EUROPEAN
COMMISSION

Brussels, 24.6.2020
COM(2020) 264 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

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

{SWD(2020) 115 final}

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

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

1 DATA PROTECTION RULES AS A PILLAR OF CITIZENS' EMPOWERMENT AND EU'S APPROACH TO DIGITAL TRANSITION

This report is the first one on the evaluation and review of the General Data Protection Regulation[1] (hereafter 'GDPR'), in particular on the application and functioning of the rules on the transfer of personal data to third countries and international organisations and of the rules on cooperation and consistency, pursuant to Article 97 GDPR.

The GDPR, which applies since 25 May 2018, is at the heart of the EU framework[2] guaranteeing the fundamental right to data protection, as enshrined in the Charter of Fundamental Rights of the European Union (Article 8) and in the Treaties (Article 16 of the Treaty on the Functioning of the European Union, 'TFEU'). The GDPR strengthened data protection safeguards, provides individuals with additional and stronger rights, increased transparency, and ensures that all those that handle personal data under its scope of application are more accountable and responsible. It equips the independent data protection authorities with stronger and harmonised enforcement powers and sets up a new governance system. It also creates a level playing field for all companies operating in the EU market, regardless of where they are established, and it ensures the free flow of data within the EU, thereby strengthening the internal market.

The GDPR is an important component of the human-centric approach to technology and a compass for the use of technology in the twin green and the digital transitions that characterises EU policy-making. This has been highlighted more recently by the White Paper on Artificial Intelligence[3] and the Communication on a European Strategy for Data[4] (hereafter the Data Strategy) of February 2020.

In an economy increasingly based on the processing of data, including personal data, the GDPR is an essential tool to ensure that individuals have better control over their personal data and that these data are processed for a legitimate purpose, in a lawful, fair and transparent way. At the same time, the GDPR helps to foster trust-worthy

---

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC - OJ L 119, 4.5.2016, p. 1–88

[2] Following its incorporation in the European Economic Area (EEA) Agreement, the Regulation also applies to Norway, Iceland and Liechtenstein.

[3] https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

[4] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy

innovation, notably through its risk-based approach and principles such as privacy by design and by default. The Commission has proposed complementing the data protection and privacy legislative framework[5] by the e-Privacy Regulation[6], which is intended to replace the current e-Privacy Directive[7]. This proposal is currently being examined by the co-legislators and it is very important to ensure its rapid adoption.

As part of the Commission's key priorities of a "Europe fit for the digital age"[8] and the "European Green Deal"[9], new initiatives may be developed to empower citizens to play a more active role in the digital transition and in harnessing the use of digital tools to bring about a climate-neutral society and a more sustainable development. The GDPR sets a framework for these initiatives and ensures that they are designed to effectively empower individuals.

The Data Strategy[10] calls for the creation of a "single European data space", a genuine single market for data, as well as of ten sectoral common European data spaces that are relevant for the twin green and digital transitions[11]. For all these priorities, a clear and workable framework for safe data sharing and increased data availability is key. The Data Strategy also announced the intention of the Commission to explore in future legislation how to enable the use of data held in public databases for scientific research purposes in a manner compliant with the GDPR. The data spaces are to be supported by European cloud federation, providing data processing and cloud infrastructure services compliant with the GDPR. The GDPR ensures a high level of protection of personal data and a central role for individuals in all these data spaces while providing the necessary flexibility to accommodate different approaches.

The need to ensure trust and the demand for the protection of personal data are certainly not limited to the EU. Individuals around the world increasingly value the privacy and security of their data. As shown by a recent global survey[12], they consider

---

[5] This legislative framework also includes the Data Protection Law Enforcement Directive (Directive 2016/680) and the Data Protection Regulation for EU institutions and bodies (Regulation 2018/1725).

[6] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - COM/2017/010 final - 2017/03 (COD)

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

[8] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en

[9] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions - The European Green Deal - COM/2019/640 final

[10] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - A European strategy for data - COM/2020/66 final.

[11] These ten sectoral common European data spaces are for: health, industrial manufacturing, energy, mobility, agriculture, financial data, public administration, a common European data skills data space, a European Green Deal data space and a European Open Science Cloud.

[12] See e.g. Cisco's Consumer Privacy Study 2019 (https://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-series-2019-cps.pdf). According to this study that surveyed 2,600 consumers worldwide, a significant number of consumers have already taken action to protect their privacy, for example, by switching companies or providers because of their data policies or data sharing practices.

this an important factor that influences their buying decisions and their online behaviour. A growing number of companies have responded to this demand for privacy notably by voluntarily extending some of the rights and safeguards provided for in the GDPR to their non-EU based customers. Many businesses also promote respect for personal data as a competitive differentiator and a selling point on the global marketplace, by offering innovative products and services with novel privacy or data security solutions. Moreover, the increased ability for private and public sector actors to collect and process data on a large scale raises important and complex questions that increasingly place privacy at the centre of the public debate in different parts of the world.

