Navigating the PSD2 and GDPR challenges faced by banks

Minds made for protecting financial services
When the financial services industry works well, it creates growth, prosperity and peace of mind for hundreds of millions of people. No other industry touches so many lives or shapes so many futures.

At EY Financial Services, we share a single focus – to build a better financial services industry, not just for now, but for the future.

We train and nurture our inclusive teams to develop minds that can transform, shape and innovate financial services. Our professionals come together from different backgrounds and walks of life to apply their skills and insights to ask better questions. It’s these better questions that lead to better answers, benefiting our clients, their clients and the wider community. Our minds are made for protecting financial services. It’s how we play our part in building a better working world.

ey.com/FSminds
PSD2 and GDPR: connecting the two

The revised Payment Services Directive (PSD2) came into force on 13 January 2018. PSD2 promises to reshape the current payments environment. Its implementation allows both traditional financial organizations and their newer FinTech rivals to provide payment services, increasing competition and – hopefully – efficiency.

PSD2 allows third parties to enter the payment market and provide new services in the area of account information and payment initiation by accessing the financial data of a payment service user (PSU): this is called the access to account rule. Incumbent banks can also choose to develop account information services (AISs) and payment initiation services (PISs). Providers of these services are called AISPs and PISPs respectively. Incumbent banks must decide either to comply with the new legislation or harness the opportunities it offers for services.

Another important piece of legislation with implications for PSD2-related activities went live on 25 May 2018: the General Data Protection Regulation (GDPR). This is a comprehensive regulation designed to protect personal data. New payment services will require access to significant amounts of personal data, and will therefore have to comply with the terms of GDPR.

Legislators took different approaches when designing PSD2 and GDPR: PSD2 is about creating access to personal data while GDPR is about protecting it. Banks planning to offer AIS- or PIS-based value propositions will need to consider both legislations when developing these new services.

### Processing of PSUs’ data transfer requests

<table>
<thead>
<tr>
<th>PSD1 situation</th>
<th>PSU or data subject</th>
<th>Bank: data controller</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSD2 situation</td>
<td>PSU or data subject</td>
<td>AISP or PISP: data processor</td>
</tr>
</tbody>
</table>
The challenges

Under PSD2, AISPs and PISPs will require access to PSUs’ bank account details to provide these services. This access to accounts results in the processing of personal data, comprising transaction information and sometimes other data, such as:

► The name of the account holder
► Their account number
► Information accompanying a transaction

This personal data is subject to GDPR legislation, thus making PSD2 and GDPR intertwined.

The interaction between the two pieces of legislation is manifold. The mechanics behind this interaction have legal implications and will affect practical outcomes. However, the different approaches taken when designing PSD2 and GDPR have resulted in the potential for contradictions in interpretation between the two.
It all comes down to consent

From a GDPR perspective, data cannot be processed without a legitimate basis. And there are a number of these, one of them being the consent of the data subject. GDPR stipulates the conditions that must be satisfied for consent to be granted. This consent is necessary to process certain data or process data in a certain way.

PSD2 dictates that consent is also necessary to provide services to PSUs. In this case, the PSUs’ “explicit consent” is needed. However, the phrase “explicit consent” is not defined in PSD2 and there is no suggestion that it has the same meaning as in GDPR. This results in a lack of clarity surrounding adequate levels of consent that payment service providers need to obtain to deliver their services.

This problem does not exist when the legitimate basis on which the processing of personal data is founded is other than consent – such as a contract.

The table below shows a rough overview of the differences in requirements for consent between GDPR and PSD2.

<table>
<thead>
<tr>
<th>Consent element</th>
<th>GDPR</th>
<th>PSD2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Consumer consent to process data must be freely given and for specific purposes.</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>2. Customers must be informed of their right to withdraw their consent.</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>3. Consent must be “explicit” in the case of sensitive personal data or transborder dataflow.</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>4. Data processing and sharing is explicitly requested by the customer.</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>5. Consent expires automatically.</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>6. Consent must be clear, specific and informed.</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Data portability and APIs

Under GDPR, PSUs have the right to transfer their personal data, which they have provided to their bank, in a structured, commonly used and machine-readable format to an AISP or PISP without hindrance: the right to data portability.

While PSD2 has no bias toward certain technologies, the Regulatory Technical Standards recommend the use of application programming interfaces (APIs) to share data with AISPs and PISPs. APIs can provide for commonly used communication standards between incumbent banks and AISPs or PISPs, but their success across Europe will depend on whether such standards can be agreed.

Alternatively, screen scraping establishes access for AISPs and PISPs to PSUs’ bank accounts via their own credentials, obscuring the ability of banks to see whether it is the PSU or a third party accessing the account. While this does not have the same technical restrictions, it does raise concerns over security, particularly around sharing customer credentials and related accountability for potential data breaches. While screen scraping makes access to PSUs’ accounts easier, the added risk limits its practical use, which makes communication through APIs the preferred option for banks.

Silent party data

When AISPs provide consolidated information regarding PSUs’ bank accounts, the PSUs’ transaction history could also contain information about third parties they conduct transactions with. It is currently unclear whether or not AISPs are allowed to show this “silent party” data as the AISP lacks a legitimate basis to show this information. There is no agreement between the AISP and the third party with regards consent to this data processing, which is a requirement under GDPR.

