PSD2 – Impacts on retail payments

Hannu Kuokka
Transaction Banking - Payments

PSD2 Seminar
13 February 2018

Agenda

01.	*PSD2 impacts on retail payments*
02.	*Short overview on GDPR (General Data Protection Regulation)*

What does the PSD2 legislate in the area of retail payments?

- Further standardization of payments
- Strengthened consumer protection
- Introduction of Third Party Providers (TPPs)
- Detailed security requirements – for strong authentication and secure communication

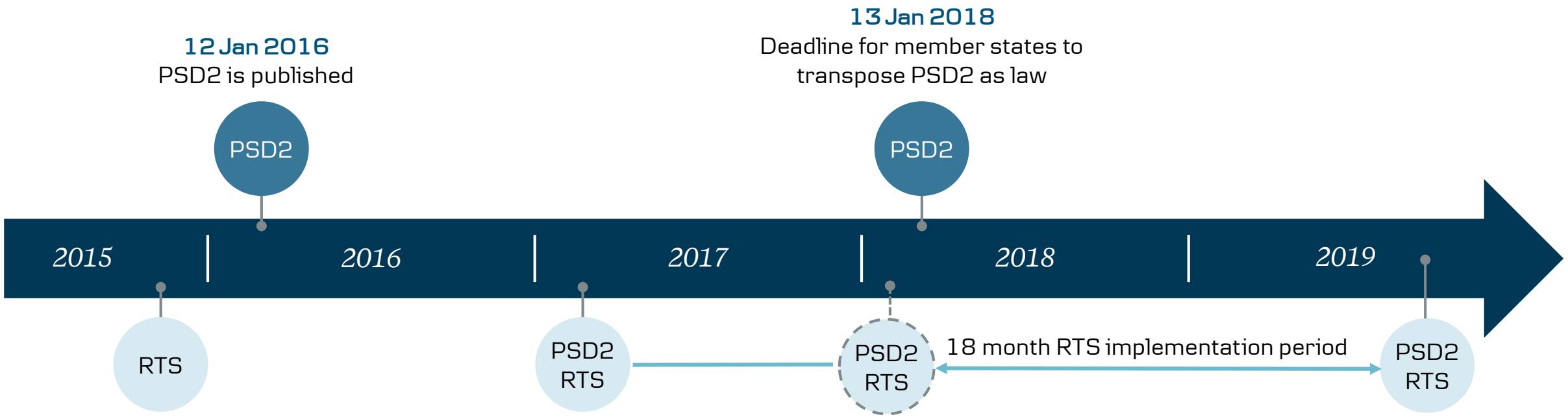
Key PSD2 Drivers

Strong Customer authentication

Access to Account
Banks to open up access to accounts via structured technical interfaces (APIs)

- Payment Initiation Services
- Account Information Services

PSD2 timeline



Dec 2015
EBA discussion paper on
- strong authentication and
- secure communication

Feb 2017
EBA Regulatory Technical Standards (RTS) published

Early 2018 (estimate)
RTS formal enforcement

Q3 2019 (estimate)
Deadline for RTS implementation

Source: Accenture

PSD2 introduces regulation of three types of Third Party Providers ('TPPs')

Third Party Providers ('TPPs')

Payment Initiation Service (PIS)

Means a service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider

Account Information Service (AIS)

Means an online service to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider

Payment Instrument Issuing (PII)

Means a payment service by a payment service provider contracting a payer to provide with a payment instrument to initiate and process the payer's payment transactions

PSD2

Consumer protection and consumer benefits

Lower liability for unauthorized payments	Consumer's maximum liability for an unauthorized transaction from EUR 150 to EUR 50
Ban on surcharging	Surcharging is banned on so called regulated transactions, i.e. consumer card transactions and SCT and SDD transactions
Other consumer related aspects	▪ Effective complaints procedure – maximum 15 day decision time for payment related issues ▪ Undisputed right for refund – across EU for core direct debit

Surcharging banned

Consumer cards (debit or credit) in a
- 4-corner model (e.g. MC)
- 3-corner model if >4% market share

SEPA CT and SEPA DD transactions

Surcharging possible

Consumer cards (debit or credit) in a
- 3-corner model if >4% market share

Commercial cards used for company expenses and a company account linked

PSD2

Strong Customer Authentication (SCA)

SCA as part of PSD2

SCA is a ***mandatory*** method of authenticating

- provided by the payer's payment service provider for
- online or other digital payments including e.g. contactless in-store
- from H2 2019 onwards as part of PSD2 RTS implementation

What is strong authentication?

