FIT FOR FUTURE Platform Opinion

Topic title	General Data Protection Rules
	AWP 2023
	Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) *Legal reference*
Date of adoption	28 November 2023
Opinion reference	2023/8
Policy cycle reference	☐ Contribution to ongoing legislative process *Commission work programme reference*
	☑ Contribution to the (ongoing) evaluation process *Title of the (ongoing) evaluation* The General Data Protection Regulation (GDPR) (EU) 2016/679 is applicable since May 2018, and lays down rules relating to the protection of natural persons with regard to the processing of personal data. It applies to personal data processing by natural and legal persons, both in the public and private sector, when such processing takes place by automated means and by other means if data forms part of a filing system. The Regulation includes principles relating to the processing of personal data that must be implemented and data subject's rights that must be respected and facilitated. It also empowers Member State-level data protection authorities to monitor and enforce the GDPR and to apply corrective powers, including issuing administrative fines. The GDPR replaced the 1995 Data Protection Directive, which created a country-by-country patchwork of data protection laws. Any natural or legal person that processes the personal data of people in the EU must comply with the GDPR, regardless of where such natural or legal person is established.

	In accordance with Art. 97 of the GDPR, the Commission submits to other institutions a report on the evaluation and review of the regulation. The first report was submitted in June 2020. The next evaluation is due in 2024.	
	☐ Included in Annex VI of the Task force for subsidiarity and proportionality	
	☐ Other	
Have your say: Simplify!	*No relevant suggestions on this topic have been received from the public.*	
Commission follow up	REFIT Scoreboard:	Personal data protection
	Annual Burden Survey:	The EU's efforts to simplify legislation (2023)

SUGGESTIONS SUMMARY

Suggestion 1: Issue standardised tools: make compliance easier
Suggestion 2: Encourage the improvement of cross-border cooperation and enforcement
Suggestion 3: Level the field: promote better enforcement against controllers and processors outside of the EU
Suggestion 4: Support, encourage and promote the use of codes of conduct

SHORT DESCRIPTION OF THE LEGISLATION ANALYSED

The General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, in application since May 2018, regulates the processing[1] by an individual, a company or an organisation of personal data relating to natural persons. It doesn't apply to the processing of personal data of deceased persons or of legal persons. Through a set of common EU-wide rules, it aims to protect individuals when their data is being processed by the private sector and the public sector[2]. It allows individuals to better control their personal data. For example, it provides for an easier access to an individual's own data (e.g. providing more information on how that data is processed, ensuring that that information is available in a clear and understandable way, etc.), a new right to data portability making it easier to transmit personal data between service providers, a clearer right to erasure (right to be forgotten) and a right to know when one's personal data has been breached.

By creating a level playing field for all companies operating in the EU internal market and its technology-neutral, innovation-friendly approach, the GDPR also modernises and unifies rules, allowing businesses to reduce red tape and to benefit from greater consumer trust. More specifically, the GDPR includes a one-stop-shop mechanism where businesses only have to deal with one single supervisory authority (in the EU Member State where the business has its main establishment) while the relevant supervisory authorities cooperate in the framework of the European Data Protection Board for cross-border cases. The GDPR scrapped as well most notification obligations and the costs associated with these. One of its aims is to remove obstacles that affect the free flow of personal data within the EU.

A data protection officer – a person appointed to facilitate compliance with the GDPR – has to be designated by public authorities as well as by businesses that perform regular and systematic monitoring of individuals on a large scale, or whose core activity is the processing of special categories of data or personal data relating to criminal convictions and offences or where required by Union or Member State law.

Companies based outside the EU must apply the GDPR when offering services or goods to, or when monitoring the behaviours of, individuals within the EU.

[1] Processing covers a wide range of operations performed on personal data, including by manual or automated means. It includes inter alia the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data;
[2] The processing of data by the relevant authorities for law-enforcement purposes is subject to the data protection law enforcement directive (LED) instead;

The GDPR offers various instruments to transfer data outside the EU, including adequacy decisions adopted by the European Commission where the non-EU country offers an adequate level of protection, pre-approved (standard) contractual clauses, binding corporate rules, codes of conduct and certification.