The adoption of the GDPR has spurred other countries in many regions of the world to consider following suit. This is a truly global trend running from Chile to South Korea, from Brazil to Japan, from Kenya to India, and from California to Indonesia. The EU's leadership on data protection shows it can act as a global standard-setter for the regulation of the digital economy and has been welcomed by important voices of the international community such as UN Secretary General António Guterres who has noted how the GDPR has "*set an example* […] *inspiring similar measures elsewhere*" and "*urge[d] the EU and its Member States to continue to lead to shape the digital age and to be at the forefront of technological innovation and regulation*".[13]

The current COVID-19 pandemic crisis offers a vivid illustration of this globalisation of the privacy debate both during the crisis and as the world seeks to emerge from it. In the EU, several Member States took emergency measures in an effort to protect public health. The GDPR is clear in that any restriction must respect the essence of the fundamental rights and freedoms, and be a necessary and proportionate measure in a democratic society to safeguard a public interest, such as public health. As containment measures are being phased out, decision makers need to address the expectation of citizens that they are offered digital solutions which are trustworthy and which respect the rights to privacy and personal data protection.

In many countries built-in privacy protections such as voluntary signing up by users, data minimisation and security as well as the exclusion of geolocation, are considered essential to ensure the reliability and societal acceptance of data-driven solutions aimed at monitoring and containing the spread of the virus, calibrating public policy countermeasures, assisting patients or implementing exit strategies. In the EU, the data protection and privacy legislative framework[14] has proven to be a sufficiently flexible tool to allow practical solutions (e.g. tracing apps) to be developed while ensuring a high level of protection of personal data. In this context, on 16 April 2020, the Commission published guidance on apps supporting the fight against the pandemic in relation to data protection.[15]

---

[13] Address of the UN Secretary-General to the Italian Senate, 18 December 2019 (available at: https://www.un.org/press/en/2019/sgsm19916.doc.htm).

[14] This framework comprises, in addition to the GDPR, the ePrivacy Directive (Directive 2002/58/EC) that provides rules, among others, on accessing and storing information on the user's terminal equipment.

[15]Communication from the Commission Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection 2020/C 124 I/01 - C/2020/2523 - OJ C 124I , 17.4.2020, p. 1–9 On 16 April 2020 EU Members States, supported by the Commission, have developed an EU toolbox for the use of mobile applications for contact tracing and warning in response to the coronavirus

Protecting personal data is also instrumental in preventing the manipulation of citizens' choices, in particular via the micro-targeting of voters based on the unlawful processing of personal data, avoiding interference in democratic processes and preserving the open debate, the fairness and the transparency that are essential in a democracy. For this reason, in September 2018, the Commission published its guidance on the application of Union data protection law in the electoral context[16].

For this evaluation and review, the Commission took into account the contributions from the Council[17], the European Parliament[18], the European Data Protection Board (hereafter 'the Board')[19] and individual data protection authorities[20], the Multi-stakeholder expert Group[21] and other stakeholders, including through the feedback provided to the roadmap[22].

The general view is that two years after it started to apply, the GDPR has successfully, met its objectives of strengthening the protection of the individual's right to personal data protection and guaranteeing the free flow of personal data within the EU[23]. However a number of areas for future improvement have also been identified. Like most stakeholders and data protection authorities, the Commission is of the view that it would be premature at this stage to draw definite conclusions regarding the application of the GDPR. It is likely that most of the issues identified by Member States and stakeholders will benefit from more experience in applying the GDPR in the coming years. Nevertheless, this report highlights the challenges encountered so far in applying the GDPR and sets out possible ways to address them.

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

---

pandemic. This is part of a common coordinated approach to support the gradual lifting of confinement measures. https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf.

[16] Commission guidance on the application of Union data protection law in the electoral context A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018 - COM/2018/638 final.

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

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

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

[20] https://edpb.europa.eu/individual-replies-data-protection-supervisory-authorities_en

[21] The Multi-stakeholder expert group on the Regulation set up by the Commission involves civil society and business representatives, academics and practitioners: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537

[22] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12322-Report-on-the-application-of-the-General-Data-Protection-Regulation/feedback?p_id=7669437

[23] See for instance Council position and findings as well as the Board contribution.

2 MAIN FINDINGS

Enforcement of the GDPR and the functioning of the cooperation and consistency mechanisms

The GDPR set up an innovative governance system, based on independent data protection authorities in the Member States and their cooperation in cross-border cases and within the European Data Protection Board ('the Board'). The general view is that data protection authorities have made balanced use of their strengthened corrective powers, including warnings and reprimands, fines and temporary or definitive processing limitations[24]. The Commission notes that the authorities made use of administrative fines ranging from a few thousand euros to several million, depending on the gravity of the infringements. Other sanctions, such as bans on processing, may have an equally if not higher deterrent effect than fines. The ultimate objective of the GDPR is to change the culture and behaviour of all actors involved for the benefit of the individuals. More detailed information on the use of the corrective powers by data protection authorities is presented in the accompanying staff working document.

