Council of the
European Union

Brussels, 26 July 2024
(OR. en)

12583/24

DATAPROTECT 269
JAI 1248
DIGIT 184
MI 730
FREMP 334

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	25 July 2024
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2024) 357 final
Subject:	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Second Report on the application of the General Data Protection Regulation

Delegations will find attached document COM(2024) 357 final.

Encl.: COM(2024) 357 final

EUROPEAN
COMMISSION

Brussels, 25.7.2024
COM(2024) 357 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

Second Report on the application of the General Data Protection Regulation

1 INTRODUCTION

This is the Commission's second report on the application of the General Data Protection Regulation (GDPR), adopted in accordance with Article 97 of the GDPR. The first report was adopted on 24 June 2020 (the '2020 report') [(1)].

The GDPR is one of the cornerstones of the EU's approach to the digital transformation. Its basic principles - fair, safe and transparent processing of personal data, ensuring that individuals remain in control - underpin all EU policies involving the processing of personal data.

Since the 2020 report, the EU has adopted a range of initiatives which aim to put individuals at the centre of the digital transition. Each initiative pursues a particular aim, such as creating a safer environment online, making the digital economy fairer and more competitive, facilitating groundbreaking research, ensuring the development of safe and trustworthy artificial intelligence (AI) and creating a genuine single market for data. Whenever personal data are concerned, these initiatives build on the GDPR. The GDPR also provides a basis for sectoral initiatives that impact the processing of personal data, e.g. in the areas of financial services, health, employment, mobility and law enforcement.

There is broad consensus among stakeholders, data protection authorities and Member States that, despite some challenges, the GDPR has delivered important results for individuals and businesses. The risk-based, technology-neutral approach provides strong protection for data subjects and proportionate obligations for data controllers and processors. At the same time, further progress should be made in a number of areas. In particular, in the coming years, the focus should be on supporting stakeholders' compliance efforts - especially small and medium sized enterprises (SMEs), small operators and researchers and research organisations, providing clearer and more actionable guidance from the data protection authorities, and achieving a more consistent interpretation and enforcement of the GDPR across the EU.

According to Article 97 of the GDPR the Commission should examine in particular the application and functioning of the international transfer of personal data to third countries (i.e. countries outside the EU/EEA) (Chapter V, GDPR) and the cooperation and consistency mechanisms between national data protection authorities (Chapter VII, GDPR). However, as with the 2020 report, this report provides a general assessment of the application of the GDPR going beyond these two elements: it also identifies a number of actions necessary to support the effective application of the GDPR in key priority areas.

This report takes into account the following sources: (i) the position and findings of the Council, adopted in December 2023 [(2)]; (ii) input gathered from stakeholders, in particular through the GDPR Multi-stakeholder group [(3)] and a public call for evidence [(4)]; and (iii) input from data protection authorities (through the contribution of

---

(1) 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, 24.6.2020 COM(2020) 264 final.

(2) https://data.consilium.europa.eu/doc/document/ST-15507-2023-INIT/en/pdf

(3) A summary of the input of the GDPR Multi-stakeholder expert group is available here: Report from Multistakeholder Expert group on GDPR application - June 2024.pdf. The input received in response to the public call for evidence and through bilateral meetings with stakeholders largely echoes the views expressed by members of the GDPR Multi-stakeholder expert group.

(4) https://ec.europa.eu/info/law/better-regulation/

the European Data Protection Board ([5]) (the Board) and a report prepared by the Fundamental Rights Agency (FRA) based on interviews conducted with individual data protection authorities ([6]) (the 'FRA report'). The report also builds on the Commission's ongoing monitoring of the application of the GDPR, including bilateral dialogues with Member States on the compliance of national legislation, active contribution to the work of the Board, and close contacts with a wide range of stakeholders on the practical application of the Regulation.

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

The GDPR's one-stop shop enforcement system aims to ensure a harmonised interpretation and enforcement by independent data protection authorities. It requires cooperation between data protection authorities in cases of cross-border processing, where data subjects in multiple Member States are substantially affected. Disputes between authorities are resolved by the Board under the GDPR's consistency mechanism.

2.1 Making handling of cross-border cases more efficient: the procedural rules proposal

The 2020 report noted the need for a more efficient and harmonised handling of cross-border cases across the EU, in particular in light of major differences in national administrative procedures and interpretations of concepts in the GDPR cooperation mechanism. Therefore, in July 2023, the Commission adopted a proposal for a Regulation on procedural rules ([7]), also drawing on a list of issues submitted by the Board to the Commission in October 2022 ([8]), and input from stakeholders ([9]) and Member States ([10]). The proposal complements the GDPR by laying down detailed rules on cross-border complaints, the involvement of the complainant, the due process rights of parties under investigation (controllers and processors), and cooperation between data protection authorities. The harmonisation of these procedural aspects would support the timely completion of investigations and the delivery of a swift remedy for individuals. The proposal is currently being negotiated by the European Parliament and the Council.

2.2 Increased cooperation between data protection authorities and use of the consistency mechanism

The number of cross-border cases has increased significantly in recent years. Data protection authorities have demonstrated increased willingness to make use of the tools for cooperation provided by the GDPR. All data protection authorities made use of the mutual assistance tool ([11]) as well as 'informal' requests to assist each other on a voluntary basis. Data protection authorities favour informal requests, which do not

([5]) Contribution of the EDPB to the evaluation of the GDPR under Article 97 | European Data Protection Board (europa.eu).

([6]) GDPR in practice – Experiences of data protection authorities | European Union Agency for Fundamental Rights (europa.eu)

([7]) Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679 (COM/2023/348 final).

([8]) https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-letter-eu-commission-procedural-aspects-could-be_en.

([9]) Through the GDPR Multi-stakeholder expert group and a call for evidence launched in February 2023.

([10]) Notably through the GDPR Member States expert group: https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&do=groupDetail.groupDetail&groupID=3461

([11]) Article 61 GDPR.

impose a deadline or a strict duty to answer. Although the Board adopted guidelines on joint operations in 2021 ([12]), authorities have still not made significant use of this tool ([13]) and cite differences in national procedures and lack of clarity on the procedure as the main reasons for its limited use.

The GDPR provides the data protection authorities concerned with the possibility to raise a relevant and reasoned objection where they disagree with a draft decision of the lead data protection authority in a cross-border case. Where data protection authorities cannot reach a consensus on a relevant and reasoned objection, the GDPR provides for dispute resolution by the Board ([14]). The most frequently raised topics in relevant and reasoned objections were: (i) the legal basis for processing; (ii) information and transparency obligations; (iii) the notification of data breaches; (iv) data subjects' rights; (v) derogations for international transfers; (vi) the use of corrective measures; and (vii) the amount of an administrative fine.

The GDPR's enforcement system is based on the premise of sincere and effective cooperation between data protection authorities. While the dispute resolution procedure plays an important role in this enforcement architecture, it should be used in the spirit in which it was designed, namely with due regard for the division of competence between data protection authorities, the need to respect due process rights, and the interest in achieving a timely resolution of the case for data subjects. Each dispute resolution procedure requires significant resources from the lead authority, the authorities concerned and the Board's secretariat, and delays the delivery of a remedy for data subjects.

Increased use of cooperation tools by data protection authorities

- Almost 2 400 case entries have been registered in the Board's information exchange system ([15]).
- Lead data protection authorities have issued around 1 500 draft decisions ([16]), of which 990 resulted in final decisions finding an infringement of the GDPR ([17]).
- Data protection authorities triggered almost 1 000 'formal' mutual assistance requests ([18]) and around 12 300 'informal' requests ([19]).
- Five joint operations have been initiated in which data protection authorities from seven Member States have participated.
- Data protection authorities from 18 Member States raised relevant and reasoned objections ([20]).

([12]) internal_edpb_document_1_2021_on_art_62_joint_operations_en.pdf (europa.eu)
([13]) Article 62 GDPR.
([14]) Article 65 GDPR.
([15]) As of 3 November 2023 (contribution of the Board).
([16]) Under Article 60(3) GDPR.
([17]) As of 3 November 2023.
([18]) The Irish authority made the most formal requests (246) while the German authorities received the most requests (516).
([19]) The Irish authority made the most informal requests (4 245) followed by German authorities (2 036).
([20]) Of 289 relevant and reasoned objections reported by authorities, 101 (35%) were raised by German authorities. The rate of success in reaching consensus on relevant and reasoned objections ranges from 15% (of objections raised by German authorities) to 100% (of objections raised by the Polish authority).

The GDPR's consistency mechanism is increasingly used by data protection authorities. It has three components: (i) opinions of the Board; (ii) dispute resolution by the Board; and (iii) the urgency procedure ([21]).

The Board increasingly addresses important issues of general application in its opinions ([22]). The Board should ensure timely and meaningful consultation before the adoption of those opinions. Cases submitted to dispute resolution have addressed questions such as the legal basis for processing data for behavioural advertising on social media and the processing of children's data online. Most of the subsequent binding decisions have been challenged before the General Court.

Transparency in the decision-making process of the Board is key to ensure respect for the right to good administration under the Charter of Fundamental Rights of the EU. The GDPR urgency procedure allows data protection authorities to derogate from the cooperation and consistency mechanism to take urgent measures where necessary to protect the rights and freedoms of data subjects. As a derogation from the normal cooperation procedure under the GDPR, tools such as the urgency procedure are designed to be used only in exceptional circumstances and where the normal cooperation procedure cannot protect the rights and freedoms of data subjects.

The consistency mechanism

- The Board has adopted 190 consistency opinions.
- Nine binding decisions have been adopted in dispute resolution ([23]). All of them instructed the lead data protection authority to amend its draft decision and several have resulted in significant fines.
- Five data protection authorities have adopted provisional measures under the urgency procedure (Germany, Finland, Italy, Norway and Spain).
- Two data protection authorities requested an urgent binding decision of the Board ([24]) and the Board ordered urgent final measures in one case.

2.3 Stronger enforcement

There has been a significant uptick in enforcement activity by data protection authorities in recent years, including the imposition of substantial fines in landmark cases against 'big tech' multinational companies. Fines were, for instance, imposed for: (i) the infringement of the lawfulness and security of processing; (ii) the infringement of processing of special categories of personal data; and (iii) the failure to comply with individuals' rights ([25]). This has led private companies to 'take data protection seriously' ([26]) and helped to embed a culture of compliance in organisations. Data protection authorities adopt decisions finding infringements of the GDPR in complaint-based and own initiative cases. Though not available in all Member States, many data protection authorities have made effective use of 'amicable settlement' procedures to

([21]) Respectively Articles 64, 65 and 66 GDPR.
([22]) Opinions under Article 64(2) GDPR.
([23]) Under Article 65(1)(a) GDPR.
([24]) Pursuant to Article 66(2) GDPR.
([25]) See 5.3.4 contribution of the Board.
([26]) FRA report, page 36.

quickly resolve complaint-based cases to the satisfaction of the complainant. The procedural rules proposal recognises the possibility for complaints to be resolved through amicable settlement ([27]).

