PSD2 In Depth - Europe Enters New Era For Payments

PaymentsCompliance

REVISED PAYMENT SERVICES DIRECTIVE (PSD2): STATUS OF NATIONAL IMPLEMENTATION

The revised Payment Services Directive was required to be transposed into national legislation in all EU countries by January 13, 2018. PaymentsCompliance has been monitoring the directive's implementation in all member states.

As of January 17, this is the status of the implementation process in the 31 jurisdictions.

Country	TBC	Draft Stage	Consultation Process	Legislative Process	Implemented
Austria			●		
Belgium				●	
Bulgaria				●	
Croatia			●		
Cyprus				●	
Czech Republic					●
Denmark					●
Estonia					●
Finland					●
France					●
Germany					●
Greece				●	
Hungary					●
Ireland					●
Italy					●
Latvia				●	
Lithuania				●	
Luxembourg				●	
Malta					●
Netherlands		●			
Poland				●	
Portugal		●			
Romania	●				
Slovakia					●
Slovenia				●	
Spain			●		
Sweden		●			
United Kingdom					●
Iceland (EEA)		●			
Liechtenstein (EEA)			●		
Norway (EEA)			●		

Practical Insight: Overlaps Between the GDPR and PSD2

HELENA REGOLI ⁞ SEPTEMBER 8, 2017

This practical guide provides an overview of the potential overlap between the revised Payment Services Directive (PSD2) and the General Data Protection Regulation (GDPR), and how these conflicts could potentially be resolved.

INTRODUCTION

The revised Payment Services Directive (Directive 2015/2366), popularly known as PSD2, must be implemented by EU member states by January 2018, a few months before the application of the General Data Protection Regulation (Regulation 2016/679) (GDPR) from May 25, 2018 in all member states.

PSD2 is a key piece of payments-related legislation in Europe. The text aims to bring into scope new types of payment services, increasing competition, enhancing security and boosting customer protection.

The text requires that all member states of the EU implement the directive nationally by January 13, 2018, with the exception of regulatory technical standards (RTS) on strong customer authentication and secure communication, which will have a different timetable.

Under the directive, payment institutions will be required to make customer data available to authorised third parties, with the account holder's explicit consent.

The GDPR is a regulation which intends to unify and strengthen data protection for data subjects within the member states and will impose new fines on firms that do not adequately safeguard their data.

The GDPR represents a significant reform of existing EU data protection law, including the introduction of a number of new rights around how data subjects can control their personal data. These include a "right to be forgotten", a right to object to certain types of data processing and a "right to data portability". Data portability is defined by the text as a right for data subjects to receive their personal data "in a structured, commonly used and machine-readable format", so that they can either obtain a re-useable copy of their data or require the controller "to transmit those data to another controller without hindrance".

Businesses that fail to protect personal data adequately under the GDPR could face fines of up to a maximum of either €20m or 4 percent of global annual turnover (whichever is the greater).

A number of payments industry stakeholders have highlighted some potential conflicts between PSD2 and the GDPR. Clarity on the interaction between the two texts, in particular regarding the basis for processing personal data, the consent model and rules around breach reporting, is consequently required.

Internal meetings within the European Commission took place in June 2016 to "clarify" the relationship between the GDPR and PSD2.

PSD2 does not refer directly to the GDPR and, likewise, no specific reference to the GDPR is made in PSD2. However, PSD2 does say that the processing of personal data for the purpose of payment services must be carried out in accordance with the existing EU Data Protection Directive (Directive 95/46/EC) and its national implementing laws. Even if Directive 95/46/EC is repealed by the GDPR from May 25, 2018, the GDPR states in Article 94 that "references to the repealed directive shall be construed as references" to the new GDPR.

As the GDPR and PSD2 do not talk about their interactions, it will fall to the national regulatory authorities to interpret the potential differences existing between both texts, with the data protection authorities enforcing the GDPR, while the appointed national financial regulators will take the responsibility of enforcing PSD2. As stated by the Information Commissioner's Office (ICO), the UK data protection authority, in a response to a consultation on the implementation of PSD2 in the UK published on March 17, 2017, "it is important that the implementation of PSD2 does not introduce requirements that conflict with data protection obligations".

This practical insight is aimed at helping organisations understand what conflicts could exist between these texts, and how these differences could potentially be resolved.

