DIGITALEUROPE

28 NOVEMBER 2023

Response to GDPR Multistakeholder Expert Group questionnaire for Commission 2024 report on the application of the GDPR

Table of contents

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

Introduction

Europe's digital legal landscape has gone through considerable changes since May 2018. In 2020, DIGITALEUROPE's report for the first review of the General Data Protection Regulation (GDPR) identified means to reach the necessary thresholds for harmonisation.[1]

Whilst the report mostly remains valid today, a flurry of digital rules and case law were since introduced, leading to new challenges. We welcome the current review as a key opportunity in a general stock-taking exercise of the new laws.[2]

[1] See DIGITALEUROPE, *Two years of GDPR: A report from the digital industry*, available at https://www.digitaleurope.org/resources/two-years-of-gdpr-a-report-from-the-digital-industry/.

[2] See DIGITALEUROPE, *Europe 2030: A digital powerhouse*, available at https://www.digitaleurope.org/news/digitaleurope-unveils-2030-vision-to-transform-europe-into-a-digital-powerhouse/.

We also identify areas where practical guidance and the promotion of different existing, but under-used, tools could help reach necessary alignment.

General comments

Overall assessment of the application of the GDPR since May 2018, and priority issues to be addressed

The GDPR has had a significant impact on the way organisations collect, use and store personal data. It has improved transparency and accountability, and increased awareness: in 2019, 73 per cent of Europeans were already aware of data subject rights.[3] Such awareness was confirmed in 2020, when it was found that 71 per cent of people in the EU had heard about their data protection authority (DPA).[4] Companies have also heavily invested in compliance tools and internal processes.

After over five years, however, the GDPR is no longer the central point of focus on the digital legislative landscape, as the legislative field has considerably expanded (to name a few: the Data Governance Act, Digital Markets Act, Digital Services Act and the Data Act). Legal certainty, for instance with respect to rules that govern data sharing, for example through anonymisation and pseudonymisation techniques, will be key for the competitiveness of Europe's single market and industry.

Further, the one-stop-shop (OSS) mechanism has provided businesses and data subjects with a level of legal certainty and consistency. We appreciate the proposal for a GDPR Procedural Regulation, looking to strengthen the OSS.[5]

However, certain specific pain points remain since 2020, where harmonisation through practical EDPB guidance are still needed. Here, priority issues to be addressed include:

- Anonymisation, for instance where the risk of identifiability has been reduced to a negligible level based on contextual factors. There is also very little guidance to support pseudonymisation and various degrees of likelihood that re-identification may occur.

[3] Charter of Fundamental Rights and General Data Protection Regulation Report, requested by the European Commission, available at https://europa.eu/eurobarometer/surveys/detail/2222.

[4] From the 2020 Fundamental Rights Agency survey *Your rights matter: Data protection and privacy*.

[5] See DIGITALEUROPE, *Fostering cooperation in GDPR enforcement across Europe*, available at https://cdn.digitaleurope.org/uploads/2023/03/Fostering-cooperation-in-GDPR-enforcement-across-Europe_-24032023.pdf.

- Distinguishing personal from non-personal data, especially with new legislation such as the Data Act, and various upcoming data spaces.[6]
- Research and innovation, particularly regarding health and artificial intelligence (AI), where practical guidance would be welcomed.[7]
- Joint controllership, notably to clarify OSS applicability and the link between determining the means and purposes and having actual and decisive influence.[8]
- Reinforcing full use of all legal bases under which data can be processed.
- The precise threshold for compensation for non-material damage, notably by updating the EDPB Guidelines on calculating administrative fines.[9]
- Lastly, considering the GDPR's impact on international relations and trade, pursuing work at a global level, notably by further developing adequacy decisions and other safeguards for data transfers.

Exercise of data subject rights

Exercise and compliance with data subject rights (Arts 15, 16, 17, 20, 21, 22)

Complaints sent to controllers also often happen to relate to customer service issues rather than data subject rights. DPAs' assessments of complaints insufficiently evaluate the data subject's good faith, the full use of internal procedures provided and the relevance to processing of personal data within the meaning of the GDPR.

[6] Anonymisation is increasingly described as a tool to turn personal data into non-personal data, see for example the study commissioned by ITRE to the Policy Department *The emergence of non-personal data markets* available here: https://www.europarl.europa.eu/RegData/etudes/STUD/2023/740098/IPOL_STU(2023)740098_EN.pdf.

