Andrea Jelinek, Chairperson, European Data Protection Board
Marcel Haag, Director Horizontal Policies, DG Financial Stability, Financial Services and CMU
Emmanual Crabit, Director Fundamental Right and Rule of Lw, DG Justice
Maria Velentza, Director Financial Services, DG Competition
Dirk Haubrich, Head of Conduct, Payments and Consumers, European Banking Authority

Brussels, 31 January 2022

Final EDPB Guidelines on the interplay of the Second Payment Services Directive and the GDPR

Dear Chairperson Jelinek,
Dear Mr Haag,
Dear Mr Crabit,
Dear Ms Velentza,
Dear Mr Haubrich,

The payments sector, represented by the undersigned associations, **remain fully committed to ensuring the protection of EU citizen's data, including within the framework of the revised Payments Services Directive (PSD2).** With this letter, we would like to address the European Data Protection Board's (EDPB) Guidelines on the interplay of PSD2 with the General Data Protection Regulation (GDPR). This follows our earlier letter sent on 27 October 2020 to highlight our concerns on the draft Guidelines. **We are still concerned that the enforcement of the Guidelines will lead to an outcome that is not in line with PSD2 objectives, therefore hindering innovation and competition in payments and creating additional burdens to all participants.**

While the final Guidelines make a step forward to clarifying certain aspects of the interplay, such as the confirmation that explicit consent under Article 94 PSD2 is different from (explicit) consent under the GDPR, **other elements remain more worrying and raise new uncertainties, notably the provisions on data minimization and processing of special categories of personal data (SCPD).** Importantly, there is still a lack of coherence with the Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Communication (RTS on SCA & CSC)[1].

Alongside these concerns is the risk that national Data Protection Authorities (DPAs) could start taking a differentiated approach to the interpretation of the provisions. **This could result in fragmentation across the EU on the Guidelines and would add to a worrying trend across Europe when it comes to GDPR implementation.**

[1] Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication

1. **Data minimisation**

a) Risk of creating a new obligation potentially in conflict with PSD2

We remain concerned on **the interpretation of data minimisation obligations** offered by the final Guidelines, notably the use of "*digital tools to only collect personal data that are necessary for the purposes for which they are processed*." While only a recommendation, it would be very difficult to implement in practice and would be contrary to PSD2 obligations.

Pursuant to PSD2, Account Servicing Payment Service Providers (ASPSPs) are obliged to provide Third Party Providers (TPPs) with the **same information from designated payment accounts and associated payment transactions made available to the payment service user (PSU) when this PSU is directly requesting access to the account information** (see Article 36(1)(a) RTS). This is the minimum but also at the same time the maximum amount of information that ASPSPs are obliged to disclose to TPPs in order to make sure that the purposes of PSD2 can be attained.

ASPSPs abide by the principle of data minimisation when they provide access to accounts in the same way as if the PSU would be directly requesting access to its account. They do not provide access to more data than these. Alongside this, **it is the responsibility of each Payment Service Provider (PSP), as the data controller, to respect the principle of data minimisation,** undertaking its own assessment and determining the scope of data minimisation in relation to the intended purposes and the risks involved. This means that data minimisation towards PSUs and any other relevant data subjects is achieved one way or another: ASPSPs provide no more information than the bare necessary to abide by the PSPD2 obligations and Article 36(1)(a) RTS. TPPs in turn take measures to only use – and dispose of appropriately if not necessary – the data they need. We would like to point out that ASPSPs have no means to be aware of the contract between the PSU and the TPP, meaning that banks cannot know the purpose for which the TPP asks to access the PSU payment account.

As a result, there is **no need to derive from the principle of data minimisation an extra obligation** on ASPSPs to amend their APIs, since the principle of data minimisation regarding the further use of data already allocates the responsibility of each data controller. Even more so if such an obligation would entail the risk that ASPSPs infringing the RTS. **Proportionality and practicability of obligations without implying a detriment for citizens should be taken into account before deriving any new obligation for firms with such a recommendation.**

TPPs, as data controllers in the terms of the GDPR and as licensed parties, are the sole party to take decisions and put in place adequate technical measures to ensure that they only use the data that will be necessary to provide their services.

