EUROPEAN FEDERATION
OF DATA PROTECTION OFFICERS

POSITION PAPER

15th July 2025

ON THE REFORM OF THE GENERAL DATA PROTECTION REGULATION (GDPR)

EUROPEAN FEDERATION
OF DATA PROTECTION OFFICERS

Since its entry into force in 2018, the General Data Protection Regulation (GDPR) has set high standards for the protection of personal data in Europe. It reflects a European understanding of fundamental rights and serves as a global benchmark for data protection. At the same time, practical experience with its application and enforcement across Europe has shown that adjustments are necessary to reduce unnecessary bureaucracy, increase legal certainty, and better align data protection with digital innovation.

In an era of increasing digitalization, increasingly complex technologies, growing cybersecurity risks, and expanding regulatory requirements, data protection officers—especially in small and medium-sized enterprises (SMEs)—play a crucial advisory role. Many organizations lack the necessary expertise to handle these issues appropriately. Qualified data protection officers can pave the way for secure and legally compliant digital transformation, provided they are appropriately integrated and their value is recognized.

The European Federation of Data Protection Officers (EFDPO) therefore advocates for a paradigm shift: manufacturers should only be allowed to offer digital solutions that are usable in a data protection-compliant manner. Mandatory compliance documentation would enable organizations and public bodies to trust that the products they use meet GDPR requirements. This would create legal certainty and ease the burden, especially on SMEs.

OUR CORE PROPOSALS

RISK-BASED DATA PROTECTION WITH UNIFORM APPLICATION AND PRACTICAL IMPLEMENTATION THROUGH "PRIVACY BY DESIGN" AS A MANDATORY OBLIGATION FOR MANUFACTURERS:

- **Manufacturers must share responsibility for compliance alongside the controller and the processor.**
- **Manufacturers may only offer products and services that can be used in a GDPR-compliant manner ("Privacy by Design").**
- **This compliance must be demonstrably ensured by the manufacturer.**
- **Products and services must be pre-configured to be as data protection-friendly as possible ("Privacy by Default").**
- **The role of the Data Protection Officer (DPO) must be expanded to relieve especially small and medium-sized enterprises (SMEs) of compliance burdens and risk management tasks.**

We call for a targeted evolution of the GDPR that provides greater legal certainty through clear and comprehensible requirements. The current version suffers from complex wording and broad interpretative leeway, which lead to uncertainty and an excessive need for legal advice.

Necessary steps include:

- Linguistic revision with clear, practicable language
- Standardized recommendation regarding processes and templates for common use cases while maintaining the option of choosing other solutions
- Binding interpretative guidance by supervisory authorities focused on solutions rather than searching for problems
- Risk-based differentiation of requirements based on the actual threat to data subject rights and at the same time taking into account the interests of controllers

Data protection is not an obstacle to innovation, but a key component of any sustainable digital strategy.

The associations within the EFDPO are working on further simplifications to the GDPR and will present these over the coming months.

1. REDUCE BUREAUCRACY, STRENGTHEN THE IMPACT OF DATA PROTECTION

The documentation and accountability requirements under the GDPR should be designed in a way that is practical and resource-efficient for micro and small enterprises. However, the level of protection prescribed by the GDPR for the rights and freedoms of data subjects must be preserved.
Therefore, we demand:

1. Strengthening the risk-based approach as a guiding principle of the GDPR:

While the GDPR includes risk-based elements in Articles 24, 25, 30, 32, and 35, their consistent and legally sound implementation is often lacking in practice. This is particularly evident in the insufficient differentiation of regulatory requirements for processing activities with varying levels of risk.

Supervisory authorities should clearly distinguish between low-risk and high-risk processing in their guidelines, audit standards, and interpretations. The GDPR must not be treated as a 'one-size-fits-all' regulation, but should allow and promote risk-appropriate implementation of data protection obligations—for instance, through simplified procedures for low-risk processing, graduated accountability requirements, and pragmatic audit standards. This would not only relieve SMEs but also strengthen fundamental rights protection where it is most needed.

2. Obligation of Manufacturers and Risk-Based Compliance Documentation:

Manufacturers of digital products and services must be required to implement privacy by design and by default. They must also provide the necessary compliance documentation aligned with the intended purpose of the product. This includes, for example:

- Records of processing activities (RoPA) templates
- Data protection impact assessment (DPIA) templates
- Sample letters for responding to data subject requests

3. Reform of Certification Structures:

Although the GDPR already provides for certifications, the current organizational structures implemented to support these processes have proven ineffective. A fundamental restart is necessary to enable manufacturers and service providers to use certification as a valid tool for demonstrating GDPR compliance.