Data protection authorities have made ample use of their corrective powers, though the number of corrective measures imposed varies widely among authorities. Other than fines, the most commonly used corrective measures were warnings, reprimands and orders to comply with the GDPR. Controllers and processors frequently challenge decisions finding infringements of the GDPR in national courts, most commonly on procedural grounds ([28]).

Stronger enforcement

- Data protection authorities have launched over 20 000 own-initiative investigations ([29]).
- They collectively receive over 100 000 complaints per year ([30]).
- The median time for data protection authorities to handle complaints (from receipt to closure of the case) ranges from 1 to 12 months, and is 3 months or less in five Member States (Denmark (1 month), Spain (1.5 months), Estonia (3 months), Greece (3 months) and Ireland (3 months)).
- Over 20 000 complaints have been resolved through amicable settlement. It is most commonly used in Austria, Hungary, Luxembourg and Ireland.
- In 2022, data protection authorities in Germany adopted the highest number of decisions imposing a corrective measure (3 261), followed by Spain (774), Lithuania (308) and Estonia (332). The lowest number of corrective measures was imposed in Liechtenstein (8), Czechia (8), Iceland (10), the Netherlands (17) and Luxembourg (22).
- Data protection authorities have imposed over 6 680 fines amounting to around EUR 4.2 billion ([31]). The authority in Ireland has imposed the highest total amount of fines (EUR 2.8 billion) followed by Luxembourg (EUR 746 million), Italy (EUR 197 million) and France (EUR 131 million). Liechtenstein (EUR 9 600), Estonia (EUR 201 000) and Lithuania (EUR 435 000) have imposed the lowest amount of fines.

While most data protection authorities consider their investigatory tools to be adequate, some require additional tools at national level, such as adequate sanctions where

([27]) Procedural rules proposal, Article 5.

([28]) In Romania all 26 decisions finding an infringement were challenged in court, while in the Netherlands the rate of challenge was 23%. The rate of success for challenges was highest in Belgium (39%).

([29]) Data protection authorities in Germany launched the highest number of own-initiative investigations (7 647), followed by Hungary (3 332), Austria (1 681), and France (1 571).

([30]) In 2022, nine data protection authorities received over 2000 complaints. The highest number of complaints were registered by Germany (32 300), Italy (30 880), Spain (15 128), the Netherlands (13 133), and France (12 193), while the lowest number were registered by Liechtenstein (40), Iceland (140), and Croatia (271).

([31]) All authorities imposed administrative fines, except Denmark, which does not provide for administrative fines. The highest number of fines were imposed in Germany (2 106) and Spain (1 596). The fewest fines were imposed in Liechtenstein (3), Iceland (15) and Finland (20).

controllers fail to cooperate or provide necessary information ([32]). Data protection authorities consider insufficient resources and gaps in technical and legal expertise to be the main factor affecting their enforcement capacity ([33]).

2.4 The Board

The Board is composed of the head of one data protection authority of each Member State and the European Data Protection Supervisor, with the Commission participating without voting rights. The Board, supported in its work by its secretariat, is tasked with ensuring the consistent application of the GDPR ([34]). Most data protection authorities consider that the Board has played a positive role in strengthening cooperation between them ([35]). Many data protection authorities dedicate significant resources to the Board's activities, though smaller authorities indicate that their size prevents them from fully engaging ([36]). Some authorities consider that the efficiency of the Board's processes should be improved, in particular by reducing the number of meetings and by paying less attention to minor issues ([37]). Depending on the outcome of the negotiations on the proposal on GDPR procedural rules, which aims to reduce the number of cases submitted to the Board for dispute resolution, there may be a need to reflect on whether the Board requires additional resources.

As of November 2023, the Board had adopted 35 guidelines. While stakeholders and data protection authorities have found them useful, both consider that guidelines should be delivered more quickly and that the quality should be improved ([38]). Stakeholders note that they are often overly theoretical, too long and do not reflect the GDPR's risk-based approach ([39]). Data protection authorities and the Board should provide concise and practical guidelines that give answers to concrete problems and reflect a balance between data protection and other fundamental rights. Guidelines should also be easy to understand for individuals without legal training, for example in SMEs and voluntary organisations ([40]). A way to achieve this is to make the preparation of the guidelines more transparent, and to consult at an early stage to enable a better understanding of market dynamics, business practices and how to apply the guidelines in practice ([41]). It is welcomed that, as part of its 2024-2027 Strategy, the Board has highlighted its goal to provide practical guidance that is accessible to the relevant audience ([42]).

Stakeholders underline the need for additional guidelines, in particular on anonymisation and pseudonymisation ([43]), legitimate interest and scientific research ([44]). In the 2020 report the Commission called on the Board to adopt guidelines on scientific research, but

([32]) FRA report, page 38.
([33]) FRA report pages 20 and 23. See also Council position and findings, paragraph 17.
([34]) Article 70(1) GDPR.
([35]) FRA report, page 64.
([36]) FRA report, page 67. In 2023, German data protection authorities dedicated the most resources to activities of the Board (26 full-time equivalents (FTEs)), followed by Ireland (16) and France (12) (contribution of the Board).
([37]) FRA report, page 67.
([38]) FRA report, page 67; summary of the feedback of the GDPR Multi-stakeholder expert group.
([39]) Summary of the feedback of the GDPR Multi-stakeholder expert group.
([40]) See also Council position and findings, paragraph 45.
([41]) See also Council position and findings, paragraph 34.
([42]) https://www.edpb.europa.eu/system/files/2024-04/edpb_strategy_2024-2027_en.pdf
([43]) See also Council position and findings, paragraph 31(d).
([44]) They require clarity in particular on the meaning of the term 'scientific research', the role of consent to processing of personal data for research, the relevant legal basis, and the roles and responsibility of the actors involved.

the guidelines have not yet been adopted. Recognising the importance of scientific research in society, in particular to monitor diseases and develop treatments, and to foster innovation, it is essential that data protection authorities act to clarify these questions without further delay ([45]). Public authorities would also benefit from guidance addressing the particular challenges they face ([46]).

2.5 Data protection authorities

2.5.1 Independence and resources

The independence of data protection authorities is enshrined in the EU Charter of Fundamental Rights and the Treaty on the Functioning of the EU. The GDPR lays down requirements to ensure the 'complete independence' of data protection authorities ([47]). The FRA report found that most data protection authorities operate independently from Government, Parliament, or any other public bodies ([48]).

Data protection authorities require adequate human, technical and financial resources to be able to effectively and independently carry out their tasks under the GDPR. In the 2020 report, the Commission noted that resourcing of data protection authorities was still not satisfactory and has consistently raised this issue with Member States. Since then, the situation has improved.

Increased resources for data protection authorities ([49])

- Between 2020 and 2024, all but two data protection authorities benefited from an increase in staff and the increase exceeded 25% in 14 Member States.
- The data protection authority in Ireland had the highest increase in staff (79%) followed by Estonia, Sweden (both 57%) and Bulgaria (56%).
- There was a slight decrease in staff at the authority in Czechia (-1%) while there was no increase in Liechtenstein and minor increases in Cyprus (4%) and Hungary (8%).
- Between 2020 and 2024, all but one data protection authority had an increase in budget, and the increase exceeded 50% in 13 Member States.
- The data protection authority in Cyprus had the largest increase in budget (130%), followed by Austria (107%), Bulgaria (100%) and Estonia (97%).
- The budget of the Greek data protection authority decreased by 15% while there were minor budget increases for the Liechtenstein (1%), Slovakia (6%) and Czech (8%) authorities.

While these statistics show a general upward trend in the resourcing of data protection authorities, the authorities themselves consider that they still lack sufficient human resources ([50]). They stress the need for very specialised technical knowledge, in

([45]) See also Council position and findings, paragraph 31(b).
([46]) Council position and findings, paragraphs 27-28.
([47]) Article 52 GDPR.
([48]) FRA report, page 31.
([49]) See section 4.4.1 contribution of the Board, also for the absolute figures.
([50]) Just five data protection authorities consider they have adequate human resources (contribution of the Board, page 33).

particular on new and emerging technologies ([51]), the lack of which affects the quantity and quality of their work, and the difficulties in competing for human resources with the private sector. Data protection authorities cite insufficient legal knowledge and lack of language skills as factors affecting their performance. Low remuneration, an inability to autonomously select staff, and heavy workload are highlighted as the key factors affecting the authorities' ability to recruit and retain staff ([52]). Data protection authorities also highlight their need for financial resources if they are to modernise and digitalise their processes, and acquire technical equipment ([53]). All data protection authorities fulfil tasks beyond those entrusted to them by the GDPR ([54]), e.g. as supervisory authorities for the Data Protection Law Enforcement Directive and the e-Privacy Directive, while many express concerns about facing additional responsibilities under new digital legislation ([55]).

2.5.2 Difficulties handling a high number of complaints

Several data protection authorities indicate that too much of their resources are used handling a high number of complaints, most of which they consider are trivial and unfounded, since handling each complaint is an obligation under the GDPR which is subject to judicial review ([56]). This means that data protection authorities cannot allocate sufficient resources to other activities, such as own initiative investigations, public awareness campaigns and engagement with controllers ([57]). As public authorities, data protection authorities have the discretion to allocate their resources as they see fit in order to fulfil each of their tasks (listed in Article 57(1) GDPR) in the public interest. Many data protection authorities have adopted strategies to increase the efficiency of complaint-handling, such as automation ([58]), the use of amicable settlement procedures ([59]) and 'grouping' complaints that relate to similar issues ([60]).

2.5.3 Interpretation of the GDPR by national data protection authorities

A central objective of the GDPR was to remove the fragmented approach to data protection that existed under the previous Data Protection Directive (Directive 95/46/EC) ([61]). However, data protection authorities continue to adopt diverging interpretations on key data protection concepts ([62]). Stakeholders identify this as the principal obstacle to the consistent application of the GDPR in the EU. The persistence of diverging interpretations creates legal uncertainty and increases costs for businesses (e.g. by requiring different documentation for several Member States), disrupting the free movement of personal data in the EU, hindering cross-border business and hampering research and innovation on urgent societal challenges.

([51]) FRA report, page 20. Some data protection authorities outsource certain tasks to external contractors, such as complaint handling, legal analysis and forensic analysis.
([52]) FRA report, page 24.
([53]) FRA report, page 22.
([54]) See section 4.4.5 contribution of the Board.
([55]) Contribution of the Board, page 32.
([56]) FRA Report, page 48.
([57]) FRA report, page 45. Data protection authorities consider ex officio investigations particularly important, since complainants may not be aware of many breaches of the GDPR.
([58]) FRA report, page 8.
([59]) FRA report, page 39.
([60]) FRA report, page 41.
([61]) Recital 9 GDPR.
([62]) Summary of the feedback of the GDPR Multi-stakeholder expert group.

