Call for evidence - Report on the General Data Protection Regulation (GDPR)
ACT | The App Association
8 February 2024

ACT | The App Association provides the following feedback to the public consultation opened by the European Commission on the Report 2024 on the application of the General Data Protection Regulation (GDPR). The feedback is based on the questionnaire *sent to members of the* GDPR multi-stakeholder expert group *in September 2023.*

1. General comments

What is your overall assessment (benefits/challenges, increase in trust and awareness, etc.) of the application of the GDPR since May 2018? Are there priority issues to be addressed?

ACT | The App Association (App Association) is grateful for the opportunity to contribute insights to the European Commission (EC) regarding our members' experiences with implementing the General Data Protection Regulation (GDPR). We remain committed to fostering European leadership in privacy policy, and we support the EC's evaluation of the GDPR's function, implementation, oversight, and enforcement.

We welcome the cross-sectoral nature of the GDPR, utilising a unified set of rules to govern data protection rights for EU data subjects. We particularly appreciate the principle-based approach embedded in the GDPR, being technology-neutral. This provides flexibility and adaptability and ensures that the framework withstands the test of time, allowing it to evolve seamlessly with advancements in technology while consistently upholding robust privacy standards across various sectors.

The App Association serves as a key resource for thought leadership and education within the small business technology developer community, particularly in the realm of privacy. We are dedicated to keeping our members informed of the latest policy and legal developments, translating complex regulations into practical guidance to facilitate compliance and alleviate burdens for our members.

The implementation of GDPR rules has posed notable challenges for our small and medium-sized entity (SME) members. The adjustment process required considerable effort and investment, particularly for micro-organisations and startups within our community. For SMEs, compliance was complex because each data processing activity requires a different response from the company, including on the various internal levels including human resources, legal, research and development, as well as in external interaction with customers. This process remains burdensome and costly for SMEs.

2. Exercise of data subject rights

From the controllers and processors' perspective: please provide information on the compliance with the data subject rights listed below, including on possible challenges (e.g., manifestly unfounded or excessive requests, difficulty meeting deadlines, identification of data subjects, etc.).

- *Information obligations, including the type and level of detail of the information to be provided (Articles 12 to 14)*

The App Association asserts that obligations should be as simple and accessible as possible for SMEs. For example, information obligations should not be disproportionate and a publicly available and understandable policy published on an app or a website should be enough.

- *Access to data (Article 15)*
- *Rectification (Article 16)*
- *Erasure (Article 17)*
- *Data portability (Article 20)*
- *Right to object (Article 21)*
- *Meaningful explanation and human intervention in automated decision-making (Article 22)*

b. Do you avail of / are you aware of tools or user-friendly procedures to facilitate the exercise of data subject rights?
c. Do you have experience in contacting representatives of controllers or processors not established in the EU?
d. Are there any particular challenges in relation to the exercise of data subject rights by children?

3. Application of the GDPR to SMEs

a. What are the lessons learned from the application of the GDPR to SMEs?
b. Have the guidance and tools provided by data protection authorities and the EDPB in recent years assisted SMEs in their application of the GDPR?
c. What additional tools would be helpful to assist SMEs in their application of the GDPR?

To comply with GDPR obligations, SMEs undertake often costly measures. Compliance for SMEs, such as our members, has been particularly challenging, as it involves developing various privacy-by-design approaches from the earliest stages of product development and the most advanced tools and methods available. We urge the Commission to acknowledge that large companies have greater resources for privacy compliance, while small enterprises face limitations. Many of our members lack dedicated privacy staff and must allocate additional time and resources to GDPR compliance.

Complying with GDPR has given some of our members a competitive benefit and has allowed for a thorough review of organisation and streamlining processes throughout the company. However, many of our members provide services for larger companies who often try to impose their obligations (such as controller and processor obligations) on the SME. Such behaviour by larger companies forces small entities to implement unnecessarily high levels of compliance that are not required for their business.

