GDPR and PSD2: a compliance burden for financial institutions

Published 18-Apr-2018 by
Kristof Van Quathem and Sophie Bertin

The financial services industry is having to adapt to increasing legislation across Europe, such as the new Payment Services Directive (PSD2), as well as major changes to data protection law under the General Data Protection Regulation (GDPR).

This article looks at the additional compliance burden caused by the interaction between PSD2, aimed at increasing the seamless sharing of data, and the GDPR, aimed at regulating such sharing.

PSD2, which took effect at the beginning of this year, puts an obligation on banks to give third-party providers (TPPs) access to a customer's payment account data, provided the customer expressly consents to such disclosure. It follows as part of what is being called the "open banking" revolution, which is intended to improve competition and innovation by opening up access to the EU market for payment services.

The GDPR, which is due to apply from May 25, 2018, however, comes with its own agenda: that is to enhance individuals' rights when it comes to protecting their personal data, ultimately giving them greater control of their data. The burden of having to comply with these developing bodies of law is increased where there is tension between the objectives of the two and a lack of any clear guidance on how to align the different, but related, requirements.

The first major compliance hurdle is understanding the nature of consent required under PSD2 and aligning this with an appropriate legal basis under the GDPR. Under PSD2, banks and TPPs shall only process personal data for the provision of their payment services with the "explicit consent" of the customer (Article 94(2), PSD2).

Under the GDPR, banks and TPPs must have a "legal basis" to process a customer's personal data. Consent is one available legal basis, but others include when the processing is necessary to perform a contract, where the processing is in compliance with a legal obligation, or the processing is in the data controllers legitimate interest.

As such, consent is only one of the available legal bases, and it has certain downsides; for example, consent can be withdrawn by the customer at any time meaning the bank and/or TPP lose their legal basis to process the customer's personal data.

Practically speaking, however, where a customer wants to initiate a payment transaction with the TPP, the TPP's processing of that customer's data could be considered necessary to perform the contract. Equally, it could be argued that where the bank is required to provide the TPP with the customer's data to carry out the transaction, the bank's processing is in compliance with a legal obligation. There should be no need for customer consent for the associated data processing operations.

PSD2 increases however the standard of protection in comparison to the GDPR by imposing an additional consent requirement. As mentioned above, when relying on customer consent, as per the GDPR, customers have the right to withdraw this consent at any time. Such withdrawal is likely to raise expectations with customers, such as a right to be forgotten, that cannot be met in full in light of conflicting obligations that banks and TPPs have. At the same time, such rights risk limiting the commercial use that banks and TPPs can make of the data.

There are various other complications regarding consent that require further guidance, such as: who is responsible for obtaining consent; what level of due diligence is expected from banks before sharing customer data with a TPP, and how to perform the due diligence (knowing that the banks cannot impose contractual obligations on TPPs – see Art. 66(5), PSD2); what is the scope of the consent and what level of granularity of choice can users expect?

Further issues arise with aligning the two pieces of legislation due to differing definitions. The GDPR contains definitions of "personal data" and "special categories" of personal data; however, PSD2 includes a definition of "sensitive payment data", not found in the GDPR.

Sensitive payment data is very broadly defined as data, including personalised security credentials which can be used to carry out fraud. Does sensitive payment data qualify as a category of special personal data under the GDPR and thus subject to stricter rules, or not?

The GDPR increases information requirements for banks and TPPs, such as having to provide customers with the legal basis for the processing and transfers of personal data. The question then arises, who is responsible for providing this information to customers?

If banks are indeed responsible, how do they ensure the customers using TPPs have access to the necessary information to satisfy their obligations under the GDPR? Another issue is how these information requirements align with financial institutions' obligations to ensure the prevention of fraud.

Under PSD2: "Member states shall permit the processing of personal data by payment systems and payment service providers when necessary to safeguard the prevention, investigation and detection of payment fraud" (Article 94(1), PSD2).

This is to be carried out "in accordance with" the GDPR, suggesting that these information requirements must be complied with. This however runs counter to other financial legislation which prohibits financial institutions from "tipping-off" customers where they are under suspicion of fraud. In addition, both pieces of legislation contain similar incident reporting obligations, albeit reporting to different authorities.

The above are just a few examples of the provisions that require alignment. Further to this, many of these issues will be flavoured by country specific implementation of the relevant legislation and, under both pieces of legislation, failure to comply carries the significant risk of penalties and other liabilities, such as civil litigation.

Breach of the GDPR can lead to fines of up to 20 million euros, or up to 4 percent of an undertaking's total worldwide annual turnover, whichever is higher. Under PSD2, member states are free to determine penalties that may be imposed by national authorities following an infringement of the law.

To avoid these significant penalties, banks will need to ensure that they have correct procedures in place to comply with both pieces of legislation, which will be a difficult task given that aligning the two is in no way straightforward.

Financial institutions will need to rigorously assess the interaction of all those provisions to address these issues and mitigate the potential risks. Without clear guidance on interpretation, financial institutions will need to develop a defensible position for why they are adopting certain interpretations or taking certain positions.

They will also need to assess the operational implications of such decisions and develop processes and records that demonstrate their compliance with the GDPR, including in relation to the increased consent requirements and other GDPR accountability obligations.

Any strategy for dealing with this increased compliance burden for financial institutions will require expertise in numerous areas of law, an ability to analyse competing outcomes and to create a series of priorities, which then need to be implemented operationally and technologically and complied with throughout the whole organisation.

Produced by Thomson Reuters Accelus Regulatory Intelligence 30-Apr-2018

THOMSON REUTERS™