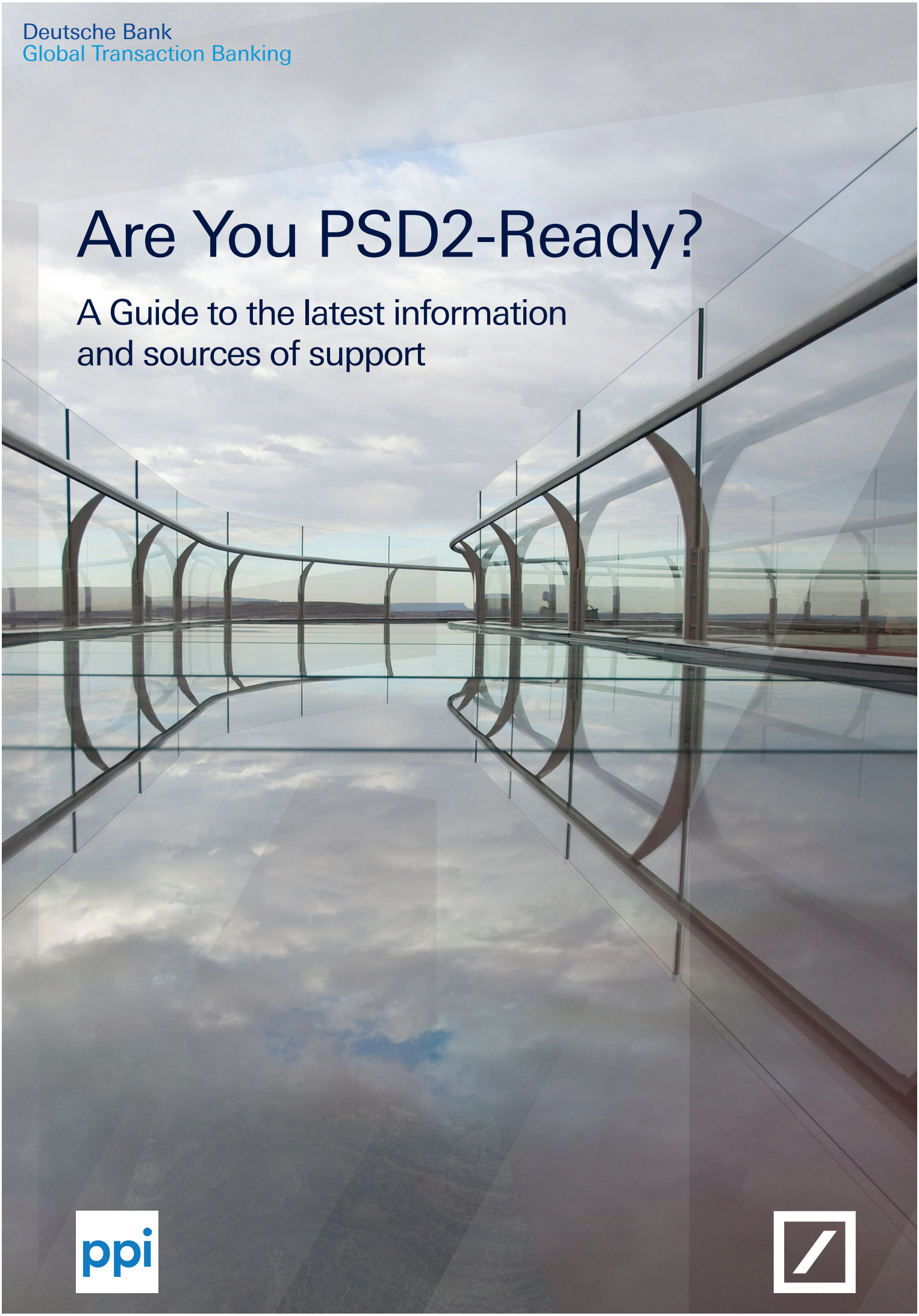
Deutsche Bank
Global Transaction Banking

Are You PSD2-Ready?

A Guide to the latest information and sources of support



ppi

Running, without a finish line

Today, users of payments services are demanding greater speed, choice and convenience from their payment service providers. In addition, they expect omni-channel functionality, and increased control of their financial information. PSD2 tackles these demands head-on – and will likely result in a new, more open, digital payments market in Europe.

There was a time when the banking industry may have looked at such radical changes – and especially the opening up of the European market to third party providers (TPPs) – with concern. However, times are changing.

Far from a threat, or even a regulatory burden, it is clear to us all that PSD2 provides impetus for necessary change. PSD2 presents a significant opportunity for banks and others that service customer accounts (Account Servicing Payment Service Providers (ASPSPs) as we will refer to them) to get Application Programming Interface (API) and Open Banking-ready – to future-proof themselves in an age of rapid technological change.

Admittedly, significant investment will be required from banks (especially with respect to API development, if that route is chosen). But the long-term returns in terms of new revenue streams, innovation and customer retention should make this worthwhile.

The changes required on the part of retail and corporate payment service users (PSUs) to ensure they are PSD2-compliant will be less significant however – a key difference from other payments initiatives, such as the Single Euro Payments Area (SEPA).

Yet, that is not to say that they will not be impacted. Indeed, PSUs will experience immediate benefits as of 13th January 2018, when the new provisions of value dating and consumer protection become effective. Further value is to be expected from 2019 onwards as a result of the innovation eco-system flourishing around third party access. Hence the transposition of PSD2 into national law and the final dates when third party access becomes available, outlined in this paper, are of particular interest to the corporate reader.

The race is therefore on to get PSD2-compliant.

Running a smart race requires a clear project strategy, underpinned by an in-depth understanding of the required legal and regulatory changes – and their timelines for implementation. It is for this reason that Deutsche Bank and PPI have collaborated to produce this white paper, which sets out to cover the most-important intricacies of the regulation (and the impact on your business), as well as the key dates and next steps for market participants.

The pace of change is rapid: member states are progressing towards implementing PSD2 into national law (admittedly, some faster than others), the European Banking Authority has drafted, and is consulting on, Guidelines and Technical Standards, while market participants have been laying the groundwork for common standards and protocol.

This has all helped provide clarity on a number of key aspects of the Directive: namely, what will be required to establish a compliant account interface and how to deal with value dating of incoming transactions in a non-euro EU/EEA currency with subsequent currency conversion in the EU/EEA into euro.

However, as ever, clarity is far from ubiquitous. With respect to the all-important third party interface, for instance, we continue to seek confirmation on whether ASPSPs will need to provide TPPs with a "fall-back" option in the event that their dedicated interface becomes unavailable. This would endorse the hotly-contested practice of "screen scraping" – and pose an additional compliance burden on ASPSPs.

There also remain issues with respect to timeline for implementation. While PSD2's overall implementation date is 13th January 2018, there remains the very real possibility that transposition into national law in some member states may be delayed beyond then.

Perhaps more concerning is the genuine – and problematic – implementation gap between the dates that PSD2 itself becomes effective (13th January 2018) and the point at which the highly important Regulatory Technical Standard (RTS) for Strong Customer Authentication (SCA) and Common Standards of Communication (CSC) becomes effective. Given its 18-month implementation period, the RTS on SCA and CSC will now come into force in the first half of 2019 (at the earliest) – more than a year after the implementation of PSD2.

What do we suggest? Start running, irrespective of the finish line.

Given the benefits to clients, there is no reason why ASPSPs shouldn't conclude their IT projects and deploy PSD2-related changes – including those outlined in the new Guidelines – as planned, prior to the January start-date.

With respect to compliance with their SCA and CSC (third party interface) obligations, we would also advise ASPSPs not to wait until late in 2018 or early 2019 to get going. Indeed, there are some significant provisions in PSD2 that are either dependent on or closely bound up with compliance to these obligations.

For example, from 13th January 2018, ASPSPs will no longer be permitted to cancel payments involving a TPP. However, if an ASPSP does not yet have a dedicated interface for TPPs, it will not be able to tell whether a transaction was initiated by a TPP or not.

Similarly, from the same date, in cases where a transaction is made by a TPP in error, the ASPSP will be obliged to reimburse payment service users in the first instance, and subsequently recover the loss from the TPP. Yet an ASPSP which has not yet fulfilled all the requirements for SCA, specifically the requirement to "dynamically link" the transaction to a specific amount and a payee, may not actually have the means of showing who changed the transaction.

As a result, we believe ASPSPs must act now, rather than wait until the final version of the RTS is adopted, let alone comes into force. If not, ASPSPs will not only miss out on some first-mover opportunities, but they may find themselves wholly under-prepared for change.

We rest on the cusp of a payments revolution. The providers that will thrive will be those that exploit the power of APIs – initially to provide TPPs access to their customers' accounts as part of PSD2, but more broadly thereafter to create innovative and convenient products and services tailored to users' changing requirements. Forward-looking corporates will be well-placed to make the most of these developments.

We hope that you find this whitepaper informative and insightful. To discuss any of the issues raised in more detail, or to find out how Deutsche Bank can support your PSD2 implementation project, please don't hesitate to get in touch.

