Council of the
European Union

Brussels, 27 August 2020
(OR. en)

9180/20
ADD 1 REV 1

DATAPROTECT 57
JAI 536
FREMP 41
DIGIT 50
RELEX 482

COVER NOTE

No. Cion doc.:	SWD(2020) 115 final/2
Subject:	COMMISSION STAFF WORKING DOCUMENT Accompanying the document COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL **Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation**

Delegations will find attached document SWD(2020) 115 final/2.

Encl.: SWD(2020) 115 final/2

EUROPEAN
COMMISSION

Brussels, 24.6.2020
SWD(2020) 115 final/2

This document corrects document SWD(2020) 115 final of 24.06.2020
Concerns the EN language version.
Footnote 3 completed.
The text shall read as follows:

COMMISSION STAFF WORKING DOCUMENT

[…]

Accompanying the document

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation

{COM(2020) 264 final}

Contents

1 CONTEXT

The General Data Protection Regulation[1] (hereafter 'the GDPR') is the result of eight years of preparation, drafting and inter-institutional negotiations, and entered into application on 25 May 2018 following a two-year transition period (May 2016 - May 2018). Article 97 of the GDPR requires the Commission to report on the evaluation and review of the Regulation, starting with a first report after two years of application and every four years thereafter.

The evaluation is also part of multi-faceted approach that the Commission already followed before the GDPR entered into application and has continued to actively pursue since then. As part of this approach, the Commission engaged into on-going bilateral dialogues with Member States on the compliance of national legislation with the GDPR, actively contributed to the work of the European Data Protection Board (hereafter 'the Board') by providing its experience and expertise, supported data protection authorities and maintained close contacts with a wide range of stakeholders on the practical application of the Regulation.

The evaluation builds on the stocktaking exercise that the Commission carried out on the first year of the GDPR application and that was summarised in the Communication issued in July 2019[2]. It also follows-up on the Communication on the application of the GDPR issued in January 2018[3]. The Commission also adopted the Guidance on the use of personal data in the electoral context published in September 2018 and the Guidance on apps supporting the fight against the COVID-19 pandemic issued in April 2020.

Although its focus is on the two issues highlighted in Article 97(2) of the GDPR, namely international transfers and the cooperation and consistency mechanisms, this evaluation takes a broader approach in order to address issues which have been raised by various actors during the last two years.

To prepare the evaluation, the Commission took into account the contributions from:

- the Council[4];
- the European Parliament (Committee on Civil Liberties, Justice and Home Affairs)[5];
- the Board[6] and individual data protection authorities[7], based on a questionnaire sent by the Commission;

---

[1] 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 - OJ L 119, 4.5.2016, p. 1–88

[2] Communication from the Commission to the European Parliament and the Council, Data Protection as a trust-enabler in the EU and beyond – taking stock – COM(2019) 374 final, 24.7.2019

[3] Communication from the Commission to the European Parliament and the Council: Stronger protection, new opportunities – Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018, COM/2018/043 final

[4] Council position and findings on the application of the General Data Protection Regulation – 14994/2/19 Rev2, 15.01.2020:
https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-2/en/pdf

[5] Letter of the LIBE Committee of the European Parliament of 21 February 2020 to Commissioner Reynders, Ref.: IPOL-COM-LIBE D (2020)6525.

- the feedback from the members of the Multi-stakeholder expert Group to support the application of the GDPR[8], also based on a questionnaire sent by the Commission;
- and ad hoc contributions received from stakeholders.

2 ENFORCEMENT OF THE GDPR AND FUNCTIONING OF THE COOPERATION AND CONSISTENCY MECHANISMS

The GDPR set up an innovative governance system and created the foundation of a truly European data protection culture that aims to ensure not only a harmonised interpretation, but also a harmonised application and enforcement of data protection rules. Its pillars are the independent national data protection authorities and the newly established Board.

As the data protection authorities are key to the functioning of the whole EU data protection system, the Commission is attentively monitoring their effective independence, including as regards adequate financial, human and technical resources.

It is still too early to fully assess the functioning of the cooperation and consistency mechanisms, given the short experience gathered so far[9]. In addition, data protection authorities have not yet used the full array of tools provided for by the GDPR to strengthen their cooperation further.

2.1 Use of strengthened powers by data protection authorities

The GDPR establishes independent data protection authorities and provides them with harmonised and strengthened enforcement powers. Since the GDPR applies, those authorities have been using of a wide range of corrective powers provided for in the GDPR, such as administrative fines (22 EU/EEA authorities)[10], warnings and reprimands (23), orders to comply with data subject's requests (26), orders to bring processing operations into compliance with the GDPR (27), and orders to rectify, erase or restrict processing (17). Around half of the data protection authorities (13) have imposed temporary or definitive limitations on processing, including bans. This demonstrates a conscious use of all corrective measures provided for in the GDPR;

---

6 Contribution of the Board to the evaluation of the GDPR under Article 97, adopted on 18 February 2020: https://edpb.europa.eu/our-work-tools/our-documents/other/contribution-edpb-evaluation-gdpr-under-article-97_en

7 https://edpb.europa.eu/individual-replies-data-protection-supervisory-authorities_en

8 The Multi-stakeholder expert group on the GDPR set up by the Commission involves civil society and business representatives, academics and practitioners: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537 The report of the Multi-stakeholder Group is available at: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=21356

9 This fact is also highlighted in particular by the Council in its position and findings on the application of the GDPR and by the Board in its contribution to the evaluation.

10 The figures in parenthesis indicate the number of EU/EEA data protection authorities that made use of the listed power between May 2018 and the end of November 2019. See contribution from the Board on pages 32-33.

the data protection authorities did not shy away from imposing administrative fines in addition to or instead of other corrective measures, depending on the circumstances of individual cases.

Administrative fines:

Between 25 May 2018 and 30 November 2019, 22 EU/EEA data protection authorities issued approximately 785 fines. Only a few authorities have not yet imposed any administrative fines, although proceedings that are currently ongoing might lead to such fines. Most of the fines related to infringements against: the principle of lawfulness; valid consent; protection of sensitive data; the obligation of transparency, the rights of data subjects; and data breaches.

Examples of fines imposed by data protection authorities include[11]:

- EUR 200 000 for non-compliance with the right to object direct marketing in Greece;
- EUR 220 000 on a data broker company in Poland for failure to inform individuals that their data was being processed;
- EUR 250 000 imposed on the Spanish football league LaLiga, for lack of transparency in the design of its smartphone application;
- EUR 14,5 million for infringement of data protection principles, in particular unlawful storage, by a German real estate company;
- EUR 18 million for unlawful processing of special categories of data at a large scale by Austrian postal services;
- EUR 50 million on Google in France, because of the conditions for obtaining consent from users.

The success of the GDPR should not be measured by the number of fines issued, since the GDPR provides for a broader palette of corrective powers. Depending on the circumstances, for example, the deterrent effect of a ban on processing or the suspension of data flows can be much stronger.

Specific issues for the public sector

The GDPR allows Member States to determine whether and to what extent administrative fines may be imposed on public authorities and bodies. Where Member States make use of this possibility, this does not deprive the data protection authorities of using all the other corrective powers vis-à-vis public authorities and bodies[12].

Another specific issue is the supervision of courts: although the GDPR also applies to the activities of courts, these are exempted from supervision by data protection authorities when acting in their judicial capacity. However, the Charter and the TFEU oblige Member States to entrust an independent body within their judicial systems with the supervision of such processing operations[13].

---

11 Several of the decisions imposing fines are still subject to judicial review.
12 Article 83(7) GDPR.
13 Article 8(3) of the Charter; Article 16 (2) TFEU; recital 20 of the GDPR.

Cooperation with other regulators

As announced in its Communication of July 2019, the Commission supports interaction with other regulators, in full respect of the respective competencies. Promising areas of cooperation include consumer protection and competition. The Board indicated its willingness to engage with other regulators in particular in relation to concentration in digital markets[14]. The Commission recognised the importance of privacy and data protection as a qualitative parameter for competition[15]. Members of the Board participated in joint workshops with the Consumer Protection Cooperation Network on cooperation on better enforcement of the EU consumer and data protection legislation. This approach will be pursued to foster common understanding and develop practical ways to address concrete problems experienced by consumers in particular in the digital economy.

In order to ensure a consistent approach to privacy and data protection, and pending the adoption of the ePrivacy Regulation, close cooperation with the authorities competent for enforcing the ePrivacy Directive[16], the lex specialis in the area of electronic communications, is indispensable. Closer cooperation with the authorities competent under the NIS-Directive[17], and the NIS Cooperation Group, would be to the mutual benefit of those authorities and the data protection authorities.

2.2 The cooperation and consistency mechanisms

The GDPR created the cooperation mechanism (one-stop-shop system for operators, joint operations and mutual assistance between data protection authorities) and the consistency mechanism in order to foster a uniform application of the data protection rules, through a consistent interpretation and the resolution of possible disagreement between authorities by the Board.

The Board, gathering all data protection authorities, has been established as an EU body with legal personality and is fully operational, supported by a secretariat[18]. It is crucial for the functioning of the two mechanisms mentioned above. By the end of 2019, the Board had adopted 67 documents, including 10 new guidelines[19] and 43 opinions[20][21].

---

[14] Cf. the statement of the Board on the data protection impacts of economic concentration, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_economic_concentration_en.pdf.

[15] See Case COMP M. 8124 Microsoft/LinkedIn.

[16] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) - OJ L 201 , 31/07/2002 P. 0037 - 0047

[17] 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 - OJ L 194, 19.7.2016, p. 1–30

[18] See details on the secretariat activities in the contribution from the Board, pages 24-26.

[19] In addition to the 10 guidelines adopted by the Article 29 Working Party in the run-up to the GDPR's entry into application and endorsed by the Board. Moreover, the Board has adopted 4 additional guidelines between January and end May 2020, and updated an existing one.

[20] 42 of these opinions were adopted under Article 64 of the GDPR and one was adopted under Article 70(1)(s) of the GDPR and concerned the adequacy decision with respect to Japan.

[21] See contribution from the Board, pages 18-23 for a complete overview of the Board's activities.

The important role of the Board emerged where there was a need to rapidly provide for consistent interpretation of the GDPR and to find immediately applicable solutions at EU level. For example in the context of the COVID-19 outbreak, in March 2020 the Board adopted a statement on the processing of personal data, which deals inter alia with the lawfulness of processing and the use of mobile location data in that context[22], and in April 2020 it adopted guidelines on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak [23] and guidelines on the use of location data and contact tracing tools in the context of the COVID-19 outbreak [24]. The Board also made a significant contribution to design of the EU approach to tracing apps by the Commission and the Member States.

Day-to-day cooperation between data protection authorities, whether they act in their own capacity or as members of the Board, is based on exchanges of information and notifications of cases opened by the authorities. In order to facilitate communication between authorities, the Commission gave significant support by providing them with an information exchange system[25].Most authorities consider it as adapted to the needs of the cooperation and consistency mechanisms, even though it could be further fine-tuned for example by making it more user-friendly.

Although it is still early days, a number of achievements and challenges can already be identified and are presented below. They show that, so far, data protection authorities have made an effective use of the cooperation tools, with a preference for more flexible solutions.

One-stop-shop

As a general rule, in cross-border cases, a Member State's data protection authority can be involved either (i) as lead authority when the main establishment of the operator is located in this Member State, or (ii) as a concerned authority when the operator has an establishment on the territory of this Member State, when individuals in this Member State are substantially affected, or when a complaint has been lodged with them.

Such close cooperation has become daily practice: since the date of application of the GDPR, data protection authorities in all Member States have at some point been identified either as lead authorities or as concerned authorities in cross-border cases, although to a different extent.

From May 2018 until end 2019, the data protection authority in Ireland acted as lead authority in the highest number of cross-border cases (127), followed by Germany (92), Luxembourg (87), France (64) and the Netherlands (45). This ranking reflects notably the specific situation of Ireland and Luxembourg, who host several big multinational tech companies.

---

[22] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf

[23] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032020-processing-data-concerning-health-purpose_en.

[24] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

[25] Internal Market Information System ('IMI').

The ranking is different as regards involvement as concerned data protection authorities with the authorities in Germany being involved in the highest number of cases (435), followed by Spain (337), Denmark (327), France (332) and Italy (306)[26].

Between 25 May 2018 and 31 December 2019, 141 draft decisions were submitted through the one-stop-shop procedure, out of which 79 resulted in final decisions. At the date of the publication of this report, several important decisions with a cross-border dimension and subject to the one-stop-shop mechanism are pending. Among these decisions, some involve multinational big tech companies[27]. They are expected to provide clarification and to contribute to an increased harmonisation in the interpretation of the GDPR.

Mutual assistance

Data protection authorities have made a wide use of the mutual assistance tool.

By the end of 2019, there had been 115 Mutual Assistance[28] procedures, in particular for carrying out investigations, most of them by the data protection authorities of Spain (26), Germany (20), Denmark (13), Poland (12) and Czech Republic (10). On the other hand, Ireland (19), France (11), Austria (10), Germany (10) and Luxembourg (9) had received the most requests [29].

The vast majority of authorities find mutual assistance a very useful tool for cooperation and have not encountered any particular obstacle to applying the mutual assistance procedure. The voluntary mutual assistance exchange, which does not have a legal deadline or strict duty to answer, has been used more frequently, in 2 427 procedures. The data protection authority of Ireland sent and received the highest number of mutual assistance requests (527 sent and 359 received), followed by German authorities (260 sent/356 received).

On the other hand, joint operations[30], which would make it possible for data protection authorities of several Member States to be involved already at the level of the investigations of cross-border cases, have not been conducted yet. Reflection is on-going within the Board on the practical implementation of this tool and how to promote its use.

Consistency mechanism

So far only the first leg of the consistency mechanism has been used, namely the adoption of Board opinions[31]. On the other hand, no dispute resolution at Board level[32] or urgency procedure[33] has been triggered yet.

---

26 See contribution from the Board, page 8.

27 For instance, on 22 May 2020, the Irish data protection authority has submitted a draft decision to other concerned authorities, in accordance with Article 60 of the Regulation, concerning an investigation into Twitter International Company regarding data breach notification. On the same day, the Irish data protection authority also announced that a draft decision on WhatsApp Ireland Limited for submission under Article 60 was in preparation, concerning transparency including in relation to transparency around what information is shared with Facebook.

28 Article 61 GDPR.

29 See contribution from the Board, pages 12-14.

30 Article 62 GDPR.

31 Based on Article 64 GDPR.

Between 25 May 2018 and 31 December 2019, the Board issued 36 opinions in the context of the adoption of measures by one of its members[34]. Most of them (31) concerned the adoption of national lists of processing operations requiring a data protection impact assessment. Two opinions concerned Binding Corporate Rules, two others concerned draft accreditation requirements for a code of conduct monitoring body, and one concerned Standard Contractual Clauses[35].

Furthermore, the Board adopted, on request, six opinions[36]. Three of these opinions concerned national lists identifying processing which does not require a data protection impact assessment. The others concerned respectively an administrative arrangement for the transfer of personal data between EEA and non-EEA financial supervisory authorities, the interplay between the ePrivacy Directive and the GDPR and the competence of a supervisory authority in case of a change in circumstances relating to the main or single establishment.[37]

Challenges to be addressed

Although the data protection authorities have been very actively working together in the Board and already intensively use the cooperation tool of mutual assistance, building a truly data protection common culture is still an ongoing process.

