Position Paper

Bitkom views on EDPB Guidelines 6/2020 on the interplay of the Second Payment Services Directive and the GDPR

16/09/2020

Federal Association
for Information Technology,
Telecommunications and
New Media

Rebekka Weiß, LL.M.
Head of Trust & Security
P +49 30 27576 -161
r.weiss@bitkom.org

Albrechtstraße 10
10117 Berlin
Germany

President
Achim Berg

CEO
Dr. Bernhard Rohleder

Introduction and Overview

Bitkom welcomes the opportunity to comment on the European Data Protection Board's (EDPB) draft Guidelines on the interplay of the Second Payment Services Directive and the GDPR (EDPB Guidelines). We believe that more cooperation and exchange between data protection authorities and practitioners is needed to translate the legal text of the GDPR into practice and reduce legal uncertainty, especially in the context of the interplay with the Second Payment Services Directive (PSD2) as well as with other legislation.

We therefore appreciate that the EDPB published the draft Guidelines on the interplay of the PSD2 and the GDPR and appreciate the opportunity to comment on the Guidelines. We will give detailed feedback on specific sections below. As Bitkom represents new service providers as well as traditional industry players, our paper outlines cross-industry arguments and solutions.

1. Summary

We welcome that the EDPB Guidelines clarify some important questions, especially in the interpretation of the PSD2 concept of "consent" or in the authorization to process third party data (so-called silent party data). Furthermore, the guidelines bring some clarity for the legal regime of the PSD2 and the application of the GDPR. They are therefore suitable for payment service providers, but in particular for payment initiation service providers

(PISP) and account information service providers (AISP), to be able to offer and further develop their products and innovate.

We also welcome that the areas and purposes of AIS and PIS which are not part of the payment services contract between the TPP and the payment service user (User), i.e. creditworthiness, risk checks as well as identification, are nonetheless subject to the scope of the GDPR, so that in future delimitation difficulties will be reduced and harmonization and alignment with alternative procedures can be achieved.

We see the need for amendments in the Guidelines though with regard to the proposed digital filters, which will severely restrict the business models created by the PSD2. The EDPB does not clarify how digital data filters are to be implemented and how a duty to implement such a filter can be aligned with the framework of the PSD2 and the RTS.

We detailed our concerns and proposals below in the following sections.

2. Key Aspects in Detail

2.1 Definitions

For the avoidance of doubt, we suggest to add PSD2's definition of payment service user under sect. 1.1: 'Payment service user' means a natural or legal person making use of a payment service in the capacity of payer, payee, or both. The Guidelines should also refer to the definitions in the referenced legislation:

- AML Directive means Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system or the purposes of money laundering or terrorist financing of the anti-money laundering directive;
- AISP shall have the meaning set forth in Art.4 (19) of the PSD2;
- ASPSP shall have the meaning set forth in Art.4 (17) of the PSD2;
- PISP shall have the meaning set forth in Art.4 (18) of the PSD2;

- TPP means collectively AISPs and PISPs;
- User shall have the meaning set forth in Art. 4 (10) of the PSD2.

2.2 Further Processing of Personal Data

TPPs can offer services to the User such as initiating a payment transaction, giving an overview over bank accounts held by different banks, providing budget planning, monitoring services, as well as services that entail creditworthiness assessments of the User. The EDPB Guidelines establish much needed clarity regarding the different types of services offered in respect to account information data. Processing of personal data relating to payment services are covered by the scope of application of PSD2, while processing for other services fall outside the scope of PSD2 (e.g. creditworthiness) but are nonetheless covered by the GDPR since they still constitute processing of personal data in any case.

In this sense, we welcome the clarification that the processing of personal data for the provision of the payment services is conducted in accordance with Art.6 (1) (b) of the GDPR, that is, processing which is necessary for the performance of a contract; while "further processing" of such data requires either consent within the meaning of the GDPR (Art. 6 (1) (a) of the GPDR or that such processing is mandated by an Union law or Member State law.

2.3 Consent

Regarding the processing of personal data relating to the provision of payment services, we welcome the clarification of the EDPB Guidelines with regards to "explicit consent". In our opinion, this is the most important clarification. "Explicit consent" as mentioned in Art. 94(2) of the PSD2 means a contractual consent and is not related to consent as a legal basis for the processing of personal data in accordance with Art. 6 of the GDPR. We welcome the clarification that the legal ground for the processing of personal data in the provision of payment services is the contractual relationship between the TPP and the User, in accordance with Art.6(1)(b) of the GDPR.

It also enables payment service providers to implement user-friendly processes. More elaborations in this sections and examples would we welcomed to bring more clarity with regard to this highly relevant aspect.

2.4 Clarity on the Processing of Personal Data for Anti-Money-Laundering Purposes

As recognized by the EDPB Guidelines, all PISPs and AISPs are obliged entities under Art. 3(2) of the AML Directive. As such, TPPs have the legal obligation to process personal data when applying customer due diligence measures. While the EDPB Guidelines expressly recognize this as a valid legal ground for the processing of data beyond the contractual relationship with the payment service user, we believe that such obligation should also extend to the processing of special categories of data in accordance with Art. 9(2)(g) of the GDPR (substantial public interest) and would welcome a clarification in this sense.