Shahrokh Moinian,
Global Head of Cash Products, Cash Management

Table of contents

List of abbreviations

1FA	One-Factor Authentication
2FA	Two-Factor Authentication
AISP	Account Information Service Provider
API	Application Programming Interface
ASPSP	Account Servicing Payment Service Provider
CSC	Common and Secure Communication
EBA	European Banking Authority
EBF	European Banking Federation
ECB	European Central Bank
EEA	European Economic Area
EPC	European Payments Council
ERPB	Euro Retail Payments Board
EU	European Union
GDPR	General Data Protection Regulation (EU) 2016/679
GL	Guideline
ITS	Implementing Technical Standards (to be issued by the EBA)
PISP	Payment Initiation Service Provider
PSD1	Payment Services Directive 2007/64/EC
PSD2	Revised Payment Services Directive (EU) 2015/2366
PSU	Payment Service User
PSP	Payment Service Provider
RT1	EBA Clearing's infrastructure solution for the processing of instant SEPA credit transfers at a pan-European level
RTS	Regulatory Technical Standards (to be issued by the EBA)
SCA	Strong Customer Authentication
SEPA	Single Euro Payments Area
TARGET	Trans-European Automated Real-time Gross Settlement Express Transfer System
TARGET 2	Second-Generation TARGET System
T2S	(TARGET2-Securities), Eurosystem's technical platform enabling securities settlement services in Europe
TCs	Terms and Conditions
TIPS	TARGET Instant Payment Settlement
TPP	Third Party Provider

1 Introduction

In September 2016, Deutsche Bank, in collaboration with PPI, published a white paper entitled Payment Services Directive 2: Directive on Payment Services in the Internal Market '(EU) 2015/2366', summarising the most important provisions of the Directive (PSD2), and providing the most up-to-date overview then available of its anticipated impact on the operations of affected organisations.

PSD2's intention is to update European payments market regulation to account for an age of rapid technological change, and to foster integration while, at the same time, encouraging competition and innovation in payment services. In addition, it seeks to strengthen payment security and enhance both consumer choice and consumer protection.

The Directive's implementation deadline of 13th January 2018 now looms large.

Our first white paper dealt in detail with PSD2's scope extension to include payments in all currencies, and to payments where only one provider is located in the European Union (EU)/European Economic Area (EEA) and, equally importantly, the exclusions from the scope extension with regards to payment processing and deduction handling. It also sought to add clarity – where possible – to the requirement for account servicing payment service providers (ASPSPs) to set up an account interface accessible by third party providers (TPPs), through which they will be able to access customer account information or initiate payments. Finally, the paper summarised the best understanding then available of the impact of introducing strong customer authentication (SCA) into all electronic payments and remote access to accounts.

In June 2017, we published a further article in collaboration with Innopay discussing in greater detail what we see as the foremost challenge currently facing the European payments market – the practical implementation of third party access to accounts required by PSD2. We argued that the work currently being undertaken by market participants to comply, in particular its collaborative aspect, may well prove to be an enabler of Open Banking business models.

Time has moved on, and hence we felt the need to revisit this regulation in a second paper. Indeed, although gaps and uncertainties remain, many aspects of how the Directive will work are now clearer than a year ago.

On the other hand, the Directive's implementation deadline of 13th January 2018 – by when member states are required to have implemented it into their national law – now looms large. This should act as a wake-up call to all organisations affected to ensure they are PSD2-ready.

This is why we are publishing a new white paper on PSD2 to act as a practical guide in this last and crucial implementation phase. It brings together all the latest information and directs readers to sources of further information and support for their implementation project.

Who is this paper for? The paper as a whole is written primarily for banks and others that maintain and service customer accounts (ASPSPs in the language of the Directive), the group for which PSD2 will bring the most seismic change.

Corporate customers of banks and other payment providers will not be affected by PSD2 to the same degree. However, we think they will read with interest Section 2.1 which summarises the latest developments in this area, and Section 5 which provides a Roadmap for PSD2 implementation and looks ahead at further regulatory and market change to come.

Finally, we believe that Section 2 and Section 5 of this paper, will be an important read for those that intend to become TPPs under PSD2.

2 A rapidly changing regulatory environment

2.1 What has happened since Deutsche Bank's first white paper on this topic?

Since publication of our first white paper, there have been developments on several fronts. There has been (albeit uneven) progress in member state legislatures towards implementing PSD2 into national law. There has been a great deal of activity at the European Banking Authority (EBA), tasked with setting up a new central electronic register of market participants, and with drafting and consulting on six Guidelines and five sets of Technical Standards (four Regulatory Technical Standards (RTS) and one Implementing Technical Standard (ITS)). These set out key provisions of the Directive in more detail, aiming to ensure its consistent implementation across member states.

Meanwhile, market participants have been actively preparing for the Directive's implementation by forming initiatives that are working to lay the groundwork for agreement of common standards for the new account interface. Likewise, other players in the market have been equipping and positioning themselves in anticipation of the new opportunities offered by PSD2.

Furthermore, the issuing and handling of charge codes, as well as of charge requests, in the inter-banking space has been revisited (for example, as part of the Euro Banking Association's PSD2 Practitioners' Panel). In this context, it is worth pointing out that the relevant wording of the related provisions of PSD2 has remained unchanged compared to the corresponding articles in PSD1. Accordingly, it is our understanding that existing market practice on the usage of charge codes, which has evolved since the implementation of PSD1, will continue since there has been no change to the underlying payment reality and the legislation providing its framework.

2.1.1 Activities by national legislators

PSD2 came into force on 13th January 2016, and member states' national legislatures are obliged to transpose it into national law by 13th January 2018. However, while four (Denmark, France, Germany and the UK) have transposed it into national law and a number of others have draft legislation in place ready to be passed, it appears that not all member states will be ready on time, potentially holding up integrated implementation.

2.1.2 Activity at the European Banking Authority

RTS and Guidelines

The EBA was mandated to issue six Guidelines under PSD2 addressed either to market participants or to member states' competent authorities, and to develop and submit four sets of RTS and one set of ITS for adoption by the European Commission.

Initial drafts of these documents are usually subject to a period of open public consultation, after which the EBA will collate and consider stakeholder responses and publish a revised "final draft". The Commission may adopt the EBA's draft RTS, with the amendments it considers relevant, or reject them outright. If it adopts them, they are additionally subject to scrutiny by the European Parliament and the European Council, and if one of these objects to them, they will be sent back to the EBA for redrafting.

In addition to Technical Standards, the EBA also issues Guidelines, addressed to member states' competent authorities or to financial institutions. These do not have to go through the same approval process by the other EU institutions.

The various Guidelines and Technical Standards that have so far been issued under PSD2 have made many aspects of the Directive's implementation clearer, although not all of them are yet available in their final form (see Figure 1).

	Topic	Name	Consultation Paper	Status	Final Report
Guideline	Professional liability insurance	Guidelines on the criteria on how to stipulate the minimum monetary amount of the professional indemnity insurance under PSD2	EBA/CP/2016/12	Final report available	EBA/GL/2017/08
	Authorisation of PSP	Guidelines on authorisation and registration under PSD2	EBA/CP/2016/18	Final report available	EBA/GL/2017/09
	Security measures	Guidelines on security measures for operational and security risks under the PSD2	EBA/CP/2017/04	Consultation finished – final report expected in October 2017	
	Incident reporting	Guidelines on major incidents reporting under the PSD2	EBA/CP/2016/23	Final report available	EBA/GL/2017/10
	Complaint procedure	Guidelines on procedures for complaints of alleged infringements of the PSD2	EBA/CP/2017/01	Consultation finished – final report expected in October 2017	
	Fraud reporting	Guidelines on fraud reporting requirements under PSD2	EBA/CP/2017/13	Under consultation	
RTS	Central contact point	Draft RTS on the criteria for determining the circumstances in which the appointment of a central contact point pursuant to Article 29(4) of Directive (EU) 2015/2366 is appropriate and the functions of those central contact points	EBA/CP/2017/09	Under consultation	
	Strong customer authentication and common and secure communication	Draft RTS on strong customer authentication and common and secure communication under Article 98 of PSD2	EBA/CP/2016/11	Awaiting adoption by Commission	EBA/RTS/2017/02
	Exchange of information between competent authorities for passport notifications	Draft RTS on the framework for cooperation and exchange of information between competent authorities for passport notifications	EBA/CP/2015/25	Final report available	EBA/RTS/2016/08
	Electronic central register	Draft RTS setting technical requirements on development, operation and maintenance of the electronic central register and on access to the information contained therein	EBA/CP/2017/12	Under consultation	
ITS	Public register	Draft ITS on the details and structure of the information entered by competent authorities in their public registers and notified to the EBA	EBA/CP/2017/12	Under consultation	

Schedule courtesy of PPI AG www.ppi.de

Figure 1: Guidelines and RTS/ITS published under PSD2

Guideline / RTS	Date	Customer	TPP	ASPSP	Competent Authorities
Guidelines on the criteria on how to stipulate the minimum monetary amount of the professional indemnity insurance under PSD2	Jan 13th, 18		x	(x)	x
Guidelines on authorization and registration under PSD2	Jan 13th, 18		x		x
Guidelines on Security measures for operational and security risks under PSD2	Jan 13th, 18		x	x	x
Guidelines on major incidents reporting under PSD2	Jan 13th, 18		x	x	x
Guidelines on procedures for complaints of alleged infringements of the PSD2	Jan 13th, 18	x	x	(x)	x
Guidelines on fraud reporting under PSD2	Jan 13th, 18		x	x	x
Regulatory Technical Standards on central contact points under PSD2	Jan 13th, 18*		x		
Regulatory Technical Standards on strong customer authentication and secure communication under PSD2	H1 / 2019	x	x	x	x
Regulatory Technical Standards on passporting under PSD2	Jan 13th, 18*		x	x	x
Regulatory Technical Standards on the EBA Register under PSD2	Jan 13th, 18*		x		x
Implementing Technical Standards on the details and structure of the information entered by competent authorities in their public registers	Jan 13th, 18*		x		x

Key:

* 20th day past its publication in the official journal of the EU.
x Indicates Guidelines that have a direct impact on market participants.
(x) Indicates Guidelines that have downstream implications on PSPs own operating models.