In particular, the handling of cross-border cases calls for a more efficient and harmonised approach and the effective use of all cooperation tools provided in the GDPR. There is a very broad consensus on this point since it was raised in different ways by the European Parliament, the Council, the European Data Protection Supervisor, stakeholders (within the Multi-stakeholder Group and beyond) and by the data protection authorities.

The main issues to be tackled in this context include differences in:

- national administrative procedures, concerning in particular: complaint handling procedures, the admissibility criteria for complaints, the duration of proceedings due to different timeframes or the absence of any deadlines, the moment in the procedure when the right to be heard is granted, the information and involvement of complainants during the procedure;
- interpretations of concepts relating to the cooperation mechanism, such as relevant information, the notion of "without delay", "complaint", the document which is defined as the "draft decision" of the lead data protection authority, amicable settlement (in particular the procedure leading to amicable settlement and the legal form of the settlement); and
- the approach to when to start the cooperation procedure, involve the concerned data protection authorities and communicate information to them. Complainants also lack clarity on how their cases are handled in cross-border situations, as was stressed by several members of the Multi-stakeholder Group. Moreover,

---

32 Article 65 GDPR.
33 Article 66 GDPR.
34 Under Article 64(1) GDPR.
35 Article 28(8) GDPR.
36 Under Article 64(2) GDPR.
37 See contribution from the Board, page 15.

businesses mention that in certain instances national data protection authorities did not refer cases to the lead data protection authority, but handled them as local cases.

The Commission welcomes the Board's announcement that it has started a reflection on how to address these concerns. In particular, the Board indicated that it will clarify the procedural steps involved in the cooperation between the lead data protection authority and the concerned data protection authorities, analyse national administrative procedural laws, work towards a common interpretation of key concepts, and strengthen communication and cooperation (including joint operations). The Board's reflection and analysis should lead to devising more efficient working arrangements in cross-border cases[38], including by building on the expertise of its members and by strengthening the involvement of its secretariat. In addition, it should be noted that the Board's responsibility in ensuring a consistent interpretation of the GDPR cannot be discharged by simply finding the lowest common denominator.

Finally, as an EU body the Board must also apply EU administrative law and ensure transparency in the decision making process.

2.3 Advice and guidelines

Awareness raising and advice by data protection authorities

Several data protection authorities created new tools, such as help lines for individuals and businesses, and toolkits for businesses[39]. Many operators welcome the pragmatism shown by these authorities in assisting with the application of the GDPR. In particular, several of them have actively and closely collaborated and communicated with data protection officers, including through data protection officers' associations. Many authorities also issued guidelines covering the data protection officers' role and obligations to support data protection officers during their daily activities and held seminars specifically designed for them. However, this is not the case for all data protection authorities.

Feedback received from stakeholders also points to a number of issues as regards guidance and advice:

- the lack of a consistent approach and guidance between national data protection authorities on certain issues (e.g. on cookies[40], the application of legitimate interest, on data breach notifications or on data protection impact assessments) or even between data protection authorities within the same Member States (e.g. in Germany on the notions of controller and processor);
- the inconsistency of guidelines adopted at national level with those adopted by the Board;

---

38 As also pointed out in the Council position and findings.

39 See below under point 7.

40 Pending the adoption of the ePrivacy Regulation, close cooperation with the competent authorities responsible for the enforcement of the ePrivacy Directive in the Member States is necessary. In accordance with that Directive, in some Member States the authorities competent for enforcing Article 5(3) of the ePrivacy Directive (which sets out the conditions under which "cookies" may be set and accessed on a user's terminal equipment) are not the same as the GDPR supervisory authorities.

- the absence of public consultations on certain guidelines adopted at national level;
- different levels of engagement with stakeholders among data protection authorities;
- delays in receiving responses to information requests;
- difficulties in obtaining practical and valuable advice from data protection authorities;
- the need to increase the level of sectoral expertise in some data protection authorities (e.g. in the health and pharma sector).

Several of these issues are also linked to the lack of resources in several data protection authorities (see below).

Divergent practices as regards the notification of data breaches[41]

While the Council highlights the burden caused by such notifications, there are significant discrepancies on notifications between Member States: whereas from May 2018 to end November 2019, in most Member States the total number of data breach notifications was below 2 000, and in 7 Member States between 2 000 and 10 000, the Dutch and German data protection authorities reported respectively 37 400 and 45 600 notifications[42].

This may point to a lack of consistent interpretation and implementation, despite the existence of EU-level guidelines on data breach notifications.

Guidelines of the European Data Protection Board

To date, the Board adopted more than 20 guidelines covering key aspects of the GDPR[43]. The guidelines are an essential tool for the consistent application of the GDPR and have, therefore, been to a large extent welcomed by stakeholders. Stakeholders have appreciated the systematic (6 to 8 weeks) public consultation. However, they ask for more dialogue with the Board. In this context, the practice of organising workshops on targeted topics prior to drafting guidelines should be continued and amplified to ensure the transparency, inclusiveness, and relevance of the Board's work. Stakeholders also request that the interpretation of the most contentious issues should be addressed in the guidelines, since these are subject to public consultation, and not within opinions under Article 64(2) of the GDPR. Some stakeholders also call for more practical guidelines, detailing the application of concepts and provisions of the GDPR[44]. Members of the Multi-stakeholder Group stress the need for more concrete examples to reduce the room for diverging interpretations between data protection authorities as much as possible. At the same time, the requests to clarify how to apply the GDPR and to provide legal certainty

41 Article 33 GDPR.
42 See contribution from the Board page 35.
43 The work on guidelines already started before the entry into application of the GDPR on 25 May 2018 in the context of the Article 29 Working Party. See the full list of guidelines at https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en
44 This has also been highlighted by the European Parliament and by the Council.

should not lead to additional requirements or diminish the advantages of the risk-based approach and the accountability principle.

The topics on which stakeholders would like additional guidelines from the Board include: the scope of data subjects' rights (including in the employment context); updates to the opinion on processing based on legitimate interest; the notions of controller, joint controller and processor and the necessary arrangements between the parties[45]; the application of the GDPR to new technologies (such as blockchain and artificial intelligence); processing in the context of scientific research (including in relation to international collaboration); the processing of children's data; pseudonymisation and anonymisation; and the processing of health data.

The Board has already indicated that it will issue guidelines on many of these topics and the work already started on several of them (e.g. on the application of legitimate interest as a legal basis for processing).

Stakeholders ask the Board to update and revise existing guidelines where appropriate,, taking into account the experience gathered since their publication and taking the opportunity to go into more detail where needed.

2.4 Resources of the data protection authorities

Providing each data protection authority with the necessary human, technical and financial resources, premises and infrastructure is a prerequisite for the effective performance of their tasks and exercise of their powers, and therefore an essential condition for their independence[46].

Most data protection authorities benefited from an increase in staff and resources since the GDPR entered into force in 2016[47]. However many of them still report that they do not have sufficient resources[48].

Number of staff working for national data protection authorities

The total number of staff working in EEA data protection authorities considered together has increased by 42% between 2016 and 2019 (by 62% if one considers the 2020 forecast).

The number of staff has increased in most authorities during this period, with the biggest increase (as a percentage) registered for authorities in Ireland (+169%), the Netherlands (+145%), Iceland (+143%), Luxembourg (+126%) and Finland (+114%). On the other hand, the number of staff decreased in several data protection authorities, with the sharpest decreases observed in Greece (-15%), Bulgaria (-14%), Estonia (-11%), Latvia (-10%) and Lithuania (-8%). In some authorities, the decrease in staff is also due to the departure of data protection experts to the private sector offering more attractive conditions.

---

45 Guidelines from the Board on controllers and processors are currently in preparation.
46 See Article 52(4) GDPR.
47 The Regulation entered into force in May 2016 and into application in May 2018, following a 2-year transition period.
48 See contribution from the Board, pages 26-30.

In general, the forecast for 2020 provides for an increase of staff compared to 2019, except for authorities in Austria, Bulgaria, Italy, Sweden and Iceland (where staff numbers are expected to remain stable), Cyprus and Denmark (where staff numbers are expected to decrease).

The German data protection authorities[49] together have the highest number of staff (888 in 2019/1002 in 2020 forecast), followed by the data protection authorities in Poland (238/260), France (215/225), Spain (170/220), the Netherlands (179/188), Italy (170/170) and Ireland (140/176).

The data protection authorities with the lowest staff numbers are those in Cyprus (24/22), Latvia (19/31), Iceland (17/17), Estonia (16/18) and Malta (13/15).

Budget of national data protection authorities

The total budget of EEA data protection authorities considered together has increased by 49% between 2016 and 2019 (by 64% if one considers the 2020 forecast).

The budget of most authorities increased during this period, with the biggest increase (as a percentage) registered for authorities in Ireland (+223%), Iceland (+167%), Luxembourg (+165%), the Netherland (+130%) and Cyprus (+114%). On the other hand, some authorities saw only a small budget increase, with the smallest increases registered for data protection authorities in Estonia (7%), Latvia (4%), Romania (3%) and Belgium (1%), while the authority in France experienced a decrease (-2%).

In general, the forecast for 2020 provides for an increase in budget compared to 2019, except for the authorities in Austria, Bulgaria, Estonia and the Netherlands (whose budgets are expected to remain stable).

The data protection authorities with the highest budget are those of Germany (EUR 76.6 million in 2019/EUR 85.8 million in the 2020 forecast), Italy (29.1/30.1), The Netherlands (18.6/18.6), France (18.5/20.1) and Ireland (15.2/16.9).

The authorities with the lowest budget are those of Croatia (EUR 1.2 million in 2019/EUR 1.4 million in the 2020 forecast), Romania (1.1/1.3), Latvia (0.6/1.2), Cyprus (0.5/0.5) and Malta (0.5/0.6).

The table in Annex II provides an overview of the human and budgetary resources of national data protection authorities.

Besides impacting their capacity to enforce rules at national level, the lack of resources also limits data protection authorities' capacity to participate in and contribute to the cooperation and consistency mechanisms, and to the work carried out within the Board. As highlighted by the Board, the success of the one-stop-shop mechanism depends on the time and effort that data protection authorities can dedicate to the handling of and cooperation on individual cross-border cases. The resource issue is compounded by the authorities' increased role in the supervision of large-scale IT systems that are currently being developed. Furthermore, the data

[49] There are 18 authorities in Germany, of which one is a federal authority and 17 are regional authorities (including two in Bavaria).

protection authorities in Ireland and Luxembourg have specific resource needs given their role as lead authorities for the enforcement of the GDPR vis-à-vis big tech companies, which are located mostly in these Member States.

While the Council points to the impact of the cooperation mechanism and its deadlines on the work of data protection authorities[50], the GDPR obliges Member States to provide their national data protection authorities with adequate human, financial and technical resources[51].

The secretariat of the Board, which is provided by the European Data Protection Supervisor[52], is currently composed of 20 people, including legal, IT and communication experts. It is to be assessed whether this figure needs to evolve in the future in light of the effective fulfilment of its function of analytical, administrative and logistical support to the Board and its subgroups, including through the management of the information exchange system,

3 HARMONISED RULES BUT STILL A DEGREE OF FRAGMENTATION AND DIVERGING APPROACHES

The GDPR provides for a consistent approach to data protection rules throughout the EU, replacing the different national regimes that existed under the 1995 Data Protection Directive.

3.1 Implementation of the GDPR by the Member States

The GDPR has been directly applicable in all Member States since 25 May 2018. It obliged Member States to legislate, in particular to set up national data protection authorities and the general conditions for their members, in order to ensure that each authority acts with complete independence in performing its tasks and exercising its powers in accordance with the GDPR. Legal obligations and public tasks can constitute a legal ground for the processing of personal data only if they are laid down in (Union or) national law. In addition, Member States must lay down rules on penalties in particular for infringements not subject to administrative fines and must reconcile the right to the protection of personal data with the right to freedom of expression and information. National law can also provide for a legal basis for the exemption from the general prohibition for processing special categories of personal data, for example for reasons of substantial public interest in the area of public health, including protection against serious cross-border threats to health. Furthermore, Member States must ensure the accreditation of certification bodies.

The Commission is monitoring the implementation of the GDPR in national legislation. At the time of writing this report, all Member States except Slovenia has adopted new data protection legislation or adapted their law in this area. The

[50] Article 60 GDPR.
[51] Article 52(4) GDPR.
[52] Article 75 GDPR.

Commission therefore requested Slovenia to provide clarification on the progress made to date and urged it to finalise that process[53].

In addition, the compliance of national legislation with data protection rules as regards the Schengen acquis is also assessed in the context of the Schengen Evaluation Mechanism coordinated by the Commission. The Commission and Member States jointly evaluate how countries implement and apply the Schengen acquis in a number of areas; for data protection this concerns large-scale IT systems like the Schengen Information System and the Via Information System and includes the role of data protection authorities in supervising the processing of personal data within those systems.

Work on adapting sectoral laws is still on-going at national level. Following the GDPR's incorporation into the European Economic Area Agreement, its application was extended to Norway, Iceland and Lichtenstein. These countries have also adopted their national data protection laws.

The Commission will make use of all the tools at its disposal, including infringement procedures, to ensure that Member States comply with the GDPR.

Main issues relating to national implementation

The main issues identified to date as part of the ongoing assessment of national legislation and bilateral exchanges with Member States include:

- Restrictions to the GDPR's application: some Member States, for example, completely exclude the activities of the national parliament ;
- Differences in the applicability of national specification laws. Some Member States link the applicability of their national law to the place where the goods or services are offered, others to the place of establishment of the controller or processor. This runs contrary to the objective of harmonisation pursued by the GDPR;
- National laws that raise questions on the proportionality of the interference with the right to data protection. For example, the Commission launched an infringement procedure against a Member State that had enacted legislation requiring judges to disclose specific information about their non-professional activities, which is incompatible with the right to respect for private life and the right to the protection of personal data[54];
- The absence of an independent body for the supervision of data processing by courts acting in their judicial capacity[55].
- Legislation in areas fully regulated by the GDPR beyond the margin for specifications or restrictions. This is, in particular, the case where national

[53] It has to be noted that the national data protection authority in Slovenia is set up based on the current national data protection law and supervise the application of the GDPR in that Member State.

[54] This infringement procedure concerns the Polish law on the judiciary of 20 December 2019, which affects the independence of the judges and concerns, inter alia, the disclosure of the engagement of judges in non-professional activities: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_772.

[55] See Article 8(3) of the Charter; Article 16 TFEU; recital 20 of the GDPR.

provisions determine conditions for processing based on legitimate interest, by providing for the balancing of the respective interests of the controller and of the individuals concerned, while the GDPR obliges each and every controller to undertake such balancing individually and avail itself of that legal basis.

- Specifications and additional requirements beyond processing for compliance with a legal obligation or performance of a public task (e.g. for video surveillance in the private sector or for direct marketing); and for concepts used in the GDPR (e.g. 'large scale' or 'erasure').

Some of these issues may be clarified by the Court of Justice in cases that are still pending[56].

