (including where such notification is postponed); (2) immediately after the entry into force of a court decision on dispensing with the obligation to notify the individual; or (3) immediately after the entry into force of a decision on an appeal against the measure ordered[2397]. If such data is used in an intelligence operation, it is recorded in one of the FIS' information systems and subject to the specific requirements applying to that system. The ISSO-FIS lays down specific maximum retention periods depending on each system, with periods varying from 2 (e.g., for data from public sources) to 45 years (e.g., for data relevant to national security)[2398].

As a general requirement, before disclosing personal data to any other entity (whether in Switzerland or outside), the FIS must ensure that the disclosure is lawful and necessary in a specific case[2399]. The FIS may only disclose personal data to other Swiss authorities if this is necessary to safeguard internal or external security[2400], unless doing so would be contrary to overriding public or private interests[2401]. The FIS may share data with other authorities for the

[2388] See also the annexes to the ISSO-FIS, which detail for each information system which categories of (personal) data may be recorded.
[2389] Chapter 4, Section 2 IntelSA. More detailed requirements on the granting of access rights are laid down in Article 5-6 ISSO-FIS.
[2390] Article 45(1)-(2) IntelSA. See also Articles 3-4 ISSO-FIS.
[2391] Article 45(4) IntelSA.
[2392] Article 45(5) IntelSA.
[2393] Article 13 ISSO-FIS.
[2394] Article 58(1) IntelSA.
[2395] Article 58(3) IntelSA.
[2396] Article 58(2) IntelSA.
[2397] Article 70 ISSO-FIS.
[2398] A8(2) ISSO-FIS and the specific provisions mentioned there.
[2399] Article 59 IntelSA.
[2400] Article 60(1) IntelSA.
[2401] Article 32(4) FISO.

use of the prosecution of offences, prevention of serious offences or maintaining public order, upon their request or on its own initiative[2402]. It is always required to disclose data obtained through measures requiring authorisation to a prosecution authority if the information contains specific evidence of an offence in connection with the prosecution of which the prosecution authority would have been entitled to order a comparable criminal procedural measure[2403]. Any sharing of personal data with other authorities must be recorded in writing by the FIS, including the recipient, the object and the reason for the sharing[2404]. The authorities with which personal data may be shared and the purposes for which such sharing may take place are listed in Annex 3 to the FISO, and for instance includes criminal prosecution authorities at federal and cantonal level, the Federal Department of Foreign Affairs (e.g., for the assessment of the threat situation and the security policy interests of Switzerland), the Federal Department of Home Affairs (e.g., for the enforcement of legislation on narcotics), etc.

Personal data processed by the FIS may only be disclosed to a foreign authority if it is in a country that guarantees an adequate level of data protection under the FADP 2020, or, if that is not the case, only if Switzerland maintains diplomatic relations with the relevant country and (1) Switzerland is required by law or by an international agreement to disclose the personal data to the state; (2) disclosure is required to safeguard an overriding public security interest in Switzerland or in the receiving state (such as preventing a serious criminal offence that is also qualified as such in Switzerland); (3) it is necessary in order to justify a request for information from Switzerland; (4) it is in the interest of the person concerned, who has consented to disclosure or consent may be clearly assumed in the circumstances or (5) it is necessary in order to protect the life and limb of third parties[2405]. The possibility of access online to personal data is limited to foreign security agencies whose states benefit from an adequacy decision and with which Switzerland has concluded an international agreement on international cooperation[2406]. Personal data may not be disclosed to a foreign security agency if the person concerned will be exposed to the risk of being punished twice or of serious harm to his or her life, limb or freedom under the ECHR or other international agreements that Switzerland has ratified[2407]. For each disclosure to a foreign authority, the FIS must inform the addressee of the purpose for which the latter is exclusively authorised to use the data and the fact that the FIS reserves the right to request information on such use[2408]. The FIS must keep documentation on each disclosure, the subject thereof and the recipient[2409].

Finally, the FIS may disclose personal data to other third parties only if the individual concerned has consented to the disclosure; if the disclosure is indisputably in the interest of the individual; if the disclosure is necessary in order to repel a serious immediate danger; or if it is necessary in order to justify a request for information[2410].

[2402] Article 60(2) IntelSA.
[2403] Article 60(3) IntelSA.
[2404] Article 32(3) FISO.
[2405] Article 61(1) IntelSA.
[2406] Article 61(4) IntelSA.
[2407] Article 61(5) IntelSA.
[2408] Article 35(5) FISO.
[2409] Article 35(6) FISO.
[2410] Article 62 IntelSA.

To the extent that the IntelSA and other laws/ordinances to do not provide specific data processing rules, the FADP 2020 applies (see the information provided in section 2.2.2)[2411].

2.3.3. Oversight

The activities of the FIS are supervised by different bodies.

First, the FDPIC oversees compliance of data processing by the FIS with the FADP 2020 and other federal data protection requirements (in particular those following from the IntelSA and its accompanying Ordinances)[2412]. In carrying out this task, the FDPIC makes use of all of its powers, as described in section 1.2, including to adopt binding decisions.

Second, the activities of the FIS and cantonal authorities to whom the FIS has delegated tasks are supervised by the Independent Oversight Authority for Intelligence Activities (OA-IA)[2413]. In carrying out its tasks, it has access to all relevant information and documents, as well as the premises of the FIS/cantonal authorities and their information systems[2414]. The OA-IA may audit these activities to confirm their legality, expediency and effectiveness[2415]. Following an audit, the OA-IA provides the DDPS with a written report, which may include recommendations[2416]. The DDPS is required to implement such recommendations and must submit any recommendation it intends to reject to the Federal Council for a decision[2417]. According to information received from the Swiss government, all recommendations from OA-IA have so far been implemented. According to its annual reports, the OA-IA issued 55 recommendations in 2020, 18 recommendations in 2021 and 13 recommendations in 2022[2418]. In 2022, the OA-IA for instance conducted audits of the information gathering management by the FIS, as well as the collection of information from telecommunication providers[2419].

Third, the use of radio and cable communications intelligence is, in addition to the supervision by the OA-IA, also subject to oversight by a separate independent body – the Independent Control Authority (ICA)[2420]. The ICA is in charge of verifying the legality of radio communication intelligence and supervising the conduct of authorised and cleared cable

[2411] The same applies to the Army Intelligence Service.
[2412] Article 4(1) FADP 2020. The Army Intelligence Service is also subject to the oversight of the FDPIC.
[2413] The IntelSA provides that the OA-IA carries out its task independently, free from any instructions from other authorities, with its own budget and staff, while being assigned to the DDPS for administrative purposes (Article 76(1), Article 77 IntelSA). The head of the OA-IA is appointed by the Federal Council upon a proposal from the DDPS for a renewable period of six years (Article 76(2)-(5) IntelSA). The Federal Council may remove the head from the post only if (s)he breaches his official duties wilfully or through gross negligence or becomes permanently incapable of exercising office. The Army Intelligence Service is also subject to the oversight of the OA-IA, see Article 99(5) Army Act.
[2414] Article 78(4) IntelSA.
[2415] Article 78(1) IntelSA.
[2416] Article 78(6) IntelSA.
[2417] Article 78(7) IntelSA.
[2418] See the annual reports available at: https://www.ab-nd.admin.ch/en/jahresbericht-ab-nd.html.
[2419] Annual report 2022 of the Independent Oversight Authority for Intelligence Activities OA-IA, available at: https://ab-nd-taetigkeitsbericht.ch/en/.
[2420] Article 79 IntelSA. The ICA consists of three to five members appointed for a term of four years by the Federal Council (on the proposal of the DDPS), which must have expertise in the fields of telecommunications, security policy and the protection of fundamental rights (Article 79(4) IntelSA, Article 7 OSIA). The ICA acts independently and is not bound by directives/instructions from other authorities (Article 79(1) IntelSA). Radio exploration carried out by the Army Intelligence Service is also subject to the oversight of the ICA, Article 99(1bis) Army Act

communications intelligence assignments given to the CEO[2421]. In particular, it may review cable network exploration applications, approval and validation decisions, analyse the results obtained via radio and cable exploration, annually verify radio exploration mandates, etc.[2422]. To carry out its oversight activities, it has access to all relevant information and facilities[2423]. In addition, the intelligence services must notify the ICA of every new radio or cable intelligence order and must provide the ICA with an updated and complete list of all keywords used and inform the ICA of completion of mandates[2424]. The ICA lay issue recommendations, request that radio communications intelligence assignments are terminated, and that collected information is deleted[2425].

Finally, intelligence services are also subject to parliamentary oversight by the CDel[2426] of the Federal Assembly, which oversees the legality, expediency and effectiveness of activities of the intelligence services[2427]. In carrying out its oversight tasks, the CDel has unrestricted access to information, including secret intelligence information[2428]. According to the "Action principles of the Control Delegation" developed by the CDel itself[2429], it may request reports from the intelligence services, carry out regular inspections/investigations and on-site visit, etc. As a result of an investigation, the CDel can issue recommendations addressed to the relevant intelligence service[2430]. The CDel also publishes the annual report[2431]. In 2019, the CDel concluded an investigation on the basis of a petition from an NGO, in which it included several recommendations on the processing of data by the FIS in different databases and the impact thereof on the possibility for individuals to exercise their right of access, as well as applicable retention periods[2432].

2.3.4. Redress

The Swiss system provides different avenues to obtain redress, including compensation for damages.

First, individuals can invoke different rights against the FIS[2433]. The IntelSA specifically regulates the exercise of the right of access with respect to data processed for national security purposes[2434] (as regards data processed by the FIS for administrative or other purposes not related to national security, the IntelSA specifies that the FADP 2020 applies[2435]). The FIS

[2421] Article 79(1) IntelSA.
[2422] Article 10 OSIA.
[2423] Article 79(2) IntelSA.
[2424] Article 9(1) OSIA.
[2425] Article 79(3) IntelSA.
[2426] The Army Intelligence Service is also subject to the oversight by the CDel, see Article 99(5) Army Act.
[2427] Article 52(2) Act on the Federal Assembly.
[2428] See Article 169(2) of the Federal Constitution, which provides that secrecy rules do not apply to special delegations of supervisory committees established by law.
[2429] Principes d'action de la Délégation des Commissions de gestion, avalable at : https://www.parlament.ch/centers/documents/fr/gpdel-handlungsgrundsaetze-f.pdf.
[2430] Article 158 Act on the Federal Assembly.
[2431] See 2003 Report, available at: https://www.parlament.ch/press-releases/Pages/2013/mm-gpdel-2013-09-05.aspx.
[2432] Rapport annuel 2019 des Commissions de gestion et de la Délégation des Commissions de gestion des Chambres fédérales, p. 2939.
[2433] With respect to data processed by the Army Intelligence Service, individuals can exercise the rights under the FAPD 2020, as described in section 1.1 and below.
[2434] Article 63(2) IntelSA.
[2435] Article 63(1) IntelSA.

will defer its response (through a standard notification) (1) if and to the extent that there are overriding interests that justify preserving secrecy that are connected with the fulfilment of the FIS' intelligence tasks or a prosecution or other investigation; (2) if and to the extent that it is required because of overriding interests of third parties; or (3) if no data about the individual is being processed[2436]. As soon as there are no longer overriding interests in preserving secrecy and at the latest on expiry of the applicable data retention period, the FIS must provide the individual with the information required under the FADP 2020 in response to access requests, unless this would involve excessive work and expense[2437]. According to its annual report, the FIS received a total of 675 access requests (under the IntelSA and the FADP) in 2022. In 594 cases, the individuals were provided with the relevant information in response to their requests, whereas the answer was deferred in 50 cases, in accordance with the criteria of the IntelSA[2438].

