Feature

KEY POINTS

- Payments services providers must comply with both the applicable payments regime and the relevant data protection regime, though the two are not perfectly aligned.
- Both regimes feature different concepts of individual consent, each with relatively onerous standards.
- The distinction between the two sets of consent requirements is not always clear-cut. Payments services providers face particular uncertainty over the extent to which they can use personal data for further associated services.
- Transparency may be the key for payments services providers to mitigate their risk around consent in practice, and to bring a degree of consistency to payments and data protection consent compliance.

Authors Fiona Maclean, Christian McDermott, Calum Docherty and Amy Smyth

Consent under PSD2 and the GDPR: squaring the circle

The scope for misalignment between the payments and the data protection regimes in Europe and the UK gives rise to a number of challenges for banks and fintechs. This issue is particularly evident in relation to the potentially inconsistent requirements for individual consent.

INTRODUCTION

In 2019, more than half of all payments in the UK were made by card and contactless methods, according to the trade association UK Finance. Further, the organisation's research found that more than two-thirds of UK adults used online banking, and more than half used mobile banking, with consumers making more than a billion remote banking payments. The COVID-19 pandemic has accelerated the shift towards a cashless society, as governments across Europe encourage citizens and businesses to adopt cashless solutions. This surge in card transactions and online and mobile banking raises questions about how to manage the vast array of personal data and other information generated from each payments transaction, within multiple legal regimes.

In the EU, activities in the payments sector are subject to the revised Payment Services Directive (2015/2366, known as PSD2), as transposed into national law. PSD2 also introduced and regulates account information services and payment initiation services. PSD2 was implemented into UK national law prior to the UK's exit from the EU, primarily by way of the UK Payment Services Regulations 2017 (UK Payments Regulations). The UK's implementation of PSD2 also provides a foundation for the UK's open banking regime, including an open banking standard for sharing and accessing banking and payments data.

The material aspects of the EU and UK payments regimes remain closely aligned following 1 January 2021, though there is of course potential for divergence in the future as the UK is no longer bound by EU law developments.

A key requirement of PSD2 is that regulated firms must process personal data in compliance with applicable data protection law, which is substantially set out in the General Data Protection Regulation (GDPR) for the EU, and in the UK GDPR and the Data Protection Act 2018 for the UK. As with PSD2, the EU and UK data protection regimes remain similarly closely aligned for now, though there is scope for future divergence in this area, too.

Payments services providers operating across Europe and the UK may be subject to both the EU and the UK data protection and payments regimes, depending on how their services are structured. These payments and data protection regimes impose separate regulatory requirements that at times can seem incongruous. This potential misalignment is particularly evident in relation to the respective consent requirements and gives rise to a number of specific challenges for the banks and fintechs that are required to comply with these two regimes. The primary guidance on this topic to date is the European Data Protection Board's (EDPB's) Guidelines on the interplay between PSD2 and the GDPR, published in final form in December 2020 (Guidelines). The Guidelines focus on what account information service providers (AISPs) and payment initiation service providers (PISPs) (together, third-party providers or TPPs) should do to comply with the GDPR and mitigate data protection risk, in the context of their respective PSD2 obligations.

CONSENT UNDER PSD2

PSD2 and the UK Payments Regulations provide that TPPs shall access, process, and retain only the personal data that is necessary for the provision of their payment services, and only with the "explicit consent" of the payment service user. AISPs are also required to collect "explicit consent" for the provision of their services.

In light of PSD2's and the UK Payments Regulations' remit being limited to the contractual relationship between a TPP and its users, the EDPB's view as stated in the Guidelines, is that the "explicit consent" referred to in PSD2 is a contractual consent, distinct from and additional to "consent" under the GDPR. According to the Guidelines, "explicit consent" in the PSD2 context means that individuals should be fully aware of the data processed under the relevant service, as well as the purpose of the processing. They also must explicitly agree to these clauses and accept these purposes. These information requirements therefore overlap with the GDPR's prior-information requirements for obtaining consent, and broader transparency requirements for all personal data activities. Further, under PSD2 and the UK Payments Regulations, the payment service user must be able to

Biog box
Fiona Maclean is a partner in the Data & Technology Transactions practice in Latham & Watkins' London office. Fiona advises clients on data privacy compliance with a particular focus on cloud computing and data strategy in the financial services industry.
Email: fiona.maclean@lw.com

choose whether or not to use the service (and cannot be forced to do so).