Specific issues raised by stakeholders include: (i) the fact that data protection authorities in three Member States each take a different view on the appropriate legal basis for the processing of personal data when conducting a clinical trial; (ii) there are frequently diverging views on whether an entity is a controller or processor; and (iii) in some cases data protection authorities do not follow the Board's guidelines or they publish guidelines at national level that conflict with those of the Board ([63]). These issues are compounded when multiple data protection authorities within a single Member State adopt conflicting interpretations.

Some stakeholders also consider that certain data protection authorities and the Board adopt interpretations that deviate from the risk-based approach of the GDPR, which poses a challenge for the development of the digital economy ([64]) and the freedom and plurality of the media. They mention as areas of concern: (i) the interpretation of anonymisation; (ii) the legal basis of legitimate interest and consent ([65]); and (iii) the exceptions to the prohibition of automated individual decision-making ([66]). It should be recalled that data protection authorities and the Board are tasked with ensuring both the protection of natural persons in relation to processing of their personal data and the free flow of personal data within the EU. As recognised in the GDPR ([67]), the right to protection of personal data must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.

2.5.4 Engagement with controllers and processors

Stakeholders underline the benefit of having the opportunity to engage in constructive dialogue with data protection authorities to ensure that they comply with the GDPR from the start, in particular in relation to emerging technologies. Stakeholders note that some data protection authorities actively engage with controllers, while others are slow to respond, provide vague responses, or do not respond at all ([68]).

3 IMPLEMENTATION OF THE GDPR BY MEMBER STATES

3.1 Fragmentation in national application

While the GDPR, as a regulation, is directly applicable, it requires the Member States to legislate in certain areas and provides them the possibility to further specify its application in a limited number of areas ([69]). When legislating at national level, Member States must do so under the conditions and within the limits laid down by the GDPR. As in 2020, stakeholders report encountering difficulties arising from fragmentation in national rules where Member States have the possibility to specify the GDPR, in particular concerning:

- the minimum age for a child's consent in relation to the offer of information society services to this child ([70]);

([63]) Summary of the feedback of the GDPR Multi-stakeholder expert group.
([64]) Summary of the feedback of the GDPR Multi-stakeholder expert group.
([65]) Respectively Articles 6(1)(f) and 6(1)(a) GDPR.
([66]) Article 22(2) GDPR.
([67]) Recital 4.
([68]) Summary of the feedback of the GDPR Multi-stakeholder expert group.
([69]) e.g. the minimum age for child's consent in relation to information society services (Article 8(1) GDPR).
([70]) Article 8(1)GDPR.

- the introduction by Member States of further conditions concerning the processing of genetic data, biometric data or data concerning health ([71]);
- the processing of personal data relating to criminal convictions and offences ([72]), which creates difficulties in certain regulated sectors.

At the same time, importantly, many stakeholders report that issues of fragmentation arise principally from diverging interpretations of the GDPR by data protection authorities, rather than from the use of facultative specification clauses by Member States.

Member States consider that a limited degree of fragmentation may be acceptable and the specification clauses provided by the GDPR remain beneficial, in particular for processing by public authorities ([73]). The GDPR requires Member States to consult their national data protection authority when preparing legislation that relates to the processing of personal data ([74]). The FRA report found that some governments set very tight deadlines for those authorities, and in some cases do not consult them at all ([75]).

3.2 Monitoring by the Commission

The Commission monitors the implementation of the GDPR on an ongoing basis. The Commission has launched infringement procedures against Member States on issues such as the independence of data protection authorities (including remaining free from external influence and the availability of a judicial remedy in case of dismissal) ([76]) and the right to an effective judicial remedy for data subjects where the data protection authority does not handle a complaint ([77]). As part of its monitoring, the Commission also requests that data protection authorities provide, on a strictly confidential basis, regular information ([78]) on ongoing large-scale cross-border cases, notably those concerning big tech multinational companies.

The Commission regularly communicates with Member States on GDPR implementation. As set out in the 2020 report, the Commission has continued to use the GDPR Member States expert group ([79]) to facilitate discussions and sharing of experience on the effective implementation of the GDPR. The expert group has had specific discussions on: (i) the supervision of courts acting in their judicial capacity (Article 55 GDPR; Article 8 of the Charter); (ii) the reconciliation of the right to data protection with the right to freedom of expression (Article 85 GDPR); and (iii) the right to an effective judicial remedy against a supervisory authority (Article 78 GDPR). Following these discussions, the Commission compiled overviews of the approaches taken to the implementation of those provisions in the Member States ([80]). The

([71]) A possibility provided for by Article 9(4) GDPR.
([72]) Article 10 GDPR.
([73]) Council position and findings, paragraph 30.
([74]) Article 36 GDPR.
([75]) FRA report, page 11.
([76]) Belgium (2021/4045) and Belgium (2022/2160).
([77]) Finland (2022/4010) and Sweden (2022/2022).
([78]) With information on the case reference, the investigation type (own initiative or complaint based), a summary of the investigation scope, the concerned data protection authorities, the key procedural steps taken and dates, the investigatory or any other measures taken and dates.
([79]) https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&do=groupDetail.groupDetail&groupID=3461
([80]) https://ec.europa.eu/transparency/expert-groups-register/screen/meetings/consult?lang=en&meetingId=31754&fromExpertGroups=3461

Commission also used this group to exchange views with Member States when preparing the proposal on procedural rules.

The compliance of national legislation and practice with the data protection rules set out in the body of EU law on the Schengen area is also assessed as part of the Schengen evaluations, jointly conducted by Member States and the Commission. At least five onsite data protection evaluations are conducted per year, currently focusing on large-scale IT systems and the Schengen Information System, the Visa Information System as well as on the supervisory role of the national data protection authorities over those systems.

The Commission is actively contributing to the large number of cases in front of the Court of Justice (with around 30 preliminary rulings per year in recent years), which play a central role in the consistent interpretation of key concepts of the GDPR. A growing body of case law of the Court has provided several clarifications, such as on the definition of personal data ([81]), special categories of personal data ([82]), controller ([83]), consent ([84]), legitimate interest ([85]), the right of access ([86]), the right to erasure ([87]), the right to compensation ([88]), automated individual decision-making ([89]), administrative fines ([90]), data protection officers ([91]), publication of personal data in registers ([92]) and the application of the GDPR to the activities of parliaments ([93]).

4 DATA SUBJECT RIGHTS

Individuals' awareness about the GDPR and data protection authorities (2024 Eurobarometer 549 on Justice, rights and values)

- 72% of respondents across the EU indicate having heard of the GDPR, including 40% who know what it is.
- In 19 Member States, more than 70% respondents indicate being aware of the GDPR, with respondents in Sweden (92%) being the most aware, followed by the Netherlands (88%), Malta and Denmark (84%), while respondents in Bulgaria (59%) are least aware, followed by Lithuania (63%) and France (64%).
- 68% of respondents across the EU indicate that they have heard of a national authority responsible for protecting their data protection rights, with 24% of all respondents stating they also know which public authority is responsible.

([81]) Case C-319/22, ECLI:EU:C:2023:837.
([82]) Cases C-184/20, ECLI:EU:C:2022:601; C-252/21, ECLI:EU:C:2023:537.
([83]) Cases C-683/21, ECLI:EU:C:2023:949; C-604/22, ECLI:EU:C:2024:214; C-231/22, ECLI:EU:C:2024:7.
([84]) Case C-61/19, ECLI:EU:C:2020:901.
([85]) Cases C-597/19, ECLI:EU:C:2021:492; C-252/21, ECLI:EU:C:2023:537.
([86]) Cases C-307/22, ECLI:EU:C:2023:811; C-154/21, ECLI:EU:C:2023:3.
([87]) Case C-460/20, ECLI:EU:C:2022:962.
([88]) Case C-300/21, ECLI:EU:C:2023:370; Case C-687/21, ECLI:EU:C:2024:72; Case C-667/21, ECLI:EU:C:2023:1022.
([89]) Joined Cases C- 26/22 and C- 64/22, ECLI:EU:C:2023:958.
([90]) Cases C-807/21, ECLI:EU:C:2023:950; Case C-683/21, ECLI:EU:C:2023:949.
([91]) Case C-453/21, ECLI:EU:C:2023:79.
([92]) Cases C-439/19, ECLI:EU:C:2021:504; C-184/20, ECLI:EU:C:2022:601.
([93]) Cases C-33/22, ECLI:EU:C:2024:46; C- 272/19, ECLI:EU:C:2020:535.

- In all Member States, at least half of the respondents have heard of such a national authority, with the highest levels in the Netherlands (82%), Czechia, Slovenia and Poland (all 75%), and Portugal (74%). Respondents in Austria (56%) and Spain (58%) are least aware of this authority.

Individuals are increasingly familiar with and actively exercise their rights under the GDPR ([94]). Data protection authorities allocate substantial resources to promoting awareness of data protection rights and obligations among the general public, such as through social media and television campaigns, helplines, newsletters and presentations in educational institutions ([95]). Many of these initiatives have benefited from EU funding ([96]). The Fundamental Rights Agency notes that while awareness of data protection among the general public has increased, understanding of data protection is still lacking, as evidenced by a large number of trivial or unfounded complaints ([97]). Several user-friendly digital tools have been developed to make it easier for data subject to exercise their rights ([98]). Legislative acts, most notably the Data Governance Act ([99]) should lead to the creation of additional ways for data subject to exercise their rights in future. Businesses note that the right to erasure is increasingly used, while it is rarely the case for the right to rectification and the right to object.

4.1 The right of access

Controllers report that the right of access (Article 15 GDPR) is the most frequently invoked right by data subjects. While the Board adopted guidelines on this right in 2022, controllers continue to report challenges, for example when interpreting the notion of 'unfounded or excessive requests' ([100]), when responding to a high number of requests, and when dealing with requests which are made for purposes unrelated to data protection, for example to gather evidence for legal proceedings ([101]). Civil society organisations note that responses to access requests are often delayed or incomplete, while the data received is not always in a readable format ([102]). Public authorities cite difficulties in the interaction between the right of access and rules on public access to documents ([103]). It is therefore welcome that the Board launched a Coordinated Enforcement Framework joint action on the right of access in February 2024 ([104]).