If the response is deferred, the FIS must inform the individual that he or she has the right to request the FDPIC to examine whether the data, if any, is being lawfully processed and whether overriding interests in preserving secrecy justify the deferral[2439]. Upon request from an individual, the FDPIC conducts an examination and informs the individual (through a standard notification) that either (1) no data is being processed unlawfully in relation to him or (2) that the FDPIC has found errors in the processing of the data/regarding the postponement of the information and has opened an investigation pursuant to the FAPD 2020[2440]. In the context of an investigation, the FDPIC can make use of its different investigatory and enforcement powers foreseen in the FADP 2020. In addition, the IntelSA provides that the FDPIC may order the FIS to rectify any errors in the processing of data or regarding the postponement of the reply to the individual[2441]. Moreover, if an individual credibly demonstrates that (s)he will suffer significant irreparable damage by postponing the disclosure of information in response to an access request, the FDPIC may order the FIS to immediately provide the information, provided that this does not endanger internal or external security[2442].

In addition to a right of access, individuals also have a right of correction, erasure and a right to object with respect to personal data processed by the FIS, pursuant to the FADP 2020. In response to a request for deletion, the FIS may, instead of deleting the data, restrict its processing if this is necessary for an overriding public interest (in particular Swiss internal or external security) or deleting the data may jeopardise an enquiry, investigation or administrative/judicial procedure[2443].

As regards the processing of personal data by cantonal bodies, when they are carrying tasks in the area of national security, individuals are granted rights of access, correction, deletion and

[2436] Article 63(2) IntelSA. The FIS is required to notify individuals whose data is not being processed of this fact no later than three years after receipt of their request (Article 63(5) IntelSA).
[2437] Article 63(4) IntelSA.
[2438] Switzerland's security 2023, p. 86, available at: https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-95984.html.
[2439] Article 63(3) IntelSA.
[2440] Article 64(1)-(2) IntelSA. This notification cannot be contested by the individual (Article 66(2) IntelSA).
[2441] Article 64(4) IntelSA.
[2442] Article 64(5) IntelSA.
[2443] Article 41(3)(c) FADP 2020.

objection under cantonal data protection laws, which can be enforced before cantonal data protection authorities and courts[2444].

Second, individuals can lodge complaints before different bodies concerning the (unlawful) processing of their data by intelligence under the FADP 2020. Anyone that has a legitimate interest (i.e., whose data is being processed[2445]) may request a national security authority to (1) stop unlawful processing of personal data, (2) redress the consequences of the unlawful processing or (3) declare the processing to be unlawful[2446]. The response from a public authority to such a request is considered a "ruling" that can be challenged by the individual (e.g., arguing that the ruling/decision is inadequate or that discretionary powers have been abused) before the Federal Administrative Court[2447], which may amend the contested decision if it violates federal law or is based on an incorrect or incomplete determination of the facts of the case[2448]. Moreover, any individual may lodge a complaint before the FDPIC about compliance with the FADP 2020 and data protection provisions in the IntelSA and accompanying ordinances. The FDPIC may make use of all of its various investigatory and enforcement power, as described in section 1.2.

Third, under the same conditions as explained in section 2.2.4, any individual that has an interest worthy of protection may request an injunction from an intelligence authority, whose response can be challenged by the individual before the Federal Administrative Court (whose decisions can in turn be appealed before the Federal Supreme Court)[2449]. In this respect, a Supreme Court judgment has for instance clarified that, because surveillance measures in the context of radio and cable intelligence are secret and individuals are not able to demonstrate that they are individually affected (and therefore cannot establish a legal interest to challenge an individual surveillance measure), a complainant is considered to have such a legal interest if there is a sufficient probability (i.e., a "reasonable likelihood", interpreted in accordance with the standard developed by the ECtHR) that the FIS processes their data in the context of radio and cable intelligence[2450].

Fourth, under the same conditions as explained in section 2.2.4, any individual may obtain compensation for damage caused by federal public authorities (including criminal law enforcement authorities) on the basis of the Federal Act on the Liability of the Confederation, Members of its Authorities and Officials[2451].

Finally, after exhausting domestic remedies, any individual may obtain judicial redress before the European Court of Human Rights concerning the collection and use of their data by Swiss intelligence agencies.

[2444] Since the data is processed on behalf of the FIS (tasks in the area of national security), the FIS is the data controller and the provisions of the IntelSA, notably Art. 63, also apply.
[2445] See the case law of the Federal Supreme Court, e.g., TF, 1C_377/2019.
[2446] Article 41 FADP 2020.
[2447] Article 25a(2), in conjunction with Article 5 and 49 APA.
[2448] Article 62 APA.
[2449] Article 25a(2), in conjunction with Article 5 and 49 APA; Article 83(1) IntelSA.
[2450] Supreme Court judgment in case TF, 1C_377/2019. See in particular para. 7.2.2 and the cross-reference to para. 122 of the ECtHR Kennedy judgment.
[2451] Article 3 Federal Act on the Liability of the Confederation, Members of its Authorities and Officials.

XI. EASTERN REPUBLIC OF URUGUAY

1. RULES APPLYING TO THE PROCESSING OF PERSONAL DATA

1.1. Relevant developments in the data protection framework of Uruguay

On 21 August 2012, the Commission adopted a decision in which Uruguay was considered providing an adequate level of protection for personal data[2452]. The Article 29 Working Party had adopted a positive opinion on the level of protection of personal data in Uruguay on 12 October 2010[2453]. At the time of the adoption of the adequacy decision, the protection of personal data in Uruguay was governed by the Law 18.331 on the Protection of Personal Data and the Habeas Data Action 2008[2454] *(Ley de Protección de Datos Personale*s, LPDP) and Decree No. 414/009 Regulating Law 18.331 Relating to the Protection of Personal Data[2455] (*Reglamentación de la ley 18.331, relativa a la Protección de Datos Personales*, RPDP).

Since the adoption of the adequacy decision, certain specific aspects of the LPDP were amended in 2012[2456] and 2015[2457]. In 2018 Uruguay started a legislative process for a more comprehensive modernisation and strengthening of its data protection regime, taking inspiration from Regulation (EU) 2016/679 (GDPR)[2458]. As described in more detail below, the territorial scope of the data protection legislation was broadened and new accountability requirements were introduced, including impact assessments and data protection by design and by default, data breach notification and the appointment of data protection officers. These new provisions were introduced by Law No. 19.670 on Accountability and Budgetary Execution Balance Exercise 2017[2459] that the Parliament of Uruguay passed in October 2018. The Law entered into force in January 2019 and has been further developed through a decree published in February 2020[2460]. Further changes to the LPDP concerning the regime applicable to the processing of biometric data were introduced through Law 19.924 of 18 December 2020. In addition, Uruguay ratified Convention 108 through Law No. 19.030 on the approval of the Council of Europe's Convention for the Protection of Individuals with

[2452] Commission Implementing Decision 2012/484/EU of 21 August 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the Eastern Republic of Uruguay with regard to automated processing of personal data, OJ L 227, 23.8.2012, p. 11–14.

[2453] Opinion 6/2010 on the level of protection of personal data in the Eastern Republic of Uruguay (WP 177) of 12 October 2010, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp177_en.pdf.

[2454] Law 18.331 of 11/08/2008, available at: https://www.impo.com.uy/bases/leyes/18331-2008.

[2455] Available at: https://www.impo.com.uy/bases/decretos/414-2009.

[2456] Law 18.996 of 07/11/2012, Article 43, available at the following link: https://www.impo.com.uy/bases/leyes/18996-2012. The amendment concerned sources that are available to access by the public. The concept is defined in Article 4(I) LPDP as "those databases which may be consulted by any person, not prevented by a restrictive rule or without any requirement other than, where appropriate, the payment of a fee". The reform from 2012 introduced a new Article 9bis to clarify which data sources or documents can be considered as sources of public access in accordance with the LPDP, notably official gazettes, telephone directories, media, etc.

[2457] Law 19.355 of 19/12/2015, Article 83, available t: https://www.impo.com.uy/bases/leyes/19355-2015. The reform clarified the procedure for the data protection authority (Unidad Reguladora y de Control de Datos Personales, URCDP) to request the competent judicial authority to close a database.

[2458] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[2459] Law 19.670 of 15/10/2018, Articles 37 to 40, available at: https://www.impo.com.uy/bases/leyes/19670-2018.

[2460] Decree 64/2020, available at: https://www.impo.com.uy/bases/decretos/64-2020.

Regard to Automatic Processing of Personal Data and its Additional Protocol. More recently, Uruguay has been the first country from the American continent to ratify also the modernised Convention 108 (Convention 108+)[2461].

Like the GDPR, the LPDP has a broad scope of application, applying to both private operators and public authorities[2462]. The definitions of 'personal data', 'controller', 'processor', 'data subject' and 'processing'[2463] (which are similar to those used in the GDPR) have not changed since the adoption of the adequacy decision. However, the amendments to the LPDP that were introduced in 2018 have further increased convergence with the GPDR by extending the territorial scope of the LPDP, subject to conditions that are similar to those in Article 3 GDPR. The LPDP now applies also to the processing of personal data by controllers or processors not established in Uruguay when they offer goods or services to data subjects in Uruguay, and to processing activities aimed at the monitoring of their behaviour[2464]. This confirms the intention of the Uruguayan legislator to strengthen the effectiveness of Uruguay's data protection regime.

The main data protection principles and obligations that were already provided by the LPDP at the time of the adoption of the adequacy decision have remained in place without substantial changes. This is notably the case for the principles of lawfulness[2465], purpose limitation[2466], accuracy and data minimisation[2467] and proportionality[2468] and data retention[2469] and data security[2470]. At the same time, several principles and obligations have been further strengthened, bringing Uruguay's data protection framework closer to the requirements of the GDPR.

With respect to the principle of data security, an obligation to report data breaches has been introduced into the LPDP[2471]. Similarly to what is required under the GDPR, a controller or processor that becomes aware of a data breach affecting the protection of personal data must inform as soon as possible the URCDP[2472], and also the affected individuals if they have suffered a significant impact on their rights[2473]. Controllers and processors are required to adopt mitigating measures in the first 24 hours following the detection of a data breach. Once

[2461] Through the Law 19.948 of 16 April 2021.
[2462] Article 3 LPDP.
[2463] All definitions included in Article 4 LPDP.
[2464]Article 37 Law 19670, available at: https://www.impo.com.uy/bases/leyes/19670-2018/37.
[2465] Article 6 LPDP.
[2466] Article 8 LPDP.
[2467] Article 7 LPDP.
[2468] Article 7 LPDP.
[2469] Article 8 LPDP.
[2470] Article 10 LPDP.
[2471]Article 38 Law 19.670, available at: https://www.impo.com.uy/bases/leyes/19670-2018/38 and Article 4 Decree 64/2020, available at: https://www.impo.com.uy/bases/decretos/64-2020/4.
2472 When a security breach is detected the data controller or the data processor, as the case may be, must start the necessary procedures to minimize the impact of the incident within the first 24 hours (Article 3 Decree No. 64/2020). When learning about the occurrence of a data breach, data controllers must inform the URCDP within 72 hours, giving as much detail as possible about the event and the mitigating measures that have been taken. If the breach significantly affects the rights of the data subjects, they must be informed in clear and simple language (Article 4 Decree No. 64/020). Processors must directly address data controllers to inform them. Once the breach has been remedied, the controller must draw up a detailed report on the security breach and the measures taken to be sent to the URCDP.
[2473] Decree 64/2020, Article 4, available at: Decreto N° 64/020 (impo.com.uy)

the breach has been properly managed and its effects contained, the controller must prepare a detailed report for the URCDP.