[7] See DIGITALEUROPE, *Making the most of the GDPR to advance health research*, available at https://cdn.digitaleurope.org/uploads/2021/06/Making-the-most-of-the-GDPR-to-advance-health-research_DIGITALEUROPE.pdf.

[8] See DIGITALEUROPE, *Response to EDPB consultation on draft Guidelines on the concepts of controller and processor*, available at https://cdn.digitaleurope.org/uploads/2020/10/DIGITALEUROPEs-response-to-EDPB-guidelines-concepts-of-controller-and-processor.pdf.

[9] See DIGITALEUROPE, *Harmonising enforcement in methods to calculate GDPR fines* https://www.digitaleurope.org/resources/harmonising-enforcement-in-methods-to-calculate-administrative-fines/.

On Art. 12(5) GDPR, the interpretation developed around what is 'manifestly unfounded or excessive' has leaned towards individualised responses instead of positive scalable solutions, such as transparent privacy policies.

In some cases, very large datasets have to be shared in response to broad data access requests, which are difficult to translate to the issuer of the request. Data subjects should be encouraged to submit more specific requests.

Moreover, the right of access by the data subject[10] is often misused by third parties to frustrate or undermine internal data privacy processes. This could be due to a lack of liability rules to prevent the misuse of GDPR rights for 'fishing expeditions.'

We further note the need to reflect the difference between B2C and B2B cases, as the GDPR has a strong focus on protecting the privacy of consumers. Exemptions in the B2B sector could have a positive impact on the EU's competitiveness.

Tools or user-friendly procedures to facilitate the exercise of data subject rights

Self-service tools and privacy-enhancing technologies (PETs) are mentioned under Art. 25 GDPR. However, they are not always sufficiently recognised or encouraged in implementation. PETs are for instance key for controllers that need to respond to data subject requests at scale, otherwise sent to emails, sometimes to various departments.

Online tools and forms allow requests to be addressed at scale, in a consistent, secure and timely manner. They can also ensure that requests come from verified users.

A number of different tools have been developed by companies in the EU, for instance by giving data subjects more control in settings, in making data protection-related information accessible, in designing privacy policies, in various options to automatically delete information, confidential computing or homomorphic encryption.

Challenges in relation to the exercise of data subject rights by children

The GDPR allows data subjects, including children, to exercise their rights, but uncertainties persist regarding parents' ability to exercise these rights on behalf of children. In 2020, we already flagged that Member States adopted different thresholds for parental consent, varying from 13 to 16.

[10] Art. 15 GDPR.

Application of the GDPR to SMEs

Lessons learned from the application of the GDPR to SMEs

It is key to simplify and streamline GDPR compliance to avoid disengagement from SMEs. Data protection impact assessments (DPIAs) are one example where implementing the GDPR should not become overly technical.

Based on the nine criteria determined by the EDPB, DPIAs are often required. However, they are difficult to complete without skilled professionals in the field, specialised lawyers and/or specialised compliance officers. External consultancies charge high fees, often without the assurance that the DPIAs are conducted in a sufficiently thorough manner. There is a need for standardised DPIAs from DPAs, or the recognition that SMEs can provide simplified DPIAs.

Guidance and tools provided by data protection authorities and the EDPB for SMEs

Guidance and tools from DPAs are often too high-level, and still require specialised legal expertise to fully understand some of the GDPR's implications.

Examples where further practical guidance for SMEs could be helpful are:

- DPIA templates that are ready to complete and contain explanations;
- Examples of how specific documents should be to reach the transparency requirements; and
- Templates to obtain consent for various purposes.

Use of representative actions under Art. 80 GDPR

The use of collective redress mechanisms under Art. 80 is expected to increase. Preventing duplicative actions will be key to avoid burdens on local courts and companies alike.

Experience with DPAs

Experience in obtaining advice from DPAs

Having a single interlocutor via the OSS has been beneficial to foster dialogue between authorities and controllers/processors. However, companies at times face a lack of pragmatism from DPAs in providing concrete guidance, recommendations or standards to follow in order to comply with the relevant requirements. Guidance from DPAs should remain practical, without reluctance to offer definitive legal advice.

There is also a lack of regular, transparent processes for stakeholder engagement.

We would also welcome a more proactive role for DPAs in engaging with other regulators to clarify their areas of competence to avoid conflicting rulings, which will be all the more important with the multiplication of rules applicable to data processing in the coming years.

Member States must also ensure that DPAs are appropriately resourced.

EDPB guidelines and the practical application of the GDPR

Guidelines adopted by the EDPB are important as they support the practical application of the GDPR and set a standard when it comes to implementation in the different Member States.

