EU: How does PSD2 interplay with the GDPR? New regulatory guidelines published

In brief

Questions continue to arise over the interplay of the second Payment Services Directive (PSD2) with the General Data Protection Regulation (GDPR). Both PSD2 and the GDPR are complex legislation and the relationship between distinct provisions of each law and how they work together is not altogether clear, which has led to uncertainty for payment service providers, including banks. For example, when is "consent" required to access payment data and what does consent mean? To this end, the European Data Protection Board (EDPB) has published draft guidelines for consultation, but alongside other industry bodies and firms, the European Banking Federation (EBF) has voiced concerns over their workability for the sector.

Key takeaways

- PSD2 and the GDPR are complex legislation and the relationship between distinct provisions of each law and how they work together is not altogether clear, which has led to uncertainty for payment service providers (e.g., banks, standalone payment firms and the new PSD2 payment initiation and account information service providers).

- The draft guidelines propose narrow interpretations of the GDPR that, if adopted, would potentially increase the compliance burden on payment service providers.

- There are concerns in the payments sector that aspects of the draft Guidelines may be practically difficult to implement and unduly restrict future innovation. It is also clear that many banks, as account service providers, are concerned that the draft guidelines place a data protection burden on them as regards the new third party services under PSD2 that should more properly fall on those providers.

- The draft guidelines state that where there is a contract in place with the payment service user, the most appropriate lawful basis will be "contract performance". However, the EDPB emphasises that payment service providers must assess whether processing is objectively necessary for contract performance.

- Regarding the further processing of personal data, the EDPB points out that PSD2 and the GDPR restrict the possibilities for other purposes.

- The EDPB states that "explicit consent" under PSD2 is different from (explicit) consent under the GDPR. However, when determining whether explicit consent has been given for the purposes of PSD2, the test is likely to be analogous with the test under the GDPR.

- The draft guidelines state that financial transactions can in some circumstances reveal "special categories of personal data", the processing of which could be justified, provided that all conditions are fully met, via "explicit consent" or the derogation that processing is necessary for "substantial reasons of public interest". If there is no derogation available, the EDPB requires putting in place "technical measures" to prevent its processing.

- With regard to silent party data, the EDPB states that "legitimate interests" could be a legal basis. However, it points out that effective and appropriate measures must be taken to ensure that reasonable expectations of silent parties are respected.

In more detail

The EDPB — the EU body composed of representatives of the data protection authorities of each Member State, responsible for the consistent application of the GDPR across Member States — published draft guidelines in July 2020. The public consultation period ended on 16 September 2020. Although the EBF has generally welcomed the draft guidelines, it has expressed certain concerns in its consultation response and emphasised that they should be coherent with payments regulation, its terminology and regulatory technical standards, for example, on Strong Customer Authentication.

PSD2, which provides a legal and regulatory framework for payment service providers offering payment services in the EU, stipulates that the processing of personal data must be in accordance with the GDPR and its principles of data protection, such as data minimisation, transparency, proportionality, storage limitation and security measures. The draft guidelines focus primarily on the processing of personal data by the providers of payment initiation and account information services that access customers' payment accounts. In general terms, the draft guidelines interpret both PSD2 and the GDPR narrowly (consistent with the approach taken in previous guidance from the EDPB and Article 29 Working Party), thereby restricting and making more burdensome the ability of payment service providers to process personal data. As the draft guidelines focus on the new PSD2 services, the EBF calls for greater clarity on the use of terminology and to what extent they apply to conventional payment firms and banks.

Payment service providers will act either as a controller or as a processor under the GDPR. The EDPB does not discuss these roles further in the draft guidelines, but instead notes it is currently working on guidelines on the concepts of controller and processor under the GDPR (which have in the meantime been published — see here — but they discuss the roles in general). Since various actors are involved in providing the payment services, the EBF suggests being clear on the addressees of the various obligations.

From a GDPR perspective, it is necessary to rely on a legal basis to process personal data, such as one of six legal grounds under Article 6 of the GDPR.

Necessary for the performance of a contract

Where there is a contract in place with the payment service user, in the EDPB's view, the most appropriate lawful basis will generally be that processing is **necessary for the performance of a contract** for payment services to which the payment service user (the data subject) is a party. The EDPB expressly refers to its earlier EDPB guidelines (2/2019) to make clear that this does not cover processing which facilitates a payment service provider's other business purposes, but which is not "objectively" necessary to perform the contractual service. The EDPB's position on the scope of the "necessary for performance of a contract" is consistent with previous guidance on this topic and reiterates that this lawful basis should be interpreted narrowly. In particular, as regards additional services that are not among those defined and regulated by PSD2, but incorporated into the contract as an additional service, the EDPB emphasises that payment service providers must assess whether processing is objectively necessary for the performance of the contract and, if not, find another legal basis.

