EUROPEAN FEDERATION
OF DATA PROTECTION OFFICERS

# POSITION PAPER

February 2024

## GDPR EVALUATION 2024

Since May 25, 2018, the General Data Protection Regulation (GDPR) has become binding law in all EU (and little later in all EEA) member states - a crucial and correct step. Data protection symbolizes trust and has become a competitive advantage for many businesses. In light of the upcoming second evaluation of the GDPR in 2024, this paper by the European Federation of Data Protection Officers (EFDPO) highlights how, from the perspective of data protection practitioners, the business sector - particularly small and medium-sized enterprises (SMEs) - can be better supported in meeting data protection requirements within the context of increasing digitization.
We are aware that any opening up of an important regulation such as the GDPR is unlikely at this time. Nevertheless, we believe that several points that could be modified or added to the GDPR should be considered in the current evaluation or in the future.

# 1. Leveraging the Cross-Competence of Data Protection Officers, especially in SMEs, for Enhanced Data Security

The position of data protection officers (DPOs) introduced by the GDPR has quickly become an integral part of the activities of many controllers and processors. Data protection officers have been firmly established in data protection law of several member states even before the adoption of GDPR, in some case (for example Germany) for more than half a century. They provide essential expertise for responsible parties in public and private institutions, allowing them to plan and carry out the processing of personal data in compliance with the law and while safeguarding the rights of affected individuals throughout the data lifecycle. In times of acute ransomware, hacking, cyberattacks, leaks, and other digitally-driven attacks on both public and private entities, the obligation to appoint DPOs is a crucial instrument for protecting the personal data of citizens. DPOs also have advisory functions regarding the security of processing personal data for various groups of affected individuals – especially in SMEs that do not have additional experts dedicated to cybersecurity. Through internal audits, DPOs can monitor the effectiveness of the protective measures in place and advocate for improvements.

Especially in small and medium-sized enterprises (SMEs), the versatility of DPOs, resulting from the professional qualifications required for this role, offers an advantage in supporting company management. Without this cross-competence of DPOs, particularly those working with SMEs, there is a risk of significant economic damage resulting from successful attacks on the security of data processing.

This is because, especially for SMEs that may not afford to engage multiple specialized consultants, the cross-cutting expertise provided exclusively by DPOs represents cost savings. Therefore, DPOs should also be effectively supported at the level of European law. With possible changes to the GDPR, some of the ambiguities associated with the performance of the function of DPOs could be addressed. An example is the vague obligation (or privilege) of secrecy and confidentiality that the GDPR (see Art. 38/5) envisages but that has not been implemented at all in some Member States.

## DPOs are Part of the Solution, Not the Problem

Regardless of whether a DPO is appointed, the GDPR imposes obligations for processing personal data on companies, government bodies, and other entities, for example through GDPR Articles 5, 24, and 32. Responsible parties are required to proactively implement appropriate technical and organizational measures (TOMs) for prevention and to review and update them reactively. This requires expertise and experience within the organization, as reflected in the cross-competence of DPOs. DPOs are the key instrument in the toolbox of internal self-control for companies, government bodies, and other entities. They help them to be protected from the risk of being informed about deficiencies and errors in the implementation of data protection law only through potentially sanctioned inspections by the competent supervisory authority. At the same time, DPOs limit the impact of IT disruptions, both from internal and external sources, by providing advice on necessary and appropriate protective measures. When carrying out their legal duties, especially informing and advising top management, DPOs provide valuable input for the continuous improvement of legally required data protection measures and their adequacy. With responsibility for all departments in which employees and data processors process personal data, they serve as the link ensuring compliance with data protection regulations and strategies while advising employees and data processors on following management's requirements. Considering the increasing importance of digitization initiatives, DPOs are indispensable consultants and supporters for the legality of planned projects. Their advice, when included early and properly in planning data protection-compliant processing, contributes proactively to compliance, as well as reactively to addressing omissions.

# 2. Tailoring Bureaucratic Obligations for Personal Data Protection to Risk Levels

The GDPR employs a pronounced compliance methodology, which results in documentation and notification requirements for accountability and organizational obligations for every action. For example, the question of the permissibility of processing under Article 6 of the GDPR is accompanied by documentation obligations under Article 5(2) (the so-called accountability principle), the requirement to specify the legal basis to data subjects under Articles 13 and 14 of the GDPR, and the duty to record this processing activity within the records of processing activities under Article 30 of the GDPR.

Consequently, even a simple permissibility assessment (e.g., processing an employee's bank account details for salary payments) triggers three additional obligations. Furthermore, these associated obligations are not harmonized but rather each has its own specific requirements for documentation in terms of what and how to document.

Every company must ensure transparency in processing personal data. This means that data subjects must be proactively informed comprehensively about the processing of their personal data and provided with reactive information upon request. Under the GDPR, these obligations not only need to be fulfilled but also documented under Article 5(2) in conjunction with Article 30 of the GDPR. In addition, regardless of company size, extensive registers of processing activities must be kept, technical and organizational measures (TOMs) must be implemented according to Article 12 of the GDPR to meet these transparency requirements.

It is evident that a significant portion of the bureaucratic and cost-intensive effort imposed by the GDPR arises from the fact that even straightforward assessments of the permissibility of processing personal data, which occur in every company, trigger several additional obligations and workloads.