Figure 2: Impact of PSD2 on market participants

New central electronic register of market participants

The EBA has additionally been tasked to develop, maintain and operate a new central electronic register containing information on market participants notified to it by member states' competent authorities. It also has had to draft RTS, and ITS, detailing the setting up and running of the register and the information to be collected, stored and accessed there. Public consultation on this was open until 18th September 2017, with the EBA's final report expected in December 2017 and adoption of the RTS and ITS estimated in Q2 of 2018. The register will probably go live in Q3 or Q4 of that year, and must be available 20 days after the effective date of the respective Guideline.

2.1.3 Market initiatives supporting implementation

However, while much has become clearer, there are areas of PSD2 still lacking specificity or certainty. Industry initiatives have therefore sprung up both to try and fill in some of these gaps (for example by agreeing common approaches and standards, in particular for the new third party interface), and to provide practical advice on implementation.

While the European Central Bank (ECB) has set up a number of working groups to clarify certain aspects of the Directive, other initiatives have been facilitated by banking associations, and at a national level (see Annex 2 and also the Overview of PSD2-related market initiatives compiled by the Euro Banking Association).

The work of all these groups is helping to shed light on and prepare the way for the market's implementation of PSD2.

2.2 What has become clearer?

2.2.1 Guidelines requiring implementation by January 2018

There are six Guidelines relating to PSD2, all coming into force on 13th January 2018 (see Figure 1). Final Guidelines have been adopted on major incident reporting, on authorisation and registration under PSD2, and on criteria for stipulating the minimum amount of professional indemnity insurance required by TPPs.

Consultation on the Guidelines on security measures for operational and security risks, and on the Guidelines on procedures for complaints is complete, but in both cases we still await publication and adoption of their final versions, both expected in October 2017. Consultation on the Guidelines on fraud reporting will only be completed in November 2017.

Once a Guideline has been finalised and published by the EBA, member states' national authorities may either accept and incorporate the Guideline exactly as published, or they may decide to deviate from it in one or more respects. In the latter case, they must provide reasons for doing so to the EBA. They may also indicate to affected institutions a date from which they intend to audit compliance with the Guideline, which may be later than the official implementation date (albeit the Guideline will be in force from this date).

Payment Service Providers (PSPs) in all member states will therefore wish to monitor their own national authorities' statements of intention concerning the dates from which they will be auditing compliance with Guidelines directly affecting them. This is particularly the case for those Guidelines which raise direct requirements towards the PSP (as indicated with an "x" in Figure 2).

PSPs should also monitor and understand the content of, and progress on, those Guidelines which have downstream implications for their own operating models (marked with (x) in Figure 2). Given the remaining Guidelines address TPPs, with which PSPs will start to interact through the third party interface, risk management, and should therefore be monitored as well.

As previously mentioned, affected organisations in some member states will have a grace period within which to start complying with some Guidelines (albeit they will officially be in force). However, this should not be taken as a reason to delay preparing for their implementation – compliance will in most cases eventually be required, and best advice is to start preparing for the necessary changes as soon as possible. Even in the case of the Guidelines that are not yet out in final form, much is already known of their content and can be acted upon.

2.2.2 Clearer options now emerging on the third party interface

There was previously much market speculation as to what would be required to establish a compliant account interface. Following publication of the EBA's final draft RTS in February 2017, the requirements for a dedicated interface for TPPs, or direct access with additional technical requirements, have now become much clearer, and market initiatives have been working to help flesh out the details and develop common standards.

What is not yet clear is whether the Commission will oblige ASPSPs to provide TPPs direct access to their customer account interface as a contingency measure or a "fall-back" option in the event that their dedicated interface becomes unavailable or is lacking in performance, in effect endorsing a form of the current practice of "screen scraping".

If this happens, it will place an additional compliance burden on ASPSPs. The European Banking Federation (EBF) has said that mandating this upgraded form of "screen scraping" will amount to building a completely new interface. ASPSPs would have to adapt their customer interface to make it PSD-compliant, in particular to allow TPPs to identify themselves and communicate securely with ASPSPs and with each other, and to ensure that they would access only the data required by them to provide their given service. Hence the full extent and nature of affected organisations' preparations for account access is at present contingent on the Commission's decision.

2.2.3 The handling of foreign currency payments

Initially, there was discussion among payments market stakeholders concerning value dating of incoming transactions in a non-euro EU/EEA currency with subsequent currency conversion in the EU/EEA into euro.

In general, it has now become clear that the value date for the payment service user (PSU) is based on the same standards that apply to transactions under PSD1. If funds reach the payment account of the recipient ASPSP in foreign currency, the value date for the payee has to be the day on which the funds are credited to the ASPSP in the target currency.

In case of an incoming transaction in a non-EU/EEA currency with subsequent currency conversion in the EU/EEA into an EU/EEA currency, we understand that the value date should be the same as the credit note of the target currency for the ASPSP, with availability of funds as soon as possible. This includes time for currency conversion, and should be two days later at the latest (common market practice today – see Figure 3).

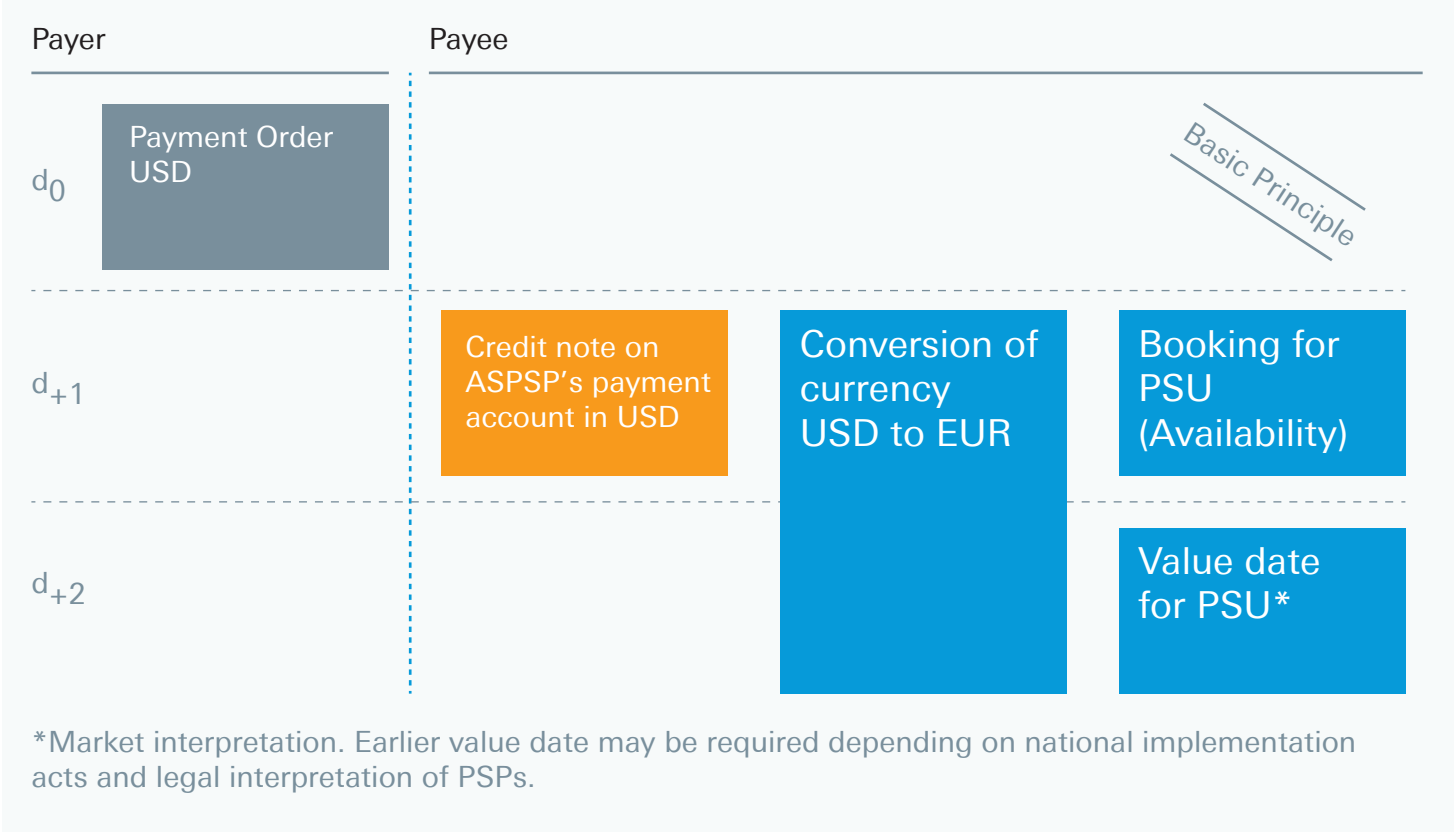


Figure 3: Handling of incoming transactions with currency conversion from non-EEA currency
Figure courtesy of PPI AG www.ppi.de

2.2.4 PSD2's impact on legal documentation provided to customers

Various provisions of PSD2 will impact on ASPSPs' contractual documentation with their PSUs. Figure 4 gives examples showing which sets of terms and conditions (TCs) may be affected by certain elements of PSD2's provisions for an ASPSP located in Germany, where transposition of PSD2 into national law has already been completed.