4.2 The right to portability

In the 2020 report, the Commission committed to explore practical means to facilitate increased use of the right to portability (Article 20 GDPR) by individuals, in line with the data strategy. The Commission has since adopted a number of initiatives which complement this right. These initiatives facilitate easy switching between services, thereby creating increased choice for individuals, supporting competition and innovation,

([94]) Council position and findings, paragraph 13.
([95]) Contribution of the Board, section 6.
([96]) https://commission.europa.eu/law/law-topic/data-protection/eu-funding-supporting-implementation-general-data-protection-regulation-gdpr_en
([97]) FRA report, pages 9 and 48.
([98]) Summary of the feedback of the GDPR Multi-stakeholder expert group.
([99]) Article 10, Regulation (EU) 2022/868 (Data Governance Act), OJ L 152, 3.6.2022, p. 1–44.
([100]) Article 12(5) GDPR.
([101]) However, the Court of Justice has clarified that the data subject is not required to state the reasons for requesting access to personal data: Case C-307/22, ECLI:EU:C:2023:811, paragraph 38.
([102]) Summary of the feedback of the GDPR Multi-stakeholder expert group.
([103]) Council position and findings, paragraphs 27-28.
([104]) https://www.edpb.europa.eu/news/news/2024/cef-2024-launch-coordinated-enforcement-right-access_en.

and allowing individuals to reap the benefits of the use of their data. The Data Act provides users of smart devices with an enhanced right to portability of data generated through such devices -and mandates that the design of the product or a backend server of the manufacturer or data holder makes such portability technically possible. The Digital Markets Act requires providers of core platform services identified as 'gatekeepers' to provide effective portability of users' data, including continuous and real-time access to such data. Several other Commission initiatives currently under negotiation or on which political agreement has been achieved provide for enhanced portability rights in specific fields, such as the Platform Work Directive ([105]), the European Health Data Space ([106]) and the Framework for Financial Data Access ([107]).

4.3 The right to lodge a complaint

As evidenced by the large number of complaints, there is broad awareness of the right to lodge a complaint with a data protection authority. Civil society organisations highlight unjustified differences in national practices for handling complaints, an issue which is tackled by the Commission's proposal on procedural rules. Few Member States have exercised the option under the GDPR to provide a non-profit body with the right to take actions independently of the mandate of a data subject (Article 80(2)). However, the Representative Actions Directive ([108]), adopted in 2020, will lead to more harmonisation in this respect by facilitating collective actions by individuals for breach of the GDPR. National measures implementing the Directive became applicable in June 2023.

4.4 The protection of children's personal data

Children require specific protection when their personal data are processed ([109]). The GDPR is part of a comprehensive legal framework that ensures that children are protected offline as well as online ([110]). Given the increased presence of children online, a number of actions at EU and national level have been taken in recent years to support the protection of children online. Data protection authorities have imposed significant fines on social media companies for violation of the GDPR when processing children's data. They also cooperate with other authorities to call for more protection of children in the area of advertising. In the 2020 report, the Commission invited the Board to adopt guidelines on the processing of children's data and this work is currently under way ([111]). The Digital Services Act includes specific provisions to ensure a high level of privacy, safety and security of children using online platforms.

Some stakeholders report challenges with the exercise of data subject rights, when the data subjects are children. In particular, they report that children do not fully understand

([105]) Platform workers: Council confirms agreement on new rules to improve their working conditions - Consilium (europa.eu).
([106]) Proposal for a Regulation on the European Health Data Space (COM/2022/197 final).
([107]) Proposal for a Regulation on a framework for Financial Data Access and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010, (EU) No 1095/2010 and (EU) 2022/2554 (COM/2023/360 final).
([108]) Directive (EU) 2020/1828 of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC - OJ L 409, 4.12.2020, p. 1–27.
([109]) Recital 38 GDPR.
([110]) Recommendation on developing and strengthening integrated child protection systems in the best interests of the child: https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/rights-child/combating-violence-against-children-and-ensuring-child-protection_en.
([111]) See also Council position and findings, paragraphs 31(a).

their rights, lack digital literacy skills and may be subject to undue influence ([112]). The Commission has funded several initiatives at national level on the protection of children's data and on promoting data protection awareness among children ([113]). Under the Better Internet for Kids (BIK+) strategy, the Commission is providing awareness-raising resources and trainings to children on their digital rights, including data protection (e.g. digital consent) ([114]). There is increasing focus on the need for effective and privacy-friendly age verification tools. In early 2024, the Commission set up a taskforce on age verification with Member States, the Board and the European Regulators Group for Audiovisual Media Services, with the aim of discussing and supporting the development of a EU-wide approach to age verification. This work will now continue under the Digital Services Act Board, in the Protection of Minors Working Group. In the context of the EU Digital Identity Regulation ([115]), which entered into force in May 2024, the Commission is working to ensure that the European Digital Identity Wallet is offered to all EU citizens and residents in 2026, including for age verification. Meanwhile, before the Wallet ecosystem is fully operational, a short-term solution for age verification will be developed and become available across the EU.

5 OPPORTUNITIES AND CHALLENGES FOR ORGANISATIONS, IN PARTICULAR SMES

The GDPR has created a level playing field for businesses operating in the internal market, and its technology-neutral, innovation-friendly approach allows businesses to reduce red tape and to benefit from greater consumer trust ([116]). Many businesses have developed an internal culture of data protection and view privacy and data protection as key parameters of competition. Businesses value the risk-based approach of the GDPR as a guiding principle allowing for flexibility and scalability of their obligations ([117]).

5.1 Toolbox for businesses

The GDPR provides a toolbox of instruments to enable organisations to flexibly manage and demonstrate their compliance, including codes of conduct, certification mechanisms and standard contractual clauses. As announced in the 2020 report, the Commission adopted standard contractual clauses on the controller-processor relationship in 2021 ([118]). These standard contractual clauses provide a ready-made and easy-to-implement voluntary compliance tool, which is particularly useful for SMEs or organisations that may not have the resources to negotiate individual contracts with their commercial partners. Businesses report mixed feedback on the use of the standard contractual clauses, in the sense that some companies (mainly SMEs) use them entirely

([112]) Summary of the feedback of the GDPR Multi-stakeholder expert group.
([113]) https://commission.europa.eu/law/law-topic/data-protection/eu-funding-supporting-implementation-general-data-protection-regulation-gdpr_en.
([114]) https://digital-strategy.ec.europa.eu/en/policies/strategy-better-internet-kids.
([115]) Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework OJ L, 2024/1183, 30.4.2024.
([116]) As recognised by the report of the 'Fit for future' platform, a high-level expert group set up to help the Commission in its efforts to simplify EU laws and to reduce related unnecessary costs: https://commission.europa.eu/law/law-making-process/evaluating-and-improving-existing-laws/refit-making-eu-law-simpler-less-costly-and-future-proof/fit-future-platform-f4f_en. See also the summary of the feedback of the GDPR Multi-stakeholder expert group and Council position and findings, paragraph 12.
([117]) Summary of the feedback of the GDPR Multi-stakeholder expert group.
([118]) Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) GDPR and Article 29(7) GDPR (C/2021/3701) - OJ L 199, 7.6.2021, p. 18–30.

or partially, while others (mostly larger companies) tend not to use them because they prefer to use their own clauses.

Businesses emphasise that codes of conduct have major potential as a sector-specific and cost-effective compliance tool ([119]). However, the development of codes of conduct has been limited ([120]). According to the information available to date, only two EU-wide codes have been approved (both in the cloud sector), while six codes have been approved at national level ([121]). Stakeholders report burdensome requirements (including the need to set up an accredited monitoring body), lack of engagement from data protection authorities, and a lengthy approval process as the main factors limiting the uptake of codes of conduct ([122]).

There is a need for increased transparency in the process and for clear approval timelines. Data protection authorities and, in the case of EU-wide codes, the Board, should more actively encourage the drawing up of the codes of conduct by collaborating with the associations developing the codes. This will help to resolve differences in interpretation and to speed up the approval process. Stakeholders regret the long delays in the adoption of codes of conduct, brought about by issues being discussed in parallel as part of the work on guidelines. Businesses similarly report that certification is not widely used because the process for development is slow and complex. As with codes of conduct, data protection authorities should provide clearer timelines for the review and approval of certifications.

The Board has committed in its 2024-2027 strategy to continue to support compliance measures such as certification and codes of conduct, including by engaging with key groups of stakeholders to explain how the tools can be used ([123]).

5.2 Specific challenges for SMEs and small operators

In the 2020 report, the Commission called for efforts to support SMEs' compliance with the GDPR to be intensified. In recent years, data protection authorities and the Board have continued to develop compliance tools for SMEs, supported in part by funding from the Commission ([124]). In April 2023, the Board launched a data protection guide for small business ([125]), which provides practical information for SMEs in an accessible and easily understandable format.

SMEs in many Member States underline the benefits of tailored support from their local data protection authorities. However, varying approaches to awareness raising and guidance by data protection authorities means that SMEs in certain Member States perceive compliance as complex and fear enforcement ([126]). Data protection authorities should redouble their efforts to address these challenges, including by proactively engaging with SMEs to allay any unfounded compliance concerns. Data protection authorities should focus on providing tailor-made support and practical tools, such as templates (e.g. for conducting data protection impact assessments), helplines, illustrative

([119]) Summary of the feedback of the GDPR Multi-stakeholder expert group.
([120]) Council position and findings, paragraph 25.
([121]) https://www.edpb.europa.eu/our-work-tools/accountability-tools/register-codes-conduct-amendments-and-extensions-art-4011_en?f%5B0%5D=coc_scope%3Anational
([122]) Summary of the feedback of the GDPR Multi-stakeholder expert group.
([123]) https://www.edpb.europa.eu/system/files/2024-04/edpb_strategy_2024-2027_en.pdf
([124]) https://commission.europa.eu/law/law-topic/data-protection/eu-funding-supporting-implementation-general-data-protection-regulation-gdpr_en
([125]) https://edpb.europa.eu/sme-data-protection-guide/home_en
([126]) Summary of the feedback of the GDPR Multi-stakeholder expert group.

examples, checklists, and guidance on specific processing operations (e.g. billing or newsletters) and technical and organisational measures. Since most SMEs do not have in-house data protection expertise, any guidance directed at SMEs should be easily understood by those without legal training ([127]).

In line with the GDPR's risk-based approach, SMEs carrying out low-risk processing activities do not bear a substantial compliance burden. While the derogation to maintain records of processing activities ([128]) applies in limited circumstances ([129]), SMEs carrying out low-risk processing may comply by maintaining simplified records based on templates provided by data protection authorities. Furthermore, such records should be seen as a useful tool for SMEs to take stock of their processing activities.

5.3 Data protection officers

Data protection officers play an important role in ensuring GPDR compliance in the organisations in which they work. In general, data protection officers operating in the EU have the necessary knowledge and skills to perform their tasks under the GDPR, and their independence is respected ([130]). However, several challenges remain, including: (i) difficulties in appointing data protection officers with the required expertise; (ii) the lack of EU-wide standards for education and training; (iii) failure to adequately integrate data protection officers in organisational processes; (iv) lack of resources; (v) additional tasks outside of data protection; and (vi) insufficient seniority ([131]). The Board noted that there is a need for data protection authorities to step up awareness-raising activities, as well as their information and enforcement actions to ensure that data protection officers can fulfil their role under the GDPR ([132]).

