

Second report on the application of the GDPR

Since the General Data Protection Regulation (GDPR) entered into force in 2018, the European Commission has published two reports on its application. The second report stresses the need for consistent interpretation and enforcement of the GDPR, highlighting ongoing challenges such as divergent national interpretations, difficulties in cooperation among regulatory bodies, and obstacles faced by organisations in achieving compliance.

First report on the application of the GDPR

In its [2020 report](#), the Commission **assessed** the application of the [GDPR positively](#). At the same time, it identified several shortcomings, and made recommendations for improvement. Among the **shortcomings**, it underlined GDPR enforcement challenges, including inconsistent application by data protection authorities (DPAs), fragmented rules, and a lack of adequate resources allocated to DPAs. The Commission found that data subjects' rights and international data transfer mechanisms had not yet reached optimal levels of implementation. It also expected challenges in applying the GDPR to new technologies such as artificial intelligence (AI), making continuous monitoring necessary.

To address these shortcomings, the Commission **recommended** further aligning national legal frameworks with the GDPR, improving cooperation between DPAs, and allocating sufficient resources to DPAs. Supporting stakeholders and research was also a key focus, as the report noted the need for clear, unambiguous guidelines and practical tools such as forms, as well as codes of conduct and standard contractual clauses (SCCs). Finally, to facilitate international data transfers, the Commission envisaged modernising the SCCs, accelerating the procedure for binding corporate rules (BCRs), and continuing to promote convergence with the GDPR at an international level.

Second report on the application of the GDPR

Since the first report, the European Parliament and the Council, as co-legislators, have adopted several regulations to govern the digital sector, including the [Data Governance Act](#) (DGA), the [Data Act](#), the [Artificial Intelligence Act](#) (AI Act), the [Digital Services Act](#) (DSA) and the [Digital Markets Act](#) (DMA). The [2024 report](#) identifies a broad range of achievements and improvements, as well as some perennial shortcomings, in the light of these developments.

Enforcement of the GDPR

Functioning of the cooperation and consistency mechanisms

For consistent interpretation and robust enforcement of the GDPR, [cooperation](#) between DPAs in cases of cross-border data processing is crucial. If DPAs disagree on the appropriate course of action, the European Data Protection Board (EDPB) resolves the dispute as part of the consistency mechanism. According to the Commission, DPAs' increased use of the mechanisms for cooperation and consistency suggests that differing opinions are resolved at cross-border level. The Commission has proposed additional procedural rules to improve and accelerate cooperation and dispute resolution. This **proposal** is currently under negotiation by the [European Parliament](#) and the [Council](#). [Various stakeholders](#) have criticised the Commission proposal's effectiveness and adequacy.

Appropriate enforcement

Enforcement activity has increased significantly, and most DPAs consider their investigatory tools adequate. However, some ask for additional tools at national level, such as sanctions for non-cooperation or failure to provide information. A persistent shortage of resources, along with gaps in technical and legal expertise, continue to undermine some DPAs' enforcement capacity.

European Data Protection Board

Most DPAs consider that the EDPB plays a key role in promoting consistency and cooperation. However, some smaller DPAs face challenges when it comes to participating effectively and engaging with the EDPB,



while others call for processes that are more efficient. The EDPB's guidelines are deemed useful, although feedback highlights a need for more concise and practical guidance. DPAs also state a need for specific guidelines, in particular on anonymisation, pseudonymisation, [legitimate interest](#), and scientific research.

Data protection authorities

Although Member States did allocate more resources to them, DPAs still report a lack of human resources, particularly against the backdrop of having to deal with a high number of complaints. Another issue highlighted is that DPAs continue to adopt diverging interpretations on key concepts. This creates legal uncertainty and increases costs for businesses. In some cases, DPAs publish national guidelines that contradict those of the EDPB. While stakeholders appreciate being able to engage in constructive dialogue with DPAs, they also note that some DPAs are too slow, do not respond, or provide unhelpful answers.

Implementation of the GDPR

The report finds that divergences between national legislation still exist. Opening clauses and interpretative ambiguities have led to fragmentation, in particular regarding the minimum age for a child's consent, and the conditions for processing genetic, biometric or health data, as well as personal data relating to criminal convictions and offences. While Member States consider that some degree of fragmentation may be beneficial, companies operating in multiple Member States find fragmentation challenging, and report that it can lead to differing levels of protection.

Data subjects' rights

Individuals are increasingly exercising their rights over personal data, as provided under the GDPR. Data controllers face interpretative challenges, for instance in defining 'unfounded or excessive requests'. Civil society organisations highlight unjustified differences between Member States in handling complaints. Some stakeholders report challenges arising from limited digital literacy or poor understanding of rights.

Challenges for organisations, in particular small and medium-sized enterprises

The GDPR seeks to create a level playing field for businesses. However, small organisations, such as SMEs and civil society organisations, may lack the knowledge and/or resources to comply fully with the GDPR. Although compliance tools such as codes of conduct, certification mechanisms and SCCs have been used, businesses report mixed feedback on their application. Burdensome requirements, lack of support from DPAs, and lengthy approval processes are reportedly hampering uptake. Data protection officers play a crucial role in making sure that organisations comply with the GDPR, but often lack adequate training, qualifications and resources.

Digital policies and the GDPR

The adoption of digital regulations calls for cooperation between supervisory authorities across regulatory fields. The report highlights the need for more structured and efficient approaches to such cooperation.

International data transfers

According to the report, tools such as adequacy decisions, SCCs and BCRs are widely used. However, data exporters often have difficulties carrying out transfer impact assessments (TIAs) where transfers are not covered by an adequacy decision, as they are complex and costly. They are calling for additional guidance and new tools (such as templates and risk catalogues) to assist with performing TIAs. At the same time, stakeholders continue to report that the burdensome approval process is preventing BCRs' widespread adoption. Since the 2020 report, the EDPB has helped increase the adoption of certification and codes of conduct, but approval processes have remained complex.

Recommendations for improvement

To ensure strong data protection and the free flow of personal data within the EU, the report recommends that: the **co-legislators** adopt the Commission proposal on procedural rules; **DPAs and the EDPB** provide proactive support for stakeholders; **digital regulators** cooperate more effectively, to ensure coherent interpretation and implementation; and the **Commission** advance its international strategy on data protection. The report notes that 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'.