8 February 2024

EBF_046379

# European Banking Federation (EBF) response to the European Commission Call for Evidence on the Report on the General Data Protection Regulation (Art. 97)

## General comments

This response complements the questionnaire response provided to the European Commission Multi-Stakeholder Expert Group of which the European Banking Federation is a member of.

The introduction of the GDPR resulted in a significant increase in the attention for and the application of data protection rules. The banking sector has a long tradition of compliance and affinity with customer data protection since even before the entry into force of the Directive 95/46/EC. Adapting to the updated requirements introduced by the GDPR has taken place through internal compliance programs. This enduring commitment underscores the industry's dedication to maintaining the highest standards of data security and privacy for its clients.

The principle and risk-based approach of the Regulation remains one of its main benefits and should remain at the core of the GDPR. This is important for banks in light of the many sectoral regulations they have to abide by and for their ongoing digital transformation.

However, challenges remain, and we would like to highlight the following general points:

### 1. Ensuring the uniform application and implementation of the GDPR across member states

The risk of fragmentation due to different interpretations of the GDPR by Data Protection Authorities (DPAs) remains a challenge. A uniform application is crucial to avoid operational burdens and legal uncertainties and to foster cross-border services and contribute to a unified market for retail financial services.

### 2. Practical consideration of the interplay between the GDPR and other regulations, including at the sectoral level

A recurring challenge for the financial sector is the **interaction of the GDPR** with **sectoral requirements**. Examples include the interplay with the anti-money laundering (AML) obligations and with the revised Payment Services Directive (PSD2). Positive steps have been taken in the updated frameworks for AML and payments (currently under discussion by co-legislators) in areas such as information sharing. An important area where interplay remains to be addressed is sanctions regulations, where there are still uncertainties when it comes to data retention and, because of this, may make it difficult for banks to demonstrate compliance with regulations upon request from supervisory authorities.

**European Banking Federation aisbl**
**Brussels /** Avenue des Arts 56, 1000 Brussels, Belgium / +32 2 508 3711 / info@ebf.eu
**Frankfurt /** Weißfrauenstraße 12-16, 60311 Frankfurt, Germany
**EU Transparency Register /** ID number: 4722660838-23

European Data Protection Guidelines (EDPB) guidelines may also benefit from a more sectoral-level approach, which can be overlooked when guideline are issued, for example, on the right of access, which take a very prescriptive approach and do not take into account sector specific obligations (e.g. including in the text that the scope of the right of access includes "data inferred or other data, rather than directly provided by the data subject (e.g., to assign a credit score or comply with anti-money laundering rules…." ) Sharing this type of (very sensitive) data poses serious risks to a bank. For example, certain aspects of AML compliance are under a duty of secrecy; divulging information for example on whether a transaction is suspicious or that an institution is investigating it, for a possible report to the Financial Intelligence Unit, constitutes a breach of AML legislation (tipping off prohibition).

To help address this gap, we suggest:

- More **dedicated exchanges or outreach with DPAs allowing for sharing operational constraints and sectoral experiences**. Currently experiences vary, in some cases limited contact with a bank's DPA and difficulties in being heard on operational aspects/specifics of the sector mean that no practical recommendations are provided to banks, even when they share their practices and views.
- Increased **collaboration between the EDPB, and sectoral authorities**, for example the European Banking Authority, and organisations representing the industry to avoid conflicting interpretations and diverging rules. For instance, the final EDPB guidelines on the interplay between GDPR and the revised Payment Services Directive (PSD2) left many concerned entities, including banks, with a choice of which legislation to comply with in light of the recommendations presented in the guidance.

Overall, DPAs, play a key role on awareness raising, and more initiatives, including targeting different sectors, would be highly valuable. Learnings should be drawn from the experiences of the past 5 years and shared with the general public.

## 3. Preserving the risk-based approach of the GDPR.

Guidelines and recommendations published by the EDPB are non-binding yet hold great persuasive value and may contribute to reducing the margin of manoeuvre of data controllers in abiding by the principles of the GDPR. Moreover, the diminishing risk-based approach is also affecting the developments in the jurisprudence, as shown, for example, by recent CJEU case law.

The GDPR created the accountability principle to allow companies to take their responsibilities and find the best way for their organisation to comply with the regulation. For banks, this includes performing DPIAs, registering their data processing, hiring a DPO and performing audits, among other actions. However, often banks are limited by the EDPB guidelines, which are largely too prescriptive with details or rules to implement certain obligations, which **undermine the accountability principle and the risk-based approach put forward by the GDPR.** There is limited space to autonomously decide (e.g., *EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*).

Indeed, the more strict and rigid guidelines are, the less margin of manoeuvre is left for data controllers in the sector to attain the same goal by using mechanisms or

making choices that are more appropriate for the sector and/or their organisations. Given the fact that these guidelines have great influence, if one company attains the objectives of the GDPR slightly differently than how it is described in the guidelines, that company can be seen as being non-compliant, without this being the case.