Finally, it also establishes a system of completely independent supervisory authorities in charge of monitoring and enforcing compliance.

Sources:
General Data Protection Regulation (GDPR) Regulation (EU) 2016/679

PROBLEM DESCRIPTION

Existing evidence suggest the following issues:

In June 2020 the Commission presented its first report on the evaluation and review of the 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. Amongst others, the report concluded that two years after it started to apply, the GDPR has successfully met its objectives. However, a number of areas for future improvement have also been identified although it was deemed premature to draw definite conclusions regarding the application of the GDPR. The next evaluation is due in 2024.

The one-stop-shop mechanism, which some view as a key asset of the internal market, is used to decide cross-border cases. The first evaluation report drew preliminary conclusions that the 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. The handling of cross-border cases calls for a more efficient and harmonised approach and the effective use of all cooperation tools provided in the GDPR. Since 2020, the European Data Protection Board, which has the task of ensuring the consistent application of the GDPR, has developed numerous guidelines which contribute to a more harmonised application and ensure a more efficient enforcement by data protection supervisory authorities[3].

Furthermore, in line with CWP 2023, the Commission has proposed to harmonise some aspects of the administrative procedure applied by data protection authorities when enforcing the GDPR in cross-border cases. The Commission's aim is to support the smooth functioning of the GDPR cooperation mechanism in accordance with the initial objective of the GDPR to provide a quick

[3] As examples of guidelines relevant in cross-border cases can be mentioned the following: guidelines 8/2022 on identifying a controller or processor's lead supervisory authority Guidelines 8/2022 on identifying a controller or processor's lead supervisory authority | European Data Protection Board (europa.eu); guidelines 9/2020 on relevant and reasoned objection Guidelines, Recommendations, Best Practices | European Data Protection Board (europa.eu); guidelines 3/2021 on the application of Article 65(1)(a) GDPR (dispute resolution mechanism between DPAs in cross-border cases) Guidelines 03/2021 on the application of Article 65(1)(a) GDPR | European Data Protection Board (europa.eu); guidelines 2/2022 on the application of Article 60 GDPR (cooperation procedure between the lead supervisory authority and other supervisory authorities concerned) Guidelines 02/2022 on the application of Article 60 GDPR | European Data Protection Board (europa.eu);

and effective remedy for the data subject. This initiative seeks to address many of the procedural issues referred to in the first evaluation report, taking into account the "wish list" of the European Data Protection Board as well as the feedback received from stakeholders and through the *Call for Evidence*.

The GDPR requires Member States to legislate in some areas and provides them with the possibility to further specify the GDPR in others. This necessarily results in some differences between the Member States in the levels of data subject protection[4]. This situation can also create challenges, including burdens, to conducting cross-border business, innovation, in particular as regards new technological developments and cybersecurity solutions.

It is also important to note that—not unlike SMEs—municipal governments and local administrations also encounter difficulties with GDPR compliance when attempting to develop and implement cross-border, data-based citizen services. In practice, public administration systems in the member states vary significantly, and national Data Protection Authorities often lack the capacity to offer case-specific advice to all of their municipalities and local governments. The fragmentation of the GDPR's implementation, the lack of European guidelines on the interpretation of regulation and management of everyday procedures, and the lack of common supporting tools are the main obstacles to a fully GDPR-compliant digital transformation of local administrations.

In terms of awareness of their rights, EU citizens are increasingly informed and increasingly use their rights although there is a need to facilitate their exercise and their full enforcement, through addressing 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). These issues have been addressed at last to some degree through various initiatives under the Data Strategy, such as the Commission proposal for a Data Act.