Reconciliation of the right to the protection of personal data with freedom of expression and information

A specific issue concerns the implementation of the obligation for Member States to reconcile by law the right to the protection of personal data with freedom of expression and information[57]. This issue is very complex, since an assessment of the balancing between these fundamental rights must also take into account provisions and safeguards in press and media laws.

The assessment of Member State legislation shows different approaches to the reconciliation of the right to the protection of personal data with freedom of expression and information:

- Some Member States lay down the principle of precedence of freedom of expression or exempt in principle the application of entire chapters mentioned in Article 85(2) GDPR if processing for journalistic purposes and for academic, artistic and literary expression is at stake. To a certain extent, media laws provide for some safeguards as regards data subject rights.
- Some Member States lay down the precedence of the protection of personal data and exempt the application of data protection rules only in specific situations, such as where a person with public status is concerned.
- Other Member States provide for a certain balancing by the legislator and/or a case-by-case assessment as regards derogations from certain provisions of the GDPR.

The Commission will continue its assessment of national legislation on the basis of the requirements of the Charter. The reconciliation must be provided for by law, respect the essence of those fundamental rights, and be proportional and necessary (Article 52(1) of the Charter). Data protection rules should not affect the exercise of freedom of expression and information especially by creating a chilling effect or by being interpreted as a way to put pressure on journalists to disclose their sources.

[56] For example, the exemption of a parliamentary committee from the application of the GDPR is subject to a pending court case for a preliminary ruling (C-272/19).

[57] Article 85 GDPR.

3.2 Facultative specification clauses and their limits

The GDPR gives Member States the possibility to further specify its application in a limited number of areas. This margin for national legislation is to be distinguished from the obligation to implement certain other provisions of the GDPR as mentioned above. The clauses for facultative specifications are listed in Annex I.

The margins for Member State law are subject to the conditions and limits set by the GDPR and do not allow for a parallel national data protection regime[58]. Member States are obliged to amend or repeal the national data protection laws, including sectoral legislation with data protection aspects.

Furthermore, related Member State legislation must not include provisions which might create confusion regarding the direct application of the GDPR. Therefore, where the GDPR provides for specifications or restrictions of its rules by Member State law, Member States may incorporate elements of the GDPR in their national law, to the extent necessary to ensure coherence and to render the national provisions comprehensible to the persons to whom they apply[59].

Stakeholders consider that Member States should reduce or refrain from using facultative specification clauses since they do not contribute to harmonisation. The national divergences in both the implementation of the laws and their interpretation by data protection authorities considerably increase the cost of legal compliance across the EU.

Fragmentation linked to the use of facultative specification clauses

- Age limit for children consent for information society services

A number of Member States have made use of the possibility to provide for a lower age than 16 years for consent in relation to information society services (Article 8(1) GDPR). Whereas nine Member States apply the 16 years' age limit, eight Member States opted for 13 years, six for 14 years and three for 15 years.[60]

Consequently, a company providing information society services to minors across the EU has to distinguish between the ages of potential users, depending in which Member State they reside. This is contrary to the key objective of the GDPR to provide for an equal level of protection to individuals and of business opportunities in all Member States.

Such differences lead to situations where the Member State in which the controller is established provides for another age limit than the Member States where the data subjects are residing.

---

[58] The widely used term of "opening clauses" to mean specification clauses is misleading since it might give the impression that Member States have margins of manoeuvre beyond the provisions of the Regulation.

[59] Recital 8 of the GDPR.

[60] 13 years for Belgium, Denmark, Estonia, Finland, Latvia, Malta, Portugal and Sweden; 14 years for Austria, Bulgaria, Cyprus, Spain, Italy and Lithuania; 15 years for Czech Republic, Greece and France; 16 years for Germany, Hungary, Croatia, Ireland, Luxembourg, the Netherlands, Poland, Romania and Slovakia.

- Health and research

When implementing derogations from the general prohibition for processing special categories of personal data[61], Member State legislation follows different approaches as regards the level of specification and safeguards, including for health and research purposes. Most Member States introduced or maintained further conditions for the processing of genetic data, biometric data or data concerning health. This is also true for derogations related to data subject rights for research purposes[62], both as regards the extent of the derogations and the related safeguards.

The Board's future guidelines on the use of personal data in the field of scientific research will contribute to a harmonised approach in this area. The Commission will provide input to the Board, in particular as regards health research, including in the form of concrete questions and analysis of concrete scenarios that it received from the research community. It would be helpful if these guidelines could be adopted before the launch of Horizon Europe Framework Programme in view of harmonising data protection practices and facilitating data sharing for research advancements. Guidelines from the Board on the processing of personal data in the area of health could also be useful.

The GDPR provides a robust framework for national legislation in the area of public health and explicitly includes cross-border health threats and the monitoring of epidemics and their spread[63], which was relevant in the context of the fight against the COVID-19 pandemic.

At EU level, on 8 April 2020 the Commission adopted a Recommendation for a toolbox for the use of technology and data in this context, including mobile applications and the use of anonymised mobility data[64], and on 16 April 2020 a guidance on apps supporting the fight against the pandemic in relation to data protection[65]. The Board published a statement on data processing in this context on 19 March 2020[66], followed on 21 April 2020 by guidelines on data processing for research purposes and on the use of localisation data and contact tracing tools in this context[67]. These recommendations and guidelines clarify how the principles and rules on the protection of personal data apply in the context of the fight against the pandemic.

- Extensive restrictions of data subjects' rights

Most national data protection laws that restrict data subject's rights do not specify the objectives of general public interest safeguarded by these restrictions and/or do not sufficiently meet the conditions and safeguards required by Article 23(2) of the

---

61 Article 9 GDPR.
62 Article 89(2) GDPR.
63 See Article 9(2)(i) GDPR and recital 46.
64 https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf .
65 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020XC0417 (08) & from = EN.
66 https://edpb.europa.eu/news/news/2020/statement-processing-personal-data-context-covid-19-outbreak_en.
67 https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en.

GDPR[68]. Several Member States leave no room for the proportionality test or extend the restrictions even beyond the scope of Article 23(1) of the GDPR. For example, some national laws deny the right of access for reasons of disproportionate effort on the side of controller, for personal data which are stored on the basis of a retention obligation or related to the performance of public tasks without limiting such restriction to objectives of general public interest.

- Additional requirements for companies

Although the requirement of a mandatory data protection officer is based on the risk-based approach[69], one Member State[70] extended it to a quantitative criteria, obliging companies in which 20 employees or more are permanently involved in the automated processing of personal data to designate a data protection officer, independently of the risks connected with the processing activities[71]. This has led to additional burdens.

4 EMPOWERING INDIVIDUALS TO CONTROL THEIR DATA

The GDPR makes fundamental rights effective, in particular the right to the protection of personal data, but also the other fundamental rights recognised by the Charter, including the respect for private and family life, freedom of expression and information, non-discrimination, freedom of thought, conscience and religion, freedom to conduct a business and the right to an effective remedy. These rights must be balanced against each other in accordance with the principle of proportionality[72].

The GDPR provides individuals with enforceable rights, such as the right of access, rectification, erasure, objection, portability and enhanced transparency. It also gives individuals the right to lodge a complaint with a data protection authority, including through representative actions, and to judicial redress.

Individuals are increasingly aware of their rights, as shown in the results of the July 2019 Eurobarometer[73] and the survey carried out by the Fundamental Rights Agency[74].

According to the Fundamental Rights Survey carried out by the Fundamental Rights Agency:

- 69% of the population aged 16+ in the EU have heard about the GDPR;
- 71% of respondents in the EU have heard about their national data protection authority; this figure ranges from 90% in the Czech Republic to 44% in Belgium;

[68] For instance because they simply repeat the wording of Article 23(1) GDPR.
[69] Article 37(1) GDPR.
[70] Germany.
[71] Making use of the specification clause in Article 37(4) GDPR.
[72] Cf. recital 4 of the GDPR.
[73] https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2956
[74] European Union Agency for Fundamental Rights (FRA) (2020): Fundamental Rights Survey 2019. Data protection and technology: https://fra.europa.eu/en/publication/2020/fundamental-rights-survey-data-protection

- 60% of respondents in the EU are aware of a law that allows them to access their personal data as held by public administration; however, this percentage decreases to 51% for private companies;
- more than one in five respondents (23%) in the EU do not want to share personal data (such as one's address, citizenship or date of birth) with public administration, and 41% do not want to share these data with private companies.

Individuals are increasingly using their right to lodge complaints with data protection authorities, either individually or by representative actions[75]. Only a few Member States have allowed non-governmental organisations to launch actions without a mandate, in line with the possibility provided by the GDPR. The proposed Directive on representative actions for the protection of the collective interests of consumers[76] is expected, once adopted, to strengthen the framework for representative actions also in the field of data protection.

Complaints

The total number of complaints between May 2018 and end of November 2019 as reported by the Board is around 275 000[77]. However, this figure should be considered with much caution given that the definition of a complaint is not identical among authorities. The absolute number of complaints received by data protection authorities[78] is very different between Member States. The highest numbers of complaints were registered in Germany (67 000), the Netherlands (37 000), Spain and France (18 000 each), Italy (14 000), Poland and Ireland (12 000 each). Two-thirds of authorities reported the number of complaints as ranging between 8 000 and 600. The lowest numbers of complaints were registered in Estonia and Belgium (around 500 each), Malta and Iceland (fewer than 200 each).

The number of complaints is not necessarily correlated to the size of the population or GDP, with for instance close to twice as many complaints in Germany compared to the Netherlands, and four times as many compared to Spain and France.

Feedback from the Multi-stakeholder Group shows that organisations have put in place a variety of measures to facilitate the exercise of data subjects' rights, including implementing processes that ensure individual review of requests and a reply from the controller, the use of several channels (mail, dedicated email address, website, etc.), updated internal procedures and policies on the timely internal handling of requests, and staff training. Some companies have put in place digital portals accessible through the company's website (or the company's intranet for employees) to facilitate the exercise of rights by data subjects.

However, further progress is needed on the following points:

- Not all data controllers comply with their obligation to facilitate the exercise of data subjects' rights[79]. They need to ensure that data subjects have an effective point of contact to whom they can explain their problems. This can be the data

[75] Article 80 GDPR.
[76] COM/2018/0184 final - 2018/089 (COD)
[77] Both under Articles 77 and 80 GDPR.
[78] See contribution from the Board, pages 31-32.
[79] Article 12(2) GDPR.

protection officer, whose contact details have to be provided pro-actively to the data subject[80]. The contact modalities must not be limited to e-mails, but must also enable the data subject to address the controller through other means.

- Individuals still face difficulties when requesting access to their data, for instance from platforms, data brokers and adtech companies.
- The right to data portability is not used to its full potential. The European Strategy for Data (hereafter Data Strategy)[81], adopted by the Commission on 19 February 2020, emphasised the need to facilitate all possible uses of this right (e.g. by mandating technical interfaces and machine-readably formats allowing portability of data in (near-to) real-time). Operators note that there are sometimes difficulties in providing the data in a structured, commonly used machine-readable format (due to the lack of standard). Only organisations in particular sectors, such as banking, telecommunications, water and heating meters, report having implemented the necessary interfaces[82]. New technological tools have been developed to facilitate the exercise by individuals of their rights under the GDPR, not limited to data portability (e.g. personal data spaces and personal information management services).
- Rights of children: Several members of the Multi-stakeholder Group stress the need to provide information to children and the fact that many organisations ignore that children may be concerned by their data processing. The Council stressed that particular attention could be paid to the protection of children when drafting codes of conduct. The protection of children is also a focus of data protection authorities[83].
- Right to information: some companies have a very legalistic approach, taking data protection notices as a legal exercise, with information being quite complex, difficult to understand or incomplete, whereas the GDPR requires that any information should be concise and use clear and plain language[84]. It seems that some companies do not follow the Board's recommendations, for example as regards listing the names of the entities with whom they share data.
- Several Member States extensively restricted data subjects' rights through national law, and some even beyond the margins of Article 23 of the GDPR.
- The exercise of the rights of individuals is sometimes hampered by the practices of a few major digital players that make it difficult for individuals to choose the settings that most protect their privacy (in violation of the requirement of data protection by design and default[85])[86].

---

80 Article 13(1)(b) and Article 14 (1)(b) GDPR.

81 https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf

82 See report from the Multi-stakeholder Group.

83 See the results of a public consultation on children's data protection rights carried out by the Irish data protection authority: https://www.dataprotection.ie/sites/default/files/uploads/2019-09/Whose%20Rights%20Are%20They%20Anyway_Trends%20and%20Hightlights%20from%20Stream%201.pdf. The French data protection authority also launched a public consultation in April 2020: https://www.cnil.fr/fr/la-cnil-lance-une-consultation-publique-sur-les-droits-des-mineurs-dans-lenvironnement-numerique

84 Article 12(1) GDPR.

85 Article 25 GDPR.

The Board's guidelines on data subjects' rights are eagerly awaited by stakeholders.

5 OPPORTUNITIES AND CHALLENGES FOR ORGANISATIONS, IN PARTICULAR SMALL AND MEDIUM SIZE ENTERPRISES

Opportunities for organisations

The GDPR fosters competition and innovation. Together with the Free Flow of Non-Personal Data Regulation[87], it ensures the free flow of data within the EU and creates a level playing field with companies not established in the EU. By creating a harmonised framework for the protection of personal data, the GDPR ensures that all actors in the internal market are bound by the same rules and benefit from the same opportunities, regardless of whether they are established and where the processing takes place. The technological neutrality of the GDPR provides the data protection framework for new technological developments. The principles of data protection by design and by default incentivises innovative solutions, which include data protection considerations from the outset and may reduce the cost of compliance with data protection rules.

In addition, privacy becomes an important competitive parameter that individuals increasingly take into consideration when choosing their services. Those who are more informed and sensitive to data protection considerations look for products and services that ensure effective protection of personal data. The implementation of the right to data portability has the potential to lower the barriers to entry for businesses offering innovative, data-protection-friendly services. The effects of a potentially broader use of this right on the market in different sectors should be monitored. Compliance with the data protection rules and their transparent application will create trust on the use of the people's personal data and thus new opportunities for businesses.

Like all regulation, data protection rules have inherent compliance costs for companies. However, these costs are outweighed by the opportunities and advantages of strengthened trust in digital innovation and the societal benefits resulting from respecting a fundamental right. By ensuring a level playing field and equipping data protection authorities with what they need to enforce the rules effectively, the GDPR prevents non-compliant companies from free-riding on the trust built by those who follow the rules.

Specific challenges for Small and Medium size Enterprises (SMEs)

---

[86] See report by the Norwegian Consumer Council, Deceived by Design, which highlighted the "dark patterns", default settings and other features and techniques used by companies to nudge users towards intrusive options:
https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design/
See also the research published in December 2019 by the Transatlantic Consumer Dialogue and the Heinrich-Böll-Stiftung Brussels European Union analysing the practices of three major global platforms:
https://eu.boell.org/en/2019/12/11/privacy-eu-and-us-consumer-experiences-across-three-global-platforms

[87] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union - OJ L 303, 28.11.2018, p. 59–68

There is a general perception by stakeholders, but also by the European Parliament, the Council and data protection authorities that applying the GDPR is especially challenging for micro, small and medium size enterprises, and to small voluntary and charitable organisations.