In terms of accountability, the LPDP now expressly provides that controllers and processors are responsible for any violation of the data protection law. In exercising their responsibilities, they must put in place adequate technical and procedural measures in order to ensure fair processing and they must demonstrate the effective implementation of such measures[2474]. Moreover, the reform of 2018 modernised the accountability requirements that applied under the previous regime by introducing obligations that are also part of the GDPR, in particular to implement the principles of data protection by design[2475] and by default[2476], to appoint a data protection officer in specific cases[2477], to carry out data protection impact assessments[2478] and to consult the URCDP prior to starting any processing activities which, according to the assessment, would result in a high risk for the individual if no measures to mitigate the risks are taken[2479].

In addition to the strengthening of data protection principles and obligations, the protections for special categories of data (i.e., sensitive data) have been reinforced since the adoption of the adequacy decision. The LPDP already offered additional protections for most of the categories of personal data that are considered sensitive in the GDPR, i.e., for data about an individual's ethnic origin, religion, philosophy, political opinions or sexual life, as well as for health data (including genetic data[2480]) and data revealing membership in a political organisation or trade union[2481]. In the context of the amendment of the LPDP in 2020, additional protections were introduced also for biometric data. First, a definition of biometric data processed for the purpose of uniquely identifying a natural person has been added to the

[2474] Article 12 LPDP, as amended by Article 39 Law No 19.670.
[2475] Article 8 Decree 64/2020.
[2476] Article 9 Decree 64/2020.
[2477] Article 40 Law 19.670, available at: https://www.impo.com.uy/bases/leyes/19670-2018/38 and Articles 10 to 15 Decree 64/2020, available at: https://www.impo.com.uy/bases/decretos/64-2020/. The obligation to appoint a Data Protection Officer applies to public entities, private entities that are wholly or partly state-owned, as well as to private entities that process sensitive data as their main business or that process large volumes of data. Data protection officers are tasked among others with providing advice on the development and implementation of data protection safeguards, as well as with monitoring compliance and proposing measures, where relevant. They also act as a link with the Data Protection Authority.
[2478]The new rules also have also introduced the obligation to carry out, in specific cases and before the processing starts, a data protection impact assessment. This is for instance the case when the processing of sensitive data is the core business of the controller or when it concerns profiling activities. The processing of personal data of minors or sensitive groups also carries with it the obligation of performing an impact assessment, as does the processing of high volumes of data. Finally, international data transfers to third countries or international organisations that do not ensure an appropriate level of protection are also subject to this obligation. Controllers and processors must also inform the URCDP when the result of the assessment indicates a significant risk for the protection of individual rights.
[2479]Article 7 Decree 64/2020, available at: https://www.impo.com.uy/bases/decretos/64-2020/7. A data protection impact assessment must be carried out inter alia when the processing of sensitive data is the core business of the controller or when it concerns profiling activities, if personal data of minors or sensitive groups is processed or if the processing concerns a large amount of personal data. Finally, the transfer of personal data to third countries or international organisations that do not ensure an appropriate level of protection – as far as such transfers are possible - is also subject to this obligation. Controllers and processors must inform the URCDP when the result of the assessment indicates a significant risk for the protection of individual rights.
[2480] The definition of 'health data' provided bv Article 4(D) Decree 414/2009 states that data relating to the genetic information of an individual is considered health data.
[2481] The definition of sensitive data is included in Article 4(E) LPDP. Similarly to what is provided in the GDPR, Article 18 LPDP allows the processing of sensitive data only where the data subject has given explicit consent or where processing is based on a law.

LPDP and that definition is very close to the one provided by the GDPR[2482]. Second, the LPDP now provides that biometric data can be processed only after an impact assessment has been carried out[2483]. Uruguay has also ratified Convention 108+ that requires to treat genetic and biometric data uniquely identifying a person as special categories of data[2484]. Finally, the protection of sensitive data has been strengthened more generally by requiring an impact assessment whenever the processing of special categories of data is the core business of the controller[2485].

As regards individual rights, the rights that were already guaranteed by the LPDP at the time of the adoption of the adequacy decision have remained in place without substantial changes, including the right to obtain information about the processing[2486], the right of access[2487], the right to rectification[2488] and the right to object decisions based on automated processing, including profiling[2489]. Concerning the right to erasure[2490], the URCDP has established through various decisions a 'right to be forgotten'[2491] similar to the one recognised in the EU (i.e., a right to the de-indexation of information available through search engines) by extending the rights to deletion and objection and drawing on the principles of purpose limitation and data accuracy set out in the LPDP. Moreover, the URCDP created an obligation for controllers assessing this type of request to carry out a balancing between the right to data protection and the rights to freedom of the press and freedom of expression. More recently, the exercise of the 'right to be forgotten' was upheld in a decision of a civil court[2492] which was based on the arguments used in decisions of the URCDP[2493]. The URCDP has also issued guidance and made available online tools to facilitate the exercise of individual rights[2494].

[2482] Article 4(Ñ) LPDP, added through Article 3 Law 19924 of 18/12/2020.
[2483]See Article 18-bis Law 18.331, introduced through Article 94 Law 19.924 of 18/12/2020, available at: Ley N° 18331 (impo.com.uy) The impact assessment has to be carried out in accordance with the procedures set out in Articles 6 and 7 of Decree 64/2020. Moreover, having ratified the Council of Europe's modernised Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data and its Additional Protocol (Convention 108+), Uruguay will be required under Article 6 of the Convention to treat biometric data as a special category of data once the Convention has entered into force.
[2484] Article 6 Convention 108+.
[2485] Article 7 Decree 64/2020.
[2486] Article 13 LPDP.
[2487] Article 14 LPDP.
[2488] Article 15 LPDP, that also recognises the right to seek the update of personal data, the right to have personal data included in a database.
[2489] Article 21 LPDP also recognises the right to object in the context of processing of personal data for marketing purposes, including profiling.
[2490] Article 15 LPDP
[2491] Recent decisions and reports on the application of the right to be forgotten are the report 305/019 of 13 September 2019, available at: Informe Nº 305/019, de 13 de setiembre de 2019 | Unidad Reguladora y de Control de Datos Personales (www.gub.uy) and 17/2016 of 14 September 2016, available at: Dictamen N° 17/016 | Unidad Reguladora y de Control de Datos Personales (www.gub.uy)). Other relevant decisions are decisions 1040/2012 of 20 December 2012, available at: Resolución N° 1.040/012 | Unidad Reguladora y de Control de Datos Personales (www.gub.uy)) and decisions 2/014, available at: Dictamen N° 2/014 | Unidad Reguladora y de Control de Datos Personales (www.gub.uy)) and 6/016 of 9 March 2016, available at: Resolución N° 6/016 | Unidad Reguladora y de Control de Datos Personales (www.gub.uy).
[2492] Decision 60/2021 of the Civil Court number 2 of 19 October 2021.
[2493] Notably decision 17/2016 of 14 September 2016, available at: Dictamen N° 17/016 | Unidad Reguladora y de Control de Datos Personales (www.gub.uy)).
[2494] Recent decisions and reports on the application of the right to be forgotten are the report 305/019 of 13 September 2019 and 17/2016. Other relevant decisions are decisions 1040/2012 and decisions 2/014 and 6/016/

According to the LPDP, transfers to third countries or international organisations that do not provide an adequate level of protection according to international or regional data protection standards are in principle prohibited[2495]. The URCDP can determine which countries provide such adequate level of protection. In practice, EU/EEA Member States as well as countries or territories benefitting from an adequacy finding from the European Commission under Directive 95/46/EC (Data Protection Directive)[2496] or the GDPR have been recognised by the URCDP as countries providing an adequate level of protection[2497]. A first list of countries that were considered to provide an adequate level of protection was published in June 2009[2498], using Uruguay's own rules and the Data Protection Directive as the standard for assessment. In June 2019, a new instruction of the URCDP modified the assessment criteria, setting the GDPR and the Ibero-American Standards approved in 2017 by the Ibero-American Data Protection Network as the standard for an adequacy finding[2499].

Subject to authorisation from the URCDP, data transfers to non-adequate countries or organisations can also take place if sufficient guarantees for the protection of private life and the fundamental rights and freedoms of individuals, including the exercise of individual rights, are provided[2500]. These guarantees can be provided through contractual clauses or codes of conduct within multinational companies or international organisations[2501]. The URCDP has recently issued an instruction setting out the "minimum content" of contractual clauses which ensure the level of protection required by the LPDP[2502]. These clauses must provide details of the transfer and the processing activities, including their purpose, definitions of relevant terms, rules on the use of processors and sub-processors, the obligation to notify data breaches and to put in place accountability measures, a right to information and to deletion, limited data retention and rules on onward transfers, dispute resolution clauses, clauses ensuring the exercise of individual rights and clauses on the competence of the supervisory authority, as well as rules regarding confidentiality and access to information by government authorities[2503].

Finally, the transfer of personal data to third countries not considered adequate is allowed in certain limited situations which are similar to the derogations recognised by the GDPR, notably where the individual has given its unambiguous consent, where transfers are necessary for the performance of contracts between the data subject and the controller,

[2495] Article 23 LPDP, first paragraph.
[2496] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[2497] See https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-63023 and, as regards companies participating in the EU-US Data Privacy Framework, https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-70023.
[2498] Available at: https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-17009.
[2499] Available at: https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-4019.
[2500] Article 23 LPDP, penultimate paragraph.
[2501] Article 35 RPDP.
[2502] https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-41021.
[2503] In addition, the Ibero-American Data Protection Network, of which the URCDP is a member, has recently approved the "Standard Contractual Clauses for Latin American Countries" which aim at offering common contractual clauses for Latin America convergent with the modernised EU Standard Contractual Clauses.

including for pre-contractual relationships, in case of important public interests and for the vital interests of the individual[2504].

Importantly, prior to any transfer of data to a non-adequate country or international organisation, a data protection impact assessment must be carried out[2505]. In those cases in which the impact assessment concludes that there are high risks for the protection of personal data, the data controller is required to inform the URCDP[2506], which can in turn exercise its role of monitoring compliance with the LPDP, including through inspections[2507].

1.2. Oversight, enforcement and redress

The independent entity in charge of overseeing compliance with the data protection rules in Uruguay is the URCDP. The Agency can act either on its own initiative or on the basis of complaints from data subjects[2508]. It carries out a number of tasks, such as promoting public awareness in relation to data protection, giving its opinion on administrative and legislative measures relating to data protection, promoting the awareness of controllers and processors of their obligations, monitoring and informing about relevant developments regarding data protection in Uruguay and abroad, and publishing annual reports on its activities. In carrying out its supervisory duties, the Agency has access to all relevant information, as well as to the premises where processing operations are carried out or administered and where data or technical equipment are stored or used[2509].

Under the LPDP, compliance with data protection requirements is ensured through a combination of different measures. The LPDP provides the URCDP with a broad range of powers that are similar to those foreseen in the GDPR, in particular to issue warnings, reprimands and orders (inter alia to suspend processing or engaging in Court proceedings to request the closure of a database[2510], bring processing into compliance with the Act, implement security measures and rectify, erase or restrict processing), and to make its decisions public[2511]. The URCDP can issue fines that can amount up to 500 000 Indexed Units[2512].