We are disappointed in the lack of strong and uniform enforcement of the GDPR, years after its adoption. The additional costs and burdens related to GDPR compliance can lead to anticompetitive effects between GDPR-compliant SMEs and GDPR non-compliant companies, as the latter would have the opportunity to invest those resources in other ways, which may provide more efficient competition advantages. We believe that strong and uniform enforcement is a crucial aspect of successful regulation. Therefore, we request the European Commission to take measures to ensure a stronger uniform enforcement of the GDPR.

The App Association welcomes the guidance tools provided by data protection authorities and the European Data Protection Board (EPDB), which are important and useful resources for SMEs. Any additional tools—easy to use for SMEs—translated into different European languages would be welcome. Those tools could take the form of risk assessment tools, templates, and checklists for IT security.

4. Use of representative actions under Article 80 GDPR

From the controllers and processors' perspective: are you aware of representative actions being filed against your organization?

5. Experience with Data Protection Authorities (DPAs)

a) What is your experience in obtaining advice from DPAs?
b) How are the guidelines adopted so far by the EDPB supporting the practical application of the GDPR?
c) Are DPAs following up on each complaint submitted and providing information on the progress of the case?
d) Are you aware of guidelines issued by national DPAs supplementing or conflicting with EDPB guidelines? (please explain)

There is a pressing need for improved alignment and coordination among DPAs across the EU. Currently, the varying degrees of national GDPR implementation and divergent interpretations of the Regulation poses challenges for small businesses, especially concerning the appointment of Data Protection Officers (DPOs) and international data transfers. The App Association advocates for enhanced coordination among DPAs to harmonise policies and address inconsistencies, ensuring consistent compliance and reduced burdens for SMEs.

With limited resources, App Association members rely on the guidance provided by the European Commission, EDPB, and DPAs to support them with compliance. The App Association calls on the EDPB to develop more guidance on the EU level—and at the national level—to adequately address unclear rules, limits, and liabilities. Clear and coherent guidelines applicable all over Europe and in a similar way in each country should be developed; This point is of particular importance for our members. Guidelines should be as accessible and easy to use as possible as SMEs do not always have access to lawyers and full legal department services.

6. Experience with accountability and the risk-based approach

a. What is your experience with the implementation of the principle of accountability?
b. What is your experience with the scalability of obligations (e.g., appropriate technical and organisational measures to ensure the security of processing, Data Protection Impact Assessment for high risks, etc.)?

7. Data protection officers (DPOs)

a. What is your experience in dealing with DPOs?
b. Are there enough skilled individuals to recruit as DPOs?
c. Are DPOs provided with sufficient resources to carry out their tasks efficiently?
d. Are there any issues affecting the ability of DPOs to carry out their tasks in an independent manner (e.g., additional responsibilities, insufficient seniority, etc.)?

The App Association underlines the importance for its SME members with internal Data Protection Officers (DPO) functions to have access to clear guidelines and recommendations on this role.

Certain provisions of the GDPR, such as Article 27, impose additional obligations on non-European firms, increasing the cost and risk associated with handling data of EU citizens. For instance, the requirement to appoint a physical representative in the EU can pose significant challenges for small businesses outside the EU seeking to enter the European market. This requirement may act as a barrier to entry and hinder the expansion of small businesses.

8. Controller/processor relationship (Standard Contractual Clauses)

a) Have you made use of Standard Contractual Clauses adopted by the Commission on controller/processor relationship?
b) If yes, please provide feedback on the Standard Contractual Clauses?

9. International transfers

a. *For controllers and processors: Are you making use of the Standard Contractual Clauses for international transfers adopted by the Commission8? If yes, what is your experience with using these Clauses?*
b. *Are you using other tools for international data transfers (e.g., Binding Corporate Rules, tailor-made contractual clauses, derogations)? If yes, what is your experience with using these tools?*
c. *Are there any countries, regional organizations, etc. with which the Commission should work in your view to facilitate safe data flows?*

The GDPR, since its enforcement, has posed challenges to transferring data outside the EU, potentially inhibiting the growth of small businesses in the digital economy. Constructs such as the newly adopted EU-U.S. Data Privacy Framework are crucial for sustaining innovation, growth, and job creation. The App Association is pleased to see this new development, as it makes global operations easier for some businesses.