While it is still early to fully assess the functioning of the new cooperation and consistency mechanisms, data protection authorities developed their cooperation through the one-stop-shop mechanism[25] and through a large use of mutual assistance[26]. The one-stop-shop mechanism, which is a key asset of the internal market, is used to decide many cross-border cases[27]. Important decisions with cross-border dimension that will be subject to the one-stop-shop mechanism, are currently pending. These decisions, involving often multinational big tech companies, will have a substantial impact on individuals' rights in many Member States.

However, developing a truly common European data protection culture between data protection authorities is still an on-going process. Data protection authorities have not yet made full use of the tools the GDPR provides, such as joint operations that could lead to joint investigations. At times, finding a common approach meant moving to the lowest common denominator and as a result, opportunities to foster more harmonisation were missed[28].

Further progress is needed to make the handling of cross-border cases more efficient and harmonised across the EU, including from a procedural point of view, for instance on issues such as complaint handling procedures, the admissibility criteria for complaints, the duration of proceedings due to different timeframes or the absence of deadlines in the national administrative procedural law, the moment in the procedure where the right to be heard is granted, or the information and involvement of the complainants during the procedure. The reflection process launched by the Board in

[24] See point 2.1 of the Staff Working Document.
[25] If a company is processing data cross-border, the competent data protection authority is the one of the Member States where the company has its main establishment.
[26] See point 2.2 of the Staff working Document.
[27] Between 25 May 2018 and 31 December 2019, 141 draft decisions were submitted through the one-stop-shop procedure, out of which 79 resulted in final decisions.
[28] For instance the national lists of the kinds of processing operations which requires data protection impact assessment under Article 35 of the GDPR could have been better harmonised.

relation to this is welcomed, and the Commission is participating in these discussions[29].

The activities and the guidance of the Board are of key importance for the consistent further development of exchanges between the Board and stakeholders[30]. As of the end of 2019, the Board had adopted 67 documents, including 10 new guidelines[31], and 43 opinions[32]. Stakeholders generally welcome the guidelines from the Board and request additional ones on key concepts of the GDPR, but also point to inconsistencies between the national guidance and the Board guidelines. They underline the need for more practical advice, in particular more concrete examples, and the need for data protection authorities to be equipped with the necessary human, technical and financial resources to effectively carry out their tasks.

The Commission consistently stressed the obligation for Member States to allocate sufficient human, financial and technical resources to national data protection authorities[33]. Most authorities benefitted from an increase in staff and budget between 2016 and 2019[34], with the Irish, Dutch, Icelandic, Luxembourgish and Finnish authorities having benefitted from the largest relative increases in staff. Given that the largest big tech multinationals are established in Ireland and Luxembourg, the data protection authorities of these countries act as lead authorities in many important cross-border cases and may need larger resources than their population would otherwise suggest. However, the situation is still uneven between Member States and is not yet satisfactory overall. Data protection authorities play an essential role in ensuring that the GDPR is enforced at national level and that the cooperation and consistency mechanisms within the Board functions effectively, including in particular the one-stop-shop mechanism for cross-border cases. Member States are therefore called upon to provide them with adequate resources as required by the GDPR[35].

Harmonised rules but still a degree of fragmentation and diverging approaches

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

[29] See point 2.2 of the Staff Working Document.
[30] In particular business and civil society representatives. See point 2.3 of the Staff Working Document.
[31] They are in addition to the 10 guidelines which were adopted by the Article 29 Working Party in the run-up to the entry into application of the Regulation and endorsed by the Board. The Board has also adopted 4 additional guidelines between January and the end of May 2020, and updated an existing one.
[32] 42 of these opinions were adopted under Article 64 of the GDPR and one was adopted under Article 70(1)(s) of the GDPR and concerned the adequacy decision with respect to Japan.
[33] Communication from the Commission to the European Parliament and the Council, Data Protection as a trust-enabler in the EU and beyond – taking stock – COM(2019) 374 final, 24.7.2019
[34] Overall there has been a 42% increase in staff and 49% in budget for national data protection authorities taken together in the EEA between 2016 and 2019.
[35] See point 2.4 of the Staff Working Document.

Slovenia[36] has been requested to provide clarifications to the Commission on the finalisation of that process[37].

The GDPR provides for a consistent approach for data protection rules throughout the EU. However, it requires Member States to legislate in some areas[38] and provides them with the possibility to further specify the GDPR in others[39]. As a result, there is still a degree of fragmentation which is notably due to the extensive use of facultative specification clauses. For instance, the difference between Member States in the age of children consent in relation to information society services creates uncertainty to children and their parents as to the application of their data protection rights in the Single Market. This fragmentation also creates challenges to conducting cross-border business, innovation, in particular as regards new technological developments and cybersecurity solutions. For the effective functioning of the internal market and to avoid unnecessary burden on companies, it is also essential that national legislation does not go beyond the margins set by the GDPR or introduces additional requirements when there is no margin.