As regards the rules to establish the amounts of the fines, the URCDP issued an instruction in 2015 which groups the possible infringements of the LPDP under four categories (very minor, minor, serious and very serious infringements) and sets a range for the amount of the

[2504] Article 23 LPDP.
[2505] Article 6(f) Decree 64/2020.
[2506] Article 7 Decree 64/2020, available at: Decreto N° 64/020 (impo.com.uy). Also relevant the guidance on how to carry out an impact assessment, available at: Guía de Evaluación de Impacto en la Protección de Datos | Unidad Reguladora y de Control de Datos Personales (www.gub.uy).
[2507] Article 34 (D) LPDP gives the URCDP the power to monitor compliance with the legal regime, in particular with the rules on legality, completeness, accuracy, proportionality and security of the processing activities, and in order to do so the URCDP may carry out the relevant checks and inspection actions.
[2508] Article 34 LPDP and Chapter V Decree 414/2009.
[2509] Article 34(d)(4) LPDP.
[2510] Following the amendment of Article 35(5) LPDP through Law 19.355 of 19/12/2015, Article 83, available at: https://www.impo.com.uy/bases/leyes/19355-2015.
[2511] Article 25 Decree 414/2009.
[2512] An Indexed Unit is a unit of value that is readjusted according to inflation as measured by the Consumer Price Index. This unit varies daily so that at the end of the month it accumulates a variation with respect to the value of the UI of the previous month. In June 2022, the value of one indexed unit equalled to around 5.5 Uruguayan pesos.

administrative fines for each category[2513]. The instruction also sets out the factors to be taken into account when deciding on whether to impose a fine and on its amount[2514]. Those factors are similar to the factors listed in the GDPR and include the gravity and reiteration of the infringement, previous records of the controller as well as the categories of personal data affected, the volume of the processing, the existence of security measures, the affected individual rights, the damage caused to the affected data subjects, the benefits derived from the infringing processing activities and any other circumstances relevant to assess the infringement.

As regards possibilities for individuals to obtain redress, the Uruguayan system continues to offer various avenues, including the possibility to lodge a complaint with the Data Protection Agency[2515], obtain judicial redress directly against controllers and processors (both private operators and public authorities) through the habeas data action[2516] and to obtain compensation for damages.

The URCDP plays an active role in Uruguay and Latin America when it comes to exercising its oversight role, engaging with stakeholders and cooperating with other authorities at regional and international level.

As part of its supervisory powers, the URCDP carries out supervision and enforcement activities, including inspections, and handles notifications, written questions and complaints. For example, in 2021 the URCDP issued three administrative fines. In 2020, 14 decisions with observations to data controllers, 24 decisions including warnings and eight administrative fines, as well as 20 calls on data controllers to adapt processing activities to the requirements of the LPDP[2517]. In 2019[2518], four administrative fines were imposed[2519]. In 2018[2520] the URDCP issued three decisions with observations to data controllers, seven decisions including warnings and three administrative fines.

The URCDP is also active in terms of awareness-raising and providing guidance. Its website includes resources for data controllers, data processors and individuals, including the possibility to lodge complaints online[2521] and to seek advice[2522] using online tools. A new

[2513] From 100 to 12000 indexed units in the case of minor infringements, from 12 001 to 90 000 indexed units in the case of serious infringements, and from 90 001 to 500 000 indexed units in the case of very serious infringements. Very minor infringements are subject to warnings by the URCDP.

[2514] Available at: https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-1052015.

[2515] Article 34(a) LPDP.

[2516] Chapter VIII LPDP.

[2517] Annual report 2020, available at: Memoria anual 2020 | Unidad Reguladora y de Control de Datos Personales (www.gub.uy).

[2518] All the relevant resolutions issued by the URCDP in 2019 are available at: Resoluciones | Unidad Reguladora y de Control de Datos Personales (www.gub.uy).

[2519] Decision 22/019, available at: Resolución Nº 22/019, de 14 de mayo de 2019 | Unidad Reguladora y de Control de Datos Personales (www.gub.uy)), Decision 25/019, available at: Resolución Nº 25/019, de 28 de mayo de 2019 | Unidad Reguladora y de Control de Datos Personales (www.gub.uy)), Decision 43/019, available at: Resolución Nº 43/019, de 24 de setiembre de 2019 | Unidad Reguladora y de Control de Datos Personales (www.gub.uy)) and Decision 48/2019, available at: Resolución N° 48/019, de 22 de noviembre de 2019 | Unidad Reguladora y de Control de Datos Personales (www.gub.uy).

[2520] All the relevant resolutions issued by the URCDP in 2018 are available at: Resoluciones | Unidad Reguladora y de Control de Datos Personales (www.gub.uy).

[2521] Available at: Denuncias ante la unidad reguladora y de control de datos personales - URCDP. | Trámites (www.gub.uy).

functionality allowing online data breach notification[2523] has been recently added. In the context of the Covid-19 pandemic, the URCDP advised the Government and the public on issues relating to data protection (e.g., as regards the processing of personal data in a situation of national emergency, the processing of sensitive data as part the vaccination strategy or the processing of personal data in the telework context) [2524].

The URCDP has also provided extensive guidance through the publication of user guides. Among the most recent are the general guide on data protection in Uruguay[2525], the guidance on processing by foreign controllers subject to the LPDP [2526], the guidance on management and notification of personal data breaches[2527], the guidance on how to carry out a data protection impact assessment[2528], the guidance on data protection officers[2529], the guidance on data processing activities carried out by telecommunications operators[2530], the guidance on data processing in the education sector[2531] and the guidance for data processing activities in the public administration[2532]. The URCDP also carries out training activities addressed to public authorities, controllers and the general public. Recent examples are the workshops for data protection officers[2533] or activities with schools[2534] and public administrations.

In terms of international engagement, the URCDP held the Presidency of the Ibero American Data Protection Network[2535] from 2016 to 2020 and is also part of the Bureau of the Consultative Committee for the protection of individuals with regard to the automatic processing of personal data (Convention 108)[2536].

2. ACCESS TO AND USE OF PERSONAL DATA TRANSFERRED FROM THE EUROPEAN UNION BY PUBLIC AUTHORITIES IN URUGUAY

[2522] Available at: Consultas a la Unidad Reguladora y de Control de Datos Personales - URCDP | Trámites (www.gub.uy).
[2523] Available at: Sistema de gestión de la URCDP | Unidad Reguladora y de Control de Datos Personales (www.gub.uy).
[2524] Annual reports covering years 2012 to 2018 available at: https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/informacion-gestion/memorias-anuales .
[2525] Available at: Guía general de Protección de Datos Personales en Uruguay | Unidad Reguladora y de Control de Datos Personales (www.gub.uy).
[2526] Available at: Guía para el cumplimiento de obligaciones por entidades extranjeras | Unidad Reguladora y de Control de Datos Personales (www.gub.uy).
[2527] Available at: Guía para la gestión, documentación y comunicación de vulneraciones de seguridad en datos personales | Unidad Reguladora y de Control de Datos Personales (www.gub.uy).
[2528] Available at: Guía de Evaluación de Impacto en la Protección de Datos | Unidad Reguladora y de Control de Datos Personales (www.gub.uy).
[2529] Available at: Delegado de Protección de Datos Personales Documento de Trabajo | Unidad Reguladora y de Control de Datos Personales (www.gub.uy).
[2530] Available at: Manejo de datos personales en operadores de telecomunicaciones | Unidad Reguladora y de Control de Datos Personales (www.gub.uy).
[2531] Available at: Guía Educación y datos personales | Unidad Reguladora y de Control de Datos Personales (www.gub.uy).
[2532] Available at: Manejo de datos personales en la Administración Pública | Unidad Reguladora y de Control de Datos Personales (www.gub.uy).
[2533] See for instance information on the URCDP's website, available at: Curso para delegados de Protección de Datos Personales | Unidad Reguladora y de Control de Datos Personales (www.gub.uy).
[2534] Information on "your data have value" campaigns available at: Campañas | Unidad Reguladora y de Control de Datos Personales (www.gub.uy).
[2535] Information available at: Seminario "Europa-Iberoamérica: una visión común de la Protección de Datos. El nuevo Marco Europeo y su incidencia en Iberoamérica" | Red Iberoamericana de Protección de datos (redipd.org).
[2536] See information on the website of the Council of Europe, available at: Consultative Committee (coe.int).

2.1 General legal framework

When collecting and (further) processing personal data for criminal law enforcement purposes in Uruguay, public authorities are subject to precise and accessible rules governing the scope and application of a measure and imposing minimum safeguards. These limitations and safeguards follow from the overarching constitutional framework and specific laws that regulate the activities of public authorities in the areas of criminal law enforcement and national security.

First, several provisions of the Constitution of Uruguay guarantee the right to privacy. In particular, Article 28 of the Constitution provides that "the papers of private individuals, their correspondence, whether epistolary, telegraphic, or of any other nature, are inviolable, and they may never be searched, examined, or intercepted except in conformity with laws which may be enacted for reasons of public interest"; while Article 11 of the Constitution states that "the sanctity of the home is inviolable" and that "no one may enter it by night without the consent of its master, and by day only at the express order of a competent judge, in writing, and in cases determined by law". Moreover, Article 10 of the Constitution stipulates that "private actions of persons which do not in any way affect the public order or prejudice others shall be outside the jurisdiction of the magistrates". It should also be noted that although the Constitution does not expressly recognise the right to the protection of personal data, its Article 72 states that "the enumeration of rights, duties, and guarantees made in this Constitution does not exclude others which are inherent in human beings or which are derived from a republican form of government". Both case law[2537] and legal doctrine interpret rights as being "inherent in human beings" when they are part of international human rights treaties to which Uruguay is a party, such as Convention 108[2538]. Importantly, Article 1 of the LPDP expressly stipulates that "the right to the protection of personal data is inherent in human beings and it is therefore included in Article 72 of the Constitution of the Republic".

All laws must conform to the Constitution of Uruguay[2539]. As described in more detail in sections 2.2.1 and 2.3.1, the general principles following from the Constitution of Uruguay are reflected in the specific laws that regulate the powers of law enforcement and national security authorities.

Second, the right to privacy and important aspects of the right to the protection of personal data are also guaranteed through Uruguay's adherence to international conventions.

This includes Uruguay's adherence to the American Convention on Human Rights and its submission to the jurisdiction of the Inter-American Court of Human Rights[2540].

Pursuant to Article 11 of the Convention, everyone has the right to the protection of the law against arbitrary or abusive interference with his private life, his family, his home, or his correspondence. In accordance with Article 30 of the Convention, a public authority may only interfere with the right to privacy in accordance with laws enacted for reasons of general

[2537] See e.g., ruling of Supreme Court 44/021 of 9 March 2021.
[2538] See e.g., C.H. Mendes, R. Gargarella & S. Guid, *The Oxford Handbook of Constitutional Law in Latin America*, Oxford: Oxford University Press 2022, p. 272.
[2539] See Article 256 of the Constitution of Uruguay.
[2540] See the list of signatures and ratifications, available at: https://www.cidh.oas.org/basicos/english/Basic4.Amer.Conv.Ratif.htm

interest and in accordance with the purpose for which such restrictions have been established. These protections apply to all persons falling under the jurisdiction of the state parties to the Convention, irrespective of their nationality[2541].

The Inter-American Court of Human Rights has notably ruled that the protections offered by the right to privacy extend to telephone conversations[2542]. In addition, the Court has specified that, to determine if an interference with the right to privacy is arbitrary or abusive, three factors must be considered: (1) it must be established by law (2) it must have a legitimate purpose, and (3) it must be appropriate, necessary and proportionate[2543]. Regarding the first factor, the Court has clarified that the law on which the interference is based must be clear and precise with detailed rules to establish the boundaries of the restriction. This includes the specific circumstances in which the restriction applies, who can request, order and carry out the restriction, and procedurally how to implement it[2544].