Some stakeholders reported that the application of the GDPR has been challenging especially for SMEs. One specific issue raised was the required documentation of processing activities, which is considered by SMEs and small associations as a cumbersome administrative burden, even if related efforts for complying with that obligation should not be over-estimated since, where the core business of SMEs does not involve the processing of personal data, such documentation may be simple and not burdensome. Several data protection authorities have developed a number of activities and provided practical tools (e.g., templates for processing contracts and sample records for processing activities, seminars and hotlines for consultation) to facilitate the implementation of the GDPR by SMEs with low-risk processing activities. The Commission has supported this work financially through action grants under the Rights, Equality and Citizenship Programme and, since 2021, through the Citizens, Equality and Rights

[4] 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 while a company providing information society services to minors across the EU has to distinguish between the ages of potential users, depending in which Member State they reside; its first report on the evaluation and review of the GDPR, the Commission committed to exploring 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 these areas;

and Values Programme[5]. Various industry associations too have made efforts to raise awareness and inform their members, for instance through conferences and seminars, providing businesses with information on available guidance, or developing a privacy assistance service for members. Stakeholders highlighted the lack of a consistent approach and guidance between national data protection authorities on certain issues (e.g., on cookies, the application of legitimate interest, on data breach notifications or on data protection impact assessments) or even between data protection authorities within the same Member States[6]. They also raised inconsistency of guidelines adopted at national level with those adopted by the Board, the absence of public consultations on certain guidelines adopted at national level, different levels of engagement with stakeholders among data protection authorities, delays in receiving responses to information requests, difficulties in obtaining practical and valuable advice from data protection authorities or the need to increase the level of sectoral expertise in some data protection authorities[7].

Stakeholders consider codes of conduct as very useful. Many codes are implemented at national level and the operators believe that EU-wide codes of conduct could be promoted more prominently as they foster the consistent application of the GDPR across all Member States. Still, representatives from SMEs stress the importance and usefulness of codes of conduct tailored to their situation and not entailing disproportionate costs[8].

The report highlighted as well that there have been significant discrepancies on data breach notifications (as required by Art. 33 of the GDPR) between Member States[9], which may point to a lack of consistent interpretation and implementation, despite the existence of EU-level guidelines on data breach notifications[10].

The GDPR has increased awareness about the protection of personal data both within and outside the EU and has prompted companies to adapt their practices to take into account data

[5] For specific projects aimed at facilitating SMEs' application of the GDPR, please see EU funding supporting the implementation of the General Data Protection Regulation (GDPR) (europa.eu);

[6] The European Data Protection Board has adopted guidance which addresses some of these aspects, e.g. guidelines 9/2022 on data breach notifications Guidelines 9/2022 on personal data breach notification under GDPR | European Data Protection Board (europa.eu); guidelines 5/2020 on consent edpb_guidelines_202005_consent_en.pdf (europa.eu); and on-going work e.g. on guidelines on legitimate interest edpb_workprogramme_2021-2022_en.pdf (europa.eu). The EDPB has also endorsed WP29 guidelines on DPIAs 20171013_wp248_rev_01_en_D7D5A266-FAE9-3CA1-65B7371E82EE1891_47711 (3).pdf;

[7] It is important to recall that according to Art. 70 of GDPR it is the task of the EDPB (European Data Protection Board) to issue guidelines, recommendations and best practices on data protection issues falling under para. 1 of this provision. The Commission already invited the EDPB to, amongst other ensure that national guidance is fully in line with guidelines adopted by the Board (see: *Way forward* section in the Report on the evaluation and review of the GDPR);

[8] The Commission has a role in promoting the codes of conduct under Article 40(1) GDPR *("The Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation*."). The Commission implements this provision by bringing this issue up, e.g. in its contacts with stakeholders and Commission reports (e.g. Report on the evaluation and review of the GDPR). Furthermore, the EDPB is currently working on guidelines on codes of conduct, which work the Commission actively supports;

[9] From May 2018 to end November 2019, in most Member States the total number of data breach notifications was below 2 000, and in 7 Member States between 2 000 and 10 000, the Dutch and German data protection authorities reported respectively 37 400 and 45 600 notifications;

[10] The European Data Protection Board has adopted slightly updated guidelines 9/2022 on data breach notifications Guidelines 9/2022 on personal data breach notification under GDPR | European Data Protection Board (europa.eu), which might alleviate some of these concerns if properly implemented at national level;

protection principles when innovating. Despite the overall positive impact of the GDPR on innovation, civil society organisations note that the practices of major digital players have not yet fundamentally changed towards more privacy-friendly processing, leaving room for stronger and effective enforcement of the GDPR. The question remains whether this problem will be alleviated following high level administrative fines imposed on several big tech companies due to their non-compliant practices with GDPR rules.