POTENTIAL CONFLICTS ARISING FROM LEGAL BASIS FOR PROCESSING PERSONAL DATA, IN PARTICULAR CONSENT

Article 94 of PSD2 deals with data protection. It first states that payment service providers will be permitted to process personal data when "necessary to safeguard the prevention, investigation and detection of payment fraud". It goes on to say that payment service providers shall only access, process and retain personal data necessary for the provision of their payment services "with the explicit consent of the payment service user" (emphasis added).

Under Article 6 of the GDPR, consent is one of the six lawful bases for processing personal data, which also include performance of a contract, compliance with a legal obligation and the legitimate interests of the data controller. However, "explicit consent" has a very specific meaning under the GDPR. In accordance with Article 9(2) of the GDPR, "explicit consent" is one of the means by which a data controller can lawfully process sensitive personal data, for example information concerning an individual's health, racial or ethnic origin, political opinion or religious beliefs.

Payments UK, the BBA and the UK Cards Association published a response to a HM Treasury Consultation on the implementation of PSD2 on March 15, 2017, in which they highlight that "the GDPR consent requirements are such that in most cases firms should not be making consent a pre-condition for the receipt of a service". The above PSD2 provision "seems to conflict with this intention as it is requiring consent on a mandatory basis before personal data can be processed in connection with the provision of payment services". This conflict has not yet been resolved.

PSD2 also has a higher consent threshold for personal data than the GDPR. Payment or banking data is not sensitive personal data under the GDPR and so the GDPR does not require explicit consent to be obtained to process this data. Despite this, payment service providers would currently need to obtain "explicit consent" under PSD2 to process payment or banking data to comply with Article 94.

As explained by a civil servant at the European Commission to PaymentsCompliance in June 2016, as the legal bases for processing personal data are different, any conflict between these provisions "could be resolved by 'lex specialis', a legal doctrine that holds that specific rules override general ones — meaning PSD2 would trump the GDPR in certain circumstances".

In the response to the consultation on the UK implementation of PSD2 published in March 2017 by the ICO (the March Response), the regulator highlights that in its draft guidance on consent, "explicit consent must be expressly confirmed in words, rather than by any other positive action. Therefore, even if it is obvious from an individual's actions that they consent to the processing of their personal data in a particular way,

this cannot be 'explicit consent' unless it is also expressly confirmed in words." The ICO's March Response goes on to say that "whilst we appreciate 'explicit consent' is the term used in PSD2, care should be taken to ensure that the use of the term in this related context does not confuse or unnecessarily hamper the development of a reasonable user experience".

As explained by David Futter, a partner at Ashurst law firm, in light of the above, further clarity is needed from the financial service regulators to understand what approach to consent under PSD2 will need to be taken by industry.

POTENTIAL CONFLICTS REGARDING SECURITY RULES

Potential overlaps between data security rules in GDPR and PSD2 could exist as well.

Under PSD2, payment service providers are required to take specific security measures when performing a number of payment service activities. These include when confirming availability of funds for the purpose of card-based payment transactions (Article 65) and when authenticating and communicating with payment service users for payment initiation and account information services (Articles 66, 67 and 97). The specific security measures and standards that a payment services provider will need to meet when conducting these payment activities will be set by the European Banking Authority (EBA) under its regulatory technical standards on strong customer authentication and secure communication (RTS). Although PSD2 will apply from January 13, 2018, the RTS will not be finalised by the EBA until later, currently expected to be around Autumn 2018 at the earliest.

Article 98(2) of PSD2 mandates the EBA to ensure that the RTS will ensure an appropriate level of security for payment service users and payment service providers through the adoption of "effective and risk-based requirements".

In contrast, the GDPR (which will enter into force earlier than the RTS, on May 25, 2018), requires organisations to implement "appropriate technical and organisational measures to ensure a level of security appropriate to the risk".

According to the ICO, payment service providers will need to ensure that they have adequate systems in place to protect the security and integrity of the personal data they process as soon as they begin processing this data. The ICO explained in its March Response that, for payment service providers, this means that "as the draft RTS is now available, systems and procedures should be designed in line with the RTS wherever possible in order to ensure minimal disruption when the RTS eventually comes into force".

Although the EBA is of the view that there is no conflict with the GDPR at the RTS level, it also acknowledges that, during the implementation and supervision stage, the interaction between the two will need to be considered.

It is clear that the ICO is also mindful of the potential for inconsistency between the data security requirements under the GDPR and the, as yet, unfinished RTS. It stated in the March Response that it "will continue to engage with HM Treasury, the Financial Conduct Authority, industry bodies and other relevant stakeholders" to ensure that "the provisions of PSD2 are implemented in a way that is harmonious with, and complements, data protection requirements". This is encouraging news for industry.