Moreover, in 2013, Uruguay ratified Convention 108[2545]. On 5 August 2021 Uruguay also ratified the amending Protocol creating the modernised Convention 108 (Convention 108+)[2546]. Article 9 of Convention 108 provides that derogations from the general data protection principles (Article 5 Quality of data), the rules governing special categories of data (Article 6 Special categories of data) and data subject rights (Article 8 Additional safeguards to the data subject) are only permissible when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences, or for protecting the data subject or the rights and freedoms of others. The guarantees set out in Convention 108 are extended to every individual regardless of nationality or residence[2547].

Therefore, through adherence to the American Convention of Human Rights and Convention 108, as well as its submission to the jurisdiction of the Inter-American Court of Human Rights, Uruguay is subject to a number of obligations, enshrined in international law, that frame its system of government access on the basis of principles, safeguards and individual rights similar to those guaranteed under EU law and applicable to the Member States.

[2541] Article 1 of the Convention: "The States Parties to this Convention undertake to respect the rights and freedoms recognised herein and to ensure to all persons subject to their jurisdiction the free and full exercise of those rights and freedoms, without any discrimination for reasons of race, color, sex, language, religion, political or other opinion, national or social origin, economic status, birth, or any other social condition".

[2542] Inter-American Court of Human Rights, Escher et al. v. Brazil, Series C 200, judgment of 20 November 2009, paragraph 114. This is the case irrespective of the content of these conversations and can even include both the technical operations designed to record this content by taping it and listening to it, or any other element of the communication process (e.g., the destination or origin of the calls that are made, the identity of the speakers, the frequency, time and duration of the calls). See also Inter-American Court of Human Rights, Tristán Donoso v. Panama, Series C 193, judgment of 27 January 2009, paragraph 75-76.

[2543] Inter-American Court of Human Rights, Escher et al. v. Brazil, Series C 200, judgment of 20 November 2009, paragraph 129. See also Inter-American Court of Human Rights, Tristán Donoso v. Panama, Series C 193, judgment of 27 January 2009, paragraph 76.

[2544] Inter-American Court of Human Rights, Escher et al. v. Brazil, Series C 200, judgement of 20 November 2009, paragraph 130-131.

[2545] See the Chart of signatures and ratifications, available at: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108.

[2546] See the Chart of signatures and ratifications, available at: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=223. Convention 108+ has yet to enter into force.

[2547] See Article 1 of Convention 108, as explained in the Explanatory Report to the Convention, available at: https://rm.coe.int/16800ca434.

Third, the LPDP's general rights and principles apply to the processing of personal data by public authorities for law enforcement and national security purposes[2548], notably the rights to information[2549], access[2550], rectification[2551] and erasure[2552], and the principles of lawfulness[2553], purpose limitation[2554], accuracy and data minimisation[2555], proportionality[2556], data retention[2557] and data security[2558]. In addition, specific safeguards are set out for processing in the law enforcement and national security area. Article 25 LPDP specifically limits the processing of personal data by law enforcement and national security authorities to what is "necessary for the strict compliance with the duties legally assigned to such bodies for national defence, public security or the suppression of crime"[2559]. It also stipulates that law enforcement authorities shall delete personal data that is no longer necessary for the purposes that led to their storage. Moreover, Article 26 LPDP specifically confirms that data subjects may exercise their rights of access, rectification and erasure against law enforcement or national security authorities, including with respect to data that is being processed for public safety, defence, national security and law enforcement purposes. Controllers are allowed to deny, in whole or in part, requests to exercise these rights, but only to the extent necessary for specific purposes listed exhaustively in the law and similar to the purposes that allow for a restriction of data subject rights in the EU data protection framework[2560].

These abovementioned principles and safeguards can be invoked by individuals before independent administrative bodies and courts to obtain redress, in particular through the habeas data action (see sections 2.2.2, 2.2.3, 2.3.2 and 2.3.3).

2.2 Access and use by Uruguayan public authorities for criminal law enforcement purposes

In Uruguay, criminal law enforcement functions are carried out by the National Police, the National Naval Prefecture and the National Air Police. In the specific case of financial crime, the responsible authority is the Financial Information and Analysis Unit (UIAF)[2561].

[2548] While Article 3 LPDP sets out that the law does not apply to "databases whose purpose is public security, defence, State security and its activities in criminal matters, investigation and suppression of crime", the Uruguayan authorities have explicitly confirmed that in line with the obligations of the Constitution of Uruguay and Uruguay's international commitments in the area of human rights, the exemptions in Article 3 LPDP are to be understood to apply only to the obligation to register databases, but not to the main principles set out in the law. In addition, Article 25 LPDP sets out that the provisions of the Law, including the ones concerning the registration of databases, do apply to personal data which have been stored for administrative purposes in the databases of the armed forces, police or intelligence agencies. This includes personal data in files concerning criminal records.
[2549] Article 13 LPDP.
[2550] Article 14 LPDP.
[2551] Article 15 LPDP, that also recognises the right to seek the update of personal data, the right to have personal data included in a database.
[2552] Article 15 LPDP
[2553] Article 6 LPDP.
[2554] Article 8 LPDP.
[2555] Article 7 LPDP.
[2556] Article 7 LPDP.
[2557] Article 8 LPDP.
[2558] Article 10 LPDP.
[2559] Article 25 LPDP.
[2560] Article 26 LPDP. Such purposes include the defence of the State or public safety, the protection of the rights and freedoms of third parties or the needs of investigations that are being carried out.
[2561] Article 2 of Law No. 19.574 of 20 December 2017, available at: https://www.impo.com.uy/bases/leyes/19574-2017.

Uruguayan law imposes a number of limitations on the access to and use of personal data for criminal law enforcement purposes and provides oversight and redress mechanisms. The conditions under which access to personal data can take place and the safeguards applicable to the use of these powers are described in the following sections.

2.2.1 Legal bases and applicable limitations/safeguards

Personal data transferred from the EU on the basis of the adequacy decision and subsequently processed by Uruguayan controllers/processors may be obtained by Uruguayan law enforcement authorities by means of investigative measures under statutes providing for law enforcement access, the main one being the Criminal Procedure Code 2017 (CPC 2017)[2562], or on the basis of anti-money laundering and anti-terrorist financing legislation.

The CPC 2017 provides Uruguayan law enforcement authorities with a legal basis to access personal data held by controllers/processors through searches and seizures, the use of production orders or the interception of communications. It lays down clear and precise rules on the scope and application of these measures, thereby ensuring that the interference with the rights of individuals will be limited to what is necessary for a specific criminal investigation and proportionate to the purpose pursued. Moreover, as explained in more detail below, prior judicial authorisation is in principle required to exercise these powers.

More specifically, searches and seizures may only be carried out if there are reasonable grounds to believe that objects (including hard drives or other electronic devices where personal data is kept or stored) from criminal activity or objects relevant to the investigation may be found in a home or other enclosed place[2563]. In terms of procedural safeguards, a search or seizure may only take place on the basis of a court-issued warrant[2564]. Warrantless searches or seizures are allowed only in a limited number of exceptional circumstances set out in the CPC 2017[2565]. The inhabitant of the premise subject to the search is always notified of the search and in principle present when it is carried out. Where this is not the case, this must be recorded in the minutes of the search[2566].

[2562] Law No. 19.293 of 19 December 2014, available at: https://www.impo.com.uy/bases/codigo-proceso-penal-2017/19293-2014.

[2563] Article 191, 195 and 197 CPC 2017.

[2564] Article 191 and 195(1) CPC 2017. The search warrant must contain detailed information, including the name of the authorising prosecutor, the date on which the search is to be carried out, the specific purpose of the search and the precise designation of the property to be searched and seized, see Article 192(1) and 198 CPC 2017.

[2565] First, based on Article 189(2) CPC 2017, a law enforcement authority, by order of the prosecutor or on its own, giving immediate notice to the prosecutor, may inspect or order the search of open places, objects or persons, when there are sufficient grounds to consider that traces of a crime may be found or that the accused or a fugitive is in a certain place. Second, Article 195(5) CPC 2017 provides that a police report of domestic violence counts as express authorisation for the search of a home within forty-eight hours of its presentation. Third, Article 195(3) CPC 2017 provides that a search may be carried out at night, with the express consent of the head of the household, with the immediate notification of the public prosecutor and the competent judge. Fourth, Article 197(2) CPC 2017 provides that property which constitutes the corpus delicti or which is necessary for the clarification of the facts under investigation may be seized without a court order in the case of a crime committed 'in flagrante delicto' or in imminent danger of its perpetration. When there is danger due to delay, the public prosecutor must order the seizure, reporting to the competent judge and in accordance with his decision.

[2566] Article 196(1) CPC 2017. In case of a search of a premise other than a home, the prior notice of the person who is in charge of the premise may, at the discretion of the court, be dispensed with when the prior notification is considered detrimental to the effectiveness of the search, see Article 192(2) CPC 2017.

Illegal searches are subject to criminal sanctions. Article 287 of the Criminal Code provides that a public official who, by abusing his functions or without the formalities prescribed by law, orders or carries out a personal inspection or search, shall be punished with three to twelve months imprisonment[2567]. Furthermore, Article 294 provides that anyone who enters another person's home or its premises against the express or tacit will of the owner or the person acting in his stead, or who enters it clandestinely or by deception, shall be punished with three to twenty-four months imprisonment. When committed by a public official, without the conditions and formalities prescribed by law, this counts as an aggravating circumstance[2568].

Under the CPC 2017, the public prosecutor may also order the production of public or private documents that are relevant to an investigation[2569]. Whoever is in possession of the requested documents is obliged to immediately produce them or hand them over to the public prosecutor, unless he invokes a legitimate reason[2570] for not doing so, in which case it will be for the court to take a decision[2571]. Furthermore, the Public Prosecutor's Office may request from public or private institutions all necessary information that is available in their records for the investigation to be carried out, provided that the disclosure of such information does not imply interferences with the fundamental rights and guarantees applicable to individuals, including the right to privacy[2572]. Communications between the accused and his defence counsel or persons covered by professional secrecy may not be admitted as evidence or used in any other way[2573].

Specific limitations and safeguards apply to the interception of communications[2574]. This power may only be used in the context of a criminal investigation and on the basis of a judicial warrant[2575]. An interception of communications may be authorised "when there is sufficient evidence to consider that a punishable offence has been or may be committed"[2576]. Importantly, the Court of Appeals in Criminal Matters No. 2 has ruled that the judge, when assessing the application for an interception warrant, must always review the proportionality of the measure in light of the circumstances of the case and assess whether there are no other effective, less intrusive means of collecting evidence available[2577]. This standard is also enshrined in Article 208(1) CPC 2017, which provides that the judge's decision (which must be well-founded) must "expressly consider the necessity and proportionality of the measure with respect to the restriction of the exercise of the limited right, under penalty of nullity". In addition, based on settled case-law of the Inter-American Court of Human Rights, any

[2567] The Criminal Code is available at: https://www.impo.com.uy/bases/codigo-penal/9155-1933.
[2568] Article 295 of the Criminal Code.
[2569] Article 203(1) CPC 2017.
[2570] For example, documents containing anonymous statements may not be brought to trial or used in any way, unless they constitute the corpus delicti or come from the accused, see Article 173(3) CPC 2017.
[2571] Article 203(2) CPC 2017.
[2572] Article 45(k) CPC 2017.
[2573] Article 173(4) CPC 2017. This exception does not apply if these persons are also defendants, nor when they are means for the preparation, execution or concealment of the offence.
[2574] Article 208 CPC 2017. Communications include telephone, radio or other forms of communication.
[2575] The CPC 2017 does not provide for any exceptions to this requirement.
[2576] Article 208(1) CPC 2017. The court may not intercept communications between the accused and his defence counsel, unless the court orders it on the grounds that the lawyer may be criminally responsible for the acts under investigation. This must be recorded in the respective decision. See Article 208(3) CPC 2017.
[2577] Court of Appeals in Criminal Matters No. 2, Sentence 377/2013, judgement of 6 November 2013, available only at: http://bjn.poderjudicial.gub.uy/BJNPUBLICA/hojaInsumo2.seam?cid=84582.

interference with the inviolability of communications must be provided for by law, pursue a legitimate aim and comply with the requirements of suitability, necessity and proportionality[2578].