There are still several areas where there is a lack of harmonisation and guidance from the EDPB. This has already been pointed out in the previous report of 2020. In particular, guidance is needed in the following areas:

- Pseudonymisation and anonymisation;
- Secondary use of health data; and
- Scientific research.

Updated, more realistic guidelines on the concept of personal data/anonymisation are crucial for the success of the GDPR and its interplay with upcoming legislation like the Data Act.

On the other hand, guidelines should remain true not only to the spirit of the GDPR, but sometimes also its explicit language, without creating additional requirements. We need guidelines that provide solutions to real situations, achieving balanced, practical interpretations of the GDPR. This would, in particular, help companies that do not necessarily have legal teams to meet legal requirements.

We would welcome consultations where an exchange with stakeholders is possible, such as in-person public consultation meetings, and a willingness from DPAs and the EDPB not just to listen passively but to engage in a dialogue with stakeholders during these meetings.

DPA follow-up on complaints and information

We have noticed a lack of transparent and standardised procedures under the GDPR.

Conflict between DPA guidelines and EDPB guidelines

In Estonia, for example, the DPA has given very specific guidance in some areas (such as the frameworks to conduct DPIAs), which do not exist in other countries. These huge disparities worsen single market barriers and are an obstacles in particular for smaller innovative digital companies.

Accountability and the risk-based approach

Principle of accountability and the risk-based approach

The risk-based approach is one of the guiding principles of the GDPR, with a necessary balance of the right to the protection of personal data with others' rights and interests. The risk-based approach for instance includes DPIAs, privacy-by-design requirements and the legitimate interest balancing test. These tools have led to a consistent approach to assessing risks, whether posed to individuals or to organisations.

We highly encourage further discussions on the risk-based approach and the progress companies have achieved in mitigating potential risks, including with regard to Chapter V GDPR.

Scalability of obligations

In general, a risk-based approach is a prerequisite for development and deployment of anonymisation techniques and PETs to better preserve people's privacy.

Data protection officers (DPOs)

Role of DPOs

A number of digital and digitising companies had already appointed DPOs prior to the enactment of the GDPR in 2018, as this was either already required by national data protection legislation (as was the case of Germany) or because they saw the clear benefit and importance of appointing a DPO to ensure compliance.

Often a single DPO does not suffice for companies, which instead choose to dedicate entire teams with people of different business backgrounds, e.g. technical experts, auditors and attorneys. Team responsibilities can include shaping data protection policies and standards, providing advice, recommending key compliance measures, monitoring compliance, conducting audits, training of staff, and incident response. Often these teams work together with development and operational units to provide training and advice, and thus help them develop new existing data protection technologies and improve them. In addition, making employees aware of what is expected of them in this domain helps build a culture that values the protection of personal data and individuals. Ongoing privacy education and awareness training gives

employees access to the information needed to recognise and properly handle personal information, on a day-to-day basis.

The crucial role that especially in-house DPOs can play for a company's compliance efforts on all levels (as outlined above) should further be recognised and acknowledged in the review procedure.

Skills for DPO recruitment

Whilst there are many skilled professionals in the area of privacy law now, it is important they have a good understanding of the various industries they are working in. At the same time, privacy and data protection law touches upon many different areas and it is not always easy to find professionals who are skilled in different sectors relevant to organisations' needs.

Sufficient resources for DPOs

To support the DPO's important compliance role and team, it is essential that they are equipped with sufficient resources. However, this depends on the size and complexity of different companies as well as the data processing activities involved. There is no one-size-fits-all solution, and resources must be evaluated on a case-by-case basis.

Independence of DPOs

The GDPR anticipates potential conflicts and risks to the DPO's independence. The DPO must not receive any instructions from the controller or processor to exercise their tasks, and reports directly to the highest level of management of the organisation.

We note possible tensions in counterbalancing requirements for the DPO to be 'conflict free' but also 'informed' and 'appropriately qualified.' Different ways to reconcile these needs must be further recognised.

For SMEs, internal DPOs have a better understanding of the organisation and are more directly attached to its success, and may prove difficult to designate without minor conflicts of interest. We would welcome recognition of this tension, and support SMEs in designated the most appropriate individuals and teams.

International transfers

Use of SCCs for international transfers

SCCs are the most used tool to transfer data internationally, especially after the invalidation of the Privacy Shield and considering the very extensive timelines from DPAs when asked to review binding corporate rules (BCRs) or other tailor-made contractual clauses.