For the time being, the lack of guidance from supervisors indicates that it is unlikely this will be problematic to the services an AISP can deliver, as long as silent party data is only displayed and not abused. Profiling of silent parties without explicit consent should, however, be considered an abuse of their data information.
GDPR provisions influencing PSD2 services

1. **A data protection officer should be appointed**
   Data protection officers (DPOs) ensure that GDPR is applied and complied with. The nature of AISPs and PISPs indicates that it is highly likely DPOs will have to oversee their activities.

2. **Profiling is prohibited**
   Profiling means the automated processing of personal data with the purpose of evaluating personal features. It can be a useful way to deliver value-added services, such as credit scoring and expenditure evaluation.

   Legal or similar significant effects, such as refusing someone a loan, can be based solely on automated processing of personal data if this is founded on a legitimate basis. This includes explicit consent, performance of a contract and compliance with a legal obligation. However, while the process is automated, the service provider has to be able to justify every automated decision when an inquiry is made by the PSU.

3. **Data protection impact assessments are necessary**
   The nature of AISPs and PISPs indicates that it is highly likely data protection impact assessments will be necessary. The assessment should take place prior to the processing of financial data, and serves to map the risks of processing data and define mitigating measures. The supervisory authority will sometimes have to be consulted to mitigate these risks.

4. **Services should adhere to data protection by design and by default principles**
   AISPs and PISPs have to adhere to data protection by design and by default principles. These principles require service providers to think about the impact their services will have on data protection before delivering them. Appropriate measures have to be taken to ensure GDPR compliance and minimize the processing of data.

5. **Data subjects always have the right of access to information**
   Data subjects have the right to know whether their information is being processed and, if it is, they have the right to receive a copy. When designing services, providers need to take these rights into account so they can deliver the appropriate information when requested. AISPs and PISPs may charge a reasonable fee, provided the request of the PSU is unfounded or excessive.

6. **The right of erasure has big implications on services delivered**
   Data subjects have the right to ask for the erasure of all personal data that a service provider holds for them without undue delay. For AISPs and PISPs, this is particularly important in case the PSU withdraws the explicit consent on which the processing of personal data was based. When designing services, providers need to take these rights into account so they can delete personal data if requested and permissible.

**Conclusion**

PSD2 is set to give banks unprecedented opportunities in the payment sector. It is up to them to decide whether they want simply to comply with the new rules or harness them by providing new AIS and PIS propositions strengthening their competitiveness.

The main instigator for these new value propositions is the access to account rule. This PSD2 rule, however, does concern privacy protection law as well, meaning GDPR comes into play.

The interaction between PSD2 and GDPR produces challenges that banks need to address. While daunting from afar, these challenges can be navigated with robust planning and sufficient expertise.

This will enable banks, among others, to:

- Validate the consent an AISP or PISP has received or, if banks themselves want to develop AISs or PISs, gain the necessary consent of PSUs to provide these services
- Provide for safe and secure APIs to enable communication between AISPs or PISPs and themselves in a cost-efficient manner and with solid accountability allocation
- Have a system in place with strong risk-mitigating measures for silent party data, to process this data confidently
- Adhere to other GDPR provisions that influence PSD2 services while taking optimal advantage of the opportunities PSD2 provides
EY can help you with:

► Identification of, and preparation for, the risks and opportunities
► The implementation of the most promising PSD2 value propositions in your organization
► GDPR and PSD2 transformations to achieve overarching compliance, as well as shape and pursue strategic opportunities

Why EY?

EY has been at the forefront of shaping the PSD2 agenda from the outset, working closely with international banks, FinTechs and regulators. In addition, EY has experience assisting multi-national organizations in their data protection and privacy programmes, for many years.

We help to mobilize and provide PSD2 transformation programs, and play a leading role in supporting clients to become GDPR-compliant. This includes organizational transformation and road map design.

Contacts

Tony de Bos
EY EMEIA Financial Services Data Protection & Privacy Leader
Telephone: +31 88 407 2079
Mobile: +31 62908 4182
Email: tony.de.bos@nl.ey.com
Ernst & Young Accountants LLP

Hamish Thomas
EY EMEIA Financial Services Open Banking & Payments Leader
Telephone: +44 20 7951 1955
Mobile: +44 7967 176 593
Email: hamish.a.thomas@ey.com
Ernst & Young LLP

Erol Mustafa
EY EMEIA Financial Services IT Risk & Assurance Leader
Telephone: +44 20 7951 0700
Mobile: +44 7979 923 611
Email: emustafa@uk.ey.com
Ernst & Young LLP

Philippe Zimmerman
EY EMEIA Financial Services Legal Leader
Telephone: +41 58 286 3219
Mobile: +41 79 341 4571
Email: philippe.zimmermann@ch.ey.com
Ernst & Young Ltd
About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

© 2018 EYGM Limited.
All Rights Reserved.

EYG no. 010207-18Gbl
EY-000068990.indd (UK) 07/18.
Artwork by Creative Services Group London.
ED None

In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com/FSminds