Procedurally, interception requests must be submitted by the prosecutor to the competent judge[2579]. An interception warrant is only valid for a – non-renewable – maximum period of six months[2580]. The interception must be stopped if the reasons used to authorise the measure no longer exist, or once the interception warrant has expired[2581].

Specific rules govern investigative activities with respect to the prevention of money laundering and the financing of terrorism. In this respect, Article 62 of Law No 19.574 allows the use of electronic surveillance as part of a criminal investigation into any of the serious crimes listed in Articles 30 to 33 of the Law (money laundering offences) and in Article 34 of the Law (so-called "predicate offences" that precede the crime of money laundering, such as drug trafficking and related crimes)[2582]. As is the case with regard to the interception of communications under the CPC 2017, electronic surveillance measures that interfere with the inviolability of communications are only allowed insofar these measures are suitable, necessary and proportionate. This follows from the previously mentioned case-law of the Court of Appeals in Criminal Matters No. 2 and the Inter-American Court of Human Rights[2583].

Procedurally, Article 62 of the Law prescribes that requests for electronic surveillance must be submitted by the public prosecutor's office to the competent court and must be reasoned. The competent court is responsible for the supervision of the process. The results of the surveillance activities must be transcribed in certified records so that they can be incorporated into the proceedings. Once the defence council of the defendant has been appointed, the proceedings must be made available to it for its control and analysis, and the material must be submitted to the defendant for the recognition of voices and images.

Illegal wiretapping and related conduct are subject to criminal sanctions. Those who open, intercept, destroy or hide correspondence, parcels, and other postal objects with the intention of taking possession of their content or of disrupting their normal course may be punished

[2578] Inter-American Court of Human Rights, Escher and Others v. Brazil, Series C 200, judgment of 6 July 2009, paragraph 116, and its citation of the case of Tristan Donoso vs Panama, Series C 193, judgment of 27 January 2009, paragraph 56.
[2579] Article 208(1) CPC 2017. The judicial decision ordering the interception must contain the name of the person affected by the measure and, if possible, the telephone line or other means of communication to be intercepted, recorded or registered. It must also indicate the form, scope and duration of the measure, as well as the authority or official who will be in charge of the procedure. See Article 208(4) CPC 2017.
[2580] Article 208(4) CPC 2017.
[2581] Article 208(5) CPC 2017.
[2582] The object of electronic surveillance can take different forms, including telephone conversations, text messages, e-mails, video cameras, microphones and communication data (metadata). See J.L.G. González, 'Control y prevención de lavado de activos y financiamiento del terrorismo. Ley N° 18.494', *Revista de la Facultad de Derecho* 2010, p. 148, available at: http://www.redalyc.org/articulo.oa?id=568160365010.
[2583] Communications between the defendant and his defence counsel, in the exercise of the right of defence and those communications that concern issues that are not related to the object of the investigation may not be subjected to electronic surveillance in accordance with Article 62.

with one year of imprisonment or up to four years of penitentiary. When the offender is a public official, this is considered an aggravating circumstance[2584].

Finally, Article 12 and 13 of Law No. 19.574 impose an obligation on persons and undertakings subject to the law, such as financial institutions[2585], to report to the UIAF, on their own initiative, any suspicious transaction, carried out or not, and any financial transaction involving assets suspected of being illegitimate[2586]. Prior to notifying the UIAF, persons and undertakings subject to the law are required to identify their clients and take certain customer due diligence measures, including identifying the beneficial owner of the account or transaction (taking reasonable measures to verify its identity), gathering information on the purpose of the commercial relationship and the nature of the business to be conducted and monitoring the business relationship[2587]. They are furthermore required to keep records of all transactions carried out with or for their customers, both national and international, including all the information obtained during the due diligence process, for a minimum period of five years after the end of the business relationship or after the conclusion of the occasional transaction or for a longer period of up to ten years, in accordance with the provisions of the regulations. This information must be sufficient to allow for the reconstruction of transactions and to constitute elements of evidence in court, if necessary, and be available to the supervisory authorities and the competent criminal court upon request[2588].

2.2.2 Further use of the information collected

The further use of data collected by Uruguayan criminal law enforcement authorities on one of the grounds referred to in Section 2.2.1, as well as the sharing of such data with a different authority for purposes other than the ones for which it was originally collected (so-called 'onward sharing'), is subject to safeguards and limitations.

First, the LPDP contains specific protections for personal data that is processed by public authorities for law enforcement purposes, as explained in section 2.1. With respect to onward sharing, it follows from Article 25 LPDP that the dissemination of personal data by these authorities is limited to what is strictly necessary for the fulfilment of their respective tasks. In addition, Article 25 LPDP provides that personal data that is collected for law enforcement

[2584] Article 296 of the Criminal Code.
[2585] Persons and undertakings subject to the law are all natural and legal persons subject to the control of the Central Bank of Uruguay (Article 12 of Law No. 19.574) and the non-financial entities listed in Article 13 of Law No. 19.574 (e.g., casinos, real estate agents and civil law notaries).
[2586] Pursuant to Article 12 of Law No. 19.574, a suspicious transaction is defined as a transaction "that in the use and customs of the respective activity are unusual, are made without clear economic or legal justification or are presented with unusual or unjustified complexity". Pursuant to Decree No. 379/018 (Regulation of Law 19.574 against money laundering), reports of unusual or suspicious transactions must include at least the following information: (1) identification of the natural or legal persons involved, (2) a description of the transactions that are presumed to be unusual or suspicious, indicating whether or not they were carried out, their dates, amounts, type of operation and, in general, any other data or information considered relevant for these purposes, (3) details of the circumstances or indications that led the person making the communication to classify such transactions as unusual or suspicious of being related to the laundering of proceeds of crime or the financing of terrorist activities, attaching, where appropriate, a copy of the proceedings related to the analysis carried out. Decree No. 379/018 is available at: https://www.impo.com.uy/bases/decretos/379-2018.
[2587] Article 15 of Law No. 19.574.
[2588] Article 21 of Law No. 19.574.

purposes must be deleted when they are no longer necessary for the purposes for which they were stored.

Second, the different laws that allow for data collection by criminal law enforcement authorities in Uruguay impose specific limitations and safeguards as to the use and further dissemination of the information obtained in exercising the powers they grant.

As regards the powers of search and seizure, the CPC 2017 provides that the assets subject to seizure shall be registered and duly individualised, and a record shall be kept of the person who assumes the depositary[2589]. The public prosecutor or the administrative authority, with the authorisation of the court, may return the seized objects to the victim or to third parties[2590].

With respect to the interception of communications, the CPC 2017 stipulates that intercepted, recorded or registered material which is not incorporated into the investigation shall be destroyed, unless a court order to the contrary is made for good reason to keep it on file for the maximum duration of the investigation[2591]. In a similar vein, Article 62 of Law No. 19.574 provides that the court must discard material obtained through electronic surveillance that does not relate to the subject matter of the investigation. On the other hand, the court is required to preserve and safeguard the electronic media containing the obtained material until the sentence has been served.

In terms of investigative measures carried out in the context of the fight against money laundering and terrorism financing, Law No. 19.574 provides that the UIAF may disclose information relating to unusual or suspicious transactions to public authorities specialised in combating money laundering and its predicate offences, when it considers the participation of such authorities essential to complete ongoing investigations, for the purpose of obtaining the elements of judgment necessary to link the transactions under investigation with the aforementioned offences and to enable the competent criminal court to be informed[2592].

Finally, rules on mutual legal assistance in criminal matters are provided for by Law No. 19.574. These rules only apply to requests for legal assistance from foreign authorities for the investigation or prosecution of the money laundering offences referred to in Articles 30 to 33 of the law and the predicate offences referred to in Article 34 of the law. Article 72 of the law provides that in cases of requests for legal assistance in criminal matters concerning searches, lifting of the bank secrecy, seizure, confiscation and delivery of any object, including, inter alia, documents, records or effects, the acting national court shall process the request if it determines that the request contains all the information justifying the measure requested. Such measure shall be subject to the procedural and substantive Uruguayan law.

2.2.3 Oversight

Different bodies provide oversight over the processing of personal data for criminal law enforcement purposes by the relevant authorities of Uruguay.

[2589] Article 199(2) CPC 2017.
[2590] Article 200(1) CPC 2017.
[2591] Article 208(5) CPC 2017.
[2592] Article 28 of Law No. 19.574.

First, the URCDP is competent to oversee compliance with the LPDP's rights and principles in the context of processing activities carried out by criminal law enforcement authorities. Furthermore, the URCDP oversees compliance with the specific safeguards set out in Article 25 LPDP (see section 2.1 above). If the URCDP finds an infringement of the LPDP, it provides the relevant public authority with a reasoned decision, stating that the facts investigated constitute an infraction, who is responsible for that infraction, and the sanction to be applied[2593]. For example, in 2019 the URCDP delivered a number of opinions and reports addressed to the National Secretariat for the Fight against Money Laundering and Terrorist Financing[2594]. One opinion dealt with the question whether it was lawful for the Secretariat to publish the resolutions that impose sanctions to reporting entities[2595].

Second, the National Institution for Human Rights and the Ombudsman (INDDHH) adds another layer of independent oversight. The INDDHH is a specialized institution of the legislative branch, tasked to defend, promote and protect fundamental rights recognised by the Constitution and international law[2596]. It is headed by the Board of Directors, a collegiate body whose five members are elected by the Uruguayan Parliament[2597]. The INDDHH is competent to investigate alleged human rights violations at the request of a party or of its own initiative, and to report on the human rights situation at national, departmental or local level[2598]. The independence of the INDDHH is guaranteed by law[2599] and in carrying out its investigations the INDDHH has access to all relevant information and can access all relevant premises[2600].

[2593] Article 29 and 31 RPDP. Sanctions can consist of warnings, reprimands and orders (inter alia to suspend processing or engaging in Court proceedings to request the closure of a database, bring processing into compliance with the Act, implement security measures and rectify, erase or restrict processing), and to make the decision public, see Article 35 LPDP and 25 RPDP.

[2594] See the URCDP publication 'Resoluciones, dictámenes e informes 2019', available at: https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/resoluciones-dictamenes-informes-2019/resoluciones-dictamenes-informes.

[2595] Opinion 11/019, available at: https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/resoluciones-dictamenes-informes-2019/dictamenes/dictamen-11019-24.

[2596] Article 1 of Law No. 18.446, available at: https://www.impo.com.uy/bases/leyes/18446-2008. In addition to the INDDHH, the Human Rights Secretariat was set up under the Presidency of the Republic in accordance with the provisions of Articles 67 to 69 of Law No. 19.149 as the body responsible for ensuring a human rights approach by the Executive in the pursuit of public policies and in relation to society.