A specific challenge for national legislation is the reconciliation of the right to the protection of personal data with freedom of expression and information, and the proper balancing of these rights. Some national legislations lay down the principle of precedence of freedom of expression, whilst others lay down the precedence of the protection of personal data and exempt the application of data protection rules only in specific situations, such as where a person with public status is concerned. Finally, other Member States provide for a certain balancing by the legislator and/or or a case-by-case assessment as regards derogations from certain provisions of the GDPR.

The Commission will continue its assessment of national legislation. The reconciliation must be provided for by law, respect the essence of those fundamental rights, and be proportional and necessary[40]. Data protection rules (as well as their interpretation and application) should not affect the exercise of freedom of expression and information, for instance by creating a chilling effect or putting pressure on journalists to disclose their sources. The balancing of these two rights by national laws should be framed by the case law of the Court of Justice and of the European Court of Human Rights[41].

Member State legislation follows different approaches when implementing derogations from the general prohibition for processing special categories of personal data, as regards the level of specification and safeguards, including for health and research purposes. To address this issue, the Commission is, as a first step, mapping the different approaches of Member States[42] and will, as a following step, support the

[36] Most recently through a letter from Commissioner Reynders in March 2020.
[37] It has to be noted that the national data protection authority in Slovenia is established on the basis of the current national data protection law and supervising the application of the GDPR in that Member State.
[38] See point 3.1 of the Staff Working Document.
[39] See point 3.2 of the Staff Working Document.
[40] Article 52(1) of the Charter.
[41] See under point 3.1 of the Staff Working Document: Reconciliation of the right to the protection of personal data with freedom of expression and information.
[42] The Commission has launched a study on the "Assessment of the Member States' rules on health data in the light of GDPR", Chafea/2018/Health/03, specific contract No 2019 70 01.

establishment of code(s) of conducts that would contribute to a more consistent approach in this area and make the cross-border processing of personal data easier[43]. In addition, the Board's future guidelines on the use of personal data in the field of scientific research will contribute to a harmonised approach. The Commission will provide input to the Board in particular in relation to health research, including in the form of concrete questions and analysis of specific scenarios which it has received from the research community.

Empowering individuals to control their data

According to a Fundamental Rights Survey[44], 69% of the EU population above the age of 16 have heard about the GDPR and 71% of people in the EU know about their national data protection authority.

Individuals are increasingly aware of their rights: the rights of access, rectification, erasure, and portability of their personal data, the right to object to a processing, as well as enhanced transparency. The GDPR strengthened procedural rights, encompassing the right to lodge a complaint with a data protection authority, including through representative actions, and to judicial redress. Individuals are increasingly using these rights, but there is a need to facilitate their exercise and their full enforcement. The reflections being led by the Board will clarify and further facilitate the exercise of individual rights, while the proposed Directive on representative actions[45], once adopted, is expected to enable individuals to bring collective actions in all Member States and will lower the costs of cross-border actions.

The right to data portability has a clear potential, still not fully used, to put individuals at the centre of the data economy by enabling them to switch between different service providers, to combine different services, use other innovative services and to choose the most data protection-friendly services. This will, indirectly, foster competition and support innovation. Unlocking this potential is one of the Commission's priorities, in particular since, with the increasing use of 'Internet of Things' devices, more and more data are generated by consumers, who risk being faced with unfair practices and 'lock-in' effects. Portability could yield significant benefits in relation to health and wellness, reduced environmental footprint and access to public and private services, higher productivity in manufacturing and increased product quality and safety.

The Data Strategy emphasised the need to address difficulties such as lack of standards enabling the provision of data in a machine-readable format, to increase the effective use of the right to data portability, which is currently limited to a few sectors (e.g. banking and telecommunications). This could be done notably through the design of appropriate tools, standardised format and interfaces[46]. This increased use

[43] See actions announced in the European Strategy for Data, page 30.

[44] European Union Agency for Fundamental Rights (FRA) (2020): Fundamental Rights Survey 2019. Data protection and technology: https://fra.europa.eu/en/publication/2020/fundamental-rights-survey-data-protection

[45] The proposed Directive on representative actions for the protection of the collective interests of consumers (COM/2018/0184 final - 2018/089 (COD)), once adopted, is expected to strengthen the framework for representative actions also in the field of data protection.

[46] Those tools may include consent management tools, and personal information management apps.

could also be achieved notably by mandating technical interfaces and machine-readable formats allowing portability of data in real-time. An increased use of the right to portability could, amongst other things, make it easier for individuals to allow the use of their data for the public good (for instance to foster research in the health sector), if they wish to do so ('data altruism'). In preparation of the Digital Services Act package[47], the Commission will explore more broadly the role of data and data-related practices in the platform ecosystem.