POTENTIAL CONFLICTS REGARDING DATA BREACH REPORTING

A different terminology exists between the legislation. PSD2 refers to "security incidents", whereas the GDPR concerns "data breaches".

The GDPR defines a personal data breach as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed" (Article 4 of the GDPR); however, PSD2 does not offer a specific definition of what security incidents cover.

On its face, a data breach (for the purpose of the GDPR) is likely to be a result of a security incident (as understood under PSD2), such that where a payment service provider suffers a security incident involving the loss or unauthorised access to personal data, the GDPR should also apply.

The two texts apply a different threshold for reporting "security incidents" or "data breaches". Reporting obligations arise under Article 96 of PSD2 if a payment service provider suffers a "major operational or security incident". This contrasts with the GDPR which requires any personal data breach to be reported, unless the breach "is unlikely to result" in a risk to the rights and freedoms of the data subjects involved. As such, when devising their security and data reporting policies, payment service providers will need to be very clear about when an obligation to report under either or both of the legislation arises.

The language used in the GDPR and PSD2 around the timescales for reporting is also slightly different.

Reportable security incidents under PSD2 need to be notified "without undue delay" to the competent authority in the home member state of the payment service provider.

The GDPR applies a similar timeframe, in that Article 33 requires a data controller to report a personal data breach without undue delay, but also goes on to say that "where feasible" this should be no later than 72 hours after first becoming aware of the breach.

On its face, this may appear that a tighter reporting timeframe is required by the GDPR. However, according to the final guidelines on major incident reporting under PSD2 published by the EBA on July 27, 2017 (which should take effect alongside PSD2 if accepted by member states), Article 96 of PSD2 will require payments businesses to send an initial notification to the competent authority within four hours of the moment the major operational or security incident was first detected (Article 2.8). The EBA has extended this timeframe for reporting a major incident from two hours to four — a two-hour deadline was included in the draft guidelines published by the EBA in December 2016, but industry complained that the initial deadline was "unreasonable".

A second report must then be filed within three business days (Article 2.10). This is seemingly in keeping with the 72-hour timeframe afforded by the GDPR.

The EBA guidelines also require firms to submit a report if a non-major incident develops into a major one. Any breach or system failure that affects transactions worth more than €5m, or more than 25 percent of a payment service provider's transactions or clients, is classed as a major incident.

Payment service providers need to provide their regulator with a description of their security incident monitoring and handling procedures, and "where the incident has or may have an impact on the financial interests of its payment service users", inform without undue delay "its payment service users of the incident and of all measures that they can take to mitigate the adverse effects of the incident".

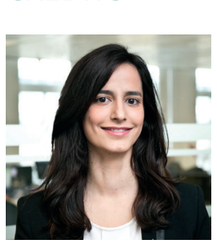
Under the GDPR, the payment service provider (if also the data controller) will need to notify the affected data subjects of the breach "without undue delay", when the personal data breach "is likely to result in a high risk to the rights and freedoms of natural persons". The difference in the amounts of fines should also be noted.

Under the GDPR, an infringement of the above data breach reporting obligations can be subject to administrative fines up to €10m, or in the case of an undertaking up to 2 percent of its total worldwide annual turnover of the preceding financial year, whichever is higher.

PSD2 does not name penalties or specify any amount so far. Article 103 states: "Member states shall lay down rules on penalties applicable to infringements of the national law transposing this directive and shall take all necessary measures to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive." It, therefore, remains open to member states to choose to impose different amounts when setting fines in relation to security incident reporting, or even levy non-financial sanctions.

As explained by David Futter, whatever sanctions imposed under PSD2, they will not be mutually exclusive to those imposed under GDPR; therefore, "where a payment service provider suffers a security incident and, as a result, breaches both the PSD2 and GDPR, it will be open to each of the ICO and relevant financial services regulators to impose as they see fit those fines and other sanctions available to them under their supervisory powers".

CREDITS



Helena specialises in Data Protection and European Union issues. She was admitted as a lawyer in France and previously worked in a Paris law firm. Helena graduated from Panthéon-Sorbonne University with two Master's degrees, and has also completed an L.L.M in Intellectual Property Law from Queen Mary University.

This report was prepared with input from David Futter, a partner at Ashurst.

