Deloitte.
Legal

PSD2 and GDPR:
An awkward match?

PSD2 and GDPR: An awkward match?

In the intersection of both rules, from a Dutch perspective

If your company processes personal data of European citizens and you are also (planning to) provide payment services in Europe, you have to comply with both the General Data Protection Regulation ("GDPR") as well as the new Payment Service Directive 2 ("PSD2"). These sets of rules are not be taken lightly, as the cost of noncompliance can lead to staggering fines such as 20 million or 4% of the worldwide turnover and in many cases also reputational damage. As the dates of effect are rapidly approaching (GDPR on May 25 2018 and PSD2 in Q2 2018), companies facing both sets of rules will need to decide on their PSD2 and GDPR strategy rather sooner than later.

Unfortunately, as is often the case with various complex EU rules and regulations, obscurities and possible conflicts seem to exist between the (implementation of) PSD2 and the GDPR. In the Netherlands, the Dutch Data Protection Authority ("DPA") has recognized these discrepancies and expressed their concern in two recommendation letters on the Draft PSD2 Implementation Act ("Implementation Act") and, most recently, the Draft PSD2 Implementation Decree ("Implementation Decree").

In this article we would like to inform you on these concerns and provide you with practical guidance. But first, a general introduction on both regulations.

PSD2

PSD2 is the successor of the first Payment Service Directive, further regulating the payment services environment. The most exciting change this second version will bring is the requirement for financial service providers to open up access to customer accounts (with permission of the customer), allowing Third-Party Providers ("TPP") to access those. At the same time PSD2 will also introduce stricter technical controls. Consumers will benefit from safer and more innovative electronic payment services, whilst new (non-financial) market players are welcomed into the world of financial data and financial institutions are given incentive to innovate. In the Netherlands, administrative fines can be imposed by De Nederlandsche Bank ("DNB").

Since PSD2 is a directive, transposition into national law is required. In the Netherlands PSD2 is expected to be transposed into Dutch law in Q2 2018 (see previous blog post) through the Implementation Act. The Implementation Act is currently under review at the House of Representatives. The consultation on the Implementation Decree, which contains detailing on the topic of consent, has been recently closed. The Dutch Ministry of Finance is currently processing the received feedback (including of the DPA) and the final version is expected to be published soon.

GDPR

In essence, the GDPR is nothing new under the sun. It contains the same basic data protection principles that we have known from the Data Protection Directive of 1995. For example purpose limitation, data minimization, transparency and data subject rights are all concepts that are addressed in the current European data protection framework. However, the GDPR goes further and introduces more and stricter obligations for controllers and processors. Also, as a regulation, the GDPR aims to harmonize the various data protection laws across the EU, as no transposition into national law is required. This in contrast to directives such as PSD2 and the "old" Data Protection Directive. Yet what really puts this topic on the regulatory radar for many companies is the new fining power of data protection authorities. Companies who do not comply can face fines up to EUR 20.000.000 or 4% of the annual turnover of their group entity.

The scope of the GDPR is, concisely stated, limited to the processing of personal data by EU based companies or, where no EU presence exists, the processing regards personal data of European citizens [1]. Both 'processing' as well as 'personal data' are tremendously stretched umbrella terms: almost any information that can be linked to an individual is considered personal data, and practically everything you can do with personal data is considered processing.

[1] Please see article 2 and 3 GDPR for the full material respective territorial scope of the GDPR.

The overlap of GDPR and PSD2

As TPP's will want to use (process) personal financial data of European customers for their products and services, they will be required to take the GDPR rules into account. Banks who provide these financial data are also obligated to do so in accordance with the GDPR, as sharing personal data is also a form of processing.

The discrepancies: the Dutch DPA advises

The intersection of PSD2 with data protection has been recognized by the EU legislature: both the preamble, a few considerations as well as the legislative text of PSD2 contain references to data protection (including one article fully dedicated to data protection). However, these references are very limited and still leave room for obscurity.

The DPA acknowledges this in their recommendation on the Implementation Act and most recently in the Implementation Decree. In both recommendations the DPA concludes, in essence, that the GDPR has not been taken in consideration adequately in the course of the Dutch implementation of PSD2.

DPA's Recommendation on the Implementation Act

Hierarchy of rules and relevant authority

The recommendation on the Implementation Act, mainly contained critique on the unclear hierarchy of rules and unclear apportionment of authority (should DNB or the DPA monitor compliance with de data protection rules of PSD2 and the affiliated laws?). In the revised Explanatory Memorandum (published last October) the legislature has taken these points into considerations but has decided that the exact discussion on applicability of rules and relevant authority should be (and is being) discussed on a European level. Therefore the DPA's request to clarify this in (the Explanatory Memorandum of) the Implementation Act is not met. However, with regard to the specific article in PSD2 on data protection, the Dutch legislature is completely clear: this article is considered a "lex specialis" to the general GDPR. This means this specific provision prevails the GDPR with regard to processing personal data for the purpose of payment services. The legislature therefore acknowledges DNB as the only relevant authority to supervise compliance with this article. Yet, it is to be noted that even in this case, the GDPR and DPA will play a role, as the other GDPR obligations will also have to be met (since data processing is concerned). Data protection (as prescribed by the GDPR) should therefore be fully considered in the design and implementation of all PSD2 related services. In that regard we recommend to presume that both authorities will be equally entitled to take enforcement measures in case of non-compliance of overlapping rules.

