German Banking Industry Committee

Die Deutsche Kreditwirtschaft

Comments

regarding Guidelines 06/2020 on the interplay of the Second Payment Service Directive and the GDPR, Version 1.0, adopted on 17 July 2020

Register of Interest Representatives
Identification number in the register: 52646912360-95

Contact:
Dr. Christian Koch
Telephone: +49 30 2021-2321
Telefax: +49 30 2021-192300
E-mail: c.koch@bvr.de

Berlin, 14. September 2020

The **German Banking Industry Committee** is the joint committee operated by the central associations of the German banking industry. These associations are the Bundesverband der Deutschen Volksbanken und Raiffeisenbanken (BVR), for the cooperative banks, the Bundesverband deutscher Banken (BdB), for the private commercial banks, the Bundesverband Öffentlicher Banken Deutschlands (VÖB), for the public-sector banks, the Deutscher Sparkassen- und Giroverband (DSGV), for the savings banks finance group, and the Verband deutscher Pfandbriefbanken (vdp), for the Pfandbrief banks. Collectively, they represent approximately 1,700 banks.

Coordinator:
National Association of German Cooperative Banks
Schellingstraße 4 | 10785 Berlin | Germany
Telephone: +49 30 2021-0
Telefax: +49 30 2021-1900
www.die-dk.de

Comments regarding Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR, Version 1.0, adopted on 17 July 2020

I. General remarks

The Guidelines released by the European Data Protection Board on the interplay of the requirements set out in the Second EU Payment Services Directive (PSD2)[1], together with its Regulatory Technical Standards in Delegated Regulation (EU) 2018/389 (RTS)[2], and the General Data Protection Regulation (GDPR)[3] are welcomed as support for implementation:

- From the perspective of the German Banking Industry Committee, it is key to harmonise the (data protection law) requirements set out in the two European Regulations in order to establish better planning and legal certainty for all parties involved: for account servicing payment service providers (ASPSP), for third-party services – payment initiation service providers (PISP) and account information service providers (AISP) –, for payment service users and for both the authorities responsible for supervision under the PSD2 and data protection supervisory authorities in the EU member states. It is also, however, important not to complicate the processing of retail payments by payment service providers, i.e. the execution of credit transfers and direct debits, within the Single Euro Payments Area (SEPA).

- It is essential to make a clear distinction between the respective data protection law responsibilities of each type of payment service providers – ASPSP, PISP and AISP – based on the roles described in the PSD2. This is because the controller, as defined in Article 4 no. 7 GDPR, is obliged to meet the requirements set out in the GDPR with regard to the legal basis for data processing (Article 6 GDPR), the information obligations (Articles 12, 13, 14, 21 GDPR, etc.) and the technical and organisational data protection measures for the controller's own sphere of responsibility.

- It is important to note that, according to the Guidelines, the PSD2 only contains provisions governing access to payment account data that is relevant for the purposes of the PSD2; further access to payment accounts or access to non-payment accounts (such as savings, credit, securities deposit accounts) is not covered by the PSD2, meaning that it has to be viewed exclusively in the context of the relevant provisions that apply in each case (data protection law, copyright law, etc.).

We refer to the section below, in which we explain these general remarks.

1. Relationship between provisions governing data access in the PSD2 and the GDPR

The provisions set out in the PSD2 and the GDPR have the same standing under European law and apply alongside each other. If personal data is processed when payment services are provided, each controller involved in this process must comply with the GDPR on the one hand, and the PSD2 together with the applicable national implementing legislation on the other, in its sphere of responsibility:

---

[1] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (PSD2). The PSD2 was transposed into German national law with effect from 13 January 2018. The Act implementing the Second Payment Services Directive (*Zahlungsdiensteumsetzungsgesetz*, "ZDUG") took account of the regulatory framework in the German Payment Services Supervision Act (*Zahlungsdiensteaufsichtsgesetz*, "ZAG") and the civil law provisions in the German Civil Code (*Bürgerliches Gesetzbuch*, "BGB").

[2] 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.

[3] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

- Insofar as Articles 66 and 67 of the PSD2 and the national legislation based on these articles specifically permit access to account data by payment initiation services and account information services, then, from the perspective of the account servicing payment service provider, these articles are permissive rules within the meaning of Article 6(1) sentence 1c of the GDPR. The Guidelines quite rightly support this classification (cf. section 2.4, paragraphs 25 et seq.).
- If a third-party service accesses customer data, it must, in turn, comply with the regulations set out in the PSD2 and the GDPR.
- The PSD2 only includes provisions governing certain aspects of data provision by account servicing payment service providers and data access by third-party services. The provisions of the GDPR, which must be complied with independently by each and every controller, are also applicable. There is no scenario involving joint controllers pursuant to Article 26 of the GDPR because the payment services legislation assumes that there is no contractual relationship between the account servicing payment service provider and the account information service accessing the payment account (cf. Article 67(3) and (4) of the PSD2). This means that the account servicing payment service provider cannot be held responsible for transactions that are exclusively within the third-party service's sphere of responsibility.