[2597] Article 36 and 37 of Law No. 18.446. The members of the Board of Directors are elected for a period of five years, renewable once (Article 41 of the law) and can only be removed by parliament with the same number of votes by which they were elected, on specific grounds, set out in Article 52(f) of the law (e.g., for engaging in conduct that makes him/her unworthy of his/her office, for acting with notorious negligence in the fulfilment of the obligations and duties of the office, for having committed a serious breach of the duties inherent to the office).

[2598] Article 4(J) and (F) of Law No. 18.446. The competence of the INDDHH, without prejudice to expressly established exceptions, extends to all public powers and bodies regardless of their legal nature and function, whether they act in the national territory or abroad, see Article 5 of Law No. 18.446.

[2599] Article 2 and 51 of Law No. 18.446. The INDDHH has its own budget, which is approved by the Parliament, see Article 74 and 75 of the law.

[2600] Article 35 of Law No. 18.446. The investigatory powers of the INDDHH set out in Article 35 include the power to a) carry out, with or without prior notice, inspection visits to any place or sector of activity of the agencies and entities under its competence, b) interview any authority, request reports, examine files, archives and any type of document, carry out interrogations or any other reasonable procedure, and c) interview any person and request the provision of reports or documentation that may be necessary to clarify the matter in which it intervenes and to carry out all other actions aimed at clarifying the facts. Public authorities and other entities falling under the competence of the INDDHH may not invoke reasons of secrecy, reserve or confidentiality, whenever the INDDHH requests information regarding human rights violations or when it is relevant to

Based on the findings of its investigation, the INDDHH may propose[2601] to the competent authorities the adoption of the measures it deems appropriate to put an end to the human rights violation it has found and establish the time period within which they must be complied with, suggesting the reparation measures it deems appropriate[2602]. In urgent cases, it may propose (at any stage of the proceedings) the adoption of interim measures in order to cease alleged violations of human rights or to prevent harm or further damage. Moreover, in that case it may also turn to the judiciary in order to request the precautionary measures it deems appropriate, and to file appeals for "*amparo*" or "*habeas corpus*" (see next section)[2603]. If the INDDHH through an investigation becomes aware of potential crimes committed by public authorities, it must bring it to the attention of the competent courts[2604]. The Ombudsman is required to lay an annual report before Parliament which must contain, inter alia, an account of the number and types of complaints submitted, those that have been rejected and the reason for their rejection, as well as those that have been investigated and their outcome[2605]. According to the last figures available, the INDDHH handled 617 cases and issued 127 resolutions in 2022[2606].

2.2.4 Redress

The Uruguayan system offers different (judicial) avenues to obtain redress, including compensation for damages.

First, individuals have a right to obtain access to and rectification or deletion of their data held by public authorities.

Article 14 LPDP provides that any data subject has the right to obtain all information about him- or herself held in public or private databases[2607]. In addition, Article 15 LPDP stipulates that, subject to certain conditions, any natural or legal person shall have the right to request

---

investigate, prevent or avoid human rights violations, see Article 72 of the law. In case of non-cooperation of the respective authority with the investigation, Article 23 of the law provides that the INDDHH may 'name and shame' the authorities and other officials who have adopted such an attitude (i.a. by mentioning their non-compliance in its annual report).

[2601] Resolutions of the INDDHH have the character of (non-binding) recommendations, see Article 3 of Law No. 18.466.

[2602] Article 25 of Law No. 18.446. In addition, it may also make general recommendations to eliminate or prevent situations that are the same or similar to those that motivated the complaint, see Article 26 of the law. In case the respective authority does not accept or implement in a timely manner the recommendation or proposal made by the INDDHH, Article 28 of the law allows the INDDHH to 'name and shame' the authorities and other officials who have adopted such an attitude (i.a. by expressly mentioning their names and positions in its annual report).

[2603] Article 24 of Law No. 18.466.

[2604] Article 30 of Law No. 18.466.

[2605] Article 68 and 69 of Law No. 18.466.

[2606] See the INDDHH's 2022 Annual Report, available at: https://www.gub.uy/institucion-nacional-derechos-humanos-uruguay/comunicacion/publicaciones/informe-anual-asamblea-general-2022-0. For a case that concerned the collection of personal data by criminal law enforcement authorities, see for example Resolution N° 729/019 with recommendations to the Minister of Interior, available at the following link: https://www.gub.uy/institucion-nacional-derechos-humanos-uruguay/institucional/informacion-gestion/resoluciones/resolucion-n-729019-recomendaciones-ministerio-del.

[2607] The information must be comprehensive and cover the entire record pertaining to the data subject, even if the request only covers one aspect of the personal data. In no case may the report disclose data belonging to third parties, even if they are linked to the data subject. The information must be provided in a clear form, free of codifications and, where appropriate, accompanied by an explanation of the terms used, in language accessible to an average member of the population.

the rectification, updating, inclusion or erasure of personal data relating to him/her included in a database[2608]. Both the right of access and the right to rectification or deletion may be exercised free of charge[2609]. The relevant public authority may only refuse requests based on the right of access and the right to rectification and deletion to the extent necessary for the purpose of safeguarding certain important public interest (i.e., the defence of the State or public security, the protection of the rights and freedoms of third parties or the needs of investigations being carried out)[2610]. These exemptions are not absolute but require the relevant authority to decide on a case-by-case basis whether to invoke them, after balancing the relevant interests at stake, including the privacy interests of the individual concerned[2611]. In addition, Article 26 LPDP gives individuals the right to ask the URCDP to check the decision of the relevant public authority when access, rectification or deletion requests are rejected. The URCDP must then determine whether the decision was appropriate (or not) in view of the documents and justification provided by the authority. As will be explained in more detail below, individuals whose requests have been denied also have the possibility to pursue the special judicial remedy of 'habeas data' to gain access to their data or to have that data rectified or deleted[2612].

Second, any individual may lodge a complaint with the URCDP concerning processing activities carried out by criminal law enforcement authorities. As described in section 2.2.3, if the URCDP finds a violation of the LPDP, it provides the relevant public authority with a decision stating that the facts investigated constitute an infraction, who is responsible for the infraction and the administrative sanction to be applied. Decisions of the URCDP may be challenged before the Court of Administrative Litigation in accordance with Decree Law No. 15.524[2613]. The court may declare the decision void, in which case the URCDP will have to take a new decision, taking the judgement of the court into account[2614].

Third, judicial redress is available to all data subjects through the habeas data action or the writ of amparo.

[2608] The deletion or suppression of personal data may be carried out in the following cases: a) damage to the rights and legitimate interests of third parties, b) obvious error and c) contravention of the provisions of a legal obligation. As explained in section 1.1., the URCDP has established through various decisions a 'right to be forgotten' similar to the one recognised in the EU by extending the rights to deletion and objection and drawing on the principles of purpose limitation and data accuracy set out in the LPDP.

[2609] Article 14 and 15 LPDP. The right of access may only be exercised free of charge at intervals of six months unless a legitimate interest has arisen again in accordance with the legal system.

[2610] Article 26 LPDP.

[2611] See for example ruling of the Civil Court No. 2, *AAA y otros c/ Google Inc. Estados Unidos y otro*, case number 60/2021, judgement of 19 October 2021, available at k: http://bjn.poderjudicial.gub.uy/BJNPUBLICA/hojaInsumo2.seam?cid=153550. In this case concerning a request to a search engine, based on Article 15 LPDP, to de-index certain search results, the court considered that "The decision to be taken must form part of our system of law, taking into account the national and international provisions analysed above, weighing up the various rights and interests at stake and weighing – ultimately and in the specific case – whether the protection of the personality rights of the actors infringes the rights to freedom of information and expression in order to determine whether or not they should be granted the 'right to be forgotten'". See also URCDP Opinion No. 6/017 of 26 July 2017 on the lawfulness of the processing of certain data published by the Ministry of Interior for security purposes, available at the following link: https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/dictamen-n-6017 .

[2612] Article 14 and 15 LPDP. The 'habeas data' remedy is set out in Article 37 LPDP and further.

[2613] Decree Law No. 15.524 of 1 September 1984 (Organic law on the Court of Administrative Litigation), available at: https://www.impo.com.uy/bases/decretos-ley/15524-1984.

[2614] Article 28 of Decree Law No. 15.524.

Through the habeas data action every person may enforce the right to access any personal data processed by public or private entities concerning him or her, as well as to receive information on the purposes of processing. In addition, the individual may seek rectification, insertion, deletion or review of his or her personal information in cases of error, misrepresentation, discrimination, data outdated or prohibition to process data[2615]. The LPDP provides the conditions for a habeas data action before courts against actions by public authorities[2616]. Once the deadline for the controller to either provide the information requested by the data subject, or to correct, delete or update the information, has expired and the controller has not complied with the request, or if the data subject considers the response insufficient, s/he may initiate a judicial habeas data procedure[2617].

After having exhausted all available judicial and administrative remedies, individuals can also file a writ of amparo against any act, omission or deed of the relevant public authority that in their opinion, injures, restricts, alters or threatens, with manifest illegitimacy, any of their rights and freedoms expressly or implicitly recognised by the Uruguayan Constitution (which, as explained in section 1.1., includes the right to protection of personal data)[2618]. If the writ is granted, individuals can obtain an injunction containing a "precise determination of what must or must not be done" to remedy the violation of the right or freedom at stake[2619].

Fourth, judicial redress is also available via the general civil law actions available against public authorities, including law enforcement authorities. Based on Article 12 LPDP and the general regulations of Uruguayan civil law, and in particular of its Civil Code, any interested party who has suffered damages as a consequence of their personal data being processed may request the relevant redress. Said redress may include the material damages suffered as well as moral damages[2620].

Finally, once all national law remedies are exhausted, data subjects may bring their case before the Inter-American Commission of Human Rights.

2.3 Access and use by Uruguayan public authorities for national security purposes

In Uruguay, the State Strategic Intelligence Secretariat (SIEE) and certain entities carrying out intelligence and counterintelligence tasks within the ministries of Interior, National Defence, Foreign Affairs and Economy and Finances may access personal data transferred from the EU to Uruguay for national security purposes[2621]. The SIEE is the highest-ranking intelligence

[2615] Article 37 LPDP.
[2616] Article 14, 15 and 38-45 LPDP.
[2617] Article 14, 15 and 38 LPDP.
[2618] Article 1 and 2 of Law No. 16.011 on the Regulation of the Amparo Writ, available at: https://www.impo.com.uy/bases/leyes/16011-1988. The writ of amparo cannot be filed against certain acts, e.g., judicial acts, whatever their nature and the organ from which they emanate.
[2619] Article 9 of Law No. 16.011.
[2620] Articles 1319 and 1324 Civil Code No. 16603.
[2621] The bodies carrying out intelligence tasks within the ministries of Interior, National Defence, Foreign Affairs and Economy and Finances are: (1) the Strategic Intelligence Directorate (DIE) of the Ministry of Defense, (2) the National Directorate of Information and Intelligence (DNII) of the Ministry of Interior, (3) the Directorate for Public Affairs of the Ministry of Foreign Affairs, (4) the Directorate of National Customs of the Ministry of Economy and Finances, (5) the Financial Information and Analysis Unit (UIAF) of the Ministry of Economy and Finances and (6) the Military Intelligence Units (Army, Navy, Air Force) of the Ministry of Defense.

agency in Uruguay and the head of the so-called National Intelligence System[2622]. The SIEE is tasked – among others[2623] – to "produce strategic intelligence in order to support strategic decision-making aimed at achieving national objectives"[2624] and to "provide for the application of intelligence and counter-intelligence measures in order to detect and deal with threats to the State"[2625]. The relevant powers of the SIEE and the other intelligence agencies, as regulated by the National Intelligence Act and its regulatory decree[2626], are described in the following sections.