David is a partner in Ashurst's dedicated Digital Economy Practice. He specialises in digital transformations, particularly within the fields of fintech and payments, having led deals for many of the major participants across the financial services value chains, including banks, processors, card schemes, technology vendors and merchants/retailers. David also advises regularly on a wide range of IT procurement, outsourcing and service contracts, consumer protection regulation and intellectual property law.

EBA Reignites Screen Scraping Row, Warns 'Legal Battles' Ahead

FRAN WARBURTON ⁞ **JANUARY 26, 2018**

A senior European Banking Authority (EBA) official has accused lawmakers of failing to clarify the legal status of screen scraping under incoming legal reforms, warning of more industry conflict and an unprecedented burden on national regulators.

Dirk Haubrich, the EBA's head of consumer protection, financial innovation and payments, urged attendees at a European Parliament scrutiny session to rethink security rules adopted by the European Commission in November.

The final regulatory technical standards, which address third-party account access under the revised Payment Services Directive (PSD2), state that a form of screen scraping could still take place, but only if a bank's dedicated technological interface fails to gain regulatory approval.

"The responsibility of the key question — is screen scraping allowed or not is not resolved, it's all pushed down to the EBA," said Haubrich.

"The resource implications, the legal battles and the conflicts we have to sort out six, 12 or 18 months further down the line are immense because of this lack of clarity."

In the EBA's initial draft standards, which were published in February last year, the industry was told that third parties would no longer be permitted to access customers' accounts by using their login credentials.

The practice was labelled a serious security risk by banks, and was deemed incompatible with the PSD2 text by the authority.

However, that sparked a backlash from existing third-party providers, which argued that a total ban on screen scraping would enable banks to choke off competition by developing low-quality or restrictive interfaces.

After another disputed draft text, the European Commission eventually settled on a compromise: if a bank has developed an interface that is approved by national regulators, third parties must use it. If not, a version of screen scraping is allowed to continue.

According to the EBA's Haubrich that created a new problem for national regulators, effectively forcing them to decide whether a bank's interface meets IT standards.

This is a task "for which the competent authorities are not equipped and the EBA is not equipped either", he said.

As assessment of an interface would also need to take into account its availability and performance, he explained, it would require every single bank to undergo an inspection by their national regulator.

"There are several thousand assessments that need to be done, because there are 6,000 banks in the European Union," Haubrich said. "So there's a huge resource implication for the EBA and the national authorities."

"We'd rather have these problems sorted out now, and think about it for another month or two to sort this out, than having lots of very difficult discussions — hundreds of them — for each individual case, for each bank," said Dirk Haubrich of the European Banking Authority.

The EBA official pointed to another issue in the commission's final draft text.

One of the conditions that national authorities will have to take into account is whether a bank's interface is "to the satisfaction of third-party providers".

That means the legality of screen scraping "is dependent on whether another set of actors a competing set of actors is satisfied with that interface".

"That is a very unusual legal construction, and we see lots of problems further down the line," he said.

European Commission officials made no secret of their opposition to the EBA's arguments.

Martin Merlin, director of the commission's financial services unit, insisted that the reaction to November's final text has been "very positive from both sides".

"We believe that the RTS [regulatory technical standards] now provides very strong incentives to all market players to work together and develop common standards for APIs [application programming interfaces]," he said.

"This should unleash a wave of fintech innovation, with banks providing platforms on which many new services can be drafted."

Merlin said a group has been established, supported by the commission and the European Central Bank, that will evaluate API developments and give advice to national authorities.

The first meeting of that group was scheduled for January 29, and it will be given six months to develop "practical modalities".

Haubrich acknowledged that the commission has the final say on the text, but expressed disappointment that "additional requirements were inserted … that we were not aware of before".

That marked a procedural precedent "which we hope will not be repeated", he said.

MEPs were generally supportive of the commission's text, with Italian representative Roberto Gualtieri describing the compromise as "a good improvement".

He admitted, however, that he was "comfortable with the original EBA suggestion" and that divergences of interpretation must be avoided at national level.

MEPs Markus Ferber and Olle Ludvigsson echoed claims that financial firms see the standards as a balanced compromise between banks and fintechs.

The commission's Merlin said he expects the European Parliament and European Council to give their blessings to the reforms around March this year, which would mean they take effect in September 2019 at the earliest.

FCA Grants Approval To 13 Third-Party Providers

JOHN BASQUILL ⁞ JANUARY 18, 2018

The UK has granted approval to 13 third-party providers, including processing giant Paysafe, looking to capitalise on the introduction of the EU's revised Payment Services Directive (PSD2).