2. Information obligations under Articles 13 and 14 of the GDPR

Account servicing payment service providers and account information services are each obliged, for their sphere of responsibility, to implement the information obligations vis-à-vis data subjects in accordance with Articles 13 and 14 of the GDPR. This is because, when account information services are provided, the account information service concerned is given access to the account holder's payment account data, held with the account servicing payment service provider, with the account holder's "explicit consent". Pursuant to Article 67(2) of the PSD2, it is the sole responsibility of the account information service to obtain the account holder's consent and, within this context, to describe the extent to which the data will be accessed and then used (cf. Articles 67(2d) to (2f) of the PSD2). This means that the account holder has also been provided with full information by the account information service on which data is processed by the latter, and for which purpose in keeping with Article 13 of the GDPR. The account servicing payment service provider does not have the knowledge to provide the account holder with information on the data processing operations of the account information service, especially since there is no contractual relationship between the account servicing payment service provider and the account information service provider (cf. Article 67(4) of the PSD2) and no responsibility as joint controllers under the data protection legislation pursuant to Article 26 of the GDPR.

The payment account data retrieved by the account information service provider may also contain information on "silent parties" (e.g. data on the payee in the payer's credit transfer record). Notification by the account information service accessing the data in accordance with Article 14(1) and (2) of the GDPR is likely to be dispensable due to the exceptions set out in Article 14(5b) of the GDPR and, in actual fact, impossible due to the lack of address information. Article 11 of the GDPR precisely does not require any further effort to obtain this information. The Guidelines should make this explicitly clear.

3. Access to account data applying the exemptions in Article 10 of the RTS

Article 10 of Delegated Regulation (EU) 2018/389 (RTS) provides for an exemption from the general obligation to apply strong customer authentication to account access pursuant to the PSD2. Instead of two factors, it may be sufficient to check only one factor for a period of 90 days. In connection with Article 36(5b) of the RTS, the account holder can allow the account information service to independently access

his/her account a maximum of four times a day. In the event that an account servicing payment service provider applies this exemption in the interest of its customers, there are again no additional verification obligations based on the GDPR.

II. Specific comments

Re: section 1.1 – Definition of "payment service provider"

The definitions are based on the definitions used in the PSD2. The term "payment service provider", which is actually an umbrella term for a number of different service providers – ASPSP, PISP and AISP – is often used later on in the Guidelines. In order to make the Guidelines precise and easy to understand, it would be helpful to specify the exact addressee(s) in the individual comments. Otherwise, misunderstandings will arise, especially from the perspective of the account servicing payment service providers (ASPSPs). Paragraphs 20 et seqq., for example, are likely aimed primarily at third-party services. With regard to paragraphs 36 and 37, it would also make sense to clarify which statements refer both to account servicing payment service providers and to third-party services and which only refer to the latter.

Re: section 2.3 – Further processing

Our understanding is that the requirements in section 2.3 are aimed at third-party services (AISP and PISP). This should be specified in this section, e.g. by using a similar sort of heading to that in section 2.4 and adding extra information so that the heading reads "*Further processing (AISP and PISP)*".

Re: section 2.4 – Lawful ground for granting access to the payment account (ASPSP)

We welcome the clarification in paragraphs 25 et seqq. that account servicing payment service providers are legally obliged, in accordance with Article 6(1) sentence 1c of the GDPR, to grant third-party service provider access to payment accounts in line with the framework set out in the PSD2 and the relevant national legislation. This also clearly defines the scope of obligations to be observed by the account servicing payment service provider on the one hand and third-party service provider on the other. While the account servicing payment service provider takes its justification from the law, the third-party service provider can only access the payment service user's payment account data with the latter's explicit consent.

Re: section 3 – Explicit consent

The comments in section 3 "Explicit consent" are to be welcomed, as they provide an appropriate assessment of the interplay between the GDPR and the PSD2. The Guidelines correctly conclude that a distinction has to be made between "explicit consent" within the meaning of the PSD2 and "explicit consent" within the meaning of the GDPR. Section 3.3 "Conclusion" explains in this respect: "*Explicit consent under Article 94 (2) of the PSD2 is an additional requirement of a contractual nature*."