6 THE GDPR AS A CORNERSTONE FOR EU POLICY IN THE DIGITAL SPHERE

6.1 Digital policy building on the GDPR

In the 2020 report, the Commission committed to support the consistent application of the data protection framework in relation to new technologies, in order to support innovation and technological developments. The EU has since adopted a range of initiatives, some of which complement the GDPR or specify how it should be applied in specific areas, in order to pursue particular objectives, as presented below.

- The Digital Services Act ([133]), which aims to provide a safe online environment for individuals and business, prohibits online platforms from showing advertisements based on profiling using 'special categories of personal data', as defined in the GDPR.

([127]) See Council position and findings, paragraph 24; summary of the feedback of the GDPR Multi-stakeholder expert group.
([128]) Article 30(5) GDPR.
([129]) Where the organisation employs fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) GDPR or personal data relating to criminal convictions and offences referred to in Article 10 GDPR.
([130]) Council position and findings, paragraph 26; EDPB 2023 Coordinated Enforcement Action Designation and Position of Data Protection Officers: https://www.edpb.europa.eu/system/files/2024-01/edpb_report_20240116_cef_dpo_en.pdf
([131]) Summary of the feedback of the GDPR Multi-stakeholder expert group.
([132]) See recommendations in EDPB Coordinated Enforcement Action.
([133]) Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) OJ L 277, 27.10.2022, p. 1–102.

- To make digital markets fairer and more contestable, the Digital Markets Act ([134]) prohibits operators designated as 'gatekeepers' from 'combining' and 'cross-using' personal data between their core platform services and other services unless the user has provided their consent, as defined in the GDPR.
- The AI Act ([135]) specifies the EU data protection rules in specific areas where AI is used, for example in remote biometric identification systems, the processing of special categories of data to detect bias and the further processing of personal data in regulatory sandboxes.
- The Directive on Platform Work ([136]) complements the GDPR in the area of employment by laying down rules on automated monitoring and decision-making systems used by digital labour platforms, and in particular limitations on processing of personal data, transparency human oversight and review and portability.
- The Political Advertising Regulation ([137]) prohibits the use of special categories of personal data in political advertising and requires greater transparency on the targeting and amplification techniques used.
- The European Digital Identity Regulation enables the creation of a universal, trustworthy and secure European digital identity wallet. This will allow individuals to prove personal attributes like age, driving licences, diplomas and bank accounts, with full control over their personal data and without unnecessary data sharing.

The proposal for an e-Privacy Regulation ([138]) to replace the current e-Privacy Directive ([139]) and complement the privacy and data protection legislative framework has been under negotiation for several years. Reflection is needed on the next steps for this initiative, including its relation with the GDPR.

The Interoperable Europe Act ([140]) aims at making digital public services interoperable across the EU. It supports the cooperation between data protection authorities in particular through interoperability regulatory sandboxes.

Several EU initiatives provide a legal basis for the processing of personal data by private entities for the prevention, investigation, detection or prosecution of criminal offences. Any such legislation must be carefully targeted to minimise interference with the right to protection of personal data and must be proportionate to the aim pursued ([141]). The Charter, the GDPR and the case law of the Court of Justice provide a framework against which these initiatives should be measured. The proposed anti-money laundering package ([142]) contains substantial safeguards for the protection of personal data, without compromising the objective of mitigating money laundering and terrorist financing risks and effectively detecting criminal attempts to misuse the EU financial system.

([134]) Regulation (EU) 2022/1925 (Digital Markets Act) OJ L 265, 12.10.2022, p. 1–66.
([135]) Regulation (EU) 2024/1689 (Artificial Intelligence Act) OJ L, 2024/1689, 12.07.2024.
([136]) Platform workers: Council confirms agreement on new rules to improve their working conditions - Consilium (europa.eu).
([137]) Regulation (EU) 2024/900 on the transparency and targeting of political advertising OJ L, 2024/900, 20.3.2024.
([138]) Proposal for a Regulation on Privacy and Electronic Communications - COM/2017/010 final.
([139]) Directive 2002/58/EC (ePrivacy Directive) - OJ L 201, 31/07/2002 P. 0037 - 0047
([140]) Regulation (EU) 2024/903 (Interoperable Europe Act) OJ L, 2024/903, 22.3.2024.
([141]) See Council position and findings, paragraph 31(f).
([142]) https://finance.ec.europa.eu/publications/anti-money-laundering-and-countering-financing-terrorism-legislative-package_en.

In this context, the Council has stressed that any new EU legislation containing provisions on the processing of personal data should be consistent with the GDPR and the case law of the Court of Justice.

6.2 A legal framework to enhance data sharing

The data strategy aims to create a single market for data, where data flows freely within the EU and across sectors for the benefit of businesses, researchers and public administrations. A key goal of the data strategy is the creation of common European data spaces which facilitates data pooling, access and sharing. Regarding personal data, the GDPR provides the framework for all initiatives that seek to enhance the free flow of data in the EU – which is itself an objective of the GDPR. As far as personal data is concerned, the protections of the GDPR are not touched upon.

The Data Governance Act ([143]) and Data Act ([144]) are pillars of the data strategy. The Data Governance Act stipulates concrete rules in the context of the re-use of public sector data containing personal data, lays down a legislative framework for data intermediation services - including personal information management services (PIMS) or personal data clouds offered in order to empower data subjects when exercising their rights under the GDPR. It also frames the conditions for use of data for altruistic purposes. The Data Act strengthens data subjects' control over the data they generate through the use of smart objects they own, rent or lease by mandating technical requirements for data access and portability.

The European Health Data Space (EHDS) ([145]) reflects the specific needs identified in the health data sector while also building upon the GDPR. It allows individuals to easily access their health data in an electronic format and share them with health professionals, including in other Member States, thereby improving healthcare delivery and increasing patients' control over their data. It also puts in place a common legal framework for the re-use of health data for purposes such as research, innovation and public health, based on a permit issued by a health data access body. To ensure the protection of personal data, the EHDS will provide a trustworthy setting for secure access to and processing of health data. The Commission continues to support work on the development of common European data spaces across 14 sectors by implementing the new legislative framework and funding sector-specific initiatives.

6.3 Governance of new digital rules

The development of digital regulations raises the need for close cooperation across regulatory fields ([146]). Such cooperation is all the more necessary since data protection issues increasingly intersect with questions of, for example, competition law, consumer law, digital markets rules, electronic communications regulation and cybersecurity. This is for instance the case when assessing the compatibility of 'pay or OK' models with EU law.

In some cases, data protection authorities are tasked with enforcing specific provisions of new EU digital legislation ([147]). New digital regulations also create bespoke structures

([143]) Regulation (EU) 2022/868 (Data Governance Act) OJ L 152, 3.6.2022, p. 1–44.
([144]) Regulation (EU) 2023/2854 (Data Act) OJ L, 2023/2854, 22.12.2023.
([145]) https://www.europarl.europa.eu/doceo/document/TA-9-2024-0331_EN.html.

([146]) See Council position and findings, paragraphs 40-41; Summary of the feedback of the GDPR Multi-stakeholder expert group.
([147]) See for example Article 37(3) of the Data Act.

which bring together competent regulators to ensure coherent enforcement, such as the Digital Markets Act high-level group, the European Data Innovation Board (set up under the Data Governance Act) and the European Board for Digital Services (set up under the Digital Services Act). The NIS2 Directive ([148]) sets out more detailed rules on cooperation between regulatory authorities and data protection authorities on handling security incidents which constitute personal data breaches.

Outside of these formal structures, data protection authorities are taking steps to ensure their actions are complementary and coherent with other regulatory fields. In July 2020, consumer and data protection authorities set up a 'group of volunteers' to determine best practices and share enforcement experiences. Data protection authorities continue to participate in joint workshops with the Consumer Protection Cooperation Network. In 2023, the Board set up a taskforce on the interplay between data protection, competition and consumer protection.

While these developments are positive, there is a need for more structured and efficient means of cooperation, in particular to address situations that affect a large number of individuals in the EU and involve several regulators ([149]). Any such structures should ensure that authorities remain at all times responsible for all questions concerning compliance with rules within their areas of competence. Member States should also work to ensure that appropriate cooperation takes place at national level ([150]).

7 INTERNATIONAL TRANSFERS AND GLOBAL COOPERATION

7.1 The GDPR transfer toolbox

Data flows have become integral to the digital transformation of society and to the globalisation of the economy. More than ever before, respecting privacy is a condition for stable, secure and competitive commercial flows, as well as an enabler for many forms of international cooperation. The GDPR transfer toolbox provided by its Chapter V offers a variety of instruments to address different transfer scenarios, while ensuring that data continues to benefit from a high level of protection when leaving the EU.

Since the 2020 report, requirements for data transfers set out in EU data protection legislation have been further clarified and the transfer toolbox has continued to evolve. An important clarification concerns the notion of 'international transfer', which has been defined by the Board ([151]) as encompassing any disclosure of personal data by a controller or processor whose processing is subject to the GDPR to another controller or processor in a third country, regardless of whether or not the processing by the latter is subject to the GDPR ([152]). This guidance of the Board was particularly important to provide legal certainty to European controllers and processors on the scenarios in which a transfer tool under Chapter V GDPR is needed.

Further clarifications have also been provided by the Court of Justice in its *Schrems II* judgment ([153]) on the protection that has to be provided by different transfer instruments

([148]) Directive (EU) 2022/2555 (NIS 2 Directive) OJ L 333, 27.12.2022, p. 80-152.

([149]) See Council position and findings, paragraphs 18, 40-41 and the summary of the feedback of the GDPR Multi-stakeholder expert group.

([150]) Germany has established a 'digital cluster', which includes regulators from various fields, with the aim of expanding their cooperation on all aspects of digitalisation and sharing knowledge and best practices: https://www.dataguidance.com/news/germany-bsi-announces-formation-digital-cluster-bonn

([151]) EDPB Guidelines 05/2021.

([152]) Section 2 of EDPB Guidelines 05/2021.

([153]) Case C-311/18, ECLI:EU:C:2020:559 (*Schrems II*).

to ensure that the level of protection guaranteed by the GDPR is not undermined ([154]). In particular, these instruments must ensure that individuals whose data are transferred outside the EU are afforded a level of protection essentially equivalent to that guaranteed within the EU ([155]). It is the responsibility of the EU data exporter to assess whether this is the case, taking into account the specific circumstances of its transfers ([156]).