CONSENT UNDER THE GDPR

Under the GDPR and the UK data protection regime, "consent" and "explicit consent" are legal bases for processing personal data and special category data, respectively. The threshold for valid consent is high: consent must be freely given, specific, fully informed, unambiguous, and capable of being withdrawn. The standard for valid explicit consent is stricter still; while not defined in legislation, explicit consent commonly requires (in addition to the high standard for consent generally) a clear and specific statement of consent, distinct from any other consent being sought.

While PSD2 consent is purely contractual, the GDPR and the UK data protection regime make a distinction between processing personal data on the basis of consent or, separately, contract. For data protection purposes, the GDPR consent requirements listed above are not applied to the contractual basis for data processing, though the broader transparency requirements under the GDPR and UK regimes do apply.

ALIGNING CONSENT REQUIREMENTS

Interpreting the meaning of consent and explicit consent differently for PSD2 and GDPR purposes is necessary to square how the two regimes, including the equivalent UK regimes, use that concept, and to avoid undermining PSD2's contractual focus. However, the distinction is not clear-cut in reality – thereby raising practical questions for businesses.

While the Guidance distinguishes PSD2 consent from GDPR consent by virtue of its contractual nature, the Guidance does not go on to clarify the extent to which their similar requirements should be interpreted equivalently. Arguably, the GDPR's consent standards – particularly those requirements relating to withdrawal of consent and the freely given nature of consent – should not be applied to contractual consent under PSD2, notwithstanding similar requirements in PSD2. In terms of transparency, it would seem reasonable that a single point of information could satisfy transparency obligations under both the GDPR and PSD2. It may also be arguable that the acknowledgement of a privacy notice could achieve PSD2 consent for the use of personal data, and equally that acceptance of a contract with clear data protection terms could be sufficient to meet the GDPR consent requirements.

THE CHALLENGE OF FURTHER DATA PROCESSING

The GDPR and PSD2, and their equivalent UK regimes, each restrict how TPPs can use personal data. Under the GDPR, data must be collected for a specified purpose and not further processed in any incompatible manner (unless a separate legal basis is established for that further processing). Under PSD2, TPPs can only process data for the payment initiation or account information services (for PISPs and AISPs, respectively) as requested by the user (Arts 66(3)(g) and 67(2)(f) PSD2).

There is a degree of uncertainty over the extent to which PSD2 and the GDPR, in conjunction, restrict further uses of data in practice. One arguable interpretation is that neither the GDPR nor PSD2 should restrict the further use of personal data for associated services, provided that use is compatible with the payment initiation or account information services (for GDPR purposes) and does not conflict with the TPP's contract with the user (for PSD2 purposes) (or if that use otherwise falls outside the scope of PSD2, eg creditworthiness or audit, or savings account services). The EDPB appears to take a different position in its Guidance, however. This discrepancy suggests that further processing of data is only permitted with user consent (as per the GDPR/UK data protection regime standard) or when the processing is laid down under EU, member state, or UK law, as relevant (eg the requirements to conduct customer due diligence in accordance with applicable anti-money laundering and terrorist financing directives).

In practice, an ability to use data for further compatible purposes (absent a relevant legal obligation to do so), is key to many TPPs' operational and commercial models. Reliance on consent poses a challenge in this context and may not be feasible, as it must satisfy the GDPR consent standards, which include an ability to withdraw consent at any time. Overall, it seems an arguable, pragmatic approach for TPPs to proceed with further personal data processing if this is:

- compatible with the payment initiation or account information services (and such compatibility assessment has been documented); and
- either outside the scope of PSD2 or does not directly conflict with the TPP's contract with its user.

EXPLICIT CONSENT FOR HANDLING SPECIAL CATEGORY DATA

Under the GDPR, special categories of personal data include information related to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health data, biometric or genetic data, and data concerning a person's sex life or sexual orientation. (In contrast, PSD2 refers to "sensitive payment data", meaning "data, including personalised security credentials, which can be used to carry out fraud".) The GDPR prohibits the processing of special categories of personal data unless there is a relevant derogation/ legal basis, distinct from the legal bases for processing other types of personal data.