This means that, from the perspective of the account servicing payment service provider, it remains possible, for example, to execute credit transfers and direct debits without the need to obtain separate consent under data protection law. That's reasonable because the explicit contractual instructions issued by the payer to the account servicing payment service provider with regard to the execution of the payment is the legal basis. Any different assessment would constitute an inexplicably formalistic approach offering no added value, also from the perspective of the data subject. Issuing payment orders would otherwise

be made considerably more difficult. The explicit instructions issued by the customer to the account servicing payment service provider and the related specification of the data required for execution include the customer's declaration regarding the purpose for which the data provided is to be processed.

Re: section 4 – The processing of silent party data

Section 4 deals with the question as to the data protection requirements that need to be met before data concerning a so-called "silent party" (e.g. data on the payee in the payer's credit transfer record) can be processed by the payment initiation service or the account information service. As emphasised above, it is once again important to make a distinction between the responsibilities of account servicing payment service providers and third-party services:

- From the perspective of the account servicing payment service provider, the customer provides the "silent party" data that is a mandatory part of the payment order and its execution under payments law (cf. also the EU SEPA Regulation[4]).
- The silent party data has to be processed by all of the parties involved in the execution of a payment order, as otherwise it would no longer be possible to address the payments.
- From the perspective of the payment initiation service, silent party data also has to be processed in order to provide the service.
- According to the understanding of the PSD2, the account information service is generally to have access to all posting data in the payment account, as otherwise the account aggregation service and the data evaluation for the customer would not be possible.
- The Guidelines appear to focus on the concern that data concerning silent parties could be processed for other purposes. Based on the roles model already mentioned, the comments should add that account servicing payment service providers have no verification and intervention obligations regarding the lawfulness of potential secondary use by the account information service provider in relation to the processing of silent party data, since responsibility for this data processing within the meaning of the PSD2 lies solely with the account information service.

Re: section 5 – The processing of special categories of personal data under the PSD2

This section examines the requirements based on which the special categories of data pursuant to Article 9 GDPR can be processed.

The last sentence of section 5.5 reads:

"*In this respect, payment service providers may explore the technical possibilities to exclude special categories of personal data and allow a selected access, which would prevent the processing of special categories of personal data related to silent parties by TPPs*."

As emphasised above, there should be made a clear distinction between the responsibilities of account servicing payment service providers and third-party services:

- With regard to account servicing payment service providers, the requirements set out in Article 9(2g) of the GDPR are always met. After all, a functioning payments system is a "*substantial public interest, including interests of systemic importance*". The exploration of payment information

[4] Regulation (EU) No 260/2012 of the European Parliament and of the Council of 14 March 2012 establishing technical and business requirements for credit transfers and direct debits in euro.

called for in the Guidelines would be equivalent to a data protection upload filter. Real-time payments would be impossible under these circumstances. "Ordinary" payments would also be at risk. The filtering of sensitive data, as envisaged in the Guidelines, would run contrary to the legislation on payment services and the functioning of the payments system if this requirement were to be aimed at account servicing payment service providers. The payee could also find him/herself unable to correctly allocate incoming payments.

- Under payment services law, all data from the customer's payment order – including the special categories – has to be processed in the context of execution and forwarded to the payment service providers used for execution.
- The scope of the use of sensitive data may be debatable in cases involving third-party services. The Guidelines should, however, make it clear that the request to implement technical measures to prevent the processing of Article 9 data can only be addressed to the payment initiation service/the account information service as the controller within the meaning of the GDPR. In accordance with the principles of the GDPR and in order to ensure that payments can be maintained, account servicing payment service providers cannot be required to filter the information on payment accounts retrieved by the account information service or payment initiation service. According to the PSD2, they have neither a verification obligation nor a right to intervene in this regard.

Re: section 6 – Data minimisation, security, transparency, accountability and profiling

As already explained above, a greater distinction should be made in the comments between account servicing payment service providers and third-party services (PISPs and AISPs). This is because there is no scenario for joint controllership pursuant to Article 26 of the GDPR.

Account servicing payment service providers are not obliged to filter the information on payment accounts retrieved by the account information service or payment initiation service. According to the PSD2, they have neither a verification obligation nor a right to intervene in this regard. The controllers – account servicing payment service providers and third-party services – are only obliged to provide information in accordance with Articles 13 et seqq. of the GDPR for their individual areas of responsibility. It is impossible for an account servicing payment service provider – under the PSD2 framework – to know what an account information service does with the payment account data retrieved. This is why the obligation to provide information lies with the account information service.