2.5 Obligations of the ASPSP

In Sect. 25 it is stated that *"The effective application of such rights would not be possible without the existence of a corresponding obligation on the ASPSP, typically a bank, to grant the payment service provider access to the account under the condition that it has fulfilled all requirements to get access to the account of the payment service user."*

For the avoidance of doubt, we recommend that the EDPB highlights that it is not the ASPSP's obligation to check whether the conditions are fulfilled; rather it is the TTPs responsibility to fulfil such conditions. This would align the Guidelines with the regulations of PSD2 / RTS, according to which ASPSPs need to provide "account information service providers with the same information from designated payment accounts and associated payment transactions made available to the payment service user when directly requesting access to the account information, provided that this information does not include sensitive payment data" (Art. 36(1)(a) RTS). It is the TPP's (PISPs' / AISPs') responsibility to access data in accordance with PSD2 / GDPR.

2.6 Silent Party Data

We welcome the clarification of the EDPB that the processing of silent party data can be conducted under the legal bases of legitimate interest (Art. 6(1)(f) GDPR) of the TPP and that such legitimate interest can be the performance of the contract with the payment service user. As the

EDPB Guidelines rightly state, a legitimate interest always requires an assessment by the controller. As this is often difficult to assess in practice, we suggest that the EDPB included examples to elaborate on the question which interests have to be balanced and included in the assessment.

The EDPB Guidelines mention that personal data in connection with a payment service which falls under the scope of PSD2 can be further processed based on legal obligations of the service provider. We would request the EDPB to expressly mention that in these regards.

The processing of silent party data may be necessary for compliance with the requirements of the AML Directive. Such processing does not seem contradictory to the reasonable expectations of the silent parties, given that it is public knowledge that TPPs are obliged entities under the AML Directive. Also considering the scope of data processing (name and IBAN of the silent party) it is not apparent why the rights and freedoms of the silent party data should generally prevail the TTPs legal obligations regarding AML.

With regard to Sec. 49 of the EDPB Guidelines, we propose an amendment as we are missing a statement on information duties in this section. It should be clarified within the Guidelines that the silent parties do not need to be informed according to Art. 14 (5) (b) of the GDPR ("provision of such information proves impossible or would involve a disproportionate effort").

2.7 Processing of Special Categories of Data

In this section EDPB describes the general requirements resulting from the processing of special categories of personal data and gives some guidance for a data protection audit - but without giving exact details. Therefore, this passage is limited to the description of the status quo. It would be advisable - independently of these guidelines, but rather in relation to Art. 9 GDPR in general - to distinguish between the relevance of the processing Art. 9 data, depending on whether the data is collected as a mere “accessory” or whether the data that falls under Art. 9 is processed specifically for a certain purpose that is targeted on using the special categories of data and therefore carries a certain risk for the data subject.

2.8 Technical Measures

With regard to Sec. 57, Sec. 62 and Sec. 63 of the EDPB Guidelines, we find that the Guidelines need to be more precise when it comes to the suggested "technical matters" that shall be but in place to prevent processing of special categories of personal data. In this sense, we would suggest that the EDPB Guidelines expressly mention that no technical measures to limit the processing of personal data by the TPP should be included on the side of the ASPSP. Otherwise, it could be misleadingly interpreted as an obligation of the ASPSP to restrict the sharing of data and limit it to certain fields the ASPSP unilaterally considers appropriate. This would contradict the very purpose of the PSD2.

The EDPB Guidelines suggest that TPPs may need to take technical measures to select relevant data categories before the data are collected. We believe this is often not feasible given that at the time of data collection it is not apparent before data collection which transaction characteristics contain special categories of personal data, in the same way as it is also not apparent before data collection which financial transactions are relevant for AML purposes.

A selected access would also be in contradiction to PSD2 / RTS, according to which ASPSPs need to provide *"account information service providers with the same information from designated payment accounts and associated payment transactions made available to the payment service user when directly requesting access to the account information, provided that this information does not include sensitive*[1] *payment data"* (Art. 36 (1) (a) of the RTS).

Moreover, any kind of filtering of special categories of personal data would be complex with a risk of not being complete or leading to over-blocking of data, as special categories of personal data are subject to constant social development and depend on context. That is why TPPs need to provide technical measures to secure such data, which they currently do, as they have the same levels of security requirements for processing and storing data as ASPSPs. The aspect the Guidelines should therefore be focussing on is giving examples and guidance on how transparency can be achieved for the user with regard to the data transfer.

[1] Sensitive payment data in this context does not mean Art. 9 GDPR data.

2.9 Access to Accounts

The EDPB Guidelines correctly state in Sec. 64 that there is no legal basis under the PSD2 to provide access with regard to personal data contained in other accounts, such as savings, mortgages or investment accounts. We would welcome a clarification, however, that this does not generally exclude access to other account types, but that such access falls outside the scope of the PSD2 and is therefore subject to general rules and consent given by the user.