## Reducing Bureaucracy for SMEs: Avoiding the One-Size-Fits-All Approach

These additional workloads are not inevitable. For example, the previous German Federal Data Protection Act, in relation to the question of permissibility or non-permissibility of processing personal data, did not offer any less protection, yet it managed to avoid these additional obligations. It was the responsibility of the data processing company to take appropriate measures depending on its size and the risk posed by the processing of personal data.

A crucial step toward relieving SMEs, in particular, is to reduce the bureaucratic superstructure that overshadows the core obligations of the GDPR and to provide for these obligations only in proportion to the associated risks (see also point 5). These obligations should not be uniformly applied to all companies based on the highest need for safeguarding. Especially when implementing requirements based on the risk to the rights and freedoms of data subjects, DPOs can serve as the appropriate "compass."

# 3. Including Manufacturers of Digital Solutions and Services in GDPR Regulations Based on the Principle of Accountability

One of the most significant challenges for users of products for digitizing everyday business operations (whether they are applications or other digital solutions and services) is that the GDPR does not directly place obligations on manufacturers. The assessment of data protection requirements thus remains the responsibility of users, even though they assume they are purchasing "plug and play" applications. The DPO is often the messenger delivering the bad news of non-compliance with legal requirements. One significant approach to relieving SMEs is to hold manufacturers accountable. SMEs would then only need to assess the specific application within their business context.

The truism that a problem must be solved where it originates has been overlooked in the GDPR's Article 25. If the manufacturer does not implement data protection requirements during the development and production of the product, the user cannot fulfill the GDPR requirements with such an application.

This can be illustrated with Article 25(2) of the GDPR: In practice, it can be challenging for a controller to fulfill the obligation to take appropriate technical and organizational measures. Often, they will not be able to implement meaningful and sufficient TOMs because both the hardware and, more importantly, the software are typically provided by an external manufacturer, not by the controller itself. The TOMs that the controller can influence often only pertain to configurations that the manufacturer voluntarily provides to the user of its software, the responsible company. In the context of these configurations, the obligation of Article 25(2) of the GDPR, to select the most data protection-friendly options, naturally applies; however, overall, the protection of personal data is lacking.

Following the example of the upcoming AI Regulation (Article 24 of the corresponding Commission proposal), manufacturers should also be obligated to take TOMs into account in data protection law. This would consolidate data protection challenges where they arise—at the beginning of the chain. This would make it easier for controllers to comply with their duty to implement appropriate TOMs.

We recommend considering whether an additional paragraph should be added to Article 25 of the GDPR, explicitly regulating the responsibility of manufacturers, ideally ensuring consistency with the definition of the manufacturer in the Product Liability Directive. This could be guaranteed by introducing a corresponding definition in Article 4 of the GDPR.

Experiences over the past years have shown that it is necessary to finally make Article 25(2) of the GDPR an effective instrument of data protection. To achieve this, it is imperative to include manufacturers in the addressees of the norm, thereby closing the existing liability gap. This would also enable claims against manufacturers under Articles 82 and 83(4)(a) of the GDPR.

# 4. De minimis principle

The GDPR does not make any difference between large-scale processing of personal data and processing of single personal data or very small dataset of personal data as long as the processing is fully or partially automated (Article 2(1) of the GDPR). Basic obligations for the large-scale and minimal processing are the same. This should be taken into account by authorities when enforcing the GDPR. A risk-based approach could be applied more consequently.

# 5. Obligation of confidentiality

From a practical point of view, it would be advisable for the GDPR to contain an explicit regulation of the obligation of confidentiality for persons who process personal data for controllers or processors, including employees. While this obligation can be inferred from Article 29 of GDPR, an explicit obligation would simplify the situation for many controllers and processors.

**FURTHER SUGGESTIONS**

During the first evaluation of the GDPR in 2020, the EFDPO had already prepared proposals on how corporate and government data protection officers, especially in SMEs, could more effectively support the fulfillment of data protection requirements if the necessary regulatory conditions were created. See: EFDPO Position Paper on GDPR Evaluation 2020.

# About EFDPO

The European Federation of Data Protection Officers (EFDPO) is the European umbrella association of data protection and privacy officers. Its objectives are to create a European network of national associations to exchange information, experience and methods, to establish a continuous dialogue with the political sphere, business representatives and civil society to ensure a flow of information from the European to the national level and to proactively monitor, evaluate and shape the implementation of the GDPR and other European privacy legal acts. In doing so, the EFDPO aims to strengthen data protection as a competitive and locational advantage for Europe. The new association is based in Brussels.

# Member associations of the EFDPO:

- Austria: privacyofficers.at – Verein österreichischer betrieblicher und behördlicher Datenschutzbeauftragter

- Brazil: ANPPD - Associação Nacional dos Profissionais de Privacidade de Dados
- Czech Republic: Spolek pro ochranu osobních údajů
- Croatia: CENTAR FERALIS
- France: UDPO, Union des Data Protection Officer – DPO
- French Polynesia: U.D.P.O PACIFIC
- Germany: Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V.; Fachverband Externe Datenschutzbeauftragte (FED) e.V.
- Greece: Hellenic Association for Data Protection and Privacy (HADPP)
- Liechtenstein: dsv.li-Datenschutzverein in Liechtenstein
- Norway: Norwegian Association of Data Protection Officers (Foreningen Personvernombudene)
- Portugal: APDPO PORTUGAL Associação dos Profissionais de Proteção e de Segurança de Dados
- Slovakia: Spolok na ochranu osobných údajov
- Switzerland: Data Privacy Community; Swiss Association of Data Protection Officers (ASDPO)