Further processing of personal data

The GDPR also allows for the further processing of personal data for a purpose other than that for which it has been collected, provided the other purpose is compatible with the one for which it was initially collected. However, in the EDPB's view, PSD2 restricts the processing possibilities for other purposes. This is because it provides that data is not to be used for any purpose other than for the provision of the service requested by the payment service user and, thus, other purposes are not compatible. This means that, for further processing, the user must either consent under Art. 6 (1) lit. a of the GDPR or the processing must be laid down in EU or Member State law to which the controller is subject, such as legal obligations regarding anti-money laundering or terrorist financing. Where a payment firm relies on consent, it must meet the requirements of consent and, in particular, show that

the payment service user had a genuine choice. The EBF takes issue with the EDPB on the basis that its interpretation would prevent a number of important and "legitimate" processing activities. The EBF argues that the concept of "further processing" and the limitations in PSD2 should be interpreted more broadly.

The draft guidelines note that an account service provider, typically a bank, granting access to necessary personal data requested by a payment initiation or account information service provider should be able to rely on Art. 6 (1) lit. c of the GDPR, namely that the processing is necessary for compliance with a legal obligation to which the controller is subject. Under PSD2, as transposed into national law, the account service provider must provide certain personal data to a payment initiation or account information service provider so that it can provide its payment services.

Explicit consent

Both the GDPR and PSD2 include the concept of "explicit consent". The GDPR sets a high standard for "consent" that, if relied on as a legal basis for processing under Art. 6 (1) lit. a of the GDPR, must be freely given, specific, informed and unambiguous. Art. 94 (2) PSD2 requires payment service providers to obtain the explicit consent of payment service users to access, process and retain their personal data. The draft guidelines helpfully clarify that the standard of explicit consent required under PSD2 is not the same as that required under the GDPR and that these are different in nature.

As mentioned above, the draft guidelines confirm that the most appropriate legal basis for processing personal data in this context is generally where it is necessary for the performance of a contract. In the view of the EDPB — and that of the EBF — consent under PSD2 should not be seen as an additional legal basis for processing personal data nor be on the same footing as explicit consent under the GDPR, but as an additional contractual requirement.

According to the EDPB, "explicit consent" in Art. 94 (2) PSD2 should be interpreted in a manner that when payment service providers enter into a contract, those customers must know (1) the specific categories of personal data that will be used and (2) the purpose of the specific payment services, and customers must explicitly agree to these clauses. The objective of explicit consent under PSD2 is to authorise payment service providers to access customers' personal data held by account providers before they actually process it, and the giving of consent obliges a bank to give access.

Although it is helpful that the EDPB has confirmed "explicit consent" as referred to in PSD2 is a "contractual consent", rather than consent as interpreted from a GDPR perspective, given the EDPB's comments regarding special categories of personal data, discussed further below, it may be that in practice explicit consent from a GDPR perspective is required in any event, depending on the context. In addition, although explicit consent required under PSD2 is not the same as defined under the GDPR, in practice the test over whether explicit consent has been given for the purposes of PSD2 is likely to be analogous with the test under the GDPR. Finally, it is suggested that these contractual clauses should be clearly distinguishable from those relating to data protection — something which the EBF views as unnecessary and potentially confusing for payment users.

Special categories of personal data

PSD2 contains a definition of "sensitive payment data" but this relates to personalised security credentials that could be used to carry out fraud, and is different from the concept of "special categories of personal data" as set out in Art. 9 (1) of the GDPR.

The draft guidelines state that financial transactions can sometimes reveal "special categories of personal data" about individuals from a GDPR perspective, for example the payment of medical bills, donations to political parties or payments to trade unions, etc. Since, in the EDPB's view, it is highly likely that financial transactions can reveal special categories of personal data, payment service providers are advised (assuming they have not already) to carry out a Data Protection Impact

Assessment to map out and categorise what kinds of personal data they will be processing. Subject to derogations under Art. 9 (2) of the GDPR, the processing of special categories of personal data (e.g., revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, etc.) is prohibited under the GDPR.