To assess the level of protection, data exporters must consider both the data protection safeguards set out in the transfer instrument concluded with a non-EU data importer (e.g. a contract), as well as relevant aspects of the legal system of the country where the data importer is located, in particular as regards possible access to the data by public authorities in that country ([157]). The latter must be assessed in light of the criteria for adequacy assessments set out in Article 45 GDPR. The Court also further elaborated on these criteria, in particular with respect to the rules on access to personal data by public authorities for law enforcement and national security purposes.

This interpretation has also been reflected in the guidance of the Board, which updated its 'adequacy referential' ([158]) (that provided guidance on the elements the Commission must take into account when carrying out an adequacy assessment). The Board also adopted new guidance providing further clarifications on: (i) the elements to be taken into account by individual data exporters when assessing the level of protection; (ii) an overview of potential sources that can be used; and (iii) examples of possible supplementary measures (e.g. contractual and technical safeguards) ([159]). The guidance specifically highlights that each assessment carried out by data exporters is unique, and that they therefore need to take into account the specific features of each transfer which can differ depending on the purpose of the data transfer, the types of entities involved, the sector in which the transfer occurs, the categories of personal data transferred, etc. ([160]).

Taking into account these different clarifications on the requirements for international data transfers, significant steps have been taken in the past years to further develop and operationalise the GDPR transfer toolbox.

7.1.1 Adequacy decisions

As also reflected in the feedback received from stakeholders, adequacy decisions continue to play a key role in the GDPR transfer toolbox ([161]), by providing a straightforward and comprehensive solution for data transfers without the need for the data exporter to provide further safeguards or obtain any authorisation. By enabling the free flow of personal data, these decisions have opened up commercial channels for EU operators, including by complementing and amplifying the benefits of trade agreements, and eased collaboration with foreign partners in a broad range of fields, from regulatory cooperation to research.

Since the 2020 report, the number of countries that have put in place modern data protection laws - providing among others for key data protection principles, individual rights, and effective enforcement by independent regulators - has continued to grow. This

([154]) *Schrems II*, point 93.
([155]) *Schrems II*, points 96 and 105.
([156]) *Schrems II*, point 131.
([157]) *Schrems II*, point 105.
([158]) EDPB Recommendations 02/2020 and Adequacy Referential, WP 254 rev. 01.
([159]) EDPB Recommendations 01/2020, complemented by Recommendations 02/2020.
([160]) See e.g. paras. 8-13, 32-33 of EDPB Recommendations 01/2020.
([161]) See e.g. contribution of the Board, pages 7-8; Council position and findings paragraph 36; Summary of the feedback of the GDPR Multi-stakeholder expert group.

trend ([162]) has also allowed the Commission to intensify its adequacy work. This includes the adoption of an adequacy decision for the United Kingdom ([163]), which is central to ensuring the proper functioning of the various agreements concluded with the UK following Brexit. To ensure that it remains future proof, the adequacy decision includes a 'sunset clause' that is set to expire in 2025, after which it may be renewed if the level of protection continues to be adequate. The Commission also adopted an adequacy decision for the Republic of Korea ([164]), which complements the EU-Korea Free Trade Agreement on personal data flows and facilitates regulatory cooperation. A first review of the adequacy decision is planned towards the end of 2024.

In addition, following the invalidation of the adequacy decision for the EU-US Privacy Shield, the Commission entered into talks with the United States (US) Government to develop a successor arrangement in compliance with the requirements as clarified by the Court ([165]). The US President adopted a new Executive Order on 'Enhancing Safeguards for United States Signals Intelligence Activities', which introduced new binding and enforceable safeguards to ensure that data can be accessed for national security purposes only to the extent necessary and proportionate, and that effective redress is available to Europeans. On that basis, the Commission adopted its adequacy decision on the EU-US Data Privacy Framework (DPF) ([166]), allowing personal data to flow freely from the EU to US companies joining the DPF. Since the safeguards put in place by the US Government in the area of national security apply to all data transfers to companies in the US, regardless of the GDPR transfer mechanism used, the use of other tools, such as standard contractual clauses and binding corporate rules, has been significantly facilitated. A first review of the functioning of the DPF will take place in the summer of 2024 in order to verify that all relevant elements have been fully implemented in the US legal framework and are functioning effectively in practice.

Adequacy negotiations are currently under way with Brazil and Kenya, as well as, for the first time, with several international organisations (adequacy talks are for instance at an advanced stage with the European Patent Organisation) ([167]). In line also with the calls of various stakeholders ([168]), the Commission has actively engaged in exploratory talks with countries in different regions of the world.

The Commission also continuously monitors developments in the countries that already benefit from adequacy findings and periodically reviews existing decisions, in accordance with its corresponding obligations under the GDPR ([169]). In April 2023, the Commission adopted its report on the first periodic review of the adequacy decision for Japan ([170]), which concluded that Japan continues to ensure an adequate level of

([162]) Implementing Commission Communication 'Exchanging and Protecting Personal Data in a Globalised World', 10.1.2017 (COM(2017) 7 final).
([163]) Commission Implementing Decision (EU) 2021/1772, OJ L 360, 11.10.2021, p. 1–68.
([164]) Commission Implementing Decision (EU) 2022/254, OJ L 44, 24.2.2022, p. 1–90.
([165]) https://commission.europa.eu/news/joint-press-statement-european-commissioner-justice-didier-reynders-and-us-secretary-commerce-wilbur-2020-08-10_en
([166]) Commission Implementing Decision EU 2023/1795, OJ L 231, 20.9.2023, p. 118–229.
([167]) The European Patent Organisation is an intergovernmental organisation set up on the basis of the European Patent Convention. Its main task is the granting of European patents. In that context, it cooperates closely with companies and public authorities in EU Member States, as well as with different EU institutions and bodies.
([168]) Contribution of the Board, pages 7-8.
([169]) Article 45(4) and (5) GDPR. See also *Schrems I*, point 76.
([170]) Commission Implementing Decision (EU) 2019/419, OJ L 76, 19.3.2019, p. 1–58. See also https://ec.europa.eu/commission/presscorner/detail/en/IP_19_421. This decision constituted the first adequacy decision adopted under the GDPR and the first reciprocal adequacy arrangement.

protection ([171]). The review demonstrated that the EU and Japanese data protection frameworks further converged since the adoption of the mutual adequacy decisions.

In addition, in accordance with Article 97 of the GDPR, the first review of the 11 adequacy decisions ([172]) adopted under the former EU data protection framework (the Data Protection Directive) was initiated as part of the 2020 evaluation of the application and functioning of the GDPR. The conclusion of this aspect of the review was postponed, notably to take into account the judgment of the Court of Justice in the *Schrems II* case and subsequent interpretation by the Board. The above-mentioned clarifications of the Court on key elements of the adequacy standard led to detailed exchanges with the countries and territories concerned on relevant aspects of their legal framework, as well as oversight and enforcement mechanisms.

On 15 January 2024, the Commission published its report on these 11 decisions, together with detailed country reports describing developments in each of the countries and territories since the adoption of the adequacy decisions, as well as the rules that apply to access to data by public authorities, in particular for law enforcement and national security purposes ([173]). The report concludes that all 11 countries and territories continue to provide an adequate level of protection for personal data transferred from the EU. It reflects that all the countries and territories concerned have in different ways modernised and strengthened their privacy legal framework. Moreover, in order to address relevant differences in the level of protection, additional safeguards for personal data transferred from Europe have been - when needed to ensure the continuity of the adequacy decision - negotiated and agreed with some of them.

These reviews also show that adequacy decisions have, rather than being an 'end point', laid the foundation for closer cooperation and further regulatory convergence between the EU and these likeminded partners. For example, the report on the first review of the adequacy decision for Japan recognises that the further strengthening of the Japanese data protection framework can pave the way to extend the adequacy decision beyond commercial exchanges, to cover transfers currently excluded from its scope, such as in the area of regulatory cooperation and research. Talks to explore such a possible extension are ongoing. In general, adequacy decisions have become a strategic component of the overall relationship of the EU with these foreign partners and are recognised as a major enabler for deepening cooperation in a broad range of areas.

Beyond providing a strong basis for increased bilateral cooperation, the growing network of countries and territories for which the EU has adopted an adequacy decision presents new opportunities to maximise the benefits of safe and free data flows and to cooperate more closely among likeminded partners on the enforcement of data protection rules. In March 2024, the Commission therefore hosted the first ever high-level meeting on safe data flows, gathering responsible Ministers and heads of the data protection authorities of 15 countries and territories for which the EU has adopted an adequacy decision, as well as the Chair of the European Data Protection Board ([174]). Several concrete action points were identified at the meeting on which follow-up work is ongoing within this group.

([171]) Commission report on the first review of the functioning of the adequacy decision for Japan, 3.4.2023, COM(2023) 275 final (and SWD(2023) 75 final).

([172]) Andorra, Argentina, Canada (for commercial operators), Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay.

([173]) Commission report on the first review of the functioning of the adequacy decisions adopted pursuant to Article 25(6) of Directive 95/46/EC, 15.1.2024, COM(2024) 7 final (and SWD(2024) 3 final).

([174]) https://ec.europa.eu/commission/presscorner/detail/en/mex_24_1307#11

More generally, through their 'network effect', adequacy decisions adopted by the European Commission are increasingly relevant also beyond the EU, as they not only allow for the free flow of data with the 30 economies of the EEA, but also with many more jurisdictions around the globe that recognise countries for which there is an EU adequacy decision as 'safe destinations' under their own data protection rules ([175]).

7.1.2 Instruments providing for appropriate safeguards

Since the 2020 report, additional tools providing for appropriate safeguards have been developed and practical guidance has been issued to facilitate their use.

As announced in the 2020 report, the Commission has adopted modernised standard contractual clauses (SCCs) ([176]), developed relying extensively on feedback from various stakeholders ([177]). The new SCCs have replaced the three sets of SCCs that were adopted under the Data Protection Directive. The main innovations include: (i) updated safeguards in line with the GDPR; (ii) a modular approach offering a single entry-point covering a broad range of transfer scenarios; (iii) increased flexibility for the use of SCCs by multiple parties; and (iv) a practical toolbox to comply with the *Schrems II* judgment.

The modernised SCCs have been welcomed by stakeholders, and the feedback received confirms that SCCs remain by far the most used tool for transfers by EU data exporters ([178]). To assist data exporters with their compliance efforts, the Commission has developed a Q&A that provide further guidance on the use of the clauses ([179]), which will be further updated if new questions arise, including in light of the further feedback received as part of this evaluation.

Many data exporters report experiencing difficulties with carrying out 'transfer impact assessments' required by the *Schrems II* judgment, referring in particular to their complexity, as well as to the costs and time needed to perform them ([180]). While welcoming the guidance of the Board and the SCCs, they call for additional guidance (e.g. on the responsibilities of involved parties and the level of detail required in transfer impact assessments) and additional tools to assist with performing such assessments (e.g. templates, general country-assessments, risk catalogues). Although stakeholders mainly provided such feedback on the SCCs, the same assessments are also required for other transfer instruments (such as binding corporate rules). It is therefore important that the Board - building on the experience with applying the *Schrems II* requirements in the past years, including as part of the enforcement activities of national data protection authorities - considers exploring ways/tools to further assist data exporters in their compliance efforts in this context.