Sources:

Report on the evaluation and review of the GDPR

The Fit for Future Platform has acknowledged the issues raised by the legislation concerned as follows:

The specific issues encountered at local and regional level are:

- The issues encountered at local and regional level are very similar to those of SMEs in terms of administrative burden and tackling the implications of a lack of standardised tools for compliance purposes, as outlined above.

SUGGESTIONS

Suggestion 1: Issue standardised tools: make compliance easier

Description: While the GDPR has been largely a remarkable success story with positive global impact on personal data protection awareness and – naturally – the processing itself, several issues remain to be addressed in order to ensure smoother compliance with the rules. As noted by the Commission's 2020 report on the evaluation and review of the GDPR (see above), some stakeholders claim the GDPR compliance process can be challenging, time-consuming and costly especially for the small and medium enterprises (SMEs).

The GDPR compliance can be challenging for small businesses due to several reasons: lack of resources, knowledge, expertise, complexity, limited budgets, and time constraints. This comes despite the fact that the vast majority of SMEs fall under the category of so-called low risk processing activities and, as such, their compliance process should be fairly simple. It is important, too, that the Commission has provided substantial financial support to national data protection authorities in order to reach out to the stakeholders, especially the individuals and small businesses[11]. Nevertheless, the perceived complexity of the GDPR persists, also due to different approaches to awareness-raising taken by different data protection authorities (DPAs).

[11] As part of the cooperation between national DPAs and the EDPB, the Commission has established the "Rights, Equality and Citizenship Programme," which provides funding for a range of activities related to data protection, including supporting the work of national DPAs. Under this program, the Commission has allocated significant funds to national DPAs to support their efforts to raise awareness about data protection issues and promote

Therefore, the Commission should encourage the European Data Protection Board and national DPAs to focus their efforts also on drafting and sharing standardised, ready-made guidance and tools, including dos and don'ts. Further development of awareness-raising common tools on the GDPR for SMEs announced in the 2023-2024 EDPB Work Programme[12] is therefore welcome.

Some guidance already exists. In June 2021, the Commission published two sets of Standard Contractual Clauses (SCC): one for the use between controllers and processors within the European Economic Area (EEA)[13] and one for the transfer of personal data to countries outside of the EEA[14]. These standardised tools assist stakeholders in their compliance efforts under the GDPR. In May 2022, the Commission published Questions and Answers (Q&As) to provide practical guidance on the use of the SCCs.

There is still work to be done to make SMEs aware of and understand what managing personal data is about, that they are most likely handling personal data in some form or another in their operations, and that GDPR is a regulation that also affects their company. Whereas formal guidance exists[15], it would be very important to increase information activities for SMEs.

In the last 5 years, a number of project-based initiatives have taken place between representatives of national data protection supervisory authorities, academia, private business and the non-governmental sector[16]. In this regard, facilitating opportunities for deepening cooperation with these stakeholders by integrating the already achieved results of project initiatives, funded under EU programmes would have a serious positive effect on achieving the objectives of the GDPR.

Expected benefits: Providing more unified practical guidance and support, such as standardised templates for privacy notices, data protection impact assessments (DPIA) and consent forms, and comprehensive dos & don'ts can help streamline the compliance process and reduce costs for businesses even more.