We expect that this matter will either be clarified on a European level (as mentioned by the Dutch legislature), or the DPA might (informally) push for more clarification on this matter in the national parliamentary process. We are monitoring this closely.

DPA's Recommendation on the Implementation Decree

The Implementation Decree contains rules on the implementation of the specific data protection article of PSD2 (which includes the topic of consent). The DPA's recommendation on the Decree, published last January, shares the central theme of critique of inconsistency on the hierarchy of rules and authority as in the recommendation on the Implementation Act. In addition, the recommendation also contains specific commentary on the lack of clarity with regard to (1) the definition of sensitive payment data and (2) consent.

1. Sensitive payment data

PSD2 indicates that "sensitive payment data" ought not to be stored by the Payment Service Provider ("PSP" which includes TPP's). The definition of sensitive payment data in PSD2 however is rather inconsistent with the definition of sensitive personal data (or special categories of data) mentioned in the GDPR. Where PSD2 defines this as *'data, including personalized security credentials which can be used to carry out fraud*', the GDPR refers *to 'personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.'* Regrettably, the Implementation Decree has adopted the same inconsistency. The DPA notes that this is a topic of concern and should be clarified.

In this regard it is recommended to at least map out and categorize precisely what kind of data will be processed and whether this falls within the definition of sensitive data under PSD2 and/or the GDPR. Most probably a DPIA will be required, which will help in this mapping exercise.

2. Consent

PSD2 states that a PSP may only access, process and retain the personal data necessary for the provision of their payment services with the explicit consent of the payment service user. This is on the whole in line with the GDPR, including the similar right of Data Portability. In addition, the GDPR contains more extensive rules on the use of explicit consent as a processing ground. For example, the consent of data subjects (customers) has to be freely given, specific and informed, the controller (PSP or TPP) has to demonstrate that this consent has been provided and the data subject has to be able to easily withdraw the consent at any time. These additional, general, rules of the GDPR supplement the specific PSD2 rules on consent.

The DPA emphasizes this additional effect of the GDPR on PSD2, but explicitly states that when a TPP asks for consent to perform a service that entails more or something different than the Account Information Service, PSD2 is (or the affiliated laws are) not applicable. The processing based on this separate consent will therefore fall completely within the scope of the GDPR. The DPA recommends to specify this more clearly in the Implementation Decree.

It is advised to identify (and document) the purposes for which the data will be used from the start of the design of the consent for an Account Information Service. This will help with determining whether (a separate) consent is necessary and which exact rules (PSD2 and/or GDPR) should be taken into account. Determining the purpose before processing personal data is also a strict GDPR requirement so this will be necessary in any event.

Another topic of discussion is whether the consent given also covers the processing of personal data of third parties, for example the recipients of the transactions with the customer. In that regard it is noteworthy that the DPA is of the opinion that the provided consent by the customer is only pertained to the personal data of the customer that gave consent. This means that personal data of third parties, such as the personal data of the beneficiary of the transaction, cannot be processed on the basis of this consent. The DPA does not state if another lawful processing ground can be applicable for this type of processing and under which conditions. We expect that controllers (banks and TTP's) will try to base the processing of third party data on the processing ground legitimate interest. As applicability of this processing ground depends on a balancing act between the legitimate interest of the controller and the (privacy) right of the data subject, the outcome is situation-dependent. If, for example, a service drifts away from the purpose of solely providing the service to the client, it is less likely that the legitimate interest can be used as a lawful processing ground. It is highly recommended to timely perform an assessment on whether, and under which conditions, the visualized processing (including the processing of third party data) is lawful under the GDPR.

Conclusion and strategic guidance

In the course of Dutch Implementation of PSD2, the details surrounding the overlapping PSD2 and GDPR topics are not crystallized yet. We expect the legislature to give clarity on these issues in the near future. In the meantime, if your company falls within the scope of both PSD2 and GDPR, there are a few strategic approaches to consider to tackle the overlapping, uncertain parts of PSD2/GDPR:

1. '**Wait and see**': The first option is to wait for more guidance from the European and Dutch legislature on the discrepancies.[2] This might be most feasible for small banks with other regulatory obligations on their mind. However, do not wait too long, as this might require some serious IT changes.
2. '**Get prepared**': There is also the proof of concept method, where you act preparatory until more clarification is given or the implementation date is reached. This approach can include testing out the infrastructure, preparing the systems/applications and outlining and drafting procedures. Such a method will (initially) take up more resources than the idle approach, but will leave less room for surprises once both GDPR and PSD2 are enforceable. For most Banks and TPP's this approach is most advisable.
3. '**Go live**': Pro-active companies with a higher risk appetite and more direct resources can choose to fully implement both PSD2 and GDPR (based on the available knowledge and the most probable outcome) and go live as soon as possible. As still some major obscurities exist, this option is most feasible for TPP's who aim to use PSD2 commercially for new services and products.

Whichever approach you choose, Deloitte can provide guidance in your PSD2/GDPR journey. Feel free to contact us via the contact details provided below.

Contact us

Anastasiya Milshina
Email: amilshina@deloitte.nl

Marloes Dankert
Email: mdankert@deloitte.nl

Peter Kits
Email: pkits@deloitte.nl

Maria van Duijvenbode
Email: mvanduijvenbode@deloitte.nl

[2] While already preparing for implementation of the certain parts of the PSD2/GDPR. It is not advised to use this approach with regard to all aspects of GDPR/PSD2 implementation.

Deloitte.
Legal