According to the risk-based approach, it would not be appropriate to provide derogations based on the size of the operators, as their size is not in itself an indication of the risks the processing of personal data that it undertakes can create for individuals. The risk-based approach pairs flexibility with effective protection. It takes into account the needs of SMEs that do not have processing of data as their core business, and calibrates their obligations in particular based on the likelihood and severity of the risks related to the specific processing they carry out.[88]

Small and low-risk processing should not be treated in the same way as high risk and frequent processing – independently of the size of the company that undertakes it. Therefore, as the Board concluded, "in any case, the risk-based approach promoted by the legislator in the text should be maintained, as risks for data subjects do not depend on the size of controllers"[89]. The data protection authorities should fully take on board this principle when enforcing the GDPR, preferably within a common European approach in order not to create barriers to the Single Market.

The data protection authorities developed several tools and stressed their intention to further improve them. Some authorities have launched awareness campaigns and will even hold free "GDPR classes" for SMEs.

Examples of guidance and tools provided by data protection authorities specifically to SMEs

- publication of information addressed to SMEs;
- seminars for data protection officers and events for SMEs that do not need to designate a data protection officer;
- interactive guides to assist SMEs;
- hotlines for consultations;
- templates for processing contracts and records on processing activities.

A description of activities carried out by data protection authorities is presented in the Board's contribution[90].

Several of the actions that specifically support SMEs received EU funding. The Commission provided financial support through three waves of grants, for a total of EUR 5 million, with the two most recent ones specifically aimed at supporting national data protection authorities in their efforts to reach out to individuals and SMEs. As a result, in 2018, EUR 2 million were allocated to nine data protection authorities for activities in 2018-2019 (Belgium, Bulgaria, Denmark, Hungary,

88 Article 24(1) GDPR.
89 See contribution from the Board, p. 35.
90 See contribution from the Board, pages 35-45.

Lithuania, Latvia, the Netherlands, Slovenia, and Iceland)[91], and in 2019 EUR 1 million was allocated to four data protection authorities for activities in 2020 (Belgium, Malta, Slovenia and Croatia in partnership with Ireland)92. An additional EUR 1 million will be allocated in 2020.

Despite these initiatives, SMEs and start-ups often report that they struggle with the implementation of the accountability principle set forth under the GDPR[93]. They notably report that they do not always get enough guidance and practical advice from the national data protection authorities, or that the time it takes to get guidance and advice is too long. There have also been cases where authorities were reluctant to engage in legal issues. When confronted with such situations, SMEs often turn to external advisors and lawyers to deal with the implementation of the accountability principle and the risk-based approach (including transparency requirements, records of processing and data breach notifications). This may also create further costs for them.

One specific issue is the recording of processing activities, which is considered by SMEs and small associations as a cumbersome administrative burden. The exemption from that obligation in Article 30(5) GDPR is indeed very narrow. However, the related efforts for complying with that obligation should not be over-estimated. Where the core business of SMEs does not involve the processing of personal data, such records may be simple and not burdensome. The same applies for voluntary and other associations. Such simplified records would be facilitated by records templates, as is already the practice of some data protection authorities. In any case, everyone who processes personal data should have an overview on their data processing as a basic requirement of the accountability principle.

The development of practical tools at EU level by the Board, such as harmonised forms for data breaches and simplified records of processing activities, may help SMEs and small associations[94] whose main activities do not focus on the processing of personal data to meet their obligations.

Various industry associations have made efforts to raise awareness and inform their members, for instance through conferences and seminars, providing businesses with information on available guidance, or developing a privacy assistance service for members. They also report an increasing number of seminars, meetings and events organised by think tanks and SME associations on matters related to the GDPR.

In order to enhance the free movement of all data within the EU and to establish a coherent application of the GDPR and the Free Flow of Non-Personal Data Regulation, the Commission also issued a practical guidance on rules governing the

---

91 https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/rec-rdat-trai- ag-2017.

92 https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules/eu-funding-supporting-implementation-gdpr_en

93 See report from the Multi-stakeholder Group.

94 See contribution from the Council.

processing of mixed datasets, composed of both personal and non-personal data, and targeting especially SMEs[95].

Toolbox for businesses

The GDPR provides for tools that help demonstrate compliance, such as codes of conduct, certification mechanisms, and standard contractual clauses.

- Codes of conduct

The Board has issued guidelines[96] to support and facilitate "code owners" in drafting, amending or extending codes, and to provide practical guidance and interpretative assistance. These guidelines also clarify the procedures for the submission, approval and publication of codes at both national and EU level by setting out the minimum criteria required.

Stakeholders consider codes of conduct as very useful tools. Although many codes are implemented at national level, a number of EU wide codes of conduct are currently in preparation (for instance on mobile health apps, health research in genomics, cloud computing, direct marketing, insurance, processing by prevention and counselling services for children)[97]. Operators believe that EU-wide codes of conduct should be promoted more prominently as they foster the consistent application of the GDPR across all Member States.

However, codes of conduct also require time and investment from operators both for their development and for the setting up of the required independent monitoring bodies. Representatives from SMEs stress the importance and usefulness of codes of conduct tailored to their situation and not entailing disproportionate costs.

Consequently, business associations in a number of sectors implemented other kinds of self-regulatory tools such as codes of good practice or guidance. While such tools may provide useful information, they do not have the approval of data protection authorities and cannot serve as a tool to help demonstrate compliance with the GDPR.

The Council stresses that codes of conduct must pay particular attention to the processing of children's data and health data. The Commission is supporting code(s) of conducts that would harmonise the approach in health and research and facilitate the cross-border processing of personal data[98]. The Board is in the process of approving draft accreditation requirements for codes of conduct monitoring bodies put forward by a number of data protection authorities[99]. Once transnational or EU codes of conduct are ready to be submitted to data protection authorities for approval, they will undergo consultation of the Board. Having transnational codes of conduct rapidly in place is especially important for areas involving the processing of significant amounts of data (e.g. cloud computing) or sensitive data (e.g. health/research).

---

95 Communication from the Commission to the European Parliament and the Council - Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union, COM/2019/250 final.

96 https://edpb.europa.eu/our-work-tools/our-documents/wytyczne/guidelines-12019-codes-conduct-and-monitoring-bodies-under_en.

97 See report from the Multi-stakeholder Group.

98 See actions announced in the European Strategy for Data, page 30.

99 Under Article 41(3) GDPR. See EDPB opinions at: https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en

- Certification

Certification can be a useful instrument to demonstrate compliance with specific requirements of the GDPR. It can increase legal certainty for businesses and promote the GDPR globally.

As pointed out in the study on certification published in April 2019[100], the objective should be to facilitate the uptake of relevant schemes. The development of certification schemes in the EU will be supported by the guidelines issued by the Board on certification criteria [101] and on the accreditation of certification bodies[102].

Security and data protection by design are key elements to be considered in certification schemes under the GDPR and would benefit from a common and ambitious approach throughout the EU. The Commission will continue to support the current contacts between the European Union Agency for Cybersecurity (ENISA), the data protection authorities and the Board.

As regards cybersecurity, following the adoption of the Cybersecurity Act the Commission requested that ENISA prepare two certification schemes including one scheme for cloud services[103]. Further schemes addressing the cybersecurity of services and products for consumers are under consideration. While these certification schemes established under the Cybersecurity Act, do not explicitly address data protection and privacy, they contribute to increasing consumers' trust in digital services and products. Such schemes may provide evidence of adherence to the principles of security by design as well as the implementation of appropriate technical and organisational measures related to the security of processing of personal data.

- Standard contractual clauses

The Commission is working on standard contractual clauses between controllers and processors[104], also in light of the modernisation of the standard contractual clauses for international transfers (see Section 7.2). A Union act, adopted by the Commission, will have EU-wide binding effect which will ensure full harmonisation and legal certainty.

6 THE APPLICATION OF THE GDPR TO NEW TECHNOLOGIES

A technology neutral framework open to new technologies

The GDPR is technology-neutral, trust-enabling, and based on principles[105]. These principles, including lawful and transparent processing, purpose limitation and data

[100] https://ec.europa.eu/info/study-data-protection-certification-mechanisms_en

[101] https://edpb.europa.eu/our-work-tools/our-documents/smjernice/guidelines-12018-certification-and-identifying-certification_en.

[102] https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies_en. Several supervisory authorities have already submitted their accreditation requirements to the EDBP, both for code of conduct monitoring bodies and for certification bodies. See the overview at: https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en.

[103] https://ec.europa.eu/digital-single-market/en/news/towards-more-secure-and-trusted-cloud-europe

[104] Article 28(7) GDPR.

[105] As recalled by the Council, the European Parliament and the Board in their contributions to the evaluation.

minimisation, provide for a solid basis for the protection of personal data, irrespective of the processing operations and techniques applied.

Members of the Multi-stakeholder Group report that overall the GDPR has a positive impact on the development of new technologies and provides a good basis for innovation. The GDPR is seen as an essential and flexible tool for ensuring the development of new technologies in accordance with fundamental rights. The implementation of its core principles is particularly crucial for data intensive processing. The GDPR's risk based and technology neutral approach provides a level of data protection that is adequate to address the risk of processing, including by emerging technologies.

In particular, stakeholders mention that the GDPR's principles of purpose limitation and further compatible processing, data minimisation, storage limitation, transparency, accountability and the conditions under which automated decision making processes[106] can be legally deployed to a large extent address the concerns related to the use of artificial intelligence.

The future-proof and risk based approach of the GDPR will also be applied in the possible future framework for artificial intelligence and when implementing the Data Strategy. The Data strategy aims at fostering data availability and at the creation of common European data spaces supported by federated cloud infrastructure services. As regards personal data, the GDPR provides the main legal framework, within which effective solutions can be devised on a case-by-case basis depending on the nature and content of each data space.

The GDPR has increased awareness about the protection of personal data both within and outside the EU and has prompted companies to adapt their practices to take into account data protection principles when innovating. However, civil society organisations note that, although the GDPR's impact on the development of new technologies appears positive, the practices of major digital players have not yet fundamentally changed towards more privacy-friendly processing. Strong and effective enforcement of the GDPR vis-à-vis large digital platforms and integrated companies, including in areas such as online advertising and micro-targeting, is an essential element for protecting individuals.

The Commission is analysing the broader issues related to the market behaviours of large digital players in the context of the Digital Services Act package[107]. As regards research in the field of social media, the Commission recalls that the GDPR cannot be used as an excuse by social media platforms to limit researchers' and fact-checkers' access to non-personal data such as statistics on which targeted ads have been sent to which categories of people, the criteria for designing this targeting, information on fake accounts, etc.

The GDPR's technologically-neutral and future-proof approach was put to the test during the COVID-19 pandemic and has proven to be successful. Its principles based rules supported the development of tools to combat and monitor the spread of the virus.

---

[106] However, stakeholders observe that not all automated decision-making processes in an artificial intelligence context fall under Article 22 GDPR.

[107] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_962

Challenges to be addressed

The development and application of new technologies do not put these principles into question. The challenges lie in clarifying how to apply the proven principles to the use of specific technologies such as artificial intelligence, blockchain, Internet of Things, facial recognition or quantum computing.

In this context, the European Parliament and the Council stressed the need for a continuous monitoring to clarify how the GDPR applies to new technologies and big tech companies. In addition, stakeholders warn that the assessment of whether the GDPR remains fit for purpose also requires a constant monitoring.

Industry stakeholders stress that innovation requires that the GDPR is applied in a principle-based way, in line with its design, rather than in a rigid and formal manner. They are of the view that Board's guidelines on how to apply the GDPR principles, concepts and rules to new technologies such as artificial intelligence, blockchain or Internet of Things, taking into account the risk-based approach, would help provide clarifications and more legal certainty. Such soft law tools are well suited to accompany the GDPR's application to the new technologies since they provide for more legal certainty and can be reviewed in line with technological developments. Some stakeholders also suggest that sectoral guidance on how to apply the GDPR to new technologies could be helpful.

The Board stated that it will continue to consider the impact of emerging technologies on the protection of personal data.

Stakeholders also underline the importance for regulators to get a thorough understanding of how technology is being used and to engage in a dialogue with industry on the development of emerging technologies. They consider that a 'regulatory sandbox' approach – as a means to obtain guidance on the application of the rules – could be an interesting option to test new technologies and help businesses apply the data protection by design and by default principle in new technologies.

In terms of further policy action, stakeholders recommend that any future policy proposals on artificial intelligence should build on the existing legal frameworks and be aligned with the GDPR. Potential specific issues should be carefully assessed, based on relevant evidence, before new prescriptive rules are proposed.

The Commission White Paper on Artificial Intelligence puts forward a number of policy options on which stakeholders' views were sought until 14 June 2020. As regards facial recognition, a technology that may significantly impact individuals' rights, the White Paper recalled the current legislative framework and opened a public debate on the specific circumstances, if any, which might justify the use of artificial intelligence for facial recognition and other remote biometric identification purposes in public places, and on common safeguards.

7 INTERNATIONAL TRANSFERS AND GLOBAL COOPERATION

7.1 Privacy: a global issue

The demand for the protection of personal data knows no borders, as individuals around the world increasingly cherish and value the privacy and security of their data.

At the same time, the importance of data flows for individuals, governments, companies and, more generally, society at large is an inescapable fact in our interconnected world. They constitute an integral part of trade, cooperation between public authorities and social interactions. In that respect, the current COVID-19 pandemic also highlights how critical the transfer and exchange of personal data are for many essential activities, including ensuring the continuity of government and business operations – by enabling teleworking and other solutions that heavily rely on information and communication technologies – developing cooperation in scientific research on diagnostics, treatments and vaccines, and fighting new forms of cybercrime such as online fraud schemes offering counterfeit medicines claiming to prevent or cure COVID-19.

Against this background, and more than ever before, protecting privacy and facilitating data flows have to go hand in hand. The EU, with its data protection regime combining openness to international transfers with a high level of protection for individuals, is very well placed to promote safe and trusted data flows. The GDPR has already emerged as a reference point at international level and acted as a catalyst for many countries around the world to consider introducing modern privacy rules.

This is a truly global trend running, to mention just a few examples, from Chile to South Korea, from Brazil to Japan, from Kenya to India, from Tunisia to Indonesia, and from California to Taiwan. These developments are remarkable not only from a quantitative but also from a qualitative point of view: many of the privacy laws recently adopted, or in the process of being adopted, are based on a core set of common safeguards, rights and enforcement mechanisms that are shared by the EU. In a world that is too often characterised by different, if not divergent, regulatory approaches, this trend towards global convergence is a very positive development that brings new opportunities for increasing the protection of individuals in Europe while, at the same time, facilitating data flows and lowering transaction costs for business operators.

To seize these opportunities and implement the strategy set out in its 2017 Communication on "Exchanging and Protecting Personal Data in a Globalised World"[108], the Commission has significantly stepped up its work on the international dimension of privacy making full use of the available transfer 'toolbox', as explained below. This included actively engaging with key partners with a view to reaching an "adequacy finding" and yielded important results, such as the creation of the world's largest area of free and safe data flows between the EU and Japan.