Suggestion 2: Encourage the improvement of cross-border cooperation and enforcement

Description: The GDPR provides the Member States with the possibility to further specify the rules in some areas. Due to these specification clauses, there is a certain degree of fragmentation on many issues (such as the difference between the age of children consent regarding use of social networks services). Because of this fragmentation, businesses that operate across borders

compliance with GDPR. For example, in 2020, the Commission allocated €2.2 million to fund 17 projects aimed at promoting awareness and compliance with GDPR across the EU. These projects included initiatives such as developing training programs for businesses and professionals, providing information and advice to individuals on their data protection rights, and conducting research on emerging data protection issues. The aim of these projects is to help national DPAs reach out to stakeholders and promote a culture of data protection across the EU;

[12] edpb_work_programme_2023-2024_en.pdf (europa.eu)

[13] Standard contractual clauses for controllers and processors in the EU/EEA (europa.eu)

[14] Standard contractual clauses for international transfers (europa.eu).

[15] See guidance at national level and the comprehensive guidance by the EDPB: The EDPB data protection guide for small business | European Data Protection Board (europa.eu)

[16] See for example SMEDATA, ARC, SMOOTH;

may face challenges in complying with different standards that might also differ in terms of citizens' protection.

Currently, the enforcement of existing rules could be improved, particularly in cross-border cases. Improving cross-border cooperation between data protection authorities and harmonising their procedure can help ensure that the GDPR is better enforced across the EU.

DPAs[17], academia[18], consumer organisations[19], digital rights organisations[20] and other stakeholders as well as the Commission's report call for improvement including harmonised procedures for handling of cross-border cases. Harmonised procedures can help to ensure that DPAs across the EU are following consistent protocols when they need to work together as well as to ensure equal and fair procedural rights. This can include harmonising the procedural rights, the process for exchanging information, coordinating investigations, and making joint decisions. In this regard, the DPAs should also collaborate with other relevant authorities, such as consumer protection authorities and labour inspection, especially during investigations related to the employment context. Strengthening such cooperation would contribute to a better understanding and coordinated approach in addressing privacy and employment-related issues.

DPAs should be accountable and transparent in their decision-making processes when working with other DPAs and when dealing with controllers and processors under investigation and complainants. This can include early and swift cooperation in cross-border cases involving DPAs closely and proactively, setting up deadlines for cooperation and information duties between DPAs, publicly reporting on cross-border cases, ensuring the rights to be heard and access to the file, reaching reasoned and comprehensive decisions, and publicising the decisions.

For this purpose, some DPAs may require additional resources to effectively deal with complaints and cooperate with each other in a timely manner[21]. This could include dedicated staff for cross-border cases, additional training, or access to specialised expertise, among other measures. The Commission should continue to urge the Member States to provide sufficient funding to their DPAs in order to ensure they can fulfil their tasks and responsibilities, including cross-border cooperation.

Expected benefits: Improving the respect for the GDPR and protection of data subjects' rights, ensuring equality of the parties, improving cooperation between data protection authorities, and harmonising their approaches in handling of cross-border cases can help ensure that the GDPR is consistently and effectively enforced across the EU.

[17] EDPB Letter to the EU Commission on procedural aspects that could be harmonised at EU level (2022);
[18] See for example: Deficient by Design? The Transnational Enforcement of the GDPR (Gentile & Lynskey, 2022); The Right to Lodge a Data Protection Complaint: OK, But Then What? An empirical study of current practices under the GDPR (González Fuster et al., 2022);
[19] BEUC's Recommendations on harmonising cross-border procedural matters in the GDPR (2023);
[20] See for example EDRi letter to EDPB on GDPR procedural issues (2022);
[21] EDPB & EDPS: "Lack of resources puts enforcement of individuals' data protection rights at risk" (2022);

Suggestion 3: Level the field: promote better enforcement against controllers and processors outside of the EU

Description: Some stakeholders claim that controllers/processors not established in the EU but active on the EU market, do not always fully comply in their data processing activities with the GDPR. This creates an uneven playing field and a competitive disadvantage for the complying EU businesses who call for more vigorous enforcement action by the data protection authorities.

The GDPR can be difficult to enforce, even against foreign businesses that did legally establish operations in the EU[22], making it especially difficult to enforce against controllers and processors outside of the EU. Therefore, data protection authorities in the EU should increase their cooperation with each other. This could include sharing information and resources to investigate potential violations of the GDPR by controllers/processors established outside of the EU.