Opportunities and challenges for organisations, in particular small and medium-sized enterprises

The GDPR, together with the Free Flow of Non-Personal Data Regulation[48] offers opportunities to companies by fostering competition and innovation, ensuring the free flow of data within the EU and creating a level playing field with companies established outside the EU[49]. The right to portability, coupled with an increasing number of individuals in search of more privacy-friendly solutions, have the potential to lower the barriers to entry for businesses and open the possibilities for growth based on trust and innovation. Some stakeholders report that the application of the GDPR is challenging especially for small and medium sized enterprises (SMEs). According to the risk-based approach, it would not be appropriate to provide derogations based on the size of the operators, as their size is not in itself an indication of the risks the processing of personal data that it undertakes can create for individuals. Several data protection authorities have provided practical tools to facilitate the implementation of the GDPR by SMEs with low risk processing activities. These efforts should be intensified and widespread, preferably within a common European approach in order not to create barriers to the Single Market.

Data protection authorities have developed a number of activities to help SMEs comply with the GDPR, for instance through the provision of templates for processing contracts and records for processing activities, seminars and hotlines for consultation. A number of these initiatives benefited from EU funding[50]. Further activities should be considered to facilitate the application of the GDPR for SMEs.

The GDPR makes a toolbox available to all types of companies and organisations to help them demonstrate compliance, such as codes of conduct, certification mechanisms and standard contractual clause. This toolbox should be used to its full extent. SMEs stress in particular the importance and usefulness of codes of conduct which are tailored to their situation and which do not entail disproportionate costs. As

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

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

[49] See point 5 of the Staff Working Document. See also COM/2019/250 final Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union, explaining the rules governing the processing of mixed datasets, composed of both personal and non-personal data, making it practical for businesses, including SMEs.

[50] The Commission provided financial support through three waves of grants, for a total of EUR 5 million, with the two most recent ones specifically aimed at supporting national data protection authorities in their efforts to reach out to individuals and small and medium-size enterprises: https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules/eu-funding-supporting-implementation-gdpr_en. An additional EUR 1 million will be allocated in 2020.

regards certification schemes, security (including cybersecurity) and data protection by design are key elements to be considered under the GDPR and would benefit from a common and ambitious approach throughout the EU. The Commission is currently working on standard contractual clauses between controllers and processors[51], building on the on-going work on the modernisation of the standard contractual clauses for international transfers[52].

The application of the GDPR to new technologies

The GDPR, having been conceived in a technology neutral way, is based on principles, and is therefore designed to cover new technologies as they develop.

It is seen as an essential and flexible tool to ensure that the development of new technologies is in compliance with fundamental rights. The data protection and privacy legislative framework proved its importance and flexibility during the COVID-19 crisis, notably in relation to the design of the tracing apps and other technological solutions to fight the pandemic. Future challenges lie ahead in clarifying how to apply the proven principles to specific technologies such as artificial intelligence, blockchain, Internet of Things or facial recognition which require a monitoring on a continuous basis. The Commission White Paper on Artificial Intelligence[53], for instance, opened up a public debate on the specific circumstances, if any, which might justify the use of artificial intelligence for remote biometric identification purposes (such as facial recognition) in public places, and on common safeguards. In this respect, data protection authorities should be ready to accompany technical design processes early on.

Moreover, strong and effective enforcement of the GDPR vis-à-vis large digital platforms and integrated companies, including in areas such as online advertising and micro-targeting, is an essential element for protecting individuals.

Developing a modern international data transfer toolbox

The GDPR offers a modernised toolbox to facilitate the transfer of personal data from the EU to a third country or international organisation, while ensuring that the data continues to benefit from a high level of protection. In the past two years, the Commission stepped up its work to harness the full potential of the tools available under the GDPR.

This has included actively engaging with key partners with a view to reaching an "adequacy decision". The effect of such a decision is to enable the safe and free flow of personal data to the concerned third country without the need for the data exporter to provide further safeguards or obtain any authorisation. In particular, the EU-Japan mutual adequacy decisions, which entered into force in February 2019, created the world's largest area of free and safe data flows. In addition, the adequacy process with the Republic of Korea is at an advanced stage and exploratory talks are ongoing with other important partners in Asia and Latin America.

[51] Under Article 28 GDPR
[52] Under Article 46 GDPR.
[53] White Paper on Artificial Intelligence - A European approach to excellence and trust - COM/2020/65 final.

Adequacy also plays an important role in the context of the future relationship with the United Kingdom, provided that the applicable conditions are met. It constitutes an enabling factor for trade, including digital trade, and an essential prerequisite for a close and ambitious cooperation in the area of law enforcement and security. Moreover, a high degree of convergence in data protection is an important element for ensuring a level playing field between two so closely integrated economies. In line with the Political Declaration on the Future Relationship between the EU and the UK, the Commission is currently carrying out an adequacy assessment under both the GDPR and the Data Protection Law Enforcement Directive[54].