Provision in PSD2	Terms and Conditions (TCs) possibly impacted
Introduction of TPP services for online customers	TCs for credit transfers, TCs for online banking
Late payment: payment must be value-dated on the date it should have been received	TCs for credit transfers, TCs for direct debits
Maximum liability for consumers lowered from €150 to €50	TCs for online banking, TCs for payment cards
Unauthorised payments: repayment of the sum improperly deducted must be within one banking day	TCs for credit transfers, TCs for direct debits, TCs for payment cards
Rules pertaining to payments in non-EU/EEA currency that are within scope of PSD2	TCs for credit transfers, TCs for payment cards
Dispute resolution	General TCs of business

Figure 4: Impact of PSD2 on Terms and Conditions

2.3 What are the known unknowns?

2.3.1 Member states' transposition timelines and options

A table setting out a select number of member states' progress in implementing PSD2 appears below (Figure 5).[1]

Member state	Current status
France	Implementing regulations finalised. The Ordinance implementing PSD2 was published on 10th August 2017, and was completed by seven Decrees which were published on 2nd September 2017.
Germany	Implementing regulations finalised. Two implementing acts (one for regulatory, one for contract law aspects) have been finalised.
Italy	Implementing regulations expected/in draft. A consultation paper on PSD2 has been published.
Netherlands	Draft implementation law has been published. Adoption of national law prior to January 2018 under revision.
Poland	Implementing regulations expected/in draft. A discussion between the Polish Bankers' Association and the Ministry of Finance is currently ongoing.
Spain	The Ministry of Economy ran a public consultation process with all relevant stakeholders before drafting the law; the consultation ended on 5th May 2017. Transposition date has yet to be announced.
UK	Implementing regulations finalised. Final form Payment Services Regulations 2017 were published on 19th July 2017.

Figure 5: Progress in transposition of PSD2 into selected countries' national law

This shows that the Directive's implementation may get off to an uneven start across member states. However, what is clear is that where PSD2 has been transposed into national law, transposition has been effected fairly consistently. There is also a pattern showing that where a member state exercised an option under PSD2's predecessor, PSD1, it is likely to exercise the same option under PSD2 (See Annex 4 for member state options).

[1]More comprehensive information is available on this in the form of the Euro Banking Association's Overview of PSD2 national transposition projects which covers all member states.

2.3.2. Delays in transposition

In case transposition into national law is delayed, we suggest that – given most provisions in PSD2 favour PSUs – ASPSPs should finalise their IT projects and deploy the PSD2 related changes, as planned, prior to 13th January 2018. The same applies to required changes as outlined in the Guidelines. Changes to legal client documentation, however, can only be conducted once the transposition has been completed. A more detailed review is suggested with regards to changes to processes. Those that are specific to PSD2 and third party access (see Section 3.2.4) may be implemented once PSD2 is transposed.

2.3.3 Implementation gap between PSD2 and the RTS on Strong Customer Authentication and Common and Secure Communication

While PSD2's overall implementation date is 13th January 2018, the highly important RTS for SCA and Common and Secure Communication (CSC) still await adoption, and – since they have an 18-month implementation period – will only come into force in the first half of 2019 at the earliest.

Bearing in mind this long implementation period, ASPSPs might be tempted to delay compliance with their third party interface and SCA obligations until late in 2018 or early 2019. However, this would be a mistake, as a number of highly significant provisions in PSD2 that are either dependent on or closely bound up with those aspects of implementation are already effective from 13th January 2018, and compliance with these will be required from that date. Hence industry bodies have noted that the effective dates of PSD2 itself, and the RTS on SCA and CSC, are not merely out of step, but that there is a genuine – and problematic – implementation gap.

There are three areas in particular (which we deal with in detail in Section 3.2.4) in which the market will have to contend with practical issues in the period from 13th January 2018 to implementation of the RTS on SCA and CSC. This will affect ASPSPs, PSUs and TPPs, but ASPSPs in particular will have to decide what steps to take to mitigate a number of new risks to which they will be exposed.

The only way to obviate these difficulties is to start implementing the third party interface and strong customer authentication as soon as is possible. There are few reasons justifying delay, but many and powerful incentives for ASPSPs to ensure they are PSD2-ready as soon as they can be. To be clear, this does not mean that changes should be carried out in a member state where transposition has not yet occurred.

2.3.4 Need for agreement of common standards under the RTS on Strong Customer Authentication and Common and Secure Open Standards of Communication

These RTS provide a framework for implementation, and outline the principles in accordance with which ASPSPs must develop interfaces that will allow third parties access to accounts, as well as outlining that all PSPs must introduce SCA for electronic payments and remote account access.

These have to be translated into technical specifications by the industry, and market participants have started working on the necessary specifications in the form of common standards and protocols. We set out in Annex 2 the range of initiatives focussing on finding common standards for the third party interface, for two-factor authentication and for registry services.

2.3.5 Content of some Guidelines

The content of the Guidelines on complaints procedures, fraud reporting and security measures has yet to be finalised (refer to Figure 1). However, it would not be wise to refrain entirely from planning and preparing their implementation. The content of all the Guidelines is known in draft and has been canvassed in public consultation with industry stakeholders, so that market participants are aware of the framework of requirements, if not the precise final detail, and can already take some steps towards implementation.

2.3.6 Interaction of PSD2 with the General Data Protection Regulation

About four months after PSD2 enters into force, on 25th May 2018, the new General Data Protection Regulations (EU) 2016/679 (GDPR) will come in. The intention behind both the Directive and the Regulations is to strengthen data protection, putting the data owner at the centre and requiring his consent to capture, store or process any data. However, there is initially likely to be an imperfect fit. The main pain points concerning the interaction of GDPR and PSD2 of which ASPSPs should be aware are:

- the different types of consent required from the natural person respectively the PSU under each piece of legislation,
- whether ASPSPs are responsible for checking that TPPs have the consent required under the GDPR to process the data to which ASPSPs are giving them access,
- what happens when TPPs change or expand the way they use that data,
- who is liable for data breaches,
- what constitutes sensitive payment data under PSD2, and
- compliance in the transitionary period between implementation of PSD2, and the RTS on SCA and CSC, if “screen scraping” continues to be permitted.

3 Content updates and specifications

While the market expected the RTS on SCA and CSC to require major change, the level of detailed work that will be required to comply with the Guidelines on major incident reporting, and on security measures for operational and security risks, may come as a surprise to many.

3.1 Details on reporting and risk management

3.1.1 Guidelines on the security measures for operational and security risks of payment services

These draft Guidelines set out the requirements that PSPs should implement in order to mitigate operational and security risks derived from the provision of payment services. The Guidelines will replace the previous Guidelines on the Security of Internet Payments (EBA/GL/2014/12 – SecurePay). However, whereas SecurePay only covers internet-based payments, they apply to all payments. Many requirements set out in the draft Guidelines are generally already known to PSPs from SecurePay. However, the Guidelines are considerably more comprehensive and more detailed. This applies to the following areas:

- governance,
- risk assessment,
- risk control and mitigation,
- incident monitoring and reporting,
- protection of sensitive payment data,
- the testing of security measures,
- outsourcing, and
- customer awareness, education and communication.

Other requirements are completely new, such as those for:

- business continuity management as well as scenario-based continuity plans
- situational awareness and continuous learning in regard to a PSP's own personnel, its partners and external stakeholders

The final version of the Guidelines is expected in Q4 2017.

3.1.2 Guidelines on major incident reporting

While PSPs already had information requirements under PSD1 and needed to monitor and report incidents under SecurePay, they may find that the requirements under PSD2, as set out by these Guidelines, introduce thresholds for incidents that must be reported, and make reporting requirements more comprehensive.

PSPs only need to focus on Guidelines 1 to 4 (Guidelines 5 to 8 address member states' competent authorities). These set out what is classified as a major incident, the notification process, delegated and consolidated reporting and PSPs' operational and security policies (see Figure 6).

Figure 6: Content of the Guidelines on major incident reporting under PSD2
Figure courtesy of PPI AG www.ppi.de

Compared to SecurePay, there will be four significant changes (see Figure 7). The first is, as mentioned earlier, the new Guidelines' scope. They apply to all payments, not just to internet payments. Secondly, they give specific deadlines within which PSPs must report: they must make an initial report within four hours after a major incident is detected, an interim report within three working days, and the final report within two weeks after the incident is resolved.

Thirdly, the new Guidelines set out a methodology which PSPs must follow to clearly distinguish between incidents. This is based on defined parameters and threshold values, and allows PSPs to determine which incidents require reporting. They may find that the threshold has been lowered, meaning they must report incidents they previously would not have been required to report. The Guidelines also provide a template that PSPs must use to collect all the relevant information and produce an incident report. Finally, for the first time these Guidelines impose on PSPs a reporting obligation to their PSUs.