Therefore, looking at the new Example 2 in the Guidelines and the wording that "*ASPSPs allow HappyPayments to request specific fields for a range of dates",* the situation **presupposes additional technical measures on the part of ASPSPs beyond obligations laid down in PSD2,** which would run in contrary to the obligations to provide the AISPs with the same information form designated payment accounts and the responsibility of *each* data controller to data minimisation. These **technical**

measures are also not included in the RTS, meaning the Guidelines de facto create a new obligation for ASPSPs and, in parallel, legal uncertainty for all actors in the PSD2 ecosystem, particularly as the compliance deadline with the level 1 EBA RTS on SCA and CSC for market participants was 14 September 2019.

Furthermore, the additional obligations that would result from the Guidelines would put additional strain on the functioning of the dedicated interfaces that ASPSPs have had to build under PSD2 because of the very detailed level of granularity. This could result in reduced performance and stability of the dedicated interface for which there are enforceable KPIs.

Please note that TPPs are subject to the principle of data minimisation as set out in Article 5(1)(c) of the GDPR. In instances where the TPP considers that not all the personal data that ASPSPs are obliged to securely provide as per the PSD2 is required in order for the TPP to provide a given TPP service, we consider the TPP may give effect to the principle of data minimisation by discarding any personal data, upon receipt, that is not required to provide the TPP service. This will ensure the TPP remains compliant with the principles relating to the processing of data as set out in Article 5 of the GDPR as well as in compliance with their contract with their customer (the payment service user).

b. Risk of fragmentation

Adding to this uncertainty is the risk of fragmentation on the interpretation of the Guidelines at national level, **which may lead to uncertainty for the banking sector as well as for TPPs in their ability to offer and develop services under the PSD2 framework**. Lack of a consistent interpretation is also a significant issue for banks with cross-border actions and puts those that may be expected to amend their APIs in a **competitive disadvantage with respect to ASPSPs in other EU countries that would not be required to do so.** The level playing field is therefore threatened with this interpretation in the Final Guidelines.

This is part of a **wider trend with regards to the implementation of the GDPR across the EU, where key provisions of the GDPR (e.g., legal basis such as legitimate interest) or now the interplay between two key pieces of legislation for the banking sector, are interpreted differently – going against the spirit of the Regulation itself.** This fragmentation needs to be stemmed at EU level. We also call upon EU authorities to include considerations of coherence with GDPR obligations **in the design of future legislative actions (such as PSD2 and future open finance framework)** in order to avoid similar issues and implementation challenges in the future.

2. Processing of special categories of personal data (SCPD)

Financial transaction data is not mentioned under Article 9(1) GDPR as a special category of personal data. The final Guidelines, however, seem to presume that financial transaction data could be special categories of personal data (SCPD). **This interpretation could have a considerable, extensive impact on the provision of payment services and financial services in general, going beyond PSD2.**

Furthermore, to extrapolate information about any category of sensitive personal data mentioned under Article 9(1) GDPR from the financial transaction data of a PSU, **processing must be intentionally undertaken by the controller (with the purpose element in mind) as clarified by the Guidelines.** In this regard, controllers would apply the conditions proscribed under Article 9 GDPR (explicit consent or the possible derogations). However, if financial transaction data are not processed in order to infer SCPD, Article 9(1) GDPR should not apply. A similar principle is included in the GDPR in Recital 51, which acknowledges that the processing of any photograph might trigger the processing of special categories of data but this should not be construed as if anyone who collects photos is processing these categories of data. Also for photographs, lacking a specific additional technical processing, there is no processing of biometric data (which are included amongst the special categories of data). We also note that while the final Guidelines softened the language with regards to implementing technical measures to prevent the processing of SCPD, for instance, by preventing the processing of certain data points, this possibility remains and could have significant repercussions. In addition to technical measures being very difficult to implement in practices**, applying any such techniques would also first necessarily imply the processing of account information to reveal SCPD, which would have a negative effect on the personal data protection of the PSU.**