As part of the first evaluation of the GDPR, the Commission is also required to review the adequacy decisions that were adopted under the former rules[55]. The Commission services have engaged in an intense dialogue with each of the 11 concerned third countries and territories[56] to assess how their data protection systems have evolved since the adoption of the adequacy decision and whether they meet the standard set by the GDPR. The need to ensure the continuity of such decisions, as a key tool for trade and international cooperation, is one of the factors that has prompted several of these countries and territories to modernise and strengthen their privacy laws. Additional safeguards are being discussed with some of these countries and territories to address relevant differences in protection. However, given that the Court of Justice in a judgment to be delivered on 16 July may provide clarifications that could be relevant for certain elements of the adequacy standard, the Commission will report separately on the evaluation of the existing adequacy decisions after the Court of Justice has handed down its judgment in that case[57].

Beside its adequacy work, the Commission is working on a comprehensive modernisation of standard contractual clauses, to update them in light of new requirements introduced by the GDPR. The aim is to better reflect the realities of processing operations in the modern digital economy and consider the possible need, including in light of the upcoming case law of the Court of Justice[58], to further clarify certain safeguards. These clauses represent by far the most widely used data transfer mechanism, with thousands of EU companies relying on them in order to provide a wide range of services to their clients, suppliers, partners and employees.

The Board has also played an active role in developing the international aspects of the GDPR. This includes updating guidance on existing transfer mechanisms, such as binding corporate rules and so-called 'derogations', as well as developing the legal

[54] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89–131.

[55] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31–50.

[56] These countries and territories are: Andorra, Argentina, Canada, Faeroe Islands, Guernsey, Jersey, Isle of Man, Israel, New Zealand, Switzerland and Uruguay.

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

[58] See Schrems II case.

infrastructure for the use of new tools introduced by the GDPR, i.e. codes of conduct and certification.

To allow stakeholders to make full use of the GDPR transfer toolbox, it is important that the Board intensifies its ongoing work on the various transfer mechanisms, including by further streamlining the approval process for binding corporate rules, finalising the guidance on codes of conduct and certification as tools for transfers, and clarifying the interplay between the rules on international data transfers (Chapter V) with the GDPR territorial scope of application (Article 3).

Another important aspect of the international dimension of EU data protection rules is the GDPR's extended territorial scope, which also covers the processing activities of foreign operators that are active in the EU market. To ensure effective compliance with the GDPR and a true level playing field, it is essential that this extension is appropriately reflected in the enforcement action by the data protection authorities. They should, in particular, involve, where necessary, the controller's or processor's representative in the EU, who can be addressed in addition to or instead of the company based outside the EU. This approach should be pursued more vigorously in order to send a clear message that the lack of an establishment in the EU does not relieve foreign operators of their responsibilities under the GDPR.

Promoting convergence and international cooperation in the area of data protection

The GDPR has already emerged as a key reference point at international level and acted as a catalyst for many countries around the world to consider introducing modern privacy rules. This trend towards global convergence is a very positive development that brings new opportunities to better protect individuals in the EU when their data is transferred abroad while, at the same time, facilitating data flows.

Building on this trend, the Commission has intensified its dialogue in a number of bilateral, regional and multilateral fora to foster a global culture of respect for privacy and develop elements of convergence between different privacy systems. In its efforts, the Commission has relied and will continue to count on the active support of the European External Action Service and the network of EU delegations in third countries and missions to international organisations. This has also allowed for greater consistency and complementarity between different aspects of the external dimension of EU policies – from trade to the new EU-Africa partnership. The G20 and G7 have also recently recognised the contribution of data protection to trust in the digital economy and data flows, in particular through the concept of 'Data Free Flow with Trust' originally proposed by the Japanese G20 Presidency.[59] The Data Strategy highlights the Commission's intention to continue promoting data sharing with trusted partners while fighting against abuses such as disproportionate access of (foreign) public authorities to personal data.

While promoting convergence of data protection standards at international level, as a way to facilitate data flows and thus trade, the Commission is also determined to tackle digital protectionism, as recently highlighted in the Data Strategy.[60] To that

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

[60] Data Strategy, p. 23.

end, it has developed specific provisions on data flows and data protection in trade agreements[61] which it systematically tables in its bilateral – most recently with Australia, New Zealand, and the UK – and multilateral negotiations such as the current WTO e-commerce talks[62]. These horizontal provisions rule out unjustified restrictions, such as forced data localisation requirements, while preserving the regulatory autonomy of the parties to protect the fundamental right to data protection.

Synergies between trade and data protections instruments should thus be further explored to ensure free and safe international data flows that are essential for the business operations, competitiveness and growth of European companies, including SMEs, in the increasingly digitalised economy.

