Open Banking: Navigating PSD2 & GDPR Implementation and Consequences

PANEL DISCUSSION| 10:00 – 11:00

Moderator/Speaker: **Erla Árnadóttir**, Partner, *LEX Law Offices*

Panelists:

Jónína Lárusdóttir, Managing Director, *Legal Division Arion Banki*

Regina Glaser, *Employment and Labour Law Partner, Heuking Kühn Lüer Wojtek*

Dr. Jur. LL.M. Hans Rudolf Trüeb, *Partner, Walder Wyss Ltd.*

Open Banking:
Navigating PSD2 & GDPR
- Implementation and Consequences -

WSG European Regional Meeting Reykjavík 29 May 2019

PSD II and GDPR – what are they?

- PSD II: EU Directive 2015/2366 replaces EU Directive 2007/64/EB (PSD I)
  - regulates payment services and payment service providers
  - meant to increase pan-European competition and participation in the payments industry, also from non-banks
  - provides access for payment service providers to bank accounts
- GDPR: EU Regulation 2016/679 replaces Directive 95/46/EC
  - provides a standardized set of data protection laws
  - safeguards the processing and movement of EU/EEA citizens' personal data
  - interpretation of PSDII should be with regard to GDPR (Art. 94 GDPR)

PSD II and GDPR – implementation

- PSD II:
  - Deadline for implementation in EU 13 January 2018.
  - EEA: Draft joint committee decision under consideration
  - Regulatory Technical Standards will apply from 14 September 2019

- GDPR:
  - Entered into force in EU on 25 May 2018
  - Should now have been implemented in all EEA states

Regulatory technical standards (RTS)

- Drafted by the European Banking Authority (EBA) in February 2017
- Adopted by the European Commission on 27 November 2017
- Published on 13 March 2018
- Will enter into force on 14 September 2019

GDPR – stakeholders

- Data Controller
  - An entity which determines the purposes and means of processing of personal data
- Data Processor
  - An entity which processes personal data on behalf of a controller
- Data Subject
  - An identified or identifiable natural person, relating to which personal data is processed
- Processing
  - Any operation performed on personal data (i.a. collection, recording, organisation, storage, retrieval, use, disclosure, erasure, destruction)

pSDII – stakeholders

- Account Servicing Payment Service Provider (PSP) – Art. 4 (17) 1(1)
  - Credit institutions, electric money institutions, payment institutions – „banks“
- Payment Initiation Service Provider (PISP) – Art. 4(15)
  - Initiates a payment order at the request of the payment service user with respect to a payment account held at another payment service provider
  - Examples: iDEAL (Netherlands), Sofort (Germany) Trustly (Sweden)
- Account Information Service Provider (AISP) – Art. 4(16)
  - Online services to provide consolidated information on one ore more payment accounts held by a payment service user with one ore more payment service provider
  - Examples: Meniga

pSDII – stakeholders (2)

- Payer – Art. 4 (8)
  - A natural or a legal person who holds a payment account and who allows a payment order from a payment account
- Payee – Art. 4(9)
  - A natural or a legal person who is the intended receipient of funds that are subject of a payment action - a „silent party“

Visions of services of AISPs

- User will be able to obtain information about several payment accounts held with one or more banks
- Analysis of the user´s spending habits
- Supply of payment data to third parties e.g. financial advisors or credit reference agencies

PISP´S Access to payment accounts – art. 66

- Payer´s explicit consent is needed
  - Payee has not provided consent
  - What are the consequences?

- PISP must identify itself at every payment initiation

- PISP must not store sensitive payment data
  - Sensitive payment data is data which can be used to carry out fraud (such as personalised security credentials)

- Bank must communicate securely with PISP

alsp´s Access to payment accounts – art. 67

- Payer´s explicit consent is needed
- Must not request sensitive payment data linked to the payment accounts
  - Sensitive payment data is data which can be used to carry out fraud (such as personalised security credentials)
- PISP must identify itself for each communication session
- Must not use access or store data for other purposes than performing the requested services, in accordance with data protection rules

consent

- PSDII requires „explicit consent“ of the payment service user - Art. 94 (2)

- GDPR allows for various legal basis of processing, *i. a.* that processing is necessary for performing a contract – Art. 6 (1) (b)

silent party

- PSDII requires „explicit consent“ of the payment service user - Art. 94 (2)

- Data subject A uses a PISP to transfer money to data subject B. – May the PISP base the processing on legitimate interest?