4. EDPB Guidelines with Minimum Legal Interpretation:

The European Data Protection Board (EDPB) should orient its guidelines and assistance materials to the legally required minimum interpretation of data protection law. Overregulation and overly cautious interpretations risk hindering innovation and usability without contributing to better protection of data subjects.

5. Clarify Data Subject Rights, Prevent Abuse:

The rights of data subjects must be designed to be more understandable for citizens, while preventing abusive or excessive requests, particularly under Article 15 GDPR. This ensures accessibility while reducing the administrative burden on controllers.

To this end, a clear regulation on the designation of Data Protection Officers (DPOs) is necessary, as already implemented in some Member States:

- Risk-based criteria should apply to the obligation to appoint a DPO
- A DPO must be appointed when Article 9 GDPR data (e.g. health data) is processed on a commercial basis and the processing goes beyond the mere fulfilment of legal obligations (e.g. by an employer)
- A DPO must be appointed when controllers use technologies that may pose a high risk to data subjects
- A DPO must be appointed when personal data is transferred to third countries

Tying the DPO obligation to the size of an organization (as is the case in some Member States) reflects an outdated "analogue" mindset. In the age of advanced technologies, organizational size plays little to no role in determining risk or compliance needs.

2. ENSURE CONSISTENT INTERPRETATION AND GUIDANCE ACROSS THE EU

Organizations and public authorities often face significant uncertainty when applying the GDPR. This is largely due to divergent interpretations of the Regulation by supervisory authorities in different EU Member States. For organisations operating across Europe, this leads to considerable legal uncertainty and hampers consistent and lawful implementation. Although the GDPR provides a basic framework that can be further specified through guidelines and decisions from supervisory authorities, there is a lack of uniform and binding standards. There is therefore a clear need for harmonised interpretation standards, practical guidance, and advisory support to enhance legal clarity and planning certainty for controllers across the EU. These standards must also enable the EU to remain competitive in the global economy.

3. CONNECTING DATA PROTECTION AND INNOVATION

New technologies are of central importance for Europe's competitiveness. The GDPR establishes conditions under which data protection-compliant innovations can be developed in a technology-neutral manner.

One of the key elements here is, for example, the legally secure use of pseudonymized and anonymized data. The EFDPO therefore calls for:

- A dedicated legal basis for the anonymization of personal data
- Standardized and legally recognized anonymization procedures
- Clear privileging of data usage after successful anonymization
- Legal certainty for organisations regarding further processing of anonymized datasets
- Simplified processes for research and development using anonymized data

These measures would notably facilitate the development of data-driven innovations such as AI systems, without endangering the protection of personal data. Anonymized data is not subject to the GDPR – however, this needs to be clarified through clear rules on anonymization.

4. TRANSPARENCY IN SANCTIONS

The current enforcement practices of supervisory authorities vary widely across EU Member States. This leads to legal uncertainty and market distortions within the European internal market. To ensure fair and effective enforcement of the GDPR, we call for:

- Harmonized enforcement and meaningful penalties that will not discourage innovation
- Binding EU-wide standards for fine procedures
- Uniform evaluation criteria across all Member States
- Coordinated enforcement strategies by supervisory authorities

- Avoidance of regulatory arbitrage and location-based advantages
- Strengthened enforcement against international corporations, e.g. through fine procedures led by the EDPB

A unified and transparent sanction regime fosters legal certainty for businesses and strengthens trust in European data protection. However, enforcement must not become a competition between Member States.

5. STRENGTHEN DATA PROTECTION OFFICERS AND SECURE THEIR QUALIFICATION

EFDPO calls for more efficient use of the expertise of Data Protection Officers (DPOs). Effective implementation of the GDPR requires specialised expertise, which is often lacking, especially in SMEs, because there is no DPO. Rather than building costly parallel structures, the role of the DPO should be legally strengthened – as an independent and qualified expert with a clearly defined role in an organisation's compliance framework.

1. Legal anchoring of extended DPO competencies:

- Mandatory delegation of operational data protection responsibilities to the DPO
- Clear definition of the DPO as the primary data protection manager
- Legal empowerment of the DPO's position while maintaining overall responsibility with top management

2. Specific allocation of responsibilities in core processes:

- Lead responsibility for Data Protection Impact Assessments (DPIAs)
- Central control of data protection risk management
- Maintenance of records of processing activities
- Management of data breaches with mandatory DPO involvement
- Coordination of data subject requests
- Quality assurance of technical and organisational measures

3. Efficient resource use through:

- Avoidance of redundant structures within organizations
- Utilization of the DPO's expertise as a single point of contact
- Standardized processes and workflows

4. Accompanying measures:

- Development of qualification standards for DPOs
- Certified training and continuing education programs
- Expansion of support services provided by authorities; DPAs should more often act more as partners for data protection officers for discussions