Besides its adequacy work, the Commission has worked closely with data protection authorities within the Board, as well as with other stakeholders, to harness the full potential of the GDPR's flexible rules for international transfers. This concerns the modernisation of instruments such as standard contractual clauses, the development of certification schemes, codes of conduct or administrative arrangements for data exchanges between public authorities, as well as the clarification of key concepts

[108] Communication from the Commission to the European Parliament and the Council 'Exchanging and Protecting Personal Data in a Globalised World', 10.1.2017 (COM(2017) 7 final).

relating to, for example, the territorial scope of EU data protection rules or the use of so-called "derogations" to transfer personal data.

Finally, the Commission intensified its dialogue in a number of bilateral, regional and multilateral fora to foster a global culture of respect for privacy and develop elements of convergence between different privacy systems. In its efforts, the Commission could count on the active support of the European External Action Service and the network of EU delegations in third countries and missions to international organisations. This also ensured coherence and greater complementarity between different aspects of the external dimension of EU policies – from trade to the new Africa-EU Partnership.

7.2 The GDPR transfer toolbox

As more and more private and public operators rely on international data flows as part of their routine operations, there is an increasing need for flexible instruments that can be adapted to different sectors, business models and transfer situations. Reflecting these needs, the GDPR offers a modernised toolbox that facilitates the transfer of personal data from the EU to a third country or international organisation, while ensuring that the data continues to benefit from a high level of protection. This continuity of protection is important, given that in today's world data moves easily across borders and the protections guaranteed by the GDPR would be incomplete if they were limited to processing inside the EU.

With Chapter V of the GDPR, the legislator confirmed the architecture of the transfer rules that already existed under Directive 95/46: data transfers may take place where the Commission has made an adequacy finding with respect to a third country or international organisation or, in the absence thereof, where the controller or processor in the EU ("data exporter") has provided appropriate safeguards, for instance through a contract with the recipient ("data importer"). In addition, statutory grounds for transfers (so-called derogations), remain available for specific situations for which the legislator has decided that the balance of interests allows a data transfer under certain conditions. At the same time, the reform has clarified and simplified the existing rules, for instance by stipulating in detail the conditions for an adequacy finding or binding corporate rules, by limiting authorisation requirements to very few, specific cases and completely abolishing notification requirements. Moreover, new transfer tools like codes of conduct or certification schemes have been introduced and the possibilities for using existing instruments (e.g. standard contractual clauses) have been expanded.

Today's digital economy allows foreign operators to (remotely but) directly participate in the EU internal market and to compete for European customers and their personal data. Where they specifically target Europeans through the offering of goods or services, or monitoring of their behaviour, they should comply with EU law in the same way as EU operators. This is reflected in Article 3 of the GDPR, which extends the direct applicability of EU data protection rules to certain processing operations of controllers and processors outside the EU. This guarantees the necessary safeguards, and moreover a level playing field for all companies operating in the EU market.

Its broad reach is one of the reasons why the effects of the GDPR have also been felt in other parts of the world. The detailed guidance issued by the Board on the GDPR territorial scope, following a comprehensive public consultation, is therefore

important to help foreign operators determine whether and which processing activities are directly subject to its safeguards, including by providing concrete examples [109].

The extension of the scope of application of EU data protection law, however, in and of itself is not sufficient to guarantee its respect in practice. As also highlighted by the Council[110], it is crucial to ensure compliance by, and effective enforcement against, foreign operators. The appointment of a representative in the EU (Article 27(1), (2) of the GDPR), who can be addressed by individuals and supervisory authorities in addition to or instead of the responsible company acting from abroad[111] should play a key role in this regard. This approach, which is also increasingly taken in other contexts[112], should be pursued more vigorously to send a clear message that the lack of an establishment in the EU does not relieve foreign operators of their responsibility under the GDPR. Where these operators fail to meet their obligation to appoint a representative[113], supervisory authorities should make use of the full enforcement toolbox in Article 58 of the GDPR (e.g. public warnings, temporary or definitive bans on processing in the EU, enforcement against joint controllers established in the EU).

Finally, it is very important that the Board finalises its work on further clarifying the relationship between Article 3 on the direct application of the GDPR and the rules on international transfers in Chapter V[114].

Adequacy decisions

The input received from stakeholders confirms that adequacy decisions continue to be an essential tool for EU operators to safely transfer personal data to third countries[115]. Such decisions provide the most comprehensive, straightforward and cost-effective solution for data transfers as these are assimilated to intra-EU transmissions, thus ensuring the safe and free flow of personal data without further conditions or need for authorisation. Adequacy decisions therefore open up commercial channels for EU operators and facilitate cooperation between public authorities, while providing

---

[109] EDPB, Guidelines 2/2018 on the territorial scope of the GDPR, 12.11.2019. The Guidelines address several of the points raised during the public consultation, for instance the interpretation of the targeting and monitoring criteria.

[110] See Council position and findings, paras 34, 35 and 38.

[111] See Article 27(4) and Recital 80 GDPR ("The designated representative should be subject to enforcement proceedings in the event of non-compliance by the controller or processor").

[112] Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings (COM/2018/226 final), Article 3; Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM(2018) 640 final), Article 16(2), (3).

[113] According to one submission to the public consultation, one of the main points to address "is effective enforcement and real consequences for those who chose to ignore this requirement […] It should be borne in mind in particular that this also places businesses established in the Union at a competitive disadvantage to those noncompliant businesses established outside the Union trading into the Union." See EU Business Partners, submission of 29 April 2020.

[114] Several submissions to the public consultation have raised this point, for instance as regards the transmission of personal data to recipients outside the EU but covered by the GDPR.

[115] Council position and findings, paragraph 17; Contribution from the Board, pp. 5-6. Several submissions to the public consultation, including from a number of business associations (like the French Association of Large Companies, Digital Europe, the Global Data Alliance/BSA, the Computer & Communication Industry Association (CCIA) or the US Chamber of Commerce) have called for stepping-up the work on adequacy findings, especially with important trading partners.

privileged access to the EU single market. Building on the practice under the 1995 Directive, the GDPR explicitly allows for an adequacy determination to be made with respect to a particular territory of a third country or to a specific sector or industry within a third country (so-called 'partial' adequacy).

The GDPR builds upon the experience of the past years and the clarifications provided by the Court of Justice by setting out a detailed catalogue of elements that the Commission must take into account in its assessment. The adequacy standard requires a level of protection that is comparable (or 'essentially equivalent') to that ensured within the EU[116]. This involves a comprehensive assessment of the third country's system as a whole, including the substance of privacy protections, their effective implementation and enforcement, as well as the rules on access to personal data by public authorities, in particular for law enforcement and national security purposes[117].

This is also reflected in the guidance adopted by the former Article 29 Working Party (and endorsed by the Board), in particular the so-called 'adequacy referential', which further clarifies the elements that the Commission must take into account when carrying out an adequacy assessment, including by providing an overview of 'essential guarantees' for access to personal data by public authorities[118]. The latter builds in particular on the case law of the European Court of Human Rights. While the standard of 'essential equivalence' does not involve a point-to-point replication ('photocopy') of EU rules, given that the means of ensuring a comparable level of protection may vary between different privacy systems, often reflecting different legal traditions, it nevertheless requires a strong level of protection.

This standard is justified by the fact that an adequacy decision essentially extends to a third country the benefits of the single market in terms of the free flow of data. However, it also means that sometimes there will be relevant differences between the level of protection ensured in the third country in question compared to the GDPR that need to be bridged, for instance through the negotiation of additional safeguards. Such safeguards should be viewed positively as they further strengthen the protections available to individuals in the EU. At the same time, the Commission agrees with the Board on the importance of continuously monitoring their application in practice, including effective enforcement by the third country data protection authority[119].

The GDPR clarifies that adequacy decisions are 'living instruments' that should be continuously monitored and periodically reviewed[120]. In line with these requirements,

---

[116] Judgment of the Court of Justice of the EU of 6 October 2015 in Case C-362/14, Maximillian Schrems v Data Protection Commissioner ('*Schrems*'), points 73, 74 and 96. See also Recital 104 of the GDPR, which refers to the standard of essential equivalence.

[117] Article 45(2) and Recital 104 GDPR. See also *Schrems* , points 75, 91-91.

[118] Adequacy Referential, WP 254 rev. 01, 6 February 2018 (available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108).

[119] Contribution from the Board, pp. 5-6.

[120] Article 45(4) and (5) GDPR require the Commission to monitor developments in third countries on an ongoing basis and to regularly – at least every four years – review an adequacy finding. They also give the Commission the power to repeal, amend or suspend an adequacy decision if it finds that the country or international organisation concerned no longer ensures an adequate level of protection. Article 97(2)(a) GDPR furthermore requires the Commission to submit an evaluation report to the European Parliament and the Council by 2020. See also the judgment of the Court of

the Commission has regular exchanges with the relevant authorities to pro-actively follow-up on new developments. For example, since the adoption of the decision on the EU-U.S. Privacy Shield in 2016[121], the Commission, together with representatives from the Board, carried out three annual reviews to evaluate all aspects of the functioning of the framework.[122] These reviews relied on information obtained through exchanges with the U.S. authorities as well as input from other stakeholders, such as EU data protection authorities, civil society and trade associations. They have allowed to improve the practical functioning of various elements of the framework. In a wider perspective, the annual reviews contributed to establishing a broader dialogue with the U.S. administration on privacy in general, and the limitations and safeguards with respect to national security in particular.

As part of its first evaluation of the GDPR, the Commission is also required to review the adequacy decisions adopted under the 1995 Directive[123]. The Commission services have engaged in an intense dialogue with each of the 11 concerned countries and territories to assess how their personal data protection systems have evolved since the adequacy decision was adopted and whether they meet the standard set by the GDPR. The need to ensure the continuity of such decisions, as they are a key tool for trade and international cooperation, is one of the factors that has prompted several of these countries and territories to modernise and strengthen their privacy laws. These are certainly welcome developments. Additional safeguards are being discussed with some of these countries and territories to address relevant differences in protection.

However, given that the Court of Justice in a judgment to be delivered on 16 July may provide clarifications that could be relevant for certain elements of the adequacy standard, the Commission will report separately on the evaluation of the mentioned 11 adequacy decisions after the Court of Justice has handed down its judgment in that case.[124]

Justice of the EU of 6 October 2015 in Case C-362/14, *Maximillian Schrems* v *Data Protection Commissioner*, point 76.

[121] Commission implementing decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield. This adequacy decision is a specific case that, in the absence of general data protection legislation in the U.S., relies on commitments made by participating companies (that are enforceable under U.S. law) to apply the data protection standards set out by this arrangement. Moreover, the Privacy Shield builds on the specific representations and assurances made by the U.S. government as regards access for national security purposes that underpin the adequacy finding

[122] Reviews took place in 2017 (Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU-U.S. Privacy Shield, COM(2017) 611 final), 2018 (Report from the Commission to the European Parliament and the Council on the second annual review of the functioning of the EU-U.S. Privacy Shield, COM(2018) 860 final) and 2019 (Report from the Commission to the Parliament and the Council on the third annual review of the functioning of the EU-U.S. Privacy Shield, COM(2019) 495 final).

[123] These existing adequacy decisions concern countries that are closely integrated with the European Union and its Member States (Switzerland, Andorra, Faroe Islands, Guernsey, Jersey, Isle of Man), important trading partners (e.g. Argentina, Canada, Israel), and countries that played a pioneering role in developing data protection laws in their region (New Zealand, Uruguay)

[124] Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems ("Schrems II"), concerns a reference for a preliminary ruling on the so-called standard contractual clauses. However, certain elements of the adequacy standard may also be further clarified by the

Implementing the strategy laid down in its 2017 Communication on "Exchanging and Protecting Personal Data in a Globalised World", the Commission also engaged in new adequacy dialogues[125]. This work already yielded significant results involving key partners of the EU. In January 2019, the Commission adopted its adequacy decision for Japan, which is based on a high degree of convergence, including through specific safeguards such as in the area of onward transfers and through the creation of a mechanism to investigate and resolve individuals' complaints concerning government access to personal data for law enforcement and national security purposes.

As the first adequacy finding adopted under the GDPR, the framework agreed with Japan provides a useful precedent for future decisions[126]. This includes the fact that it was reciprocated on the Japanese side with an "adequacy" finding for the EU. Together, these mutual adequacy findings create the largest area of safe and free personal data flows in the world, thereby complementing the EU-Japan Economic Partnership Agreement. In fact, the arrangement supports around EUR 124 billion of trade in goods and EUR 42.5 billion of trade in services every year.

The adequacy process is also at an advanced stage with South Korea. One important outcome thereof is South Korea's recent legislative reform that led to the establishment of an independent data protection authority equipped with strong enforcement powers. This illustrates how an adequacy dialogue can contribute to increased convergence between the EU's data protection rules and those of a foreign country.

The Commission fully agrees with the call from stakeholders to intensify the dialogue with selected third countries in view of possible new adequacy findings[127]. It is actively exploring this possibility with other important partners in Asia, Latin America and the Neighbourhood, building on the current trend towards upward global convergence in data protection standards. For example, comprehensive privacy legislation has been adopted or is at an advanced stage of the legislative process in Latin America (Brazil, Chile), and promising developments are taking place in Asia (e.g. India, Indonesia, Malaysia, Sri Lanka, Taiwan and Thailand), Africa (e.g. Ethiopia, Kenya) as well as in the European Eastern and Southern neighbourhood

---

Court. The hearing in this case took place on 9 July 2019 and the judgment has been announced for 16 July 2020.

[125] See supra fn 109. The Commission explained that the following criteria will be taken into account when assessing with which third countries a dialogue on adequacy should be pursued: (i) the extent of the EU's (actual or potential) commercial relations with the third country, including the existence of a free trade agreement or ongoing negotiations; (ii) the extent of personal data flows from the EU, reflecting geographical and/or cultural ties; (iii) the country's pioneering role in the field of privacy and data protection that could serve as a model for other countries in its region; and (iv) the overall political relationship with the country, in particular as regards the promotion of common values and shared objectives at international level.

[126] European Parliament, Resolution of 13 December 2018 on the adequacy of the protection of personal data afforded by Japan (2018/2979(RSP)), point 27; Contribution from the Board, pp. 5-6.

[127] See e.g. European Parliament, Resolution of 12 December 2017 on 'Towards a digital trade strategy' (2017/2065(INI)), points 8, 9; Council position and findings on the application of the General Data Protection Regulation (GDPR), 19.12.2019 (14994/1/19), paragraph 17; Contribution from the Board, p. 5.

(e.g. Georgia, Tunisia). Where possible, the Commission will work towards achieving comprehensive adequacy decisions covering both the private and public sector[128].

Moreover, the GDPR also introduced the possibility for the Commission to adopt adequacy findings for international organisations. At a time when some international organisations are modernising their data protection regimes by putting in place comprehensive rules, as well as mechanisms that provide independent oversight and redress, this avenue could be explored for the first time.

Adequacy also plays an important role in the context of the relationship with the United Kingdom following Brexit, provided that the applicable conditions are met. It constitutes an enabling factor for trade, including digital trade, and an essential prerequisite for a close and ambitious cooperation in the area of law enforcement and security[129]. Moreover, given the significance of data flows with the UK and its proximity to the EU market, a high degree of convergence between data protection rules on both sides of the Channel is an important element for ensuring a level playing field. In line with the Political Declaration on the Future Relationship between the EU and the UK, the Commission is currently carrying out an adequacy assessment under both the GDPR and the Law Enforcement Directive[130]. Considering the autonomous and unilateral nature of an adequacy assessment, these talks follow a separate track from the negotiations on an agreement on the future relationship between the EU and the UK.