## Specific comments

In terms of specific comments, we would like to flag in particular those on the following topics:

### *i. Information obligations, including the type and level of detail of the information to be provided (Articles 12 to 15).*

The right of access to data continues to be the **most requested** and known data subject right among clients. Detailed information on how to exercise the individual's right of access pursuant to Art. 15 GDPR is provided to customers. Privacy statements on the bank's website usually have information on how to exercise their rights, including that of access, and a specific link or page that clients can visit to do so.

Based on the experience of members, the great majority of access requests are made by data subjects who are involved in a dispute with their bank or are considering starting legal proceedings or other dispute resolution mechanisms against a financial entity and much less for the purpose of verifying the legitimacy of their data processing.

In these cases, the normal procedural way to obtain evidence should be used to guarantee the equality and fairness of the judicial process, not the GDPR. The rules of civil procedure should be able to coexist with the right of access of clients. We understand that obtaining a copy of the data (which in some cases this could mean providing a copy of certain documents) is necessary to guarantee the effective exercise of data subjects' access rights and that the CJEU's judgement in the Case C-307/22 indicates that data subjects can request a copy of the data for purposes not referred in to recital 63, even unrelated to data protection, but there should still be a respect for established civil procedures and an appreciation that these can be limitations, examined on a case by case basis.

In order to provide certainty for clients and for banks, we would therefore recommend to explore the relationship between local rules of civil procedure at member state level and Article 15 further (e.g., to what extent may Art. 15 "tops" traditional rules of civil procedure). The EDPB guidance on the right of access addresses this matter in a footnote.

- **Addressing a data access request**

In practice, it is sometimes difficult to understand and decide how a particular request should be treated and what would be of most use to the data subject. Engaging with the individual to clarify the purpose and reasoning of the request could be very helpful in such cases for both the controller and the data subject.

Clients that exercise their right in the particular context explained above may be disappointed with the access provided by the bank. It should be noted however that "[*a]fter all, the GDPR is not a piece of legislation on access to documents, but on data protection. Consequently, its primary focus is ensuring access to data, not to documents that contain data. Whereas in some cases the latter may necessarily imply the former, that is not always so*[1]." Certain documents are not provided simply because they fall outside the scope of the GDPR.

[1] Conclusion of the AG in the case ECLI:EU:C: 2023:811.

- **Difficulty to meet the deadlines established in the GDPR**

From practical experience, **additional time is often necessary to answer an access request**. This can be due to factors such as unclear wording, which requires asking for additional information from the data subject or that answers are not received from the data subject to the request for clarification from the controller. On occasions, members also see an influx of requests due to external factors. In these cases, if banks do not manage to process all the requests, they notify the data subjects that they require additional time to respond.

- **Avoiding a prescriptive approach**

In practice, there needs to be **an understanding of the limitations that may be placed on the right of access** whether it is in cases of protection of business secrets, safeguarding the personal data of third parties, upholding significant public interest, or where existing civil procedures need to be respected when it comes to obtaining information/evidence for court cases.

### *ii. GDPR and innovation/ new technologies*

The framework provided by the GDPR, notably the **risk based and principle-based approach, provides the room for innovation and the adoption of new technologies**. With the introduction of every new technology, the challenge is how to appropriately manage the associated risks, including data protection risks.

Taking AI, which continues to be at the top of mind, also because of the Artificial Intelligence Act, guidance on the interaction between the AI Act and the GDPR, notably Article 22 and its different elements, would be welcome, particularly with sector specific examples.

Moreover, from a data protection risk assessment perspective, the growing number of cases in which banks must deal with the integration of new technologies in their systems would benefit from clear guidelines from DPAs. For instance, members would welcome more examples of data protection risk assessment models, following the steps of authorities from other jurisdictions (such as UK) and in line with international standards (such as ISO).

Finally, we also suggest creating more spaces to test innovative technologies/new solutions (e.g., ChatGPT), for example, regulatory sandboxes with the participation of data protection authorities, which can better help to identify and deal with risks and how the implementation of data protection rules may be impacted. The sector welcomes this provision in the AI Act. It would be good that these already start and not wait until the Act is in place.

**ENDS**

**For more information:**

**Liga Semane**

Senior Policy Adviser – Data & Innovation

l.semane@ebf.eu

## About the EBF

The European Banking Federation is the voice of the European banking sector, bringing together 32 national banking associations in Europe that together represent a significant majority of all banking assets in Europe, with 3,500 banks - large and small, wholesale and retail, local and international – while employing approximately two million people. EBF members represent banks that make available loans to the European economy in excess of €20 trillion and that reliably handle more than 400 million payment transactions per day. Launched in 1960, the EBF is committed to a single market for financial services in the European Union and to supporting policies that foster economic growth.