SQUIRE PATTON BOGGS

Second Payment Services Directive and the General Data Protection Regulation – Payments and Consent for Data Sharing

January 2019

The Second Payment Services Directive (PSD2) addressed new rules for payment services or third-party payment service providers – particularly account information service providers (AISPs) and payment initiation service providers (PISPs). Under PSD2, traditional payment service providers will need to share certain data with those third-party providers to access payment accounts (e.g., current accounts) and statement details, as well as other account information held by banks and other account-servicing payment service providers (ASPSPs) where customers consent to such access. Some of that data will constitute personal data in the sense of the General Data Protection Regulation (GDPR). The sharing requirements result partly in conflicts between the two set of rules. Even after the entry into force of both legal frameworks, several uncertainties remain.

PSD2 mandates the European Banking Authority (EBA) with developing regulatory technical standards (RTS) on strong customer authentication and secure standards of communications among ASPSPs, PISPs, AISPs, payers and payees. On March 14, 2018, the Commission Delegated Regulation No 2018/389 supplementing PSD2 with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication entered into force. The obligations set forth in the RTS will apply after a transitional period of 18 months, on September 14, 2019.

Based on the standards, ASPSPs must either enable third party access to the data through the customer's normal online banking websites, or alternatively develop a new Application Programming Interface (API) for that purpose. A range of safeguards are outlined in the standards to ensure that the access rights of AISPs and PISPs are respected, including that ASPSPs provide a fall back option to ensure AISPs and PISPs can exercise their access rights where the normal interface they use is down or underperforming. However, ASPSPs do not have to provide a fall back if they benefit from an exemption. Further, a working group on API under PSD2, is to be set up by the EBA in early 2019. The EBA said its new working group, which it will chair, will consist of a mix of staff from the EBA, national authorities, EU institutions and from external stakeholders, and "will identify issues and challenges that market participants will face during the testing and use of ASPSPs' production interfaces in the crucial period leading up to September 2019."

Notably, according to Article 66 of PSD2, a PISP may only provide its services on explicit consent of the payer in accordance with Article 64 of the PSD2. PISPs have to ensure that any other information about the payment service user, obtained when providing payment initiation services, is only provided to the payee and only with the payment service user's explicit consent. In addition, they may not request any data other than necessary to provide their payment initiation services, and may not use, access or store any data for purposes other than for the provision of the payment initiation service as explicitly requested by the payer and not store sensitive payment data of the payment service user.

With regard to data sharing, Article 67 of PSD2 provides the rules on access to and use of payment account information in the case of account information services. The article gives payment service users the right to make use of services, enabling them access to designated account information. AISPs, however, can also only provide their services based on the payment service user's explicit consent. They may only access the information from designated payment accounts and associated payment transactions; they may not request sensitive payment data linked to those payment accounts, and they may not use, access, or store any data for purposes other than for performing the service explicitly requested by the payment service user, in accordance with data protection rules.

Further, Article 94 of PSD2 provides the general data protection standard of this legal framework, considering that payment service providers shall only access, process and retain personal data necessary for the provision of their payment services, with the explicit consent of the payment service user. Moreover, all personal data processing in the context of PSD2 must be compliant with GDPR. Regarding the requirements for consent, the Article 7 GDPR states that the data controller must be able to demonstrate that consent was freely given. Consent for one matter must be distinguishable from other matters, and consent may be withdrawn at any time.

Both GDPR and PSD2 use the term "consent," or even "explicit consent," but the definitions and meanings do not seem to be consistent. Moreover, it can be questioned whether explicit consent is really required if it can be argued that the processing of the payer's personal data by a third party payment service provider is necessary for the fulfilment of a contract between them – i.e., to provide a payment initiation or account information service. Under GDPR, the existence of a lawful ground means that no consent would be required, whereby under PSD2 still an explicit consent would be required.

The European Data Protection Board (EDPB) has provided some guidance on the matter in July 2018. EDPB noted that the legal framework regarding explicit consent is complex, since both rules include the concept of "explicit consent." PSD2 uses the notion of "consent" and "explicit consent" with a different meaning than that under GDPR (see e.g. Article 4 (23), Article 52 (2) (c), Article 64, Article 65 (1) (b) and (2) (a) of PSD2). This leads to the question whether "explicit consent" of PSD2 should be interpreted in the same way as explicit consent under the GDPR. First of all, the EDPB is of the opinion that the "explicit consent" referred to in Article 94 (2) of the PSD2 has to be regarded as a contractual consent. Third-party payment services provide their services based on a contract between them and the payment service user, in accordance with recital 87 of PSD2.

Accordingly, the proper functioning of credit transfers and other payment services requires that payment service providers and their intermediaries, such as processors, have contracts in which their mutual rights and obligations are laid down. In terms of the GDPR, the legal basis for the processing of personal data is Article 6(1)(b) of the GDPR, meaning that the processing is necessary for the performance of a contract to which the data subject is a party. EDPB is of the opinion that Article 94(2) of PSD2 should be interpreted, on the one hand, in a way that preserves its useful effect, on the other hand, in coherence with the applicable data protection legal framework. This means that, when entering a contract with the payment service provider under PSD2, data subjects must be fully aware of the purposes for which their personal data will be processed, and have to explicitly agree to these clauses. Such contractual clauses should be clearly distinguishable from the other matters dealt in the contract and would need to be explicitly accepted by the data subject. EDPB is therefore of the opinion, that the concept of explicit consent under Article 94(2) of the PSD2 is an additional requirement of a contractual nature and is not the same as explicit consent under GDPR. Consequently processing of personal data for the purposes, not necessary for the performance of the contract, could be based on consent under Article 6 of the GDPR, if the requirements and the condition for consent laid down in Article 7 and Article 4(11) of the GDPR are fully respected. EDPB is of the opinion that consent under GDPR is a revisable decision and that the data subject can exercise control over processing activities.

The EDPB's guidance provides a welcomed clarification that the requirement of an explicit consent under PSD2 must be seen as separate and different from the requirements of consent under GDPR.

Moreover, it allows for the processing of personal data to be seen under GDPR's lawful ground of contractual necessity, rather than imposing the lawful ground of consent in this matter. This makes consent under PSD2 more of a transparency requirement, rather than being bound to the stricter requirements of consent under GDPR.

Contact

Andreas Fillmann
Partner, Frankfurt
T +49 69 1739 2423
E andreas.fillmann@squirepb.com