However, SCCs are in some cases regrettably viewed by DPAs as an insufficient mechanism for international transfers. The fact that they require additional transfer impact assessment often implies contracting costly external legal advisors to understand the destination jurisdiction.

In general, updating SCCs can be very time and resource consuming. This is notably the case when their deployment has been complicated by new model clauses. Indeed, the exercise involves integrating different sets of SCCs into agreements, to parties whose roles may evolve. A model might apply today but not in three months, nor further down the line, simply because the other party becomes a controller and the model in the SCCs is no longer applicable and needs to be updated.

We encourage the swift adoption or validation of SCCs that apply to transfers to importers whose processing operations are subject to Art. 3(2) GDPR.

At present, there are dozens of sets of SCCs across the globe, sometimes applicable to for low-risk transfers, which makes integrating them difficult. We would welcome efforts towards mutual recognition of SCCs.

Other tools for international data transfers

We strongly welcome the analysis of different tools to facilitate and secure international data transfers. Indeed, digital and digitising industries have faced a legal maze of new and existing rules to govern data transfers, often driven by geopolitical considerations.[11] We support the work towards further legal certainty and enabling of data flows that are crucial to Europe's economy.

BCRs are an important compliance tool, especially for larger organisations. However, the process for approval is very time and resources consuming (longer than 5 years). This is regretful, as they are intended to be a tool tailored to the specific organisation, acting in a particular industry.

Other countries or regional organisations with which the Commission should work to facilitate safe data flows

We strongly welcome the Commission's continued work on reinforcing the existing adequacy frameworks, and expanding adequacy to new geographies.

Work with countries such as India, Brazil, Australia, Indonesia, Singapore, South Africa, Thailand, Malaysia, China and Hong Kong is particularly important for European industry.

Fragmentation

[11] See DIGITALEUROPE, *Data transfers in the data strategy: Understanding myth and reality*, available at https://cdn.digitaleurope.org/uploads/2022/06/DIGITALEUROPE_Data-transfers-in-the-data-strategy_Understanding-myth-and-reality.pdf.

Fragmentation in Member States' application of the GDPR

As noted above, fragmentation is still an obstacle in several areas. One example is in cookie and consent policies, where guidelines from different DPAs and regulations such as the German Telecommunications-Telemedia Data Protection Act are not aligned with other Member States.

In the area of data transfers, we noticed that some healthcare regulations (notably hospital regulations) in Member States such as Germany impose additional requirements or data localisation. We believe those regional regulations, although not 'data protection' regulations, are in direct conflict with the free flow of data within the Union, as foreseen and intended by the GDPR. They impose data localisation and do not allow transfers within the Union. In general, the area of scientific research remains fragmented due to diverging interpretations and requirements at national level.

In the sector of youth, minimum age requirements and the application of legal bases differ across Member States.

Codes of conduct, including as a tool for international transfers

Adequate use of codes of conduct

Codes of conduct remain a heavily underutilised tool, due to the burdensome process required for their creation. Codes of conduct may also require constant updating, which means they are often targeted to only part of an organisation's operations (e.g. HR).

Certifications and codes of conduct must be considered as key tools to facilitate GDPR compliance, and should be seen as having great potential for scalability: we encourage more resolute work towards pan-European codes and certifications, with DPAs' active promotion and constructive engagement.

One prominent example of a functioning code is the EU Cloud CoC. This code aims at a uniform Europe-wide data protection standard in the field of cloud computing. The EU Cloud CoC is the first transnational code of conduct for all types of cloud computing, which has become one of the key standards for cloud providers and customers. This and similar projects should be actively promoted.

Development of codes of conduct and their approval process

Timely approval of codes of conduct is needed to incentivise their development. Leaner processes and coordination must be envisaged to significantly accelerate the recognition of codes of conduct.

Certification, including as a tool for international transfers

Adequate use of certifications

So far, certification mechanisms have not been widely adopted across the EU. The Europrivacy seal is the only certification recognised at EU level, with modest uptake.

Innovation and new technologies

Overall impact of the GDPR on innovation and new technologies

We have seen a clear tendency from DPAs and the EDPB to put forward an overly restrictive interpretation of the legal framework, in some instances going against not only the spirit but also the letter of the GDPR text or relevant case law.[12] As a consequence, innovation in Europe today is risky and investment into new or improved products and services is stymied.

DIGITALEUROPE believes that going forward more stress should be put on safeguards rather than on limiting the applicability of legal bases for processing or providing unrealistic interpretations of the fairness and data minimisation principles, necessity, co-controllership or purposes. This could be done through technology itself, contractual commitments, organisational security measures as well as through the promotion of industry codes of conduct and certifications.