The Financial Conduct Authority (FCA) has confirmed to PaymentsCompliance that ten account information service providers, one payment initiation service provider and two providers offering both have received permission to operate under the new regime.

PSD2, which came into effect in the UK on January 13, creates a legal framework that allows third-party providers to gain external access to accounts held by a bank.

They can then aggregate transaction data and facilitate credit transfers directly between accounts.

"This of course will change — increase — going forward," a spokesperson for the FCA said, referring to the number of authorised firms.

The regulator revealed last week that it was considering around 40 applications in total.

Skrill, which is owned by Paysafe, received authorisation as a payment initiation service for its Rapid Transfer product.

Ardohr, trading as CreDec, and TrueLayer were granted permission to carry out both payment initiation and account information services.

The firms registered as account information service providers were: Digital Moneybox; Emma Technologies; FundingXchange; Flux Systems; Fractal Labs; Credit Data Research; Business Finance Group; Clear Score Technology; Consents Online; and Indigo Michael.

"We've actually been operating a service equivalent to a payment initiation service for a while now, under the Rapid Transfer brand," explained Elliott Wiseman, chief compliance officer and general counsel at Paysafe.

"Obviously, with the advent of the new formal authorisation for these services, we made the decision that we wanted to ensure that we can continue operating in the same way after January 13."

Wiseman said the company is already working on applications to passport payment initiation services in other EU member states.

"Initially we're looking to passport into 12 member states, probably looking at it as a phased approach and see how well it does," said Elliott Wiseman of Paysafe. "If it does well no doubt passport into the remainder."

Although Rapid Transfer remains one of the company's lesser used payment services, he said payment initiation is "clearly something that we think will gain more and more traction".

TrueLayer, which gained permission for both third-party activities, is a much younger company — it was founded in July 2016 — but took a similar view.

"The payment initiation product that we're building lives adjacent to the data API that we've already built," said Shefali Roy, the company's chief operating officer.

"It will fill a huge gap in the current payment landscape and specifically enable digital financial service to transfer money in a seamless way."

Roy said the company has connected to more than a dozen banks, estimating that it covers between 90 and 95 percent of the UK's banking population.

TrueLayer pulls information from an account, including its balance and transaction history, and will later introduce a regular payment function as an alternative to a direct debit or standing order.

Alexander Meynell, strategy director at CreDec, said the company's decision to apply for dual permissions was "all about managing the entirety of users' requirements".

"We see account information services and payment initiation services as complementary solutions for our customers," he said.

All three were highly complimentary about the FCA's role in gaining authorisation.

"They pulled out all the stops over the last couple of weeks, working with us really collaboratively, helping us make final tweaks to the application ... to ensure we were compliant with the new regulations," said Paysafe's Wiseman.

Roy said Truelayer's application was a "seamless process" despite only being submitted around two months ago.

"We had a case officer appointed within a week and a half," said Shefali Roy of TrueLayer. "In terms of questions for us, they were extremely collaborative and very helpful."

Meynell added: "The FCA appears to be coping well with the significant challenge of re-authorising the UK market in such a short window. Certainly our case officer was exemplary."

However, that speed to market on the third-party side has not been matched by the UK's banking sector.

Nationwide, this week, became the sixth bank or building society to delay the introduction of an application programming interface (API) facilitating third-party access, much to the chagrin of the Competition and Markets Authority.

The stuttering launch of open banking means third parties will remain reliant on screen scraping as an access mechanism, at least in the medium term.

"We're having to continue doing that, because at the moment there are no compliant APIs in the market to be used," said Wiseman.

"We obviously made it clear that until such time as the APIs were available to be used, there was really no other option than to screen scrape."

He welcomed the European Commission's decision not to outlaw screen scraping outright, despite pressure from banks, in secondary legislation expected to take effect next September.

"I think they've reached a sensible position and a pragmatic one until such time as the full API solution is ready to be used," he said. "We're talking to the banks now making sure that we're whitelisted, so we're not denied access going forward."

About Us

PaymentsCompliance is the leading provider of independent legal, regulatory and business intelligence to the global payments industry.

We provide the critical and timely information that helps you make sense of the complex and rapidly changing global regulatory environment.

Trusted by leading names all over the world, we power more informed understanding and effective decision making.

Our analysis of legal and policy developments comprehensively covers the needs of payment industry professionals, helping them to make informed business decisions, uncover opportunities and reduce legal fees and compliance costs.

Find out more at paymentscompliance.com

UK Office
St Clare House
30 Minories
London
EC3N 1DD
+44(0)207 921 9980