In this context, the EDPB states that to process special categories of personal data, either explicit consent or the derogation that the processing is necessary for reasons of substantial public interest on the basis of EU or national law could suffice. Where payment service providers cannot rely on a suitable derogation, they need to put in place "technical measures" to prevent its processing. Whether this is possible from a practical standpoint is not clear. The EBF and other respondents argue that financial transaction data is not in itself a special category of personal data. They recommend revising the draft guidance to the effect that payments data is not inherently a special category unless the controller is processing the data to derive such inferences. In any event, the EBF argues that bank account providers may do so. This is on the basis that they are under a legal obligation in PSD2 to comply with third-party provider requests and the GDPR allows processing as PSD2 is an EU law with a public interest objective (i.e., greater consumer control over data and market competition). More specifically, the legal obligation under PSD2 is to provide the same information to the third-party provider as the payment service user has access to online.

Silent party data

The draft guidelines address the question of processing "silent party data", an example being a person who has made payments to a payment service user who has contracted to use an account information service provider. According to the EDPB, the legal basis under the GDPR for processing silent party data (e.g., name, account number and payments amounts) could be where it is **necessary for purposes of the legitimate interests** pursued by a controller or a third party. However, this legitimate interests condition requires a balancing exercise with the rights and freedoms of the data subject. Thus, the EDPB points out that effective and appropriate measures must be taken, such as technical measures to ensure their personal data is not processed for other purposes and measures to ensure that the reasonable expectations of silent parties are respected.

The EBF asks for the draft guidelines to clarify that responsibility for such technical measures falls on the account information service provider and not the bank providing a payment account. The EDPB is clear that silent party data cannot be used for a purpose other than that for which it has been collected (e.g., direct marketing). In its view, it is not feasible to obtain consent (which would itself require processing the personal data of silent parties) and the compatibility test under Art. 6 (4) GDPR would (for obvious reasons) not be of help. Although this interpretation is not necessarily a surprise from a GDPR perspective, this is another instance where the EBF considers the EDPB's interpretation (this time over the GDPR) to be too restrictive. Instead, it suggests that the legal basis should be assessed on a case-by-case basis by payment service providers.

A payment service provider accessing account data to provide payment services must abide by the GDPR principle of data minimisation, collecting only the personal data necessary to provide the specific services requested by the payment service user. In practice, this means that an account service provider must select the relevant categories of data to be accessed when responding to a request from a payment initiation or an account information service. It may not, for instance, be necessary to include the identity of the silent party, their IBAN and the transaction characteristics. The EDPB recommends the use of digital filters by service providers to support banks in their obligation to only collect what personal data is necessary. Unsurprisingly, there is push-back on behalf of banks concerned that the draft guidelines could be read as imposing an obligation to monitor data collection by payment service providers and to ensure they only collect what data is necessary. The EBF considers that banks monitoring such collection and establishing safeguards might run the risk of contravening their obligations under PSD2. The EBF also points to the practical difficulties for account service providers, where a dedicated interface is unavailable and third-party providers, as a fallback, access accounts through the payment service user's interface.

Security standards

The draft guidelines reiterate the importance of payment service users pursuing high security standards. It considers that, given the amounts of data involved, a personal data breach could significantly affect the data subject's daily life and cause them financial loss or other harm. The EDPB warns that service providers will be held to high standards, including over Strong Customer Authentication mechanisms, as well as high security standards for technical equipment.

Similarly, payment service providers are reminded of the importance of transparency and accountability, which are key principles under the GDPR. Information and communications on the processing of personal data must be concise, transparent, intelligible and easily accessible, and contain the information included in Art. 13/14 of the GDPR. The draft guidelines recommend (consistent with previous guidance on transparency) that providers should consider using a "layered" approach where privacy notices should link to the various categories of information provided to the payment service user, rather than displaying all such information in a single notice on a screen to avoid user fatigue. Additionally, as with previous guidance on transparency, it promotes the use of a "privacy dashboard" — a single point from which payment service users can view "privacy information" and manage their preferences. Accountability requires payment firms to put in place appropriate technical and organisational measures to ensure (and to show) that their processing is GDPR compliant. The EBF considers it is inappropriate, and probably not permissible under PSD2, to interfere in contractual relationships between a payment service user and payment service provider. In its view, the guidelines should not be read as imposing a requirement for dashboards. In practice, a number of jurisdictions allow for dashboards and at least one major UK bank allows its customers to cancel authorisations to third parties under Open Banking - the UK's implementation of PSD2 third party payment services.

Profiling

In particular, account information service providers should also take heed of the draft guidelines in respect of what is said on the subject of profiling. Account information services may entail a significant evaluation of personal payment account data and employ automated processing, in which case additional requirements apply (Art. 22 of the GDPR). For example, in cases of credit applications there is the right not to be subject to a decision without any human intervention. It is, however, the case that the purpose and the legal basis for profiling are relevant as to whether it is possible to object (e.g., for payments firms to comply with legal obligations over anti-money laundering).