To complement the existing SCCs, the Commission is developing additional sets of clauses to provide EU data exporters with a comprehensive and coherent package. This will include SCCs under Regulation (EU) 2018/1725 for data transfers by EU institutions and bodies to commercial operators in third countries ([181]) and SCCs for data transfers to third country data importers whose processing operations are directly subject to the

([175]) Such as Argentina, Colombia, Israel, Morocco, Switzerland and Uruguay.
([176]) Commission Implementing Decision (EU) 2021/914, OJ L 199, 7.6.2021, p. 31–61.
([177]) This included for instance EDPB-EDPS Joint Opinion 2/2021 as part of the adoption procedure for the SCCs.
([178]) Council position and findings para. 37, Contribution of the Board page 9, Summary of the feedback of the GDPR Multi-stakeholder expert group.
([179]) https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en.
([180]) See e.g. summary of the feedback of the GDPR Multi-stakeholder expert group.
([181]) In accordance with Article 48(2)(b) of Regulation (EU) 2018/1725.

GDPR. The latter respond to the call from stakeholders to specifically cover scenarios where the data importer falls within the territorial scope of application of the GDPR (for instance because the processing in question targets the EU market in accordance with Article 3(2) GDPR) ([182]). As clarified by the Board, a transfer tool under Chapter V GDPR is required also in this case, because of the increased risks for personal data processed outside the EU, for example due to possibly conflicting national laws or disproportionate government access in the third country ([183]). The new SCCs being developed by the Commission will specifically address this scenario and will fully take into account the requirements that already apply directly to those controllers and processors under the GDPR ([184]).

As also recognised by different types of stakeholder ([185]), model clauses play an increasingly central role in facilitating data flows around the world. Several jurisdictions have endorsed the EU SCCs as a transfer mechanism under their own data protection laws, with limited formal adaptations to their domestic legal order ([186]). A number of other countries have adopted their own model clauses that share important common features with the EU SCCs ([187]). A particularly relevant example is the creation of model clauses by other international/regional organisations or networks, such as the Council of Europe Consultative Committee of Convention 108, the Ibero-American Data Protection Network and the Association of Southeast Asian Nations (ASEAN) ([188]). This opens up new opportunities to facilitate data flows between different regions of the world on the basis of model clauses. A concrete example is the EU-ASEAN Guide on the EU SCCs and ASEAN model clauses which, building on input from companies, assists them in their compliance efforts under both sets of clauses ([189]).

In addition to SCCs, binding corporate rules (BCRs) continue to be widely used for data flows between members of corporate groups or among enterprises engaged in a joint economic activity. Since the GDPR applies, the Board adopted 80 positive opinions on national decisions approving BCRs ([190]). The Board also issued guidance on the elements to be included in BCRs for controllers (and the information to be provided as part of a BCR application), which has been updated to reflect GDPR requirements and the *Schrems II* judgment ([191]). Updated guidance on BCRs for processors is also being developed ([192]). Because BCRs aim at putting binding data protection

([182]) Council position and findings paragraph 37, Contribution of the Board, page 9, Summary of the feedback of the GDPR Multi-stakeholder expert group.
([183]) EDPB Guidelines 05/2021, p. 3.
([184]) As also set out in the EDPB Guidelines 05/2021, Section 4.
([185]) Contribution of the Board, page 9, Summary of the feedback of the GDPR Multi-stakeholder expert group.
([186]) E.g. the UK (https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf) and Switzerland (https://www.edoeb.admin.ch/edoeb/en/home/datenschutz/arbeit_wirtschaft/datenuebermittlung_ausland.html).
([187]) E.g. New Zealand (https://privacy.org.nz/responsibilities/your-obligations/disclosing-personal-information-outside-new-zealand/) and Argentina (https://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/267922/norma.htm).
([188]) See https://rm.coe.int/t-pd-2022-1rev10-en-final/1680abc6b4; https://www.redipd.org/sites/default/files/2023-02/anexo-modelos-clausulas-contractuales-en.pdf and https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf.
([189]) https://commission.europa.eu/document/download/df5cd5a0-7387-4a2a-8058-8d2ccfec3062_en?filename=%28Final%29%20Joint_Guide_to_ASEAN_MCC_and_EU_SCC.pdf.
([190]) Contribution of the Board, page 9.
([191]) EDPB Recommendations 1/2022.
([192]) Contribution of the Board, page 9.

policies/programmes in place in companies, many stakeholders consider them to be a particularly useful compliance tool and a trustworthy transfer instrument ([193]). At the same time, stakeholders continue to report that the length and complexity of the approval process by national data protection authorities is preventing a broader uptake of BCRs. It is therefore important that the authorities continue to work on streamlining and shortening the approval process.

Since the 2020 report, steps have also been taken to facilitate the use of certification and codes of conduct as tools for transfers, e.g. through the adoption of dedicated guidelines on both tools by the Board ([194]). At the same time, stakeholders report the same issues concerning the timeline and complexity of the approval process as the ones mentioned above with respect to certification and codes of conduct as accountability tools.

Finally, the GDPR also provides for specific instruments - international agreements and administrative arrangements approved by data protection authorities - to be used by public authorities to transfer personal data to their counterparts in third countries, or to international organisations. The Board adopted guidelines on the safeguards that should be included in such instruments ([195]), which can support the negotiation of such agreements and arrangements.

7.1.3 Ensuring complementarity with other policies

As data flows have become essential for so many activities, ensuring that data protection policies and other policies complement one another is key. The inclusion of data protection safeguards in international instruments is not only often a precondition for data flows, but also an important enabler for stable and trustworthy cooperation.

For instance, international agreements providing for the necessary data protection safeguards, including by ensuring continuity of protection on the side of a requesting authority, are essential to ensure comity and facilitate cross-border access by law enforcement to electronic evidence held by companies and, in this way, a more effective fight against crime. This approach is reflected in the Second Additional Protocol to the Cybercrime Convention ([196]), which enhances existing rules to obtain cross-border access to electronic evidence in criminal investigations while ensuring appropriate data protection safeguards. The Protocol has in the meantime been signed by several EU Member States. Similarly, bilateral negotiations are progressing between the EU and the US on an agreement on cross-border access to electronic evidence for cooperation in criminal matters ([197]).

The exchange of Passenger name record (PNR) data is another area of the EU security policy that has benefited from the development of strong data protection safeguards. In 2023, the EU and Canada concluded their negotiations on a new PNR Agreement in line with the requirements set out by the Court of Justice in its Opinion 1/15 ([198]). Similar safeguards have been introduced in the PNR chapter of the EU-UK Trade and Cooperations Agreement. The inclusion of enhanced privacy protections in these

([193]) Summary of the feedback of the GDPR Multi-stakeholder expert group.
([194]) EDPB Guidelines 07/2022 and Guidelines 04/2021.
([195]) EDPB Guidelines 2/2020.
([196]) Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and disclosure of electronic evidence (CETS No. 224).
([197]) https://commission.europa.eu/news/eu-us-announcement-resumption-negotiations-eu-us-agreement-facilitate-access-electronic-evidence-2023-03-02_en.
([198]) Commission proposal for a Council Decision on the signing, on behalf of the European Union, of an agreement between Canada and the European Union on the transfer and processing of Passenger Name Record (PNR) data, COM/2024/94 final.

agreements, which can serve as a template for future agreements with other partners, brings legal certainty to air carriers while ensuring the stability of important exchanges of information for combating terrorism and other serious transnational crimes.

The Commission is also a proponent of strong provisions to protect privacy and boost digital trade at the World Trade Organisation in the ongoing negotiations on the Joint Statement Initiative on electronic commerce. Similar provisions on fighting unjustified obstacles to digital trade, while protecting the Parties' necessary policy space in the area of data protection, have been consistently included in the free trade agreements concluded by the EU following the entry into application of the GDPR, notably in the EU-UK TCA and in the agreements with Chile, Japan and New Zealand. Provisions for privacy and data flows are also being discussed in the ongoing digital trade negotiations with Singapore and South Korea.

7.2 International cooperation on data protection

7.2.1 The bilateral dimension

The Commission has continued to engage in dialogue with countries and international organisations on the development, reform and implementation of privacy rules, including by making submissions to public consultations on draft legislation or regulatory measures in the area of privacy ([199]), testifying before competent parliamentary bodies ([200]) and participating in dedicated meetings with government representatives, parliamentary delegations and regulators from many regions of the world ([201]). A number of these activities have been carried out through the EU-funded 'Enhanced Data Protection and Data Flows' project, which supports countries intending to develop modern data protection frameworks or to strengthen the capacity of their regulatory authorities, through training, knowledge sharing, capacity building and exchange of best practices. The Commission also contributed to other initiatives, such as the EU-CELAC Digital Alliance.

Data protection will also continue to play a key role in the Commission's enlargement-related work. EU data protection legislation is an important component of the overall effort of enlargement countries to align their legal frameworks with those of the EU (especially since the processing and exchanging of personal data are at the core of so many policies). Moreover, the independence and proper functioning of a data protection authority is a key element of overall checks and balances and rule of law, and will become increasingly important as the EU gradually integrates enlargement countries into the single market (as envisaged by initiatives such as the Western Balkans Growth Plan).

An increasingly important aspect of the EU's dialogue with third countries focuses on the exchanges between regulators. As announced in the 2020 report, the Commission has created a 'Data Protection Academy', to foster exchanges between EU and third country data protection authorities and, in this way, contribute to capacity building and improve cooperation 'on the ground'. The Academy offers tailor-made trainings at the request of third country authorities and brings together the expertise of representatives of the enforcement community, academia, the private sector and European institutions. The added value of the trainings lies in the tailoring of the different components to the interests and needs of the requesting authority. Moreover, these trainings allow EU and

([199]) This concerned consultations organised by, for example, Australia, China, Rwanda, Argentina, Brazil, Ethiopia, Indonesia, Peru, Malaysia and Thailand.

([200]) For example, before the parliamentary bodies of Chile, Ecuador and Paraguay.

([201]) This also included the organisation of seminars and study visits, for example with Kenya, Indonesia, and Singapore.

third country data protection authorities to establish contacts, share knowledge, exchange experience and best practices, and identify potential areas for cooperation. The Academy has so far provided training to the data protection authorities of Indonesia, Brazil, Kenya, Nigeria and Rwanda, and is currently in the process of preparing trainings for several other countries.