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

Finally, at a time when privacy compliance issues or data security incidents may affect large numbers of individuals simultaneously in several jurisdictions, cooperation 'on the ground' between European and international regulators should be further strengthened. In particular, this requires appropriate legal instruments to be developed for closer forms of cooperation and mutual assistance, including by allowing the necessary exchanges of information in the context of investigations. It is also in this spirit that the Commission is setting up a 'Data Protection Academy', a platform where EU and foreign data protection authorities would share knowledge, experience and best practices to facilitate and support cooperation between privacy enforcers.

3 WAY FORWARD

To meet the full potential of the GDPR, it is important to create a harmonised approach and a European common culture of data protection, and to foster a more efficient and harmonised handling of cross-border cases. This is expected by people and businesses and constitutes an essential objective of the reform of EU data protection rules. It is equally important to ensure that all tools available in the GDPR are used fully to ensure an efficient application for individuals and businesses.

---

[61] See text of horizontal provisions for cross-border data flows and for personal data protection (in EU trade and investment agreements): https://trade.ec.europa.eu/doclib/docs/2018/may/tradoc_156884.pdf

[62] 84 WTO Members are now engaged in plurilateral negotiations on e-commerce, further to a Joint Statement Initiative adopted by Ministers on 25 January 2019 in Davos. As part of this process, the EU tabled its text proposal on future rules and obligations on e-commerce on 3 May 2019. The proposal includes horizontal provisions on data flows and personal data protection: https://trade.ec.europa.eu/doclib/docs/2019/may/tradoc_157880.pdf.

The Commission will continue its bilateral exchanges with Member States on the implementation of the GDPR and, where necessary, will continue to use all the tools at its disposal to foster compliance by Member States with their obligations under the GDPR.

Given the ongoing assessment of national legislation, the short period of practical experience since the GDPR has become applicable, and the fact that sector-specific legislation is still being revised in many Member States, it is still too soon to draw definitive conclusions on the existing level of fragmentation. As regards the possible conflict of laws due to the implementation by Member States of specification clauses, it is first necessary to better understand the consequences for controllers and processors[63].

When following-up on these issues, the relevant case law of national courts and the Court of Justice helps to create a consistent interpretation of data protection rules. National courts have recently issued judgements invalidating provisions in national laws which depart from the GDPR[64].

As regards the international dimension, the Commission will continue to focus on promoting convergence of data protection rules as a way to ensure safe data flows. This includes various forms of 'upstream' work, for instance in the context of ongoing reforms for new or updated data protection laws, or the push for the 'Data Free Flow with Trust' concept in multilateral fora. It also covers various adequacy dialogues and the modernisation and expansion of our transfer toolbox through updating the standard contractual clauses and laying the groundwork for certification mechanisms. This work also includes international negotiations, such as in the area of cross-border access to electronic evidence, to ensure that data transfers will take place with appropriate data protection safeguards. Finally, by engaging in negotiations on international cooperation and mutual assistance between data protection enforcers, the Commission will strive to bring convergence 'from the books to the ground'.

Based on this evaluation of the application of the GDPR since May 2018, the actions listed below have been identified as necessary to support its application. The Commission will monitor their implementation also in view of the forthcoming evaluation report in 2024.

Implementing and complementing the legal framework

Member States should

- complete the alignment of their sectoral laws to the GDPR;
- consider limiting the use of specification clauses which might create fragmentation and jeopardise the free flow of data within the EU;
- assess whether national law implementing the GDPR is in all circumstances within the margins provided for Member State legislation.

The Commission will

[63] Cf. Council position and findings on the application of the GDPR.

[64] This has been the case in Germany and in Spain, or, in Austria, closing a gap in the national legislation.

- pursue bilateral exchanges with Member States on the compliance of national laws with the GDPR, including on the independence and resources of national data protection authorities; make use of all the tools at its disposal, including infringement procedures, to ensure that Member States comply with the GDPR;
- support further exchanges of views and national practices between Member States on topics which are subject to further specification at national level so as to reduce the level of fragmentation of the single market, such as processing of personal data relating to health and research, or which are subject to balancing with other rights such as the freedom of expression;
- support a consistent application of the data protection framework in relation to new technologies to support innovation and technological developments;
- use the GDPR Member States Expert Group (established during the transitory phase before the GDPR became applicable) to facilitate discussions and sharing of experience between Member States and with the Commission;
- explore whether, in the light of further experience and relevant case-law, proposing possible future targeted amendments to certain provisions of the GDPR might be appropriate, in particular regarding records of processing by SMEs that do not have the processing of personal data as their core business (low risk)[65], and the possible harmonisation of the age of children consent in relation to information society services.

Making the new governance system deliver its full potential

The Board and data protection authorities are invited to

- develop efficient arrangements between data protection authorities regarding the functioning of the cooperation and consistency mechanisms, including on procedural aspects, building on the expertise of its members and by strengthening the involvement of its secretariat;
- support harmonisation in applying and enforcing the GDPR using all means at its disposal, including by further clarifying key concepts of the GDPR, and ensuring that national guidance is fully in line with guidelines adopted by the Board;
- encourage the use of all tools provided for in the GDPR to ensure that it is applied consistently;
- step up cooperation among data protection authorities, for instance by conducting joint investigations.