2.3.1 Legal bases and applicable limitations/safeguards

Based on the National Intelligence Act, the SIEE and the other intelligence agencies may access personal data transferred to Uruguay as part of different activities, which are subject to specific limitations and safeguards following from the National Intelligence Act itself, the LPDP, the Uruguayan Constitution, and case law.

As an exercise of public authority, government access for national security purposes in Uruguay must be carried out in full respect of the law (legality principle)[2627]. In particular, pursuant to Article 6 of the National Intelligence Act, each intelligence agency must take the necessary measures to ensure its strict compliance with "the regulations in force on the management and use of personal data". As such, based on 25 LPDP, the accessing of personal data transferred from the EU to Uruguay by the SIEE and other intelligence agencies for national security purposes may only take place in so far this is necessary for the performance of their legal duties. In a similar vein, in accordance with Article 5(e) of the National Intelligence Act, only the necessary information may be collected (principle of balancing).

[2622] The National Intelligence System consists of (1) the SIEE, (2) the entities carrying out intelligence and counterintelligence tasks within different ministries, and (3) entities which, because of the information they manage or by means of their technical capacity, can contribute to the purpose of the National Intelligence System, see Article 9 of the National Intelligence Act. The mission of the different entities making up the National Intelligence System is "to cooperate and to exchange information in order to produce strategic intelligence", see Article 8 of the National Intelligence Act. 'Strategic intelligence' is defined in Article 3 of the Act as "knowledge elaborated at the highest level, necessary for decision making, policy formulation and elaboration of plans for the achievement of national objectives. It refers to a global view on national and international political, economic, diplomatic, environmental and military issues".

[2623] Other tasks of the SIEE include formulating the National Intelligence Plan; designing and executing the intelligence programmes and budgets included in the National Intelligence Plan; to conduct relations with the intelligence agencies of other states and to formulate norms and standardised procedures common to all the bodies of the National Intelligence System. See Article 11 of the National Intelligence Act.

[2624] Article 10 of the National Intelligence Act. In accordance with the National Defense Policy, these goals are the maintenance of the territorial, maritime, aerospace and cyberspace integrity of the country; the international integration of the Republic; the protection of the population in emergency situations; the development of the country and the realisation of human security in all its aspects; the international promotion of democracy; the protection of the environment; the protection of renewable and non-renewable strategic resources and presence in Antarctica. See Decree No. 157/022 of 30 May 2022 on the National Intelligence Policy, available at: https://www.impo.com.uy/bases/decretos-originales/157-2022#ANEXO.

[2625] Article 11 of the National Intelligence Act. In accordance with the National Defense Policy, these threats are violation of land, maritime, aerospace or cyberspace sovereignty; terrorism, per se or linked to organised crime; organised crime; cyber-attacks; meteorological phenomena, disasters or catastrophes of natural or man-made origin, affecting the population, the environment or critical infrastructures; biosecurity incidents; deterioration of the environment; pandemics and epidemics; democratic instability in the region and regional conflicts. The National Intelligence Plan contains the intelligence and counter-intelligence measures aimed at detecting and dealing with the threats defined by the National Defence Policy. See Decree No. 157/022.

[2626] Decree No. 157/022.

[2627] Article 5(d) of the National Intelligence Act. The principle of legality also includes the obligation to avoid privacy-invasive activities.

Based on Article 20 of the National Intelligence Act, any intelligence agency belonging to the National Intelligence System may obtain relevant background information, including personal data, necessary for the fulfilment of the specific operational mission of that intelligence agency, by carrying out "special procedures that may affect the freedom and privacy of citizens". Such special procedures include: (1) surveillance of telephone, computer, radio communications or correspondence in any of its forms, (2) surveillance of information systems and networks, (3) electronic listening and tapping, including of audio-visual communications and (4) interception of any other technological system intended for the transmission, storage and processing of communications or information[2628]. Any intelligence activity involving the use of these "special procedures that may affect the freedom and privacy of citizens" may only be carried out when authorised by a judicial warrant[2629]. Moreover, in accordance with the case-law of the Inter-American Court of Human Rights mentioned in section 2.2.1 with respect to the interception of communications under the CPC 2017, any surveillance measures that interfere with the inviolability of communications are only allowed insofar these measures are suitable, necessary and proportionate.

The use of the abovementioned powers is also subject to limitations and safeguards that are specifically designed to prevent their (mis)use, and to ensure the protection of fundamental rights, including those guaranteed by Article 10, 11 and 72 of the Uruguayan Constitution. In particular, the National Intelligence Act provides that no intelligence agency may (1) carry out repressive tasks or perform, on their own, police or criminal investigation functions, unless such activity is within their specific legal duties or mandated by court order in the framework of a specific case, (2) intervene in the political, social or economic activity of the country, in its foreign policy or in the internal life of political parties, or (3) influence in any way public opinion, individuals, the media, associations or groups of any kind[2630].

Finally, violations of the above-mentioned rules are subject to criminal sanctions, as detailed in section 2.2.1.

2.3.2 Further use of the information collected

The LPDP contains specific protections for personal data that is processed by the SIEE and other bodies that make up the National Intelligence System for national security purposes, as explained in section 2.1. In addition, the National Intelligence Act imposes specific limitations on the further sharing of data, including personal data, with other entities inside or outside Uruguay. When sharing data with each other or with third parties, intelligence agencies must observe the principle of balancing, requiring that the dissemination of data they have collected is limited to what is strictly necessary for the fulfilment of their respective

[2628] Article 20 stipulates that "the regulations of this law shall specifically establish the special procedures as well as the hypotheses in which they may be used". At the time of the publication of this report, these regulations had not yet been adopted.
[2629] Article 20 of the National Intelligence Act.
[2630] Article 7 of the National Intelligence Act. The overall aim of the legislative framework to establish clear boundaries for intelligence activities is also reflected in Chapter IX ('Acting in accordance with the law') of Decree No. 157/022, which specifically provides that "the fulfilment of the intelligence and counterintelligence function shall be strictly in accordance with the law" and that "the bodies of the [National Intelligence System]. shall apply the necessary diligence in order to guarantee the rights of individuals, in particular personal privacy, honour and due process".

tasks[2631]. Intelligence agencies are furthermore prohibited from revealing or divulging any type of information acquired in the exercise of their functions, outside the provisions of the National Intelligence Act, except in the case of a court order[2632].

2.3.3 Oversight

The activities of Uruguayan national security authorities are supervised by different bodies.

First, as explained in more detail in sections 2.1 and 2.2.3, the URCDP is competent to oversee compliance with the LPDP's rights and principles in the context of processing activities carried out by national security authorities. This includes overseeing compliance with the specific safeguards set out in Article 25 LPDP, which notably limits the processing of personal data by law enforcement and national security authorities to what is "necessary for the strict compliance with the duties legally assigned to such bodies for national defence, public security or the suppression of crime"[2633].

Second, as explained in more detail in section 2.2.3, INDDHH carries out independent oversight over the respect for fundamental rights, recognised by the Constitution of Uruguay and international law, by public authorities. This includes authorities responsible for protecting national security[2634].

Third, parliamentary oversight in the area of national security is ensured by the Bicameral Commission for the Control and Supervision of the National Intelligence System, which has been active since May 2020. The Commission was created by the National Intelligence Act as an independent review mechanism composed of members of the two legislative chambers covering all the parliamentary parties[2635]. It is charged with the control and supervision of all the activities carried out in the context of the National Intelligence System[2636]. The government is obliged to provide the Commission with detailed information concerning the general activities of the intelligence bodies as well as on events of particular relevance[2637]. To perform its oversight role, the Bicameral Commission may initiate *ex officio* investigations[2638]. If the investigation leads to the suspicion of a criminal offence, the Commission may recommend that the case be referred to the competent criminal court for further investigation[2639].

[2631] Article 5(e) of the National Intelligence Act. Such further sharing by these bodies must take place in accordance with their respective regulations, the provisions of the SIEE and the Act itself. The provision furthermore expressly states that "the use of the information of the System for the specific benefit of individuals, private organisations, political parties or others of any nature and purpose shall contravene this principle, and such cases shall be subject to the civil, administrative and criminal actions that may be applicable".
[2632] Article 7(4) of the National Intelligence Act.
[2633] Article 25 LPDP.
[2634] For a case that concerned the collection of personal data by national security authorities, see for example Resolution N° 729/019 with recommendations to the Minister of Interior, available at the following link: https://www.gub.uy/institucion-nacional-derechos-humanos-uruguay/institucional/informacion-gestion/resoluciones/resolucion-n-729019-recomendaciones-ministerio-del.
[2635] Article 25 of the National Intelligence Act. The Bicameral Commission has been established in May 2020.
[2636] Article 26 of the National Intelligence Act.
[2637] Article 26 of the National Intelligence Act.
[2638] Article 12 of Law No. 16.698 of 25 April 1995 on Parliamentary Committees, available at: https://www.impo.com.uy/bases/leyes/16698-1995.
[2639] Article 28 of Law No. 16.698.

The Bicameral Commission has access to all the information or documentation it requests from the bodies that make up the National Intelligence System. Such access may only be denied for imperative reasons listed in the law, notably the protection of sources or the protection of the identity of third parties[2640]. The invocation of these exemptions is regarded as an *ultimum remedium*; the exemptions must be interpreted restrictively, and their use strictly limited[2641].

The Bicameral Commission is actively performing its duties. It holds regular meetings to discuss topics and issues related to the functioning of the National Intelligence System and to exercise its oversight role. For example, in the past three years the Commission has held several meetings with the Director of the SIEE, to discuss topics such as the work of the SIEE, the National Intelligence Policy, the National Intelligence Plan and the SIEE's annual report[2642].

2.3.4 Redress

The Uruguayan system offers different avenues to obtain redress, including compensation for damages.

First, individuals have a right to obtain access to and rectification or deletion of their data processed by the SIEE or other bodies that are part of the National Intelligence System, as described in more detail in sections 2.1 and 2.2.4[2643].

Second, any individual may lodge a complaint with the URCDP concerning processing activities carried out by national security authorities, as explained in section 2.2.4.

Third, judicial redress may be sought via a habeas data action or writ of amparo against the SIEE or other bodies that are part of the National Intelligence System, subject to the same conditions described in section 2.2.4.

Fourth, the same judicial avenues as the ones described in section 2.2.4 are also available against the SIEE and the other bodies that are part of the National Intelligence System.

Finally, once all national remedies are exhausted, data subjects may bring their case before the Inter-American Commission of Human Rights.

[2640] Article 26 of the National Intelligence Act.
[2641] Chapter XV of Decree No. 157/022.
[2642] See the website of the Commission, where it publishes abbreviated minutes of its meetings: https://parlamento.gub.uy/camarasycomisiones/asambleageneral/comisiones/1186/comision-actuacion.
[2643] In accordance with Article 29 of the National Intelligence Act, all information, including background information, as well as records held by the bodies that make up the National State Intelligence System and their staff, regardless of their position, shall be considered reserved and restricted for all legal purposes, in accordance with Article 9 of Law No. 18.381 of 17 October 2008 on access to government information. The information remains classified for up to 25 years (Article 33 of the Act). However, Article 34 of the Act clearly states that the confidential character of the classified information held by intelligence services may not be invoked in any case when it relates to human rights violations, or when it is relevant to prevent or investigate such violations.