Finally, the Commission welcomes that other countries are putting in place data transfer mechanisms similar to an adequacy finding. In doing so, they often recognise the EU and countries for which the Commission has adopted an adequacy decision, as safe destinations for transfers[131]. The growing number of countries benefitting from EU adequacy decisions, on the one hand, and this form of recognition by other countries, on the other hand, has the potential of creating a network of countries where data can flow freely and safely. The Commission considers this a welcome development that will further increase the benefits of an adequacy decision for third countries and contribute to global convergence. This type of synergies can also usefully contribute to the development of frameworks for the safe and free flow of data, such as in the context of the 'data free flow with trust' initiative (see below).

Appropriate safeguards

The GDPR provides for a number of other transfer instruments beyond the comprehensive solution of an adequacy finding. The flexibility of this "toolbox" is

[128] As also requested by the Council, see Council position and findings on the application of the General Data Protection Regulation (GDPR), 19.12.2019 (14994/1/19), paragraphs 17 and 40. However, this requires that the conditions for an adequacy finding concerning data transfers to public authorities are met, including as regards independent oversight.

[129] See the negotiating directives annexed to the Council Decision authorising the opening of negotiations with the United Kingdom of Great Britain and Northern Ireland for a new partnership agreement (ST 5870/20 ADD 1 REV 3), paragraphs 13 and 118.

[130] See revised text of the political declaration setting out the framework for the future relationship between the European Union and the United Kingdom as agreed at negotiators' level on 17 October 2019, paragraphs 8-10 (available at https://ec.europa.eu/commission/sites/beta-political/files/revised_political_declaration.pdf).

[131] For example, by Argentina, Colombia, Israel, Switzerland or Uruguay.

demonstrated by Article 46 GDPR, which regulates data transfers based on "appropriate safeguards", including enforceable data subject rights and effective legal remedies. To guarantee appropriate safeguards, different instruments are available in order to cater to the transfer needs of both commercial operators and public bodies.

- Standard contractual clauses (SCCs)

The first group of these instruments concerns contractual tools, which can be either tailor-made, ad hoc data protection clauses agreed between an EU data exporter and a data importer outside the EU authorised by the competent data protection authority (Article 46(3)(a) GDPR) or model clauses pre-approved by the Commission (Article 46(2)(c), (d) GDPR[132]). The most important of these instruments are so-called standard contractual clauses (SCCs), i.e. model data protection clauses which the data exporter and the data importer can incorporate into their contractual arrangements (e.g. a service contract requiring the transfer of personal data) on a voluntary basis and that set out the requirements related to appropriate safeguards.

SCCs represent by far the most widely used data transfer mechanism[133]. Thousands of EU companies rely on SCCs in order to provide a wide range of services to their clients, suppliers, partners and employees, including services essential to the functioning of the economy. Their broad use indicates that they are very helpful to businesses in their compliance efforts and of particular benefit to companies that do not have the resources to negotiate individual contracts with each of their commercial partners. Through their standardisation and pre-approval, SCCs provide companies with an easy-to-implement tool to meet data protection requirements in a transfer context.

The existing sets of SCCs[134] were adopted and approved on the basis of the 1995 Directive. These SCCs remain in force until amended, replaced or repealed, if necessary, by a Commission decision (Article 46(5) of the GDPR). The GDPR expands the possibilities to use SCCs both within the EU and for international transfers. The Commission is working together with stakeholders to make use of these possibilities and to update existing clauses[135]. In order to ensure that the future design of SCCs is fit for purpose, the Commission has been collecting feedback on

---

[132] Standard contractual clauses (SCCs) for international transfers always require Commission approval, but may be prepared either by the Commission itself or by a national DPA. All existing SCCs fall into the first category.

[133] According to the IAPP-EY Annual Privacy Governance Report 2019, "the most popular of these [transfer] tools – year over year – are overwhelmingly standard contractual contracts: 88% of respondents in this year's survey reported SCCs as their top method for extraterritorial data transfers, followed by compliance with the EU-U.S. Privacy Shield arrangement (60%). For respondents transferring data from the EU to the U.K. (52%), 91% report they intend to use SCCs for data-transfer compliance after Brexit".

[134] There are currently three sets of standard contractual clauses adopted by the Commission for the transfer of personal data to third countries: two for transfers from an EEA-controller to a non-EEA controller and one for transfers from an EEA-controller to a non-EEA-processor. They were amended in 2016, further to the judgment of the Court of Justice in the *Schrems I* case (C-362/14), to remove any restrictions on the competent supervisory authorities to exercise their powers to oversee data transfers. See https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

[135] See also Contribution from the Board, pp. 6-7. Likewise, the Council has called on the Commission "to review and revise [the SCCs] in the near future to take into account the needs of controllers and processors". See Council position and findings.

stakeholders' experiences with SCCs, through the 'Multi-stakeholder Group on the GDPR' and a dedicated workshop held in September 2019, but also via multiple contacts with companies using SCCs as well as civil society organisations. The Board is also updating a number of guidelines that could be relevant for the review of SCCs, for instance on the concepts of controller and processor.

Building on the feedback received, the Commission services are currently working on revising the SCCs. In that context, a number of areas for improvement have been identified, in particular with regard to the following aspects:

1. Updating the SCCs in light of new requirements introduced by the GDPR, such as those concerning the controller-processor relationship under Article 28 GDPR (in particular the processor obligations), the transparency obligations of the data importer (in terms of the necessary information to be provided to the data subject), etc.
2. Addressing a number of transfer scenarios that are not covered by the current SCCs, such as the transfer of data from an EU processor to a non-EU (sub) processor, but also for instance situations where the controller is located outside the EU[136].
3. Better reflecting the realities of processing operations in the modern digital economy, where such operations often involve multiple data importers and exporters, long and often complex processing chains, evolving business relationships, etc. In order to cater for such situations, solutions being explored include, for example, the possibility to enable the signing of SCCs by multiple parties or accession of new parties throughout the lifetime of the contract.

In addressing these points, the Commission is also considering ways to make the current 'architecture' of the SCCs more user friendly, for example by replacing multiple sets of SCCs by a single comprehensive document. The challenge is to strike a good balance between the need for clarity and a certain degree of standardisation, on the one hand, and the necessary flexibility that will allow the clauses to be used by a number of operators with different requirements, in different contexts and for different types of transfers, on the other hand.

Another important aspect to consider is the possible need, in light of current litigation before the Court of Justice[137], to further clarify the safeguards as regards access by foreign public authorities to data transferred based on SCCs, in particular for national security purposes. This may include requiring the data importer or the data exporter, or both, to take action, and to clarify the role of data protection authorities in that context. Although the revision of the SCCs is well-advanced, it will be necessary to wait for the judgment of the Court to reflect any possible additional requirement in the revised clauses, before a draft decision on a new set of SCCs can be submitted to the

[136] Several submissions to the public consultation have commented on this last scenario, often raising concerns that requiring EU processors to ensure appropriate safeguards in their relationship with non-EU controllers would place them at a competitive disadvantage vis-à-vis foreign processors offering similar services.

[137] See Schrems II case.

Board for its opinion and then proposed for adoption through the "comitology procedure"[138].

In parallel, the Commission is in contact with international partners that are developing similar tools.[139] This dialogue, allowing for an exchange of experiences and best practices, could significantly contribute to further developing convergence 'on the ground', and in this way facilitate compliance with cross-border transfer rules for companies operating across different regions of the world.

- Binding corporate rules (BCRs)

Another important instrument are the so-called binding corporate rules (BCRs). These are legally binding policies and arrangements that apply to the members of a corporate group, including their employees (Articles, 46(2)(b), 47 of the GDPR). The use of BCRs allows personal data to move freely among the various group members worldwide – dispensing with the need to have contractual arrangements between each and every corporate entity – while ensuring that the same high level of protection of personal data is complied with throughout the group. They offer a particularly good solution for complex and large corporate groups and for close cooperation of enterprises exchanging data across multiple jurisdictions. Unlike for the 1995 Directive, under the GDPR BCRs can be used by a group of enterprises engaged in a joint economic activity but not forming part of the same corporate group.

Procedurally, BCRs have to be approved by the competent data protection authorities, based on a non-binding opinion by the Board[140]. To guide this process, the Board has reviewed the BCR 'referentials' (setting out substantive standards) for controllers[141] and processors[142] in light of the GDPR, and continues to update these documents on the basis of the practical experience gained by supervisory authorities. It has also adopted various guidance documents to help applicants, and streamline the application and approval process for BCRs[143]. According to the Board, more than 40 BCRs are currently in the pipeline for approval, half of which are expected to be approved by the end of 2020[144]. It is important that data protection authorities continue working on further streamlining the approval process, as the length of such

---

[138] In accordance with Article 46(2)(c) GDPR, standard contractual clauses have to be adopted through the examination procedure laid down under Article 5 of Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers - OJ L 55, 28.2.2011, p. 13–18. This involves in particular a positive decision from a committee composed of representatives of the Member States.

[139] This includes, for instance, the work currently being carried out by the ASEAN Member States to develop 'ASEAN model contractual clauses'. See ASEAN, Key Approaches for ASEAN Cross Border Data Flows Mechanism (available at: https://asean.org/storage/2012/05/Key-Approaches-for-ASEAN-Cross-Border-Data-Flows-Mechanism.pdf).

[140] For an overview of the EDPB opinions rendered so far, see https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en.

[141] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109.

[142] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614110.

[143] These documents were adopted (by the former Article 29 Working Party) following the entry into force of the GDPR, but before the end of the transition period. See WP263 (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623056); WP264 (https://edpb.europa.eu/sites/edpb/files/files/file2/wp264_art29_wp_bcr-c_application_form.pdf); WP265 (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623848).

[144] Contribution from the Board, p. 7.

procedures is often mentioned by stakeholders as a practical obstacle to the broader use of BCRs.

Finally, regarding specifically BCRs approved by the UK data protection authority – the Information Commissioner Office – companies will be able to continue to use them as a valid transfer mechanism under the GDPR after the end of the transition period under the EU-UK Withdrawal Agreement, but only if they are amended so that any connection to the UK legal order is replaced with appropriate references to corporate entities and competent authorities within the EU. The approval of any new BCRs should be sought from one of the supervisory authorities in the EU.

- Certification mechanisms and codes of conduct

In addition to modernising and broadening the application of the already existing transfer tools, the GDPR has also introduced new instruments, thereby expanding the possibilities for international transfers. This includes the use, under certain conditions, of approved codes of conduct and certification mechanisms (such as privacy seals or marks) for ensuring appropriate safeguards. These are bottom-up tools that allow for tailor-made solutions – as a general accountability mechanism (see Articles 40 to 42 of the GDPR) and, specifically, for international data transfers – reflecting, for instance, the specific features and needs of a given sector or industry, or of particular data flows. By calibrating the obligations with the risks, Codes of Conduct can also be a very useful and cost-effective way for small and medium-sized businesses to meet their GDPR obligations.

As regards certification mechanisms, although the Board adopted guidelines to foster their use within the EU, its work on developing criteria to approve certification mechanisms as international transfer tools is still ongoing. The same is true for codes of conduct, regarding which the Board is currently working on guidelines for using them as a tool for transfers.

Given the importance of providing operators with a broad range of transfer instruments that are adapted to their needs, and the potential that in particular certification mechanisms hold for facilitating data transfers while ensuring a high level of data protection, the Commission urges the Board to finalise as soon as possible its guidance in this regard. This concerns both substantive (criteria) and procedural aspects (approval, monitoring, etc.). Stakeholders have expressed a lot of interest in these transfer mechanisms and should be able to make full use of the GDPR's toolkit. The Board's guidelines would also contribute to promoting the EU model for data protection globally and foster convergence as other privacy systems are using similar instruments.

Valuable lessons can be drawn from existing standardisation efforts in the area of privacy, both at European and international level. One interesting example is the recently released international standard ISO 27701[145], which aims to help businesses meet privacy requirements and manage risks related to the processing of personal data through 'privacy information management systems' . Although certification under the standard as such does not fulfil the requirements of Articles 42 and 43 of the GDPR,

[145]The list of specific requirements making up this ISO standard is available at: https://www.iso.org/standard/71670.html.

applying Privacy Information Management Systems can contribute to accountability, including in the context of international data transfers.

- International agreements and administrative arrangements

The GDPR also makes it possible to ensure appropriate safeguards for data transfers between public authorities or bodies on the basis of international agreements (Article 46(2)(a)) or administrative arrangements (Article 46(3)(b)). While both instruments have to guarantee the same outcome in terms of safeguards, including enforceable data subject rights and effective legal remedies, they differ as to their legal nature and adoption procedure.

Unlike international agreements, which create binding obligations under international law, administrative arrangements (e.g. in the form of a Memorandum of Understanding) are typically non-binding and therefore require prior authorisation by the competent data protection authority (see also Recital 108 of the GDPR). One early example concerns the administrative arrangement for the transfer of personal data between EEA and non-EEA financial supervisors cooperating under the umbrella of the International Organisation of Securities Commission (IOSCO), on which the Board gave its Opinion[146] in early 2019. Since then, the Board has further developed its interpretation of the 'minimum safeguards' that international (cooperation) agreements and administrative arrangements between public authorities or bodies (including international organisations) need to ensure to comply with the requirements of Article 46 GDPR. On 18 January 2020 it adopted draft guidelines[147], thereby addressing the Member States' request for further clarification and guidance as to what may be considered appropriate safeguards for transfers between public authorities[148]. The Board strongly recommends that public authorities use these guidelines as a reference point for their negotiations with third parties[149].

The guidelines demonstrate the flexibility in the design of such instruments, including on important aspects such as oversight[150] and redress[151]. This should allow public

---

[146] EDPB, Opinion 4/2019 on the draft Administrative Arrangement for the transfer of personal data between European Economic Area (EEA) Financial Supervisory Authorities and non-EEA Financial Supervisory Authorities, 12.2.2019.

[147] EDPB, Guidelines 2/2020 on articles 46(2)(a) and 46(3)(b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies (draft available at: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b_en). According to the EDPB, "[t]he competent [supervisory authority] will base its examination on the general recommendations set out in these guidelines, but might also ask for more guarantees depending on the specific case." The EDPB submitted these draft guidelines to a public consultation that ended on 18 May 2020.

[148] Council position and findings, paragraph 20.

[149] At the same time, the EDPB clarifies that public authorities remain "free to rely on other relevant tools providing for appropriate safeguards in accordance with Article 46 GDPR." Regarding the choice of instrument, the EDPB underlines that "[i]t should be carefully assessed whether or not to make use of non-legally binding administrative arrangements to provide safeguards in the public sector, in view of the purpose of the processing and the nature of the data at hand. If data protection rights and redress for EEA individuals are not provided for in the domestic law of the third country, preference should be given to concluding a legally binding agreement. Irrespective of the type of instrument adopted, the measures in place have to be effective to ensure the appropriate implementation, enforcement and supervision" (paragraph 67).