Interaction between the GDPR and new initiatives under the Data Strategy

Alignment of the GDPR with the constellation of new laws for the Digital Decade is key to reach a single market, with a single set of digital rules. We are deeply concerned that the legal maze that has emerged around data processing as a result of the proposals adopted in this term will, rather than facilitate data sharing and innovation, have an opposite chilling effect. This is generated by more rules becoming applicable to the same processing operations and more authorities being able to arrive at different interpretations and enforcement decisions.

For example, the Data Act covers personal and non-personal data, thus raising concerns about different enforcement regimes and the overall interplay with the GDPR. This includes the principle of data minimisation.

[12] One such example is the restrictive interpretation of 'necessity,' as we've observed in our response to the EDPB consultation on the contract legal basis, available at https://cdn.digitaleurope.org/uploads/2019/05/DIGITALEUROPE-response-to-EDPB-public-consultation-on-draft-Guidelines-on-performance-of-a-contract-for-online-services.pdf.

Another example is in the various enforcement bodies created under the DMA, DSA, DGA, Data Act or upcoming AI Act. The lack of alignment with the GDPR's OSS mechanism in different new regulations will cause inconsistencies or a patchwork of enforcement. Formal cooperation and consistency mechanisms must be established.[13]

Last, we welcome the proposal for a GDPR Procedural Regulation to reinforce the OSS. We have made several recommendations towards strengthening the framework for amicable settlements, confidentiality of administrative files, the role of the lead supervisory authority, and ensuring the right to be heard, as well as reasonable and proportionate deadlines.[14]

FOR MORE INFORMATION, PLEASE CONTACT:

- Beatrice Ericson
  Officer for Privacy and Security Policy
  beatrice.ericson@digitaleurope.org / +32 490 44 35 66
- Alberto Di Felice
  Director for Infrastructure, Privacy and Security Policy
  alberto.difelice@digitaleurope.org / +32 471 99 34 25

[13] See DIGITALEUROPE, *Rebalancing the Data Act*, available at https://cdn.digitaleurope.org/uploads/2022/08/DIGITALEUROPE-Rebalancing-the-Data-Act-1-September-2022.pdf.

[14] See DIGITALEUROPE, *Squaring GDPR enforcement: stronger procedures for the one-stop-shop*.

About DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory environment that enables European businesses and citizens to prosper from digital technologies. We wish Europe to grow, attract, and sustain the world's best digital talents and technology companies. Together with our members, we shape the industry policy positions on all relevant legislative matters and contribute to the development and implementation of relevant EU policies, as well as international policies that have an impact on Europe's digital economy. Our membership represents over 45,000 businesses who operate and invest in Europe. It includes 106 corporations which are global leaders in their field of activity, as well as 41 national trade associations from across Europe.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Applied Materials, Amazon, AMD, Apple, Arçelik, Arm, Assent, Autodesk, Avery Dennison, Banco Santander, Bayer, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, CaixaBank, Cisco, CyberArk, Danfoss, Dassault Systèmes, DATEV, Dell, Eaton, Epson, Ericsson, ESET, EY, Fujitsu, GlaxoSmithKline, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, Honeywell, HP Inc., Huawei, ING, Intel, Johnson & Johnson, Johnson Controls International, Konica Minolta, Kry, Kyocera, Lenovo, Lexmark, LG Electronics, LSEG, Mastercard, Meta, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe, NEC, Nemetschek, NetApp, Nintendo, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Pearson, Philips, Pioneer, Qualcomm, Red Hat, RELX, ResMed, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Energy, Siemens Healthineers, Skillsoft, Sky CP, Sony, Sopra Steria, Swatch Group, Tesla, Texas Instruments, TikTok, Toshiba, TP Vision, UnitedHealth Group, Vantiva, Visa, Vivo, VMware, Waymo, Workday, Xerox, Xiaomi, Zoom.

National Trade Associations

Austria: IOÖ
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Czech Republic: AAVIT
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, SECIMAVI, numeum
Germany: bitkom, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: Infobalt
Luxembourg: APSI
Moldova: ATIC
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, Digital Poland Association
Portugal: AGEFE
Romania: ANIS
Slovakia: ITAS
Slovenia: ICT Association of Slovenia at CCIS
Spain: Adigital, AMETIC
Sweden: TechSverige, Teknikföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT Ukraine
United Kingdom: techUK