SCA payments to be authenticated using at least two of the following independent elements:

1. *Something that only the customer knows (e.g. PIN)*
2. *Something that only the customer has or possesses (e.g. card, phone)*
3. *Something that the customer is (e.g. fingerprint)*

Exemptions

There are also a number of specific exemptions to SCA, including:

- ✓ ***Low value*** - up to EUR 50 at contactless POS / EUR 30 online
- ✓ ***Low risk*** *transactions* - structured analysis of a service provider, amount etc.
- ✓ ***Trusted beneficiary*** - payer may create a white-list of trusted beneficiaries
- ✓ ***Recurring payments*** - same value to same beneficiary
- ✓ ***Etc.***

Strengthening of Data Protection

GDPR – General Data Protection Regulation

February 2018

GDPR - General Data Protection Regulation

- *a high-level overview*

Regulatory Framework

- The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC
- Data Protection Directive of 1995 was implemented in Finland by the Act on Personal Data
- GDPR will replace the existing member state legislation also in Finland – and the GDPR will be supplemented by the Data Protection Act

GDPR timeline

Jan 2012	25 May 2016	Implementation Period	25 May 2018
EU Commission proposal for renewal of data protection legislation	GDPR in force	▪ Member state regulatory requirements ▪ Interpretations by a Working Party 29	End of the Implementation Period – member state enforcement

"The EU General Data Protection Regulation (GDPR) was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy."

What is to be expected…

Some things will sustain

Existing rights of the Data Subject will basically remain

Some things will change

Regulation will establish new rights, which will modernize the legislation to be aligned with development of technology

Benefits to companies in scope

- Uniform legislation EU wide
- 'One stop shopping' principle
- Level playing field for EU and non-EU companies, same requirements for all

Increased Territorial Scope (extra-territorial applicability)

Main principle

GDPR applies to all companies processing the personal data of **data subjects residing in the EU**, regardless of the company's location

Clear rule of applicability

GPDR applies to the processing of personal data by controllers and processors in the EU, **regardless of whether the processing takes place in the EU or not**

Non-EU companies also in scope

GDPR also applies to processing of personal data in the EU **by a company not established in the EU when offering goods or services to EU citizens** or monitoring of behaviour that takes place within the EU

Data Subject's rights

Updated rights in GDPR			
Right to information	Right to data erasure ("Right to be forgotten ")	Right to access data	Right to restriction of processing
Right to rectification	Right to object	Right to Data portability	Lawfulness of processing

GDPR will introduce new requirements for companies

Requirements for Data Controller (or Data Processor processing data on behalf of Data Controller)

Accountability

- The Data Controller shall be responsible for and be able to demonstrate compliance and be able to show that data protection principles are followed

Privacy by Design

- Data to be processed only for an intended purpose and to be accessible only to those in need of access

Appointment of Data Protection Officer (DPO)

- New role in GDPR – primary entry point for data protection towards customers, authorities, employees and other 3rd parties (not mandatory for all companies – but helps showing accountability)

Breach Notification

- Mandatory responsibility to notify the Data Protection Authority of data protection breach within 72 hours of first having become aware

Effective Sanctions

Effective sanctions to be imposed in case of breach of the law	The Data Protection Authority is to ensure that imposing of sanctions is ”effective, at the right level and warning”	Sanctions have been divided into two categories: ▪ EUR 20 million or 4% of annual global turnover (which ever is higher) ▪ EUR 10 million or 2% of annual global turnover (which ever is higher)	The new Data Protection Authority’s internal ramification board to decide on sanctions

Remarkable impact – ”non compliance” is a material risk on business

Key Impacts to financial institutions as Data Controllers

Benefits (same as for all companies)

- Uniform legislation EU wide
- 'One stop shopping' principle
- Level playing field for EU and non-EU companies, same requirements for all

Obligations and costs to increase

- Organizational, administrational, planning and documenting costs
- Compliance, reputation and other risks

Danske Bank

Questions?

Danske Bank

Thank you!