[150] This may include, for instance, combining internal checks (with a commitment to inform the other party of any instance of non-compliance with independent oversight through external or at least

authorities to overcome the difficulties in, for instance, ensuring enforceable data subject rights through non-binding arrangements. An important element of such arrangements is their continuous monitoring by the competent data protection authority – supported by information and record-keeping requirements – and the suspension of data flows if appropriate safeguards can no longer be ensured in practice.

Derogations

Finally, the GDPR clarifies the use of so-called 'derogations'. These are specific grounds for data transfers (e.g. explicit consent[152], performance of a contract or important reasons of public interest) recognised in law, and on which entities can rely in the absence of other transfer tools and under certain conditions.

To clarify the use of such statutory grounds, the Board has issued specific guidance[153] and has interpreted Article 49 in a number of cases with respect to specific transfer scenarios[154]. Due to their exceptional character, the Board considers that derogations have to be interpreted restrictively, on a case-by-case basis. Despite their strict interpretation, these grounds cover a broad range of transfer scenarios. This includes in particular data transfers by both public authorities and private entities necessary for 'important reasons of public interest', for example between competition, financial, tax or customs authorities, services competent for social security matters or for public health (such as in the case of contact tracing for contagious diseases or in order to eliminate doping in sport)[155]. Another area is that of cross-border cooperation for criminal law enforcement purposes, in particular as regards serious crime[156].

---

through functionally autonomous mechanisms, as well as the possibility for the transferring public body to suspend or terminate the transfer.

151 This may include, for instance, quasi-judicial, binding mechanisms (e.g. arbitration) or alternative dispute resolution mechanisms, combined with the possibility for the transferring public authority to suspend or terminate the transfer of personal data if the parties do not succeed in resolving a dispute amicably, plus a commitment from the receiving public body to return or delete the personal data. When opting for alternative redress mechanisms in binding and enforceable instruments because there is no possibility to ensure effective judicial redress, the EDPB recommends seeking the advice of the competent supervisory authority before concluding these instruments.

152 This is a change from Directive 95/46 which merely required 'unambiguous' consent. In addition, the general requirements for consent pursuant to Article 4(11) GDPR apply.

153 EDPB, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, 25.5.2018 (available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf).

154 This includes, for instance, international transfers of health data for research purposes in the context of the COVID-19 outbreak. See EDPB, Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, 21.4.2020 (available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf).

155 See Recital 112.

156 See Brief of the European Commission on behalf of the European Union as *Amicus Curiae* in Support of Neither Party in the Case *US v. Microsoft*, p. 15: "In general, Union as well as Member State law recognize the importance of the fight against serious crime—and thus criminal law enforcement and international cooperation in that respect—as an objective of general interest. […] Article 83 of the TFEU identifies several areas of crime that are particularly serious and have cross-border dimensions, such as illicit drug trafficking." (available at:

The Board has clarified that, although the relevant public interest must be recognised in EU or Member State law, this can be also established on the basis of "an international agreement or convention which recognises a certain objective and provides for international cooperation to foster that objective can be an indicator when assessing the existence of a public interest pursuant to Article 49(1)(d), as long as the EU or the Member States are a party to that agreement or convention"[157].

Decisions by foreign courts or authorities: not a ground for transfers

In addition to positively setting out the grounds for data transfers, Chapter V of the GDPR also clarifies, in its Article 48, that orders from courts and decisions of administrative authorities outside of the EU *in themselves* do not provide such grounds, unless they are recognised or made enforceable based on an international agreement (e.g. a Mutual Legal Assistance Treaty). Any disclosure by the requested entity in the EU to the foreign court or authority in response to such an order or decision constitutes an international data transfer that needs to be based on one of the mentioned transfer instruments.[158]

The GDPR does not constitute a "blocking statute" and will, under certain conditions, permit a transfer in response to an appropriate law enforcement request from a third country. The important point is that it is EU law that should determine whether this is the case and on the basis of which safeguards such transfers can take place.

The Commission explained the functioning of Article 48 GDPR, including the possible reliance on the public interest derogation, in the context of a production order (warrant) by a foreign criminal law enforcement authority in the *Microsoft* case before the U.S. Supreme Court.[159] In its submission, the Commission stressed the EU's interest in ensuring that law enforcement cooperation takes place "within a legal framework that avoids conflicts of law, and is based on […] respect for each others' fundamental interests in both privacy and law enforcement"[160]. In particular, "from the perspective of public international law, when a public authority requires a

https://www.supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf).

157 EDPB, Derogation Guidelines (*supra* fn. 153), p. 10. The EDPB further clarified that, while data transfers based on the public interest derogation must not be "large scale" or "systematic", but "need to be restricted to specific situations and […] meet the strict necessity test", there is no requirement for them to be "occasional".

158 This is made clear by the wording of Article 48 GDPR ("without prejudice to other grounds for transfer pursuant to this Chapter") and the accompanying Recital 115 ("[t]ransfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may be the case, inter alia, where disclosure is necessary for an important ground of public interest recognised in Union or Member State law to which the controller is subject"). It is also recognised by the EDPB, see Derogation Guidelines (supra fn. 153), p. 5. As for all processing operations, the other safeguards under the Regulation must also be complied with (e.g. that data is transferred for a specific purpose, is relevant, limited to what is necessary for the purpose of the request, etc.).

159 Microsoft submission (*supra* fn. 156). As the Commission explained, the GDPR thus makes MLATs the "preferred option" for transfers as such treaties "provide for collection of evidence by consent, and embody a carefully negotiated balance between the interests of different states that is designed to mitigate jurisdictional conflicts that can otherwise arise." See also EDPB, Derogation Guidelines (*supra* fn. 153), p. 5 ("In situations where there is an international agreement, such as a mutual legal assistance treaty (MLAT), EU companies should generally refuse direct requests and refer the requesting third country authority to existing MLAT or agreement").

160 Microsoft submission (*supra* fn. 156), p. 4.

company established in its own jurisdiction to produce electronic data stored on a server in a foreign jurisdiction, the principles of territoriality and comity under public international law are engaged"[161].

This is also reflected in the Commission's proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters[162], which contains a specific 'comity clause' that makes it possible to raise an objection against a production order if compliance would conflict with the laws of a third country prohibiting disclosure in particular on the ground that this is necessary to protect the fundamental rights of the individuals concerned[163].

Ensuring comity is important, given that law enforcement – like crime and in particular cybercrime – is increasingly cross-border and thus often raises jurisdictional questions and creates potential conflicts of law[164]. Not surprisingly, the best way of addressing these issues is through international agreements that provide for the necessary limitations and safeguards for cross-border access to personal data, including by ensuring a high level of data protection on the side of the requesting authority.

The Commission, acting on behalf of the EU, is currently engaged in multilateral negotiations for a Second Additional Protocol to the Council of Europe Cybercrime ('Budapest') Convention, which aims to enhance existing rules to obtain cross-border access to electronic evidence in criminal investigations while ensuring appropriate data protection safeguards as part of the Protocol[165]. Similarly, bilateral negotiations have started on an agreement between the EU and the United States on cross-border

---

[161] Microsoft submission (*supra* fn. 156), p. 6.

[162] European Commission, Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, 17.4.2018 (COM(2018) 225 final). The Council adopted its general approach on the proposed Regulation on 7.12.2018 (available at: https://www.consilium.europa.eu/en/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-eevidence-council-agrees-its-position/#). See also EDPS, Opinion 7/19 on proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters (available at: https://edps.europa.eu/data-protection/ourwork/publications/opinions/electronic-evidence-criminal-matters_en).

[163] The Explanatory Memorandum, p. 21, makes clear that, in addition to ensuring comity with respect to the sovereign interests of third countries, protecting the individual concerned and avoiding conflicts of law for service providers, one important motivation for the comity clause is reciprocity, i.e. to ensure respect for EU rules, including on the protection of personal data (Article 48 GDPR). See also Statement of the Article 29 Working Party of 29 November 2017, Data protection and privacy aspects of cross-border access to electronic evidence (WP29 Statement) (available at: file:///C:/Users/ralfs/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/20171207_e-Evidence_Statement_FINALpdf%20(1).pdf), p. 9.

[164] See WP29 Statement (*supra* fn. 163), p. 6.

[165] See Recommendation for a Council Decision authorising the participation in negotiations on a second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No. 185), 5.2.2019 (COM(2019) 71 final). See also EDPS, Opinion 3/2019 regarding the participation in the negotiations in view of a Second Additional Protocol to the Budapest Cybercrime Convention, 2.4.2019 (available at: https://edps.europa.eu/sites/edp/files/publication/19-04-02_edps_opinion_budapest_convention_en.pdf); EDPB, Contribution to the consultation on a draft second additional protocol to the Council of Europe Convention on Cybercrime (Budapest Convention), 13.11.2019 (available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpbcontributionbudapestconvention_en.pdf).

access to electronic evidence for judicial cooperation in criminal matters[166]. The Commission counts on the support of the European Parliament and the Council, and the guidance of the EDPB, throughout these negotiations.

More generally, it is important to ensure that when companies active in the European market are called on the basis of a legitimate request to share data for law enforcement purposes, they can do so without facing conflicts of law and in full respect of EU fundamental rights. To improve such transfers, the Commission is committed to develop appropriate legal frameworks with its international partners to avoid conflicts of law and support effective forms of cooperation, notably by providing for the necessary data protection safeguards, and thereby contribute to a more effective fight against crime.

7.3 International cooperation in the area of data protection

Fostering convergence between different privacy systems also means learning from each other, through the exchange of knowledge, experience and best practices. Such exchanges are essential to address new challenges that are increasingly global in nature and scope. This is why the Commission has intensified its dialogue on data protection and data flows with a broad range of actors and in different fora, at bilateral, regional and multilateral level.

The bilateral dimension

Following the adoption of the GDPR, there has been an increasing interest in the EU's experience in the design, negotiation and implementation of modern privacy rules. Dialogue with countries going through similar processes has taken several forms.

The Commission services have made submissions to a number of public consultations organised by foreign governments considering legislation in the area of privacy, for example by the US[167], India[168], Malaysia and Ethiopia. In some third countries, the Commission's services had the privilege to testify before the competent parliamentary bodies, for example in Brazil[169], Chile[170], Ecuador, and Tunisia[171].

---

[166] See Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the EU and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, 5.2.2019 (COM(2019) 70 final). See also EDPS, Opinion 2/2019 on the negotiating mandate of an EU-US agreement on cross-border access to electronic evidence (available at: https://edps.europa.eu/sites/edp/files/publication/19-04-02_edps_opinion_on_eu_us_agreement_on_e-evidence_en.pdf).

[167] See DG Justice and Consumers submission of 9 November 2018 in response to a request for public comments on a proposed approach to consumer privacy [Docket No. 180821780-8780-01] by the US National Telecommunications and Information Administration (available at: https://ec.europa.eu/info/sites/info/files/european_commission_submission_on_a_proposed_approach_to_consumer_privacy.pdf)

[168] See DG Justice and Consumers submission of 19 November 2018 on the draft Personal Data Protection Bill of India 2018 to the Ministry of Electronics and Information Technology (available at:https://eeas.europa.eu/delegations/india/53963/submission-draft-personal-data-protection-bill-india-2018-directorate-general-justice_en).

[169] See plenary meeting of 17 April 2018 of the Brazilian Senate (https://www25.senado.leg.br/web/atividade/sessao-plenaria/-/pauta/23384), meeting of the 10 April 2019 of the Joint Committee on MP 869/2018 of the Brazilian Congress(https://www12.senado.leg.br/ecidadania/visualizacaoaudiencia?id=15392), and meeting

Moreover, within the context of ongoing reforms of data protection laws, dedicated meetings took place with government representatives or parliamentary delegations from many regions of the world (e.g. Georgia, Kenya, Taiwan, Thailand, Morocco). This included the organisation of seminars and study visits, for example with representatives of the Indonesian government and a delegation of staffers from the US Congress. This provided opportunities to clarify important concepts of the GDPR, improve mutual understanding of privacy matters and illustrate the benefits of convergence for ensuring a high level of protection of individual rights, trade and cooperation. In some cases, it also allowed cautioning against certain misconceptions of data protection that can lead to the introduction of protectionist measures such as forced localisation requirements.

Since the adoption of the GDPR, the Commission has also engaged with several international organisations, including in light of the importance of data exchanges with those organisations in a number of policy areas. In particular, a specific dialogue has been established with the United Nations, with a view to facilitate discussions with all involved stakeholders to ensure smooth data transfers and develop further convergence between the respective data protection regimes. As part of this dialogue, the Commission will work closely with the EDPB to further clarify how EU public and private operators can comply with their GDPR obligations when exchanging data with international organisation such as the UN.

The Commission stands ready to continue sharing the lessons learned from its reform process with interested countries and international organisations, in the same way it learned from other systems when developing its proposal for new EU data protection rules. This type of dialogue is mutually beneficial for the EU and its partners as it allows to obtain a better understanding of the fast evolving privacy landscape and to exchange views on emerging legal and technological solutions.

It is in this spirit that the Commission is setting up a "Data Protection Academy" to foster exchanges between European and third country regulators and, in this way, improve cooperation 'on the ground'.

In addition there is a need to develop appropriate legal instruments for closer forms of cooperation and mutual assistance, including by allowing the necessary exchange of information in the context of investigations. The Commission will therefore make use of the powers granted in this area by Article 50 of the GDPR and, in particular, seek authorisation to open negotiations for the conclusion of enforcement cooperation

---

of 26 November 2019 of the Special Committee of the Brazilian Chamber of Deputies (https://www.camara.leg.br/noticias/616579-comissao-discutira-protecao-de-dados-no-ambito-das-constituicoes-de-outros-paises/).

[170] See meetings of 29 May 2018 (https://senado.cl/appsenado/index.php?mo=comisiones&ac=asistencia_sesion&idcomision=186&idsesion=12513&idpunto=15909&sesion=29/05/2018&listado=1), 24 April 2019 (https://www.senado.cl/appsenado/index.php?mo=comisiones&ac=sesiones_celebradas&idcomision=186&tipo=3&legi=485&ano=2019&desde=0&hasta=0&idsesion=13603&idpunto=17283&listado=2) and of the Constitutional, Legislative and Justice Affairs Committee of the Chilean Senate.

[171] See meeting of 2 November 2018 of the Rights, Freedoms and External Relations Committee of the Tunisian Assembly of the Representatives of the People (https://www.facebook.com/1515094915436499/posts/2264094487203201/).

agreements with relevant third countries. In this context, it will also take into account the Board's views as to which countries should be prioritised in light of the volume of data transfers, the role and powers of the privacy enforcer in the third country and the need for enforcement cooperation to address cases of common interest.

The multilateral dimension

Beyond bilateral exchanges, the Commission is also actively participating in a number of multilateral fora to promote shared values and build convergence at regional and global level.

The increasingly universal membership of the Council of Europe's 'Convention 108', the only legally binding multilateral instrument in the area of personal data protection, is a clear sign of this trend towards (upward) convergence[172]. The Convention, which is also open to non-members of the Council of Europe, has already been ratified by 55 countries, including a number of African and Latin American States[173]. The Commission significantly contributed to the successful outcome of the negotiations on the modernisation of the Convention[174], and ensured that it reflected the same principles as those enshrined in the EU data protection rules. Most EU Member States have now signed the Amending Protocol, although the signatures of Denmark, Malta and Romania are still outstanding. Only four Member States (Bulgaria, Croatia, Lithuania and Poland) have so far ratified the Amending Protocol. The Commission urges the three remaining Member States to sign the modernised Convention, and all Member States to swiftly proceed to ratification, to allow for its entry into force in the near future[175]. Beyond that, it will continue to proactively encourage accession by third countries.