10. Problems with the national legislation implementing the GDPR

Have you experienced or observed any problems with the national legislation implementing the GDPR (e.g., divergences with the letter of GDPR, additional conditions, gold plating, etc.)?

The GDPR is transposed with slight differences in different EU countries. This causes difficulties in particular for SMEs with limited resources. The App Association encourages the European Commission to prioritise stronger and uniform enforcement as well as promoting unity across Europe instead of adding more regulatory burdens.

11. Fragmentation/use of specification clauses

a. *Please provide your views on the level of fragmentation in the application of the GDPR in the Member States (due to Member State implementation of the GDPR or the use of facultative specification clauses, such as Articles 8(1) and 9(4) GDPR).*
b. *Please specifically identify the area in which you consider there to be fragmentation and whether it is justified.*

The App Association calls on the Commission to prioritise the improvement of enforcement and uniform interpretation of the GDPR across Europe rather than introducing additional regulatory burdens.

12. Codes of conduct, including as a tool for international transfers

a. *Do you consider that adequate use is made of codes of conduct?*
b. *Have you encountered challenges in the development of codes of conduct or their approval process?*
c. *What supports would assist you in developing codes of conduct?*

The App Association supports codes of conduct built with the different stakeholders which are designed to help SMEs apply GDPR without introducing additional regulatory burdens. However, the validation procedure for codes of conduct should be shortened.

13. Certification, including as a tool for international transfers

d. *Do you consider that adequate use is made of certifications?*
e. *Have you encountered challenges in the development of certification criteria, or in their approval process?*

f. What supports would assist you in developing certification criteria?
Please clearly distinguish in your reply when certification is used for international transfers.

14. GDPR and innovation / new technologies

a. What is the overall impact of the GDPR on the approach to innovation and to new technologies?
b. Please provide your views on the interaction between the GDPR and new initiatives under the Data Strategy (e.g., Data Act, Data Governance Act, European Health Data Space, etc.)

We advocate for the Commission to consider emerging technologies, particularly artificial/augmented intelligence (AI), when evaluating the effectiveness of the GDPR. AI encompasses a range of technologies such as Machine Learning and deep learning, which enable computers to simulate human thinking. These technologies have significant implications for decision-making processes and are increasingly used in various sectors, including finance, cybersecurity, and healthcare. AI holds promise for enhancing European consumers' lives through faster decision-making and improved outcomes. Therefore, we emphasise the importance of ensuring that GDPR requirements remain flexible enough to accommodate the evolving landscape of AI technologies.

We hope the Commission will maintain a flexible, principles-based approach to regulating risks associated with emerging technologies, even beyond the scope of the GDPR. Rather than imposing direct and inflexible regulations on specific technologies, which can quickly become outdated in the face of rapid developments, we advocate for adaptable frameworks that prioritise overarching principles. Such regulatory frameworks are capable of evolving with technological advancements, ensuring relevance and effectiveness in safeguarding privacy and security.

Moreover, we hope that the Commission will ensure that any future legislative developments will continue to uphold the highest standards for privacy and data protection. For example, in the context of the Digital Markets Act (DMA), we stress the importance of upholding privacy, security, and GDPR compliance throughout its implementation and enforcement.

Additionally, privacy and data protection are increasingly valued by consumers in our rapidly evolving digital landscape. Therefore, we advocate for the integration of privacy and data protection as essential competition parameters within the EU's competition practices. We believe such inclusion accurately reflects the realities of today's market dynamics, recognising the significance of these non-price parameters in consumer choice and preference.