It could also result in the following two scenarios:

- **Legitimate use cases could be rendered impossible**. For example, an AISP that enables customers to organise and classify payments in their transaction record would not be able to function correctly if, for example, payees and / or payors were redacted. Focusing on the whole, the key objective should be that a user/PSU should experience the same usability and "see" the same data whether the entrance is via an ASPSP or through a TPP.
- If an ASPSP were to redact data transferred to TPPs or in some other way prevent their access to data to which they are entitled under **PSD2, the ASPSP would be in breach of its obligations under PSD2.** The Guidance should not recommend measures that would force firms to breach their legal obligations.

Therefore, we would welcome a recognition that Article 9 (2)g GDPR, in any case, already would provide a legal basis for the processing of SCPD.

3. Further processing under PSD2

The final Guidelines maintain that there will be no legal ground, in any case, for further processing for AISP and PISP and that the compatibility test under Article 6(4) GDPR can never reach a positive result (i.e., cannot offer grounds for further processing). However, no supporting arguments are provided as to why the end result would always be negative. This makes the decision hard to understand, but also does not give more insight in the application of this compatibility test for other use cases as well. Furthermore, it is the responsibility of the controller to assess if it is possible or not (the accountability principle and Article 24 GDPR).









4. Silent party data

Finally, we see the same risks with regard to legitimate use cases when it comes to the processing of silent party data. The final Guidelines may be interpreted in a way that TPPs only need silent party data for the purpose of contract performance and that the further processing of silent party data is generally not permissible. We believe this interpretation goes beyond the requirements of GDPR, taking into account that (i) silent party data often do not concern natural persons, but companies (phone providers, supplier of electric energy, insurances, banks, supermarkets, gas stations etc.) or public authorities and therefore, the processing of silent party data falls outside the scope of the GDPR, and (ii) that the processing of silent party data may be necessary (indispensable) for other legitimate interests. We do not see objective reasons for a general exclusion of the processing of silent party data for other legitimate interests in terms of Art. 6 (1)(f) GDPR, provided that the rights and freedoms of these silent party data subjects are adequately considered by the TPPs in the context of a balancing exercise in terms of Art. 6(1)(f) GDPR and that appropriate technical and organizational measures are taken by the TPPs for the adequate protection of silent party data.

5. Conclusion

In highlighting the concerns with regards to processing of SCPD, data minimization, and further processing under PSD2, we aim to demonstrate that uncertainties remain in the interaction of these two frameworks despite the publication of the final EDPB Guidelines. Some of these include measures which could imply a breach of obligations and detriments for all parties involved, notably payment service users.

We would therefore welcome to continue the discussion between all relevant institutions and stakeholders in the GDPR-PSD2 ecosystem to address these challenges and provide legal certainty for all actors to enable them to meet their obligations and continue to provide services for their customers. We thank you for your attention and remain available to discuss these issues further. In the meantime, we would be pleased to receive your preliminary view on our points above.

Yours sincerely,

Wim Mijs
Chief Executive
European Banking Federation (EBF)

Peter Simon
Managing Director
European Savings and Retail Banking Group (ESBG)

Nina Schindler
Chief Executive Officer
European Association of Cooperative Banks (EACB)

Ralf Ohlhausen
Chair
European Third Party Providers Association (ETPPA)

Marcel Roy
Secretary General
European Association of Public Banks (EAPB)

Elie Beyrouthy
Chair
European Payment Institutions Federation (EPIF)

Thaer Sabri
Chief Executive Officer
Electronic Money Association (EMA)

Marc Roberts
Chair
European FinTech Association (EFA)

Robrecht Vandormael
Secretary General
Payments Europe (PE)