Beyond the importance of maintaining a dialogue between regulators, there is an increasing need, as also recognised in the feedback received from the Council and the Board ([202]), 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. Indeed, as privacy violations increasingly produce effects across borders, they can often only be effectively investigated and addressed through cooperation between EU and non-EU regulators. The Commission will therefore seek authorisation to open negotiations to conclude enforcement cooperation agreements with relevant third countries (as also provided for in Article 50 of the GDPR). In this respect, the Commission notes the Board's request to specifically consider countries with the most operators directly subject to the GDPR as potential counterparts, in particular G7 countries and/or countries that benefit from adequacy decisions ([203]).

Putting in place such enforcement cooperation and mutual assistance agreements would also help to ensure compliance by, and effective enforcement against, foreign operators subject to the GDPR, for instance because they specifically target the EU market by offering goods or services. The Council notes the importance of enforcing compliance with the GDPR in such cases, and raises concerns about the level playing field with entities in the EU, as well as the effective protection of the rights of individuals ([204]). The Commission agrees with the call of the Council to explore different ways to facilitate enforcement in this scenario. While more formal forms of cooperation with third country regulators could certainly play an important role, the use of other - already existing - avenues should also be pursued more vigorously. This includes making full use of the enforcement toolbox of Article 58 of the GDPR, and involving representatives of foreign companies in the EU (appointed in accordance with Article 27 of the GDPR).

7.2.2 The multilateral dimension

The Commission also continues to actively participate in a number of international fora to promote shared values and build convergence at regional and global level.

This for instance includes actively contributing to the work of the Consultative Committee on the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), the only legally binding multilateral instrument in the area of personal data protection. So far, 31 states have ratified the Amending Protocol to modernise Convention 108 ([205]), including many EU Member States, as well as some non-members of the Council of Europe (Argentina, Mauritius and Uruguay). Among EU Member States, only the signature of one Member State ([206]) is still outstanding, while eight Member States ([207]) have so far signed, but not ratified the modernised Convention. The Commission urges the one remaining Member State to sign the modernised Convention and others to swiftly proceed to ratification, to allow for its

([202]) Contribution of the Board, page 8; Council position and findings, para. 38.
([203]) Contribution of the Board, page 8.
([204]) Council position and findings, paragraph 39.
([205]) Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223).
([206]) Denmark.
([207]) Belgium, Czechia, Greece, Ireland, Latvia, Luxembourg, the Netherlands and Sweden.

entry into force in the near future. Beyond that, it continues to proactively encourage accession by third countries.

At the level of the G20 and G7, discussions on privacy and data flows have focused on operationalising the concept of 'data free flow with trust' (DFFT), originally proposed by Japan, which acknowledges that data protection and security can contribute to trust in the digital economy and facilitate data flows ([208]). The OECD plays a particularly important role in this context, by providing a forum for a DFFT Expert Community, bringing together a wide range of stakeholders (governments, regulators, industry, civil society, academia) to provide input on specific projects and questions related to DFFT. In addition, a significant result of the DFFT initiative, to which the Commission significantly contributed, is the adoption by the OECD of a Declaration on Government Access to Personal Data Held by Private Sector Entities, the first international instrument in this area. It contains a series of shared requirements to safeguard privacy when accessing personal data for national security and law enforcement purposes. Against the background of increasing worldwide recognition that confidence in data transfers is negatively affected by disproportionate government access, this Declaration is an important contribution to facilitating trusted data flows. The Commission will continue to encourage countries to join the Declaration, which is also open to non-OECD members.

The Commission is also engaging with different regional organisations and networks that shape common data protection safeguards. This concerns for instance ASEAN, the African Union, the Asia Pacific Privacy Authorities forum, the Ibero-American Data Protection Network and the Network of African Data Protection Authorities (NADPA – RADPD). The development of the above-mentioned EU-ASEAN Guide on model clauses is a concrete example of such fruitful cooperation.

Finally, the Commission maintains a dialogue with different international organisations, including to explore ways to further facilitate data flows between the EU and such organisations. As many organisations have modernised their data protection frameworks in recent years, or are in the process of doing so, new opportunities are also arising to exchange experience and best practices. In this respect, the annual workshops with international organisations and a dedicated taskforce on international data transfers organised by the European Data Protection Supervisor have proven to be particularly useful fora to exchange and explore concrete instruments for cooperation, including the exchange of personal data ([209]).

8 CONCLUSION

In the 6 years since the GDPR became applicable, it has empowered people by allowing them to have control over their data. It has also helped create a level playing field for businesses, and provided a cornerstone for the panoply of initiatives that are driving the digital transition in the EU.

To fully achieve the twin aims of the GDPR, namely- strong protection for individuals while ensuring the free flow of personal data within the EU and safe data flows outside the EU, there needs to be focus on:

([208]) See e.g. https://www.g7germany.de/resource/blob/974430/2062292/fbdb2c7e996205aee402386aae057c5e/2022-07-14-leaders-communique-data.pdf?download=1

([209]) https://www.edps.europa.eu/data-protection/our-work/edps-worldwide/data-protection-and-international-organisations_en

- a robust enforcement of the GDPR, starting with the swift adoption of the Commission's proposal on procedural rules to deliver quick remedies and legal certainty in cases affecting individuals across the EU;
- proactive support by data protection authorities to stakeholders in their compliance efforts, especially SMEs and small operators;
- a consistent interpretation and application of the GDPR across the EU;
- effective cooperation between regulators at both national and EU level to guarantee the consistent and coherent application of the growing body of EU digital rules;
- further advancing the Commission's international strategy on data protection.

To support the effective application of the GDPR and inform further reflections on data protection, several actions identified here are needed. The Commission will support and monitor their implementation also in view of the next report in 2028.

Developing effective cooperation structures

The European Parliament and the Council are invited to swiftly adopt the proposal on GDPR procedural rules.

The Board and data protection authorities are invited to:

- establish regular cooperation with other sectoral regulators on issues with an impact on data protection, in particular those established under new EU digital legislation, and actively participate in EU-level structures designed to facilitate cross-regulatory cooperation;
- make fuller use of the tools for cooperation provided by the GDPR, so that dispute resolution is used only as a last resort;
- implement more efficient and targeted working arrangements for guidelines, opinions and decisions and prioritise key issues in order to reduce the burden on data protection authorities and to respond more quickly to market developments.

Member States need to:

- ensure the effective and full independence of national data protection authorities;
- allocate sufficient resources to data protection authorities to enable them to fulfil their tasks, in particular by providing them with technical resources and expertise necessary to deal with emerging technologies and to fulfil new responsibilities under digital legislation;
- equip data protection authorities with the investigatory tools required for them to effectively use the enforcement powers provided by the GDPR;
- support the dialogue between data protection authorities and other national regulators, in particular those established under the new digital legislation.

The Commission will:

- actively support the swift adoption of the proposal on GDPR procedural rules by the co-legislators;
- continue to closely monitor the effective and full independence of national data protection authorities;
- build synergies and consistency between the GDPR and all legislation touching upon the processing of personal data based on experience and, if necessary, take appropriate actions to provide legal certainty;

- reflect on how to better address the need for structured and efficient cross-regulatory cooperation to guarantee the effective, consistent and coherent application of EU digital rules, while respecting the competence of data protection authorities for all questions concerning the processing of personal data.

Implementing and complementing the legal framework

Member States need to:

- ensure data protection authorities are consulted in a timely manner prior to the adoption of legislation on the processing of personal data.

The Commission will:

- continue to make use of all the tools at its disposal, including infringement procedures, to ensure that Member States comply with the GDPR;
- continue to support exchanges of views and national practices between Member States, including through the GDPR Member States Expert Group;
- pursue actions to ensure that children are protected, empowered and respected online;
- reflect on the possible next steps concerning the e-privacy Regulation proposal, including its relationship with the GDPR.

Supporting stakeholders

The Board and data protection authorities are invited to:

- engage in constructive dialogue with controllers and processors on compliance with the GDPR;
- further increase efforts to support the compliance of SMEs, by providing tailor-made guidance and tools, allaying any unfounded compliance concerns of SMEs that do not have processing of personal data as their core business, and accompanying them in their compliance efforts;
- support the implementation of effective compliance measures by businesses, such as certification and codes of conduct (including as tools for transfers), by engaging with stakeholders during the approval process, providing clear timelines for approvals, and, as pledged in the Board's 2024-2027 strategy, explaining to key groups of stakeholders how these tools can be used;
- ensure that national guidelines and the application of the GDPR at national level are consistent with the guidelines of the Board and the case law of the Court of Justice;
- resolve diverging interpretations of the GDPR between data protection authorities, including between authorities within the same Member State;
- provide guidelines that are concise, practical and accessible to the relevant audience, as pledged in the Board's 2024-2027 strategy;
- ensure earlier and more meaningful consultation on guidelines and opinions in order to better understand market dynamics and business practices, give adequate consideration to the feedback received, and factor in the concrete application of the interpretations adopted;
- complete the ongoing work on guidelines on children's data, scientific research, anonymisation, pseudonymisation and legitimate interest as a priority;
- step up awareness-raising activities, information and enforcement actions to ensure that data protection officers can fulfil their role under the GDPR.

The Commission will:

- continue to provide financial support for activities of data protection authorities that facilitate implementation of GDPR obligations by SMEs;
- use all available means to deliver expedient clarifications on matters of importance to stakeholders, including SMEs, in particular by requesting opinions of the Board.

Further developing the toolkit for data transfers and international cooperation

The Board and data protection authorities are invited to:

- complete the work on streamlining and shortening the approval process for binding corporate rules, as well as on updating the guidance on elements to be found in processor binding corporate rules;
- explore ways/tools to further assist data exporters in their compliance efforts in relation to the Schrems II requirements;
- explore further ways to ensure effective enforcement against operators established in third countries falling within the GDPR's territorial scope of application.

Member States need to:

- ensure the remaining signature and ratifications of the modernised Convention 108+ of the Council of Europe as soon as possible, with a view to allow its entry into force.

The Commission will:

- make further progress in ongoing adequacy talks, explore the further development of existing adequacy findings and pursue new adequacy dialogues with interested partners;
- support increased cooperation among the network of countries benefiting from adequacy decisions;
- finalise the work on additional standard contractual clauses, in particular for data transfers to data importers whose processing is directly subject to the GDPR and transfers under Regulation (EU) 2018/1725 for data transfers by EU institutions and bodies;
- cooperate with international partners on facilitating data flows on the basis of model contractual clauses;
- support ongoing reform processes in third countries on new or modernised data protection rules by sharing experience and best practices;
- engage with international and regional organisations such as the OECD and G7 to promote trusted data flows based on high data protection standards, including in the context of the Data Flow with Trust initiative;
- facilitate and support exchanges between European and international regulators, including through its Data Protection Academy;
- contribute to facilitating international enforcement cooperation between supervisory authorities, including through the negotiation of cooperation and mutual assistance agreements.