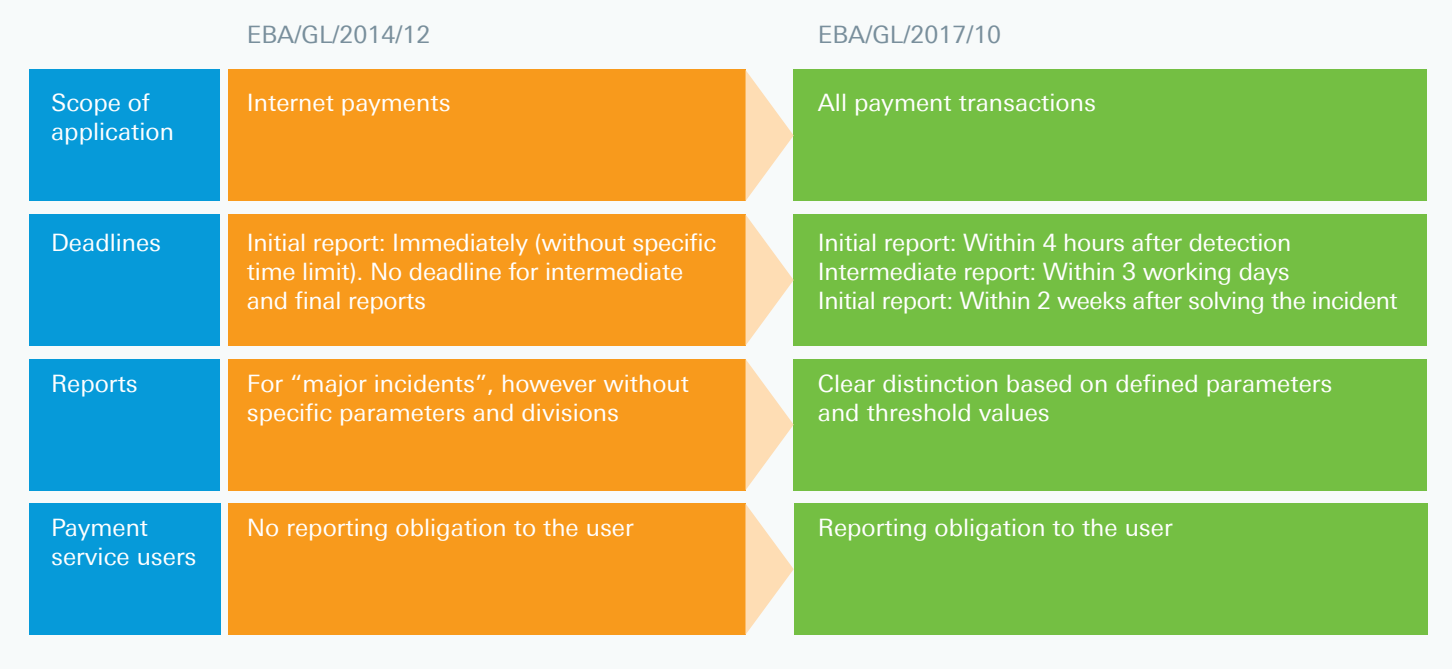


Figure 7: Significant changes in comparison to SecurePay
Figure courtesy of PPI AG www.ppi.de

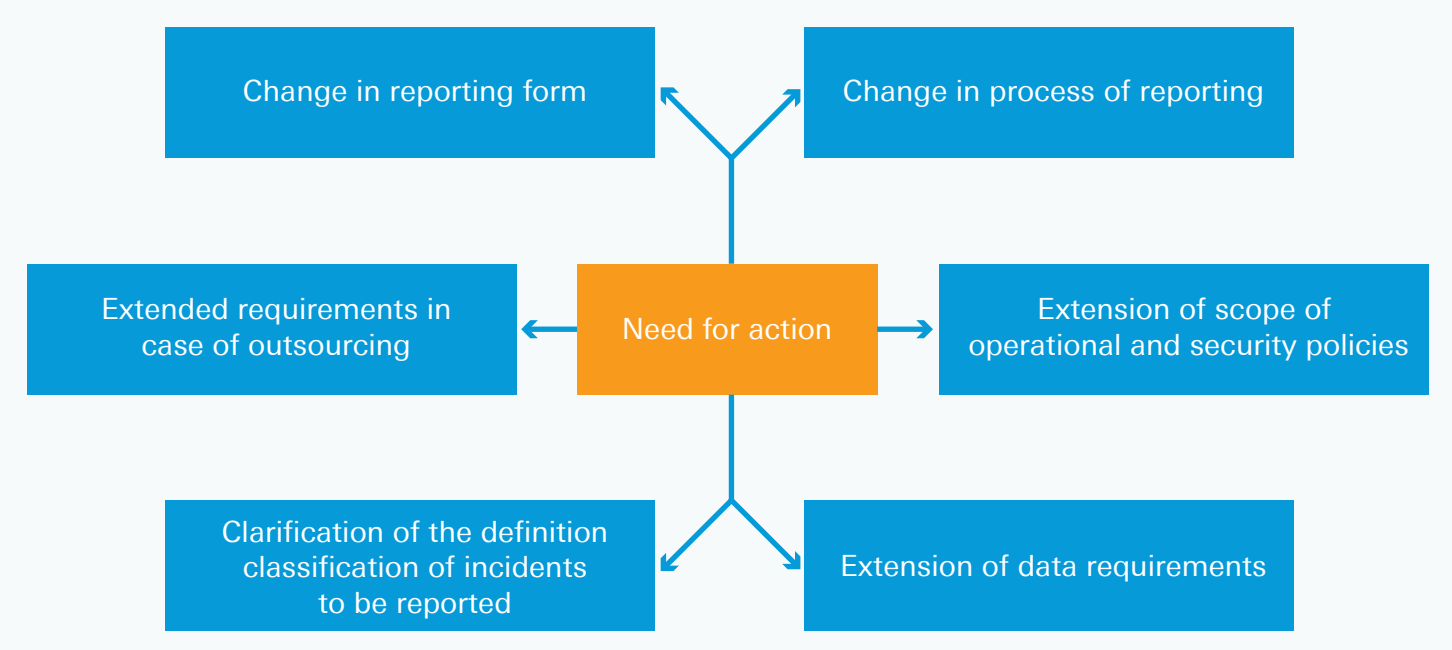


Figure 8: Where is action required?
Figure courtesy of PPI AG www.ppi.de

3.1.3 Guidelines on fraud reporting

The Guidelines on fraud reporting under PSD2 have been developed in close cooperation with the ECB with the aim of ensuring that comparable and reliable data on fraud are gathered in all member states.

As they have not yet been finalised, organisations with an excellent record of no or only minimal incidence of fraud may be tempted to put off preparing to implement these Guidelines. However, they cannot afford to do so. The Guidelines will require organisations to have in place solid and detailed reporting structures on all payment transactions, and not just on fraudulent ones, so depending on organisations' current systems and processes, compliance may require substantial upgrade work to put in place adequately detailed reporting structures.

3.2 Details of account interface and Strong Customer Authentication

In accordance with Article 98 of PSD2, the EBA has now developed, in close cooperation with the ECB, draft RTS specifying the requirements of SCA, the exemptions from the application of SCA, the requirements with which security measures have to comply in order to protect the confidentiality and the integrity of PSUs' personalised security credentials and, perhaps most significantly, the requirements for CSC between ASPSPs, PISPs, Account Information Service Providers (AISPs), payers, payees and other PSPs.

3.2.1 Timeline to implementation

In consequence of extensive public consultation and specifically the European Commission's intervention, the final text of these RTS has not yet been adopted, and will probably only be effective from Q1/Q2 of 2019 – out of step with the rest of the Directive which comes into force on 13th January 2018.

3.2.2 Secure communication for TPPs

The draft final RTS, published by the EBA on 23rd February 2017, stipulate that ASPSPs offering payers payment accounts that are accessible online must have at least one interface in place that meets the following three requirements:

- It allows AISPs, PISPS, and PSPs to identify themselves to the ASPSP,
- It allows AISPs to communicate securely, and request and receive information on one or more designated payment accounts and associated payment transactions,
- It allows PISPs to communicate securely, initiate a payment order from the payer's payment account and receive information on the initiation and execution of payment transactions.

Interface options: Dedicated interface vs direct access

ASPSPs can establish an interface either by means of a dedicated interface, or by allowing PISPs and AISPs direct access ("screen scraping").[2]

A dedicated interface involves ASPSPs providing TPPs access to their customers' accounts via a route specifically built for them. In practice, much of the industry is preparing to provide this by using open Application Programming Interfaces (APIs). Alternatively, direct access may be given by ASPSPs simply enhancing their webpage to show only the PSD2-compliant parts and offering TPPs access to these.

The API option has many advantages. Open APIs, which allow the products and services of one company to be interconnected with those of others, are an important step forward in service provision, and can help generate innovatory services benefitting customers, as well as the businesses involved. For this reason, industry participants would do well to utilise and exploit Open APIs as soon as they can.

In particular, investing in APIs based on common standards has its advantages – both over direct access and over proprietary APIs. These interfaces will be more cost-effective for ASPSPs to implement. Given that the EU has encouraged the development of common standards (see Annex 2), gaining compliance confirmation may be easier when going down this road. Finally, this course will likely encourage faster take-up by TPPs – it makes business sense for them to adapt to using standardised APIs, with a wider reach than either direct access or a proprietary interface.