security

- Payment service providers must establish a framework with appropriate mitigation measures and control mechanisms - Art. 95

- Payment service providers must apply „strong customer authentication“ - Art. 97
  - requirement of two factors
  - exemptions may apply (RTS)

Interfaces - screen scraping

- PSD II, Art. 66 and 67, impose a duty on PISPs and AISPs to authenticate themselves at every payment initiation and for each communication session

- The banks shall have in place a dedicated interface with same level of availability and performance as the client´s interface, Art. 30 and 31 RTS

- Access to the user interface used for clients (the fintechs accessing data through customers credentials) increases danger of misuse

Developments in the market

- Banks face a tremendous competition
- Developments in co-operation of banks
  - Swish in Sweden
  - Mobile Pay in Denmark
  - Vipps in Norway
  - Netherlands and Belgium: Payqonic
- Amazon payments, Amazon lendings, Google pay, Apple pay, Paypal
-

PSD II – (LEGAL) BACKGROUND

- Idea: economic benefits of integrated payments market for Single European Market
- PSD I brought about significant improvements - some regulatory failures and gaps remained
- Fast (technical) development requires legal adaptation

PSD II - objectives

- 1. Strengthen competition in the payments market
- 2. Standardise, integrate and improve payment efficiency
- 3. Promote innovation

PSD ii - objectives

- 4. Improve consumer protection and legal security

- - Strong Consumer Authentication (SCA)
- - Framework for Common and Secure Communication

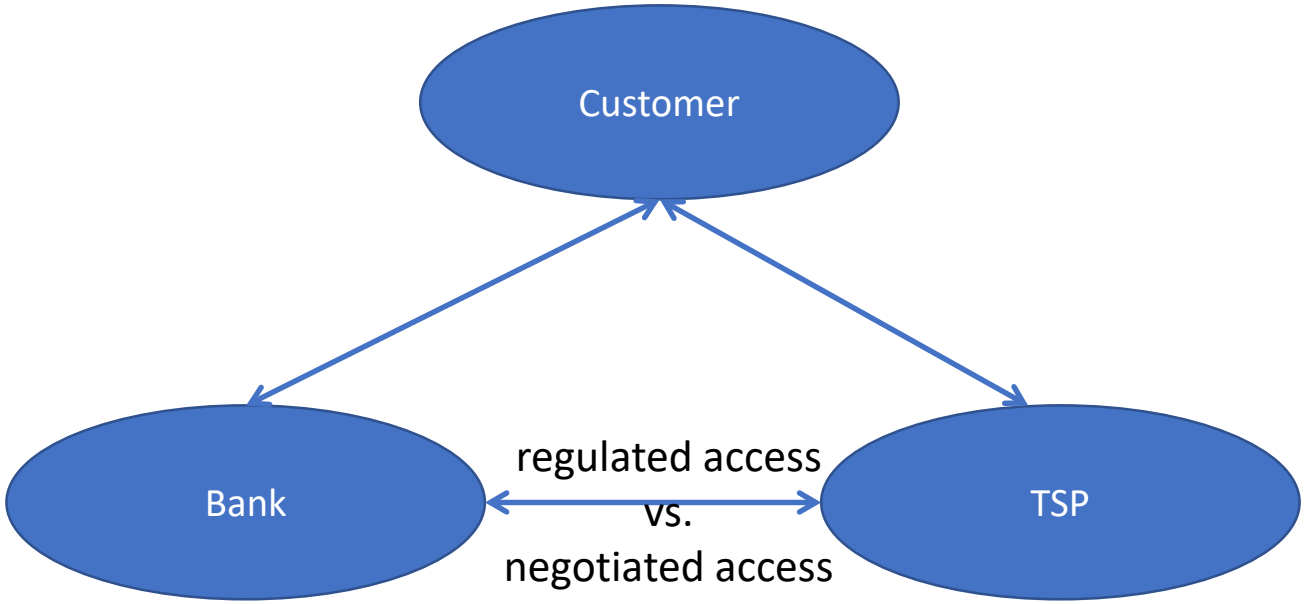
- 5. Increase choice and transparency of payment instruments

Open Banking Revisited
The Swiss Approach

Hans Rudolf Trüeb

Reykjavik, 29 May 2019

Partnership or Coercion?



Common Misconceptions

- Banking institutions are averse to innovation
- Banking institutions are averse to transparence
- Bank customers are locked into products