The Commission will

- continue to closely monitor the effective and full independence of national data protection authorities;

[65] Article 30(5) GDPR.

- encourage cooperation between regulators (in particular in fields such as competition, electronic communications, security of network and information systems and consumer policy);
- support the reflection within the Board on the procedures applied by the national data protection authorities in order to improve the cooperation on the cross-border cases.

Member States shall

- allocate resources to data protection authorities that are sufficient for them to perform their tasks.

Supporting stakeholders

The Board and data protection authorities are invited to

- adopt further guidelines which are practical, easily understandable, and which provide clear answers and avoid ambiguities on issues related to the application of the GDPR, for example on processing children's data and data subject rights, including the exercise of the right of access and the right to erasure, consulting stakeholders in the process;
- review the guidelines when further clarifications are necessary in the light of experience and developments including in the case law of the Court of Justice;
- develop practical tools, such as harmonised forms for data breaches and simplified records of processing activities, to help low-risk SMEs meeting their obligations.

The Commission will

- provide standard contractual clauses both for international transfers and the controller/processor-relationship;
- provide for tools clarifying/supporting the application of data protection rules to children[66];
- in line with the Data Strategy, explore practical means to facilitate increased use of the right to portability by individuals, such as by giving them more control over who can access and use machine-generated data;
- support standardisation/certification in particular on cybersecurity aspects through the cooperation between the European Union Agency for Cybersecurity (ENISA), the data protection authorities and the Board;
- when appropriate, make use of its right to request the Board to prepare guidelines and opinions on specific issues of importance to stakeholders;
- when necessary provide guidance, while fully respecting the role of the Board;

[66] Commission project on age identification tools – pilot project to demonstrate an interoperable technical infrastructure for child protection, including age-verification and parental consent. This is expected to support the implementation of the child protection mechanisms based on existing EU legislation relevant for children protection online.

- support the activities of data protection authorities that facilitate implementation of GDPR obligations by SMEs, through financial support, especially for practical guidance and digital tools that can be replicated in other Member States.

Encouraging innovation

The Commission will

- monitor the application of the GDPR to new technologies, also taking into account of possible future initiatives in the field of artificial intelligence and under the Data Strategy;
- encourage, including through financial support, the drafting of EU codes of conduct in the area of health and research;
- closely follow the development and the use of apps in the context of the COVID-19 pandemic.

The Board is invited to

- issue guidelines on the application of the GDPR in the area of scientific research, artificial intelligence, blockchain, and possible other technological developments;
- review the guidelines when further clarifications are necessary in the light of technological development.

Further developing the toolkit for data transfers

The Commission will

- pursue adequacy dialogues with interested third countries, in line with the strategy set out in its 2017 Communication 'Exchanging and Protecting Personal Data in a Globalised World', including where possible by covering data transfers to criminal law enforcement authorities (under the Data Protection Law Enforcement Directive) and other public authorities; this includes finalisation of the adequacy process with the Republic of Korea as soon as possible;
- finalise the ongoing evaluation of the existing adequacy decisions and report to the European Parliament and the Council;
- finalise the work on the modernisation of the standard contractual clauses, with a view to updating them in light of the GDPR, covering all relevant transfer scenarios and better reflecting modern business practices.

The Board is invited to

- further clarify the interplay between the rules on international data transfers (Chapter V) with the GDPR's territorial scope of application (Article 3);
- ensure effective enforcement against operators established in third countries falling within the GDPR's territorial scope of application, including as regards the appointment of a representative where applicable (Article 27);

- streamline the assessment and eventual approval of binding corporate rules with a view to speed up the process;
- complete the work on the architecture, procedures and assessment criteria for codes of conduct and certification mechanisms as tools for data transfers.

Promoting convergence and developing international cooperation

The Commission will

- support ongoing reform processes in third countries on new or modernised data protection rules by sharing experience and best practices;
- engage with African partners to promote regulatory convergence and support capacity-building of supervisory authorities as part of the digital chapter of the new EU-Africa partnership;
- assess how cooperation between private operators and law enforcement authorities could be facilitated, including by negotiating bilateral and multilateral frameworks for data transfers in the context of access by foreign criminal law enforcement authorities to electronic evidence, to avoid conflicts of law while ensuring appropriate data protection safeguards;
- engage with international and regional organisations such as the OECD, ASEAN or the G20 to promote trusted data flows based on high data protection standards, including in the context of the Data Flow with Trust initiative;
- set up a 'Data Protection Academy' to facilitate and support exchanges between European and international regulators;
- promote international enforcement cooperation between supervisory authorities, including through the negotiation of cooperation and mutual assistance agreements.