There can be further advantages of using APIs. ASPSPs could use them as a basis for shared services and cost savings. For example, ASPSPs could spread the cost of testing facilities; of the interface documentation required by PSD2; of a helpline, or of repository or registry services, as provided by PRETA (see Annex 2).

If direct access in the form of "screen scraping" is to be made PSD2-compliant, it will of course also require TPPs to be able to identify themselves, and ASPSPs will have to be able to ensure that only PSD2-compliant content, and no other, is being shared with TPPs. Making this route successful will therefore clearly also require considerable adaptation work to any pre-existing customer-facing interface – yet it will not bring the added benefits offered by APIs.

Make or Buy?

As a second step, ASPSPs will need to consider whether to start their own API development programme (possibly in collaboration with others) or engage a provider to supply their needs.

This choice will depend entirely on the individual ASPSP's service offering, market sector, long-term strategy and resources.

In Annex 1, we list some providers that can offer support in this area. Readers should, however, be aware that this is a highly dynamic market and new providers may have entered the market since this white paper went to press.

[2]NB. PIISP services will need to be added via a dedicated interface – they are not possible via direct access.

Required fall-back

The European Commission is currently considering whether to overrule the recommendations of the EBA and oblige ASPSPs to offer TPPs access to the information they need by using the ASPSP's customer interface as a "fall-back" option. The rationale for mandating this is two-fold: it is to be made available if the dedicated interface is not available; and also if that interface should be lacking in functional services. (The ECB is currently trying to clarify to the market what services the dedicated interface should be supplying to TPPs.)

What the Commission may require as a fall-back option appears to amount to what an alliance of European fin-tech companies had previously called "secure authenticated direct access", arguing that it was an established, safe option that could be made PSD2-compliant, and would level the playing field between ASPSPs and TPPs.

The EBA had on the other hand made clear that it intended to ban the practice of "screen scraping" within the scope of PSD2's operation. It suggested that monitoring and publication of defined key performance indicators and service level targets for availability and performance of the dedicated interface – and making that interface available for testing three months ahead of its going live – would offer TPPs sufficient safeguards. The EBF and the European Consumer Organisation BEUC have also both objected to the continued practice of "screen scraping" once PSD2 comes into force.

We await the Commission's decision. Any RTS it adopts must then be approved by the European Parliament and the European Council, which are each entitled to reject them. However, the expectation currently is that the RTS will probably be adopted in Q4 of 2017, and come into application 18 months later, so probably in the first half of 2019.

If, as is possible, the Commission insists that ASPSPs offer TPPs the upgraded direct access fall-back option, ASPSPs will face the costs and burden of adapting their customer interface for PSD2-compliant access by TPPs, potentially in addition to those of their API development programme.

3.2.3 Strong Customer Authentication

As an integral component of opening up the payments market to TPPs through open common and secure communication provided by the third party interface, PSD2 also seeks to strengthen security in payments and of customers' personalised credentials by mandating SCA. This is to be provided (subject to certain exemptions) in every case where PSUs access payment accounts online, initiate electronic payment transactions or carry out any other action through a remote channel that may carry a risk of payment fraud or other abuses.

Requirements for SCA

PSPs must implement security measures enabling them to apply SCA, protect PSUs' security credentials; and establish common and secure open standards of communication, and these must be documented, periodically tested, evaluated and audited in accordance with the PSP's audit framework.

The RTS sets out the requirements for SCA. Where a PSP applies SCA, authentication is based on two or more elements categorized as knowledge, possession and inherence. This results in the generation of an authentication code which is accepted once only. Authentication must also be dynamically linked to the amount of the transaction and the payee.

PSPs must adopt measures mitigating the risks of the various elements of SCA being uncovered by an unauthorised party. These elements must also be independent of each other, and PSPs must adopt measures in terms of technology, algorithms and parameters, to ensure the breach of one of the elements does not compromise the reliability of the others.

PSPs must also ensure confidentiality and integrity of the PSUs' personalised security credentials, ensure that they are created in a secure environment, that they are associated only with that particular PSU, and that their delivery, and that of authentication devices and software, to the PSU is carried out in a secure manner designed to address the inherent risks.

PSPs can find support and suppliers of the necessary hard- and software and expertise to implement Two-Factor Authentication (2FA). Annex 1 contains a list of such suppliers.

Exemptions

There are a number of circumstances in which payments or account access are exempt from the requirement for SCA, primarily in the context of internet purchases and "one-click" payment experiences. While similar exemptions are available for online banking offerings, it remains questionable whether they add to the user experience or just raise the complexity of the offering.

3.2.4 Effective provisions from 13th January 2018

It is essential for PSPs to bear in mind that certain provisions in PSD2 relating to the TPP interface become effective on 13th January 2018[1], whether or not the interface is live. ASPSPs in particular will have to decide how they plan to mitigate the new risks to which this will expose them.

One such area is liability for errors in payments involving a TPP: from 13th January, the risk profile for ASPSPs of payments involving a TPP will entirely change. Currently, if a transaction initiated by a TPP was made in error, and for example the PSU says he did not give the relevant instruction to change it, the PSU must recover any loss from the TPP. From 13th January 2018, however, ASPSPs will be obliged to reimburse PSUs in the first instance, and subsequently recover the loss from the TPP.

An ASPSP using One-Factor Authentication (1FA)/2FA for payment authorisation without a dynamic element may have no means of showing who changed the transaction. One clear solution to this difficulty would be to fast-track and put in place 2FA with a dynamic element – which will be required in any event from implementation of the RTS on SCA and CSC. With this in place, it will be clear who changed the transaction.

[1]In countries where the transposition is delayed, 13th January 2018 should be viewed as a placeholder for the respective national effective date.

A second, similar but distinct, area is that of cancelled payments. Currently, PSUs can ask their ASPSPs to cancel a payment initiated by a TPP, but from 13th January 2018 ASPSPs will no longer be permitted to cancel payments involving a TPP. If an ASPSP does not yet have a dedicated interface for TPPs, it will not be able to tell whether a transaction was initiated by a TPP or not. One solution would be for the ASPSP's terms and conditions of acting for its PSU to state that PSUs are not entitled to cancel such transactions. Better still, however, to have the interface in place.

In this connection PSPs should note that there is as yet no dispute resolution procedure in place to settle disputes arising between ASPSPs and TPPs. The ECB has noted this gap and the European Payments Council (EPC) ad-hoc task force on access to payment accounts is addressing it.

4 Market offerings supporting implementation

In the time that has passed since publication of Deutsche Bank's first white paper, there has been time for sources of help and support for ASPSPs' implementation efforts to increase. These range from consulting firms to providers of key elements of infrastructure, software and services that ASPSPs will have to put in place to comply with PSD2.

4.1 Types of support available

A list of providers can be found in Annex 1. They fall roughly into three categories: consulting firms, interface providers, and strong authentication providers.

4.1.1 Consulting firms

Consulting firms may help PSPs plan or update their PSD2 implementation project, clarify the steps they need to take, which business lines and departments they need to involve, and what types of partner they may need to engage.

4.1.2 Interface providers

A range of services may be on offer, from providing and managing the entire third party interface for an ASPSP to plugging gaps by supplying specific applications, software or services.

For those wishing to go beyond compliance and to take advantage of the new opportunities offered by open APIs, additional analytics may be a help to cross-selling or offering new services.

4.1.3 Strong Customer Authentication providers

These will provide two- or multi-factor authentication, offer a wide range of potential authenticators, security applications, and help with authentication management including risk management and compliance documentation.

4.2 How to find the right fit in partner

While the chief consideration must always remain whether the potential partner has the right expertise and track-record to provide the specific products and services required, other factors may weigh in the balance when making a choice between equally competent candidates.

For long-term collaborations in particular, potential partners' corporate culture, management style and values should be considered, as well as which market sectors and client bases they service. Particular synergies may have the potential to open up new business opportunities.

5 Roadmap for a PSD2 project

5.1: Reviewing your PSD2 project

5.1.1 A unitary approach

ASPSPs will already be aware that implementing PSD2 is a significant project for them, requiring buy-in from across their entire organisation, not merely from Compliance, but at the very least also from Legal, Product Management and IT, for all business sections.

In addition, it is of paramount importance to ensure at the project's outset, and to keep under review throughout, that the project as a whole is based on a clear and consistent understanding and interpretation of PSD2, and that this remains common to, and understood by, all business sections and departments, as well as by participating partners and collaborators. This is crucial to ensure it remains on course as a whole, and rolls out successfully in each of its detailed manifestations.

5.1.2 Timing and resources

Furthermore, relevant resources are likely to become increasingly stretched as the implementation date approaches. This applies to both internal and external resources, as every PSP across Europe dedicates increasing amounts of time, attention, and expertise to implementing PSD2. This is especially the case with respect to the additional implementation requirements outlined by the Guidelines, which introduce a wide set of new stakeholders to the project.

Being ahead of the game is even more important under these circumstances, especially as not all the relevant detail is yet known. Having preparations in place for each step will ensure that implementation is on track and able to cope with new information delivered at short notice further down the line.

5.2 Roadmap: Two milestones to success

There are two major milestones in terms of complying with PSD2. The first is to ensure compliance with the bulk of PSD2, and as far as is possible with all its Guidelines, by 13th January 2018. This first milestone will involve for example changes to business terms & conditions and possibly some client procedures. At this early stage, organisations will be concentrating on understanding and implementing the legal and regulatory changes that will be required, with Legal and Compliance taking the lead, but involving Product Management. The IT side of preparation is likely to focus on core payment processing.