For TPPs, the most relevant (potentially the only relevant) legal basis is likely to be the explicit consent of the user. As set out above, the GDPR threshold for explicit consent is very high. TPPs may not find it feasible or commercially efficient to obtain in this context, or even possible at all in the case of a "silent party" (ie an individual whose personal data is processed by the TPP but who is not the user of the service and has no relationship with the TPP). In this case, the Guidelines suggest that TPPs investigate "technical measures […] to prevent the processing of special categories of personal data, for instance by preventing the processing of certain data points". However, any operational and process changes in order to exclude access

Feature

Biog box

Christian McDermott is a partner in the Data & Technology Transactions practice in Latham & Watkins' London office and leads Latham's UK Payments Practice. Christian has more than 13 years' experience in the payments sector and regularly acts on transactions involving the biggest names in the industry. Email: christian.mcdermott@lw.com

to special categories of personal data are likely to have significant technical and cost implications for the TPP.

The Guidance also refers to the substantial public interest basis as a potential option; however, TPPs must look to UK, EU, or member state national law (as relevant) for a substantial public interest condition (which must specifically provide for a GDPR derogation to process special categories of data), and such conditions are not currently available in all jurisdictions. Further, reliance on a substantial public interest condition, even if available in national law, requires the TPP to assess the proportionality and necessity of the processing, ensure safeguards for individuals' rights and interests, and comply with any additional national law requirements.

TPPs may, understandably, have considered themselves relatively immune from the enhanced requirements and strict conditions for processing special category personal data. In general, regulators, including the EDPB in other guidance, take a restrictive view of the scope of specific category personal data. The typical approach suggests that, in order to constitute special category data, the information should either explicitly fall within the definition, or should genuinely and unequivocally infer data within the definition (whether by profiling or otherwise). However, in the Guidance, the EDPB suggests a considerably broader interpretation in relation to financial transactions, stating that "even single transactions can contain special categories of personal data" and "the chances are considerable that a service provider processing information on financial transactions of data subjects also processes special categories of personal data". The reasoning behind this broader interpretation in the context of payment initiation and account information services is unclear and does not appear consistent with either the EDPB's previous approach or the approach of national regulators.

Arguably, the personal data handled by TPPs is, in practice, unlikely to be sufficiently comprehensive so as to explicitly reveal special category personal data. Equally, TPPs are unlikely to handle sufficiently detailed data to enable them to infer or assume any special category data, at least when interpreted in accordance with the regulators' more typical, narrower approach to the scope of that data. This may become a critical argument for TPPs, in order to avoid the costly implications of either seeking explicit consent to handle special category data (which is unlikely to be a reliable option in the long term in any case) or implementing operational changes to exclude access to that data.

SQUARING THE CIRCLE IN PRACTICE

Transparency is arguably the key for TPPs to mitigate risk around consent in practice, and to bring a degree of consistency to PSD2 and GDPR consent compliance.

While not directly addressed in the Guidelines or otherwise, it seems feasible that the same set of disclosures (whether layered through a number of different sites, pages, or documents, or presented as a single point of information) could satisfy the transparency and prior-information obligations for consent under both the GDPR and PSD2 regimes. It also seems reasonable that the same consent mechanism and user journey could achieve consent for both PSD2 and GDPR purposes. Each of these approaches is conditional upon, but should not be precluded by, the prior-information and consent meeting the respective thresholds of both PSD2 and the GDPR (which includes each relevant consent being sufficiently specific and distinct, not bundled with other terms, and adequately brought to the users' attention and acknowledged).

Effective transparency can also facilitate the identification and necessary compatibility assessments for any further processing of personal data envisaged by TPPs. In turn, that assessment may be a helpful tool to ensure and document the compatibility of such further processing with the relevant services, and therefore reduce the compliance risks associated with the current uncertainty surrounding further processing by TPPs. Similarly, comprehensive transparency information should document the scope of the personal data being processed by the TPP and may be a useful tool to explain and evidence that the TPP is not processing any special category personal data (as relevant in practice for the TPP). This may help to reduce the specific risks of special category data in a payments context. ■

Further Reading:

- Opening innovation or opening up to risk? The potential liability framework for Open Finance (2021) 1 JIBFL 31.
- Opening Pandora's Box: PSD2, consumer control and combatting fraud (2020) 1 JIBFL 48.
- LexisPSL: Banking & Finance: Practice Note: Open Banking – one minute guide.

Biog box

Calum Docherty is an associate in the Data & Technology Transactions practice in Latham & Watkins' London office who advises a variety of EU and global clients on all aspects of European privacy law, including large-scale GDPR compliance projects, product development and M&A transactions. Email: calum.docherty@lw.com

Amy Smyth is a knowledge management lawyer for the Data & Technology Transactions Practice, with extensive experience in a broad range of data, technology, and commercial law matters, including complex data governance and compliance. Email: amy.smyth@lw.com