8 February 2024

Response of the European Association of Public Banks (EAPB) on the call for evidence for the Commission 2024 Report on the application of the GDPR

I. General Comments

The GDPR establishes a consistent legal framework throughout the EU, ensuring a high standard of data protection, which is generally deemed successful in the banking sector.

However, it was noted by our members that ensuring GDPR compliance presents significant challenges for medium-sized and small companies, lacking the financial means and organizational capacity to employ all necessary experts, including DPOs and CISOs. Many of these smaller entities provide various services as data processing entities (e.g., training providers, external accounting firms, event organizers), making it crucial for data controllers to choose service providers that have implemented appropriate technical and organizational measures in their operations.

Potential for improvements was noted in the following areas, in particular:

- **Art. 5 GDPR**: Administrative relief potential lies in addressing extensive accountability and documentation obligations, which have significantly increased since the GDPR's introduction.
- **Lack of differentiation between private and business-related personal data** in the B2B context: Treating all personal data equally, regardless of its nature, poses challenges, especially in deleting business documents with personal data. Simplifying regulations in the B2B context is desirable. (see also below).
- The **relationship between the GDPR and other legal regulations** poses practical challenges, with financial institutions subject to various special requirements linked to risk management and requirements stemming from the EBA Guidelines on ICT and security risk management. These should serve as guidelines to avoid overwhelming independent assessments.
- **Reporting of data breaches (Art. 33 GDPR):** To prevent excessive reporting and legal uncertainties, the regulation should consider the existence of a foreseeable high risk to rights and freedoms. The prescribed reporting timeframe seems too narrow, especially for breaches discovered on Fridays or before holidays. As an example, due to national occupational safety regulations, such as the German Working Hours Act, there is generally a prohibition of employment on Sundays and holidays (see § 9 (1) ArbZG).
- **Data protection by design and by default (Article 25):** Article 25 addresses only data controllers, not manufacturers. This compels controllers to assess products for privacy vulnerabilities before use, incurring significant effort. The ongoing debate on the privacy-compliant use of Microsoft 365 products highlights this issue. Manufacturers should be obligated to consider data protection laws in product development, aligning with the state of the art to enable controllers to fulfill their obligations.

The obtention of consent and the duration of its validity was also reported to pose challenges in some situations, because of national regulators' room for interpretation. A lack of resources in national data protection authorities was noted in some countries.

II. Exercise of data subject rights

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

The information obligations outlined in Articles 13 and 14 are overly detailed and extensive. To prevent individuals from being overwhelmed, it is advisable to streamline these requirements reasonably. A two-tiered approach, offering an overview initially and detailed information upon request or in a second step, would be a preferable solution.

2. Access to data (Article 15)

Article 15 is often misused for non-data protection purposes in practice, such as in employment termination disputes during negotiations for severance agreements. A legal clarification is desirable, stating that Article 15 of the GDPR is limited to data protection matters, requiring the data subject to demonstrate this. Additionally, a more nuanced regulation of the restrictive counter-rights under Article 15 of the GDPR at the GDPR level would be desirable. This aims to limit individuals' right to access information, considering factors similar to the catalog of restrictions under national law such as the German Freedom of Information ACT, with restrictions such as trade secrets, personal data of third parties, important public interests, and irrelevant information requests.

This would also involve reining in recent extensive jurisprudence on the scope and extent of the right to access, especially regarding the right to obtain a copy under Article 15(3) Sentence 1 of the GDPR, taking into account the ongoing case at the Court of Justice of the European Union (CJEU) with reference to Case C-307/22 and the available Advocate General's opinion.

3. Erasure (Article 17)

The deletion of data can be technically challenging, leading to the suggestion of permanently blocking relevant personal data in cases of disproportionate or technically unfeasible deletion (according to Articles 5 and 17 of the GDPR). Overall, there should be consideration given to qualifying or limiting the existing high deletion requirements, especially by placing stronger emphasis on technical feasibility in implementing deletion requests and enabling alternative protective measures in cases of lacking technical feasibility.

Deleting data, particularly in the B2B context, poses significant challenges, including obligations to delete documents and information containing personal data. The GDPR currently protects contact data with personal reference in business correspondence, similar to other personal data, which extends beyond the GDPR's primary purpose of safeguarding the fundamental rights and freedoms of data subjects. As an example, the handling of the mailbox of departed employees was mentioned. Facilitating measures for personal data in the B2B context would be desirable.

4. Meaningful explanation and human intervention in automated decision making (Article 22)

The criterion of human intervention should be clarified, specifying that the controller is required to examine and apply the data subject's input to the decision-making parameters. There should not be an additional scope for intervention beyond this.

III. Data protection officers (DPOs) (Question 7)

To enable Data Protection Officers (DPOs) to perform their duties properly, it would be helpful if the GDPR stipulated that, in addition to the DPO, one or more Data Protection Managers could also assume operational tasks.

IV. International transfers (Question 9)

It is suggested that the EU Commission consistently evaluates criteria for a Transfer Impact Assessment (TIA) concerning the use of EU Standard Contractual Clauses in connection with individual third countries. These criteria should not only consider specific data recipients but also encompass the overall legal framework and data protection standards in these countries. The outcomes of these assessments should be publicly disclosed to aid companies in conducting individual assessments, promoting transparency, and saving resources.

Additionally, Transfer Impact Assessments for third-country transfers should be publicly accessible through data protection supervisory authorities.