Once Milestone One has been attained, there may be a significant change both in the composition of the implementation project team and in governance representation, as the second, far more technical and IT- and process-related phase of implementation begins: putting in place the third party interface and secure customer authentication.

As we have said, Milestone Two will have a deadline of 18 months after the adoption of the RTS on SCA and CSC. However, here especially, best advice is not to wait for that time to run, but aim to become compliant with the RTS on SCA and CSC as early as possible, and well ahead of the deadline. No organisation should wait until the final version of the

RTS is adopted, let alone comes into force, to start preparations. Implementing early will avoid most of the issues raised by the implementation gap (see Section 2.3.4), allow difficulties to be resolved before they become compliance or operationally critical, benefit customers, and generally take the pressure off the organisation. Most importantly of all, it stops organisations being narrowly compliance-driven and frees them up to focus on new business opportunities that may arise in the wake of PSD2.

5.3: Beyond PSD2

5.3.1 Outlook for the European payments market

PSD2 is not the only regulatory change to affect payments in the near future. Besides bringing EU financial services regulation up to speed with technological change and increasingly sophisticated customer demand, these changes aim to further integrate the European payments market, wherever possible consolidating services onto central platforms, and continuing to harmonise technical standards, communication protocols and messaging formats.

We have already mentioned the GDPR, which comes into force in May 2018, affecting all data captured, stored and processed in the course of making payments and offering other payment-related services. Add to this the advent of SEPA 2.0, bringing an important update of the original SEPA regulations to the market.

Furthermore, as part of the Eurosystem's "Vision 2020" plans, the ECB is also currently investigating further enhancements to TARGET 2, its automated real-time gross settlement system. This is is planned to be consolidated with T2S, the Eurosystem's platform enabling core pan-European securities settlement services. This sits well with the migration from existing SWIFT Fin MT messaging formats to ISO 20022/XML formats which will bring significant changes to the entire European banking industry.

In addition, the ECB and those involved in the European payments system are strongly pushing for the introduction of instant payments in Europe via TARGET Instant Payment Settlement (TIPS), and through RT1, EBA Clearing's instant payment scheme for processing pan-European credit transfers. This will dramatically increase the speed at which electronic retail payments are made and received in Euro in the EU, putting it on par in this respect with payments made in the UK and Singapore. The payee's account will be credited, and confirmation sent to the payer, within seconds of the payment initiation.

Looking at the broader picture, we consider there are three major consequences of PSD2's introduction. The first is a regulatory one. The introduction of PSD1 formed the legal basis for the SEPA which transformed the European payments market, introducing the SEPA credit transfer and the SEPA direct debit as payment instruments to the market. PSD2 could be regarded as the legal basis for a new single European payments area, extending the regulatory remit of SEPA credit and SEPA direct debit transfers to all payments effected by parties located in the EU/EEA area in all currencies, not just in Euro or the currency of another member state.

The second change is the market opening up in ways that both constrain and offer new opportunities to all its participants. New players are joining the market, adding new

types of service to payments that clearly add value for PSUs, but they will henceforth be constrained by regulation. To enable them to participate in the first place, existing ASPSPs are being obliged to allow them access to their customer account interface. However, this means that ASPSPs also have the opportunity of gaining a slice of this new market by registering and acting as AISPs and PISPs themselves.

Finally, we believe that all these market and regulatory changes will work together to offer PSUs faster, safer and more convenient payments, together with access to aggregated account and other financial information. However, we believe that the momentum we now see in payments will carry over into other banking services. We predict this is just the first step in a broader sweep of API-fication which will exploit this technology to offer a range of services to bank customers, from for example accessing their stock portfolios to monitoring their online securities transactions or managing their borrowings, and doubtless all these new services will also be duly regulated.

5.3.2 Making the new ecosystem work for you

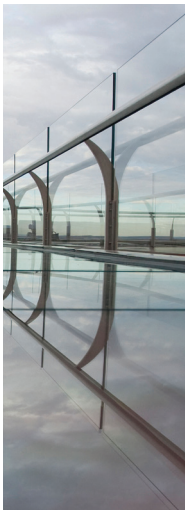
Europe has flourished under the first payments revolution which brought convenient, fast and safe digital payments to millions of PSUs in member states. Now the second revolution in payments and potentially in wider banking services is about to begin. Against a background of pan-European standardisation and an emerging open payments market, the winners are likely to be those exploiting APIs to leverage their existing assets, and possibly collaborating with new partners, to create innovative and convenient new products and services

6 Conclusion

All PSPs, and ASPSPs in particular, should regard the implementation deadline of 13th January 2018 for PSD2 as a wake-up call not just to get PSD-ready – which this white paper and our client advisors can help organisations do – but to take a leap forward towards getting API- and Open Banking-ready as well. PSD2 is a project requiring significant investment from organisations, but in the long term may prove the first step towards new ways of doing business and provide the seedbed for new revenue, business, and partnership models.

Annex 1: List of providers

1 Access to Accounts/ Interface Providers



	Provider	Webpage
1.	accourate	www.accourate.io
2.	Axway	www.axway.com/de
3.	BANKSapi	https://banksapi.de
4.	DSER	www.dser.de
5.	Equens Worldline	http://de.worldline.com
6.	Figo	www.figo.io
7.	finAPI	www.finapi.io
8.	Kontomatik	www.kontomatik.com
9.	NDigit	http://nextdigitalbanking.com
10.	Omikron	www.omikron.de
11.	ppi	www.ppi.com
12.	RedHat	www.redhat.com/de
13.	SIA	www.sia.eu
14.	Starfinanz	www.starfinanz.de
15.	Vipera	www.vipera.com

2 Strong Customer Authentication providers

	Provider	Webpage
1.	AUTHADA	https://authada.de/de
2.	CensorNet	https://www.censornet.com/de/
3.	Centrify	https://www.centrify.com/de/
4.	CREALOGIX	https://www.crealogix.com/de/de/
5.	Cronto	https://www.cronto.com/
6.	Duo Security	https://de.duo.com/
7.	Gemalto	https://www.gamalto.com/deutschland
8.	HID	https://www.hidglobal.de/identity-management
9.	Infineon	https://www.infineon.com/cms/de/applications
10.	Infinigate Distributor	https://www.infinigate.de/
11.	Kobil Systems	https://www.kobil.com/de/
12.	RSA	https://www.rsa.com/de-de
13.	Seal One	https://www.seal-one.com/index.de
14.	Signicat	https://www.signicat.com
15.	SolidPass	https://www.solidpass.com/
16.	Vasco	https://www.vasco.com/de-de/

Annex 2: Overview of market initiatives

The following initiatives offer support to PSPs in implementing PSD2 by way of networks, pooled knowledge and common standards.

Initiatives drafting specifications and building consensus for compliance

The 'Berlin Group' is a pan-European payments interoperability standards and harmonisation initiative, developing an implementation specification for an interface covering application, security and transport levels and an organisational framework for its future maintenance.

PRETA, a subsidiary of EBA CLEARING, is heading up an initiative geared towards helping banks comply with PSD2 and intends to provide a common, reliable, up-to-date directory to the market with shared information on ASPSPs and TPPs.

The multi-stakeholder coalition CAPS initiative is working towards a common framework to support PSD2-compliance by both ASPSPs and TPPs, addressing the technical interface, but also aiming to make PDS2 work in practice on a pan-European level, covering broader operational services such as directories, fraud management and dispute resolution. It supports new business models for both ASPSPs and TPPs.

FIDO Alliance's uses technology based on public key cryptography and aims to develop technical specifications defining an open, scalable, interoperable set of mechanisms to deliver secure customer authentication, facilitate world-wide adoption and submit mature technical specifications to recognized standards development organizations.

„Security of TPP architectures" is a working group of ISO/TC 68, a technical committee formed by the International Standards Organisation ISO.

Initiatives set up by the European Central Bank

The Euro Retail Payments Board (ERPB) has set up a working group with the participation of other relevant stakeholders to identify conditions for the development of an integrated, innovative and competitive market for payment initiation services (PIS) in the EU.

The European Payments Council has set up a "mirror working group" to this one.

Banking Association Initiatives

The PSD2 Practitioners' Panel's (hosted by the Euro Banking Association) aims to accompany the PSD2 implementation process and foster exchange on practical implementation issues among ASPSPs at a pan-European level, to provide explanations on open issues around key areas of impact of PSD2 for ASPSPs, support a pan-European perspective and avoid market fragmentation

The Open Forum on Open Banking facilitated by the Euro Banking Association addresses all interested market participants and covers Open Banking and PSD2 topics, and specifically preconditions and requirements of access to accounts for TPPs.

The Open Transaction Alliance, facilitated by Innopay, is a cross-industry group of banks, payment service providers, account information providers, payments processors, merchant groups, and other relevant stakeholders seeking to define a set of principles covering essential elements of PSD2 payment initiation and account information, to ensure effective and secure implementation on a pan-European scale.

National Initiatives

The Deutsche Kreditwirtschaft (DK)/German Banking Industry Committee (GBIC) is a national initiative also working with Austrian STUZZA and Swiss SIX. It favours uniform interoperable communication between third-party service providers and banks in Europe, requiring a common interface standard, and has published a white paper on the requirements for such an interface.