In more practical terms, the data protection authorities should, where necessary, involve the controller's or processor's representative in the EU, who can be addressed instead of the company based outside the EU. Additionally, the full enforcement toolbox provided under the GDPR (e.g., public warnings, temporary or definitive bans on processing in the EU, financial penalties) could be used more vigorously by data protection authorities as a tool to enforce GDPR requirements against foreign operators.

Overall, better enforcement of the GDPR rules against controllers/processors established outside of the EU will most likely require a multi-pronged approach that includes cooperation between EU data protection authorities, formal agreements with non-EU countries, financial penalties, and the use of diplomatic channels. To this end, a permanent contact between the Commission, DPAs and third country governmental authorities is encouraged.

Expected benefits: Creating a true level playing field for EU and non-EU companies will provide several benefits, including fair competition, protection of consumer privacy, improved trust in the digital economy, enhanced innovation, and enhanced data protection.

Suggestion 4: Support, encourage and promote the use of codes of conduct

Description: Member States, DPAs, the EDPB, and the European Commission all have an obligation under Article 40 of the GDPR to "encourage the development of codes of conduct intended to contribute to the proper implementation of this Regulation". However, it is still deeply challenging for a trade association or similar body to develop a code of conduct for approval by a DPA. The costs—both financial and resource-wise—of doing so would be considerable, which is why only a few major trade associations have had their codes approved.[23] Also, the trade associations call for the EDPB's demands on monitoring and supervisors to be

[22] As evidenced by at least 28 cases by the Irish Data Protection Commission against the so-called Big Tech companies, only a few of the cases result in fines, which leads to frustration among other DPAs. See: MEPs rue lack of GDPR sanctions issued by Irish data authority (Stolton, 2021);
[23] See EDPB records on Codes of Conduct, amendments and extensions

proportionate and realistic, considering the possibilities of SMEs and micro businesses in particular.

Therefore, we call on the EDPB and national DPAs to engage in policy dialogue with draftees of codes of conduct to identify potential issues with the codes at an early stage and to facilitate that codes submitted by associations meet the standards set in the GDPR and the EDPB 01/2019 Guidelines on Codes of Conduct.

Codes of conduct can be a very useful tool to make the provisions of the GDPR more concrete, "taking into account the specificities of the different sectors in which processing takes place, and the specific needs of micro, small, and medium-sized enterprises" (Article 40(1)). When the GDPR was introduced, codes of conduct were considered an important tool for clarifying and simplifying its application.

Given this, it may be useful to look at further measures to advance new codes of conduct more quickly, in areas highlighted by industry. One such step could be to give the Commission more extensive responsibility for—in cooperation with industry representatives—initiating, organising and administering the work on codes of conduct. Such a task for the Commission would not preclude similar initiatives being taken at the national level.

In its 2019 report[24], Confederation of Swedish Enterprise suggested that the government should mandate selected authorities and provide funds to support the business community's work in developing codes of conduct in key areas for businesses. In its 2020 evaluation, the Commission encouraged the use of codes of conduct. Although the EDPB approved two EU-wide codes of conduct[25] and has published the national and trans-national codes of conduct that have been already approved[26], progress has been slow.

We recall the need to ensure that sufficient financial and human resources are allocated to the EDPB to ensure that the GDPR is enforced in a robust manner, including by approving within a reasonable timeframe valid codes of conduct where they contribute to enhancing the compliance with the GDPR by the organisations subject to a given code of conduct.

Expected benefits: More Codes of conducts will provide clarity and certainty.

ABSTENTIONS

- 1 member

[24] What's wrong with the GDPR? (Brinnen, Westmann, 2019);
[25] The EU Code of Conduct for Data Protection in Cloud Infrastructure and the EU Data Protection Code of Conduct for Cloud Service Providers;
[26] Codes of Conduct, amendments and extensions | European Data Protection Board (europa.eu).