Data flows and protection have recently also been addressed within the G20 and G7. In 2019, global leaders for the first time endorsed the idea that data protection contributes to trust in the digital economy and facilitates data flows. With the

---

[172] Importantly, the modernised Convention is not just a treaty setting out strong data protection safeguards, but also creates a network of supervisory authorities with tools for enforcement cooperation and, with the Convention Committee, a forum for discussions, exchange of best practices and development of international standards.

[173] See full list of members: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures. Countries from Africa include Cabo Verde, Mauritius, Morocco, Senegal and Tunisia, from Latin America Argentina, Mexico and Uruguay. Burkina Faso has been invited to join the Convention.

[174] See the text of the modernised Convention: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf.

[175] According to its Decision on the Amending Protocol of 18 May 2018, the Committee of Ministers "urged member States and other Parties to the Convention to take without delay the necessary measures to allow the entry into force of the Protocol within three years from its opening for signature and to initiate immediately, but in any case no later than one year after the date on which the Protocol has been opened for signature, the process under their national law leading to ratification..." It also "instructed its Deputies to examine bi-annually, and for the first time one year after the date of opening for signature of the Protocol, the overall progress made towards ratification on the basis of the information to be provided to the Secretary General by each of the member States and other Parties to the Convention at the latest one month ahead of such an examination." See https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016808a3c9f.

Commission's active support[176], leaders endorsed the concept of "data free flow with trust" (DFFT) originally proposed by Japan in the G20 Osaka Declaration[177] as well as the G7 summit in Biarritz[178]. This approach is also reflected in the Commission's 2020 Communication on "A European strategy for data"[179] which highlights its intention to continue promoting data sharing with trusted partners while fighting against abuses such as disproportionate access of (foreign) public authorities to data.

In doing so, the EU will also be able to rely on a number of tools in different policy areas that increasingly take into account the impact on privacy: for example the first-ever EU framework for the screening of foreign investment, which will become fully applicable in October 2020, gives the EU and its Member States the possibility to screen investment transactions that have effects on "access to sensitive information, including personal data, or the ability to control such information" if they affect security or public order[180].

The Commission is working with like-minded countries in several other multilateral fora to actively promote its values and standards. One important forum is the OECD's recently created Working Party on Data Governance and Privacy (DGP), which is pursuing a number of important initiatives related to data protection, data sharing, and data transfers. This includes the evaluation of the 2013 OECD Privacy Guidelines. Moreover, the Commission actively contributed to the OECD Council Recommendation on Artificial Intelligence[181] and ensured that the EU human-centric approach, meaning that AI applications must comply with fundamental rights and in particular data protection, was reflected in the final text. Importantly, the AI Recommendation – which has subsequently been incorporated into the G20 AI Principles annexed to the G20 Osaka Leaders' Declaration[182] – stipulates the principles of transparency and explainability with a view "to enable those adversely affected by an AI system to challenge its outcome based on plain and easy-to-understand information on the factors and the logic that served as the basis for the prediction, recommendation or decision", thereby closely mirroring the principles of the GDPR as regards automated-decision making[183].

---

[176] In the margin of the April 2019 EU-Japan Summit, President Juncker expressed support for Japan's 'data free flow with trust' initiative and the launching of the 'Osaka Track' and committed the Commission to "play an active role in both initiatives".

[177] See text of the G20 Osaka Leaders' Declaration: https://www.consilium.europa.eu/media/40124/final_g20_osaka_leaders_declaration.pdf

[178] See text of the G7 Biarritz Strategy for an open, free and secure digital transformation: https://www.elysee.fr/admin/upload/default/0001/05/62a9221e66987d4e0d6ffcb058f3d2c649fc6d9d.pdf

[179] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European strategy for data, 19.2.2020 (COM(2020) 66 final) (https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf), pp. 23-24.

[180] Art. 4(1)(d) Regulation (EU) 2019/452 of the European Parliament and of the Council of 19.03.2019 establishing a framework for the screening of foreign direct investment into the Union (OJ L 79I, 21.03.2019).

[181] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

[182] G20 Ministerial Statement on Trade and Digital Economy: https://g20trade-digital.go.jp/dl/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf

[183] See Articles 13(2)(f), 14(2)(g), 22 GDPR.

The Commission is also stepping up its dialogue with regional organisations and networks that are increasingly playing a central role in shaping common data protection standards[184], promoting the exchange of best practices, and fostering cooperation between enforcers. This concerns, in particular, the Association of Southeast Asian Nations (ASEAN) – including in the context of its ongoing work on data transfer tools –, the African Union, the Asia Pacific Privacy Authorities (APPA) forum and the Ibero-American Data Protection Network, all of which launched important initiatives in this area and provide fora for fruitful dialogue between privacy regulators and other stakeholders.

Africa is a telling example of the complementarity between the national, regional and global dimensions of privacy. Digital technologies are quickly and deeply transforming the African continent. This has the potential to accelerate the achievement of the Sustainable Development Goals by boosting economic growth, alleviating poverty and improving people's lives. Having in place a modern data protection framework attracting investment and fostering the development of competitive business while contributing to the respect for human rights, democracy and the rule of law is a key element of this transformation. The harmonisation of data protection rules across Africa would enable digital market integration, while convergence with global standards would facilitate data exchanges with the EU. These different dimensions of data protection are interlinked and mutually reinforcing.

There is now a growing interest in data protection in many African countries, and the number of African countries that have adopted or are in the process of adopting modern data protection rules, have ratified Convention 108[185] or the Malabo Convention[186] continues to increase[187]. At the same time, the regulatory framework remains highly uneven and fragmented across the African continent. Many countries still offer few or no data protection safeguards. Measures restricting data flows are still widespread and hamper the development of a regional digital economy.

To harness the mutual benefits of convergent data protection rules, the Commission will engage with its African partners both bilaterally and in regional fora[188]. This

[184] See, for instance, the African Union *Convention on Cyber Security and Personal Data Protection* ('Malabo Convention') and the *Standards for Data Protection for the Ibero-American States* developed by the Ibero-American Data Protection Network.

[185] Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=DW5jevqD

[186] African Union Convention on Cyber Security and Personal Data Protection https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection. In addition, several of the Regional Economic Communities (RECs) have developed data protection rules, for instance, the Economic Community of West African States (ECOWAS) and the Southern African Development Community (SADC). See, respectively, http://www.tit.comm.ecowas.int/wp-content/uploads/2015/11/SIGNED-Data-Protection-Act.pdf and http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/docs/SA4docs/data%20protection.pdf.

[188] Inter alia, through the Policy and Regulation Initiative for Digital Africa (PRIDA), see information at: https://www.africa-eu-partnership.org/en/projects/policy-and-regulation-initiative-digital-africa-prida.

builds on the work of the EU-AU Digital Economy Task Force within the context of the New Africa-Europe Digital Economy Partnership[189]. It is also in furtherance of such objectives that the scope of the Commission's partnership instrument 'Enhanced Data Protection and Data Flows' has been extended to include Africa. The project will be mobilised to support African countries that intend to develop modern data protection frameworks or that wish to strengthen the capacity of their regulatory authorities, through training, knowledge sharing and exchange of best practices.

Finally, while promoting convergence of data protection standards at international level, as a way to facilitate data flows and thus trade, the Commission is also determined to tackle digital protectionism, as recently highlighted in the Data Strategy.[190] To that end, it has developed specific provisions on data flows and data protection in trade agreements which it systematically tables in its bilateral – most recently with Australia, New Zealand, and the UK – and multilateral negotiations such as the current WTO e-commerce talks. These horizontal provisions rule out unjustified restrictions, such as forced data localisation requirements, while preserving the regulatory autonomy of the parties to protect the fundamental right to data protection.

Whereas dialogues on data protection and trade negotiations must follow separate tracks, they can complement each other. In fact, convergence, based on high standards and backed-up by effective enforcement, provides the strongest foundation for the exchange of personal data, something that is increasingly recognised by our international partners. Given that companies more and more operate across borders and prefer to apply similar sets of rules in all their business operations worldwide, such convergence helps creating an environment conducive to direct investment, facilitating trade and improving trust between commercial partners. Synergies between trade and data protection instruments should thus be further explored to ensure free and safe international data flows that are essential for the business operations, competitiveness and growth of European companies, including SMEs, in our increasingly digitalised economy.

[189] See Joint Communication of the European Commission and the High Representative for Foreign Affairs and Security Policy 'Towards a comprehensive strategy for Africa' (available at: https://ec.europa.eu/international-partnerships/system/files/communication-eu-africa-strategy-join-2020-4-final_en.pdf); Digital Economy Task Force, New Africa-Europe Digital Economy Partnership: Accelerating the Achievement of the Sustainable Development Goals (available at: https://www.africa-eu-partnership.org/sites/default/files/documents/finaldetfreportpdf.pdf).

[190] https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf, p. 23.

ANNEX I – Clauses for facultative specifications by national legislation

Subject	Scope	GDPR articles
Specifications for legal obligations and public task	Adapting the application of provisions with regard to the processing for compliance with a legal obligation or a public task, including for specific processing situations under Chapter IX	Article 6(2) and 6(3)
Age limit for consent in relation to information society services	Determination of the minimum age between 13 and 16 years	Article 8(1)
Processing of special categories of data	Maintaining or introducing further conditions, including limitations, for the processing of genetic data, biometric data or data concerning health.	Article 9(4)
Derogation from information requirements	Obtaining or disclosure expressly laid down by law or for professional secrecy regulated by law	Article 14(5)(c) and (d)
Automated individual decision-making	Authorisation for automated decision-making in derogation from the general prohibition	Article 22(2)(b)
Restrictions of data subject rights	Restrictions from Articles 12 to 22, Article 34 and corresponding provisions in Article 5, when necessary and proportionate to safeguard exhaustively listed important objectives	Article 23(1)
Consultation and authorisation requirement	Requirement for controllers to consult or obtain authorisation from the data protection authority for processing for a task in the public interest	Article 36(5)
Designation of a data protection officer in additional cases	Designation of a data protection officer in cases other than the ones in paragraph 1 of Article 37	Article 37(4)
Limitations of transfers	Limitation of transfers of specific categories of personal data	Article 49(5)
Complaints and court actions of organisations in their own right	Authorisation of privacy organisations to lodge complaints and court actions independently from a mandate by data subjects	Article 80(2)
Access to official documents	Reconciliation of public access to official documents with the right to the protection of personal data	Article 86

Processing of the national identification number	Specific conditions for the processing of the national identification number	Article 87
Processing in the employment context	More specific rules for processing employees' personal data	Article 88
Derogations for processing for archiving in the public interest, research or statistical purposes	Derogations from specified data subject rights in so far as such rights are likely to render impossible or seriously impair the achievement of specific purposes	Article 89(2) and (3)
Reconciliation of data protection with obligations of secrecy	Specific rules on investigative powers of data protection authorities in relation to controllers or processors subject to obligations of professional secrecy	Article 90

ANNEX II – Overview of the resources of data protection authorities

The table below presents an overview of the resources (staff and budget) of data protection authorities per EU/EEA Member State[191].

When comparing the figures between Member States, it is important to bear in mind that authorities may have tasks assigned to them beyond those under the GDPR, and that these may vary between Member States. The ratio of staff employed by the authorities to one million inhabitants and the ratio of the budget of the authorities to one million euro of GDP are only included to provide additional elements of comparison among Member States of similar size and should not be looked at in isolation. The absolute figures, ratios and evolution over the past years should be considered together when assessing the resources of a given authority.

	STAFF (Full Time Equivalents)					BUDGET (EUR)				
EU/EEA Member States	2019	Forecast 2020	% growth 2016-2019	% growth 2016-2020 (forecast)	Staff per million inhabitants (2019)	2019	Forecast 2020	% growth 2016-2019	% growth 2016-2020 (forecast)	Budget per million EUR of GDP (2019)
Austria	34	34	48%	48%	3,8	2.282.000	2.282.000	29%	29%	5,7
Belgium	59	65	9%	20%	5,2	8.197.400	8.962.200	1%	10%	17,3
Bulgaria	60	60	-14%	-14%	8,6	1.446.956	1.446.956	24%	24%	23,8
Croatia	39	60	39%	114%	9,6	1.157.300	1.405.000	57%	91%	21,5
Cyprus	24	22	NA	NA	27,4	503.855	NA	114%	NA	23,0
Czech Rep.	101	109	0%	8%	9,5	6.541.288	6.720.533	10%	13%	29,7
Denmark	66	63	106%	97%	11,4	5.610.128	5.623.114	101%	101%	18,0
Estonia	16	18	-11%	0%	12,1	750.331	750.331	7%	7%	26,8
Finland	45	55	114%	162%	8,2	3.500.000	4.500.000	94%	150%	14,6
France	215	225	9%	14%	3,2	18.506.734	20.143.889	-2%	7%	7,7
Germany	888	1002	52%	72%	10,7	76.599.800	85.837.500	48%	66%	22,3
Greece	33	46	-15%	18%	3,1	2.849.000	3.101.000	38%	50%	15,2
Hungary	104	117	42%	60%	10,6	3.505.152	4.437.576	102%	155%	24,4
Iceland	17	17	143%	143%	47,6	2.272.490	2.294.104	167%	170%	105,2
Ireland	140	176	169%	238%	28,5	15.200.000	16.900.000	223%	260%	43,8
Italy	170	170	40%	40%	2,8	29.127.273	30.127.273	46%	51%	16,3
Latvia	19	31	-10%	48%	9,9	640.998	1.218.978	4%	98%	21,0
Lithuania	46	52	-8%	4%	16,5	1.482.000	1.581.000	40%	49%	30,6
Luxembourg	43	48	126%	153%	70,0	5.442.416	6.691.563	165%	226%	85,7
Malta	13	15	30%	50%	26,3	480.000	550.000	41%	62%	36,3
Netherlands	179	188	145%	158%	10,4	18.600.000	18.600.000	130%	130%	22,9
Norway	49	58	2%	21%	9,2	5.708.950	6.580.660	27%	46%	15,9
Poland	238	260	54%	68%	6,3	7.506.345	9.413.381	66%	108%	14,2
Portugal	25	27	-4%	4%	2,4	2.152.000	2.385.000	67%	86%	10,1
Romania	39	47	-3%	18%	2,0	1.103.388	1.304.813	3%	22%	4,9
Slovakia	49	51	20%	24%	9,0	1.731.419	1.859.514	47%	58%	18,4
Slovenia	47	49	42%	48%	22,6	2.242.236	2.266.485	68%	70%	46,7
Spain	170	220	13%	47%	3,6	15.187.680	16.500.000	8%	17%	12,2
Sweden	87	87	81%	81%	8,5	8.800.000	10.300.000	96%	129%	18,5
TOTAL	**2.966**	**3.372**	**42%**	**62%**	**6,6**	**249.127.139**	**273.782.870**	**49%**	**64%**	**17,4**

Source of raw figures: contribution from the Board. Calculations from the Commission.

[191] Except for Liechtenstein.