The PSD2 Advisory Group (facilitated by Payments UK) is a national group supporting the work of the UK Competition and Markets Authority Implementation Entity to deliver Open Banking. It wishes to align the scope of Open Banking with that of PSD2 wherever possible.

STET is a French API standard which will allow TPPs to access payment accounts.

Annex 3: Sources of information on PSD2

The European Banking Authority

The Euro Banking Association

The European Banking Federation

The European Commission

The European Central Bank

The Euro Retail Payments Board

PSD1 – The Payment Services Directive 2007/64/EC

PSD2 – The Revised Payment Services Directive (EU) 2015/2366

Draft Implementing Technical Standards on the details and structure of the information entered by competent authorities in their public registers and notified to the EBA

Draft Regulatory Technical Standards on the criteria for determining central contact points under PSD2

Draft Regulatory Technical Standards on the framework for cooperation and exchange of information between competent authorities for passport notifications under PSD2

Draft Regulatory Technical Standards setting technical requirements on development, operation and maintenance of the electronic central register

Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2):

European Banking Authority's Final Report 23rd February 2017

European Commission's Letter to the European Banking Authority dated 24th May 2017

Opinion of the European Banking Authority 29 June 2017ssociation

Draft Regulatory Technical Standards delivered with that Opinion

Guidelines on authorisation and registration under PSD2

Guidelines on the criteria on how to stipulate the minimum monetary amount of the professional indemnity insurance under PSD2

Guidelines on fraud reporting under PSD2

Guidelines on major incidents reporting under the PSD2

Guidelines on procedures for complaints of alleged infringements of the PSD2

Guidelines on security measures for operational and security risks under the PSD2

The Berlin Group

The CAPS Initiative

Deutsche Kreditwirtschaft/German Banking Industry Committee (GBIC)

The Euro Retail Payments Board

FIDO Alliance

Open Forum on Open Banking

Open Transaction Alliance

PRETA

PSD2 Advisory Group

PSD2 Practitioners' Panel

„Security of TPP architectures" working group of ISO/TC 68

Further information on this topic from Deutsche Bank

"Making the most of PSD2", Deutsche Bank with Finextra, video (July 2017)

"PSD2 sparks innovation in open banking systems", Deutsche Bank with Innopay, article (June 2017)

"PSD2, an "open, digital payments market in Europe", Deutsche Bank's Shahrokh Moinian, Global Head of Cash Management Corporates, writing in the Trade and Forfaiting Review: (TFR, January 2017)

"PSD2 will transform the payments landscape" Deutsche Bank with Finextra, video (December 2016)

"Payment Services Directive 2: Directive on Payment Services in the Internal Market "(EU) 2015/2366", white paper by Deutsche Bank (September 2016)

Annex 4: Member state options

This section sets out the options granted to member states when transposing PSD2 into national law. Decided at local level, the following table lists all member state options, citing the relevant articles (of both PSD1 and PSD2) and summarising their content.

PSD1	PSD2	
Article reference		Description
2 (3)	2 (5)	MS may exempt institutions referred to in points (4) to (23) of Article 2(5) of Directive 2013/36/EU from the application of all or part of the provisions of this Directive => a special purpose institutions Extract of DIRECTIVE 2013/36/EU Art. 2.5 No. 2-23: (4) in Belgium, the Institut de Réescompte et de Garantie/ Herdiscontering-en Waarborginstituut; (6) in Germany, the Kreditanstalt für Wiederaufbau, undertakings which are recognised under the Wohnungsgemeinnützigkeitsgesetz as bodies of State housing policy and are not mainly engaged in banking transactions, and undertakings recognised under that law as non-profit housing undertakings; (10) in Spain, the Instituto de Crédito Oficial; (11) in France, the Caisse des dépôts et consignations ; (12) in Italy, the Cassa depositi e prestiti; (16) in the Netherlands, the Nederlandse Investeringsbank voor Ontwikkelingslanden NV, the NV Noordelijke Ontwikkelingsmaatschappij, the NV Industriebank Limburgs Instituut voor Ontwikkeling en Financiering and the Overijsselse Ontwikkelingsmaatschappij NV; (17) in Austria, undertakings recognised as housing associations in the public interest and the Österreichische Kontrollbank AG;

2 Title II – Member state options

PSD1	PSD2	
Article reference		Description
7 (3)	8 (3)	Derogation for MS not to apply the calculation of own funds (Art. 9) to PIs which are included in the consolidated supervision of the parent credit institution.
9 (2) and (3) and (4)	CANCELLED	Calculation of safeguarding requirements when funds can be used for future payment transactions and for non–payment services. Application of safeguarding requirements to genuine (non hybrid activities) PIs. Threshold of EUR 600 for applying safeguarding requirement.
8 (1 Method A)	9 (1 Method A)	Competent authorities may adjust the own fund requirement in the event of a material change in a PI's business since the preceding year.
8 (3)	9 (3)	The competent authorities may, based on an evaluation of the risk management processes, risk loss data base and internal control mechanisms of the PI, require the PI to hold an amount of own funds which is up to 20% higher than the amount which would result from the application of the method chosen in accordance with paragraph 1, or permit the payment institution to hold an amount of own funds which is up to 20% lower than the amount which would result from the application of the method chosen in accordance with § 1.
22 (3)	24 (3)	MS may apply this Article taking into account, mutatis mutandis, Article 53 to 61 of Directive 2013/36/EU. à Professional secrecy.
	29 (2) NEW	The competent authorities of the host MS may require that PI having agents or branches within their territories shall report to them periodically on the activities carried out in their territories.
	29 (4) NEW	MS may require PI that operate on their territory through agents under the right of establishment and the head office of which is situated in another MS, to appoint a central contact point in their territory to ensure adequate communication and information reporting on compliance with Titles III and IV...
26 (1)	32 (1)	MS may exempt or allow their competent authorities to exempt from the application of all or part of the procedure and conditions set out in Sections 1 to 3, with the exception of Articles 14,15,22,24,25 and 26, natural or legal persons providing payment services listed in points 1 to 6 of Annex I,…
26 (4)	32 (4)	MS may also provide that any natural or legal person registered in accordance with paragraph 1 of this Article may engage only in certain activities listed in Article 18.

3 Title III – Member state options

PSD1	PSD2	
Article reference		Description
30 (2)	2 (5)	Extension of the scope, as microenterprises should be considered equally to consumers
33 (optional)	Manda-tory	PSP has to prove that its compiling with the defined information requirement
34 (1) & (2)	42 (2)	Frame for derogation from information requirements: – Reduction or increase of transaction amount or spending limits – Increase to EUR 500 specifically for prepaid payments
45 (6)	55 (6)	Opportunity to provide more favourable conditions (charges & duration) for PSUs, in regard to the termination of framework contracts
47 (3) 48 (3)	57 (3) 58 (3)	Information on individual payment transactions should be provided to payers and payees, free of charge, on paper or on another durable medium at least ones a months

4 Title IV – Member state options

PSD1	PSD2	
Article reference		Description
51 (2) and (3)	Article 61 (2) and (3)	MS may provide that Article 102 [ADR procedures] does not apply where the PSU is not a consumer. MS may provide that provisions in this Title [i.e. Title IV] are applied to micro enterprises in the same way as to consumers.
52 (3)	Article 62 (5)	MS may prohibit or limit the right of the payee to request charges taking into account the need to encourage competition and promote the use of efficient payment instruments.
53 (2) and (3)	Article 63 (2) and (3)	For national payment transactions, MS or their competent authorities may reduce or double the amounts referred to in par. I. They may increase them for prepaid payment instruments up to EUR 500. Ms may limit that derogation to payment accounts on which the electronic money is stored or payment instruments of a certain value.
61 (3)	Article 74 (1b)	Where the payer has neither acted fraudulently nor with intent failed to fulfil its obligations under Article 69, MS may reduce the liability referred to in the first subparagraph, taking into account, in particular, the nature of the personalised security credentials of the payment instrument and the specific circumstances under which the payment instrument was lost, stolen or misappropriated.
	Article 76 (4) NEW	For direct debits in currencies other than euro, MS may require their PSPs to offer more favourable refund rights in accordance with direct debit schemes providing that they are more advantageous to the payer.
72	Article 86	For national payment transactions, MS may provide for shorter maximum execution times than those provided for in this section.
	Article 101 (2) NEW	MS may introduce or maintain rules on dispute resolution procedures that are more advantageous to the PSU than the one outlined in the first subparagraph. Where they do so, those rules shall apply.

5 Title V – Member state options

No member state options have been introduced within Title V.

6 Title VI – Member state options

PSD1	PSD2	
Article reference		Description
88 (3)	Article 109 (2) and (4)	MS may provide that legal persons referred to in the first subparagraph or paragraph 1 of this Article shall be automatically granted authorisation and entered in registers referred to in Articles 14 and 15 if the competent authorities already have evidence that the requirements laid down in Articles 5 and 11 are complied with. The competent authorities shall inform the legal persons concerned before the authorisation is granted.
88 (4)	CANCELLED	Transitional provision for natural or legal persons eligible for the waiver under article 26.

Contributors:

Dr. Hubertus von Poser
Member of the
Management Board
PPI AG

Christian Fraedrich
Product Manager, Treasury Payments &
Euro Clearing, Cash Management
Deutsche Bank

Swaantje Anneke Haß
Managing Consultant
PPI AG

Christian Schaefer
Head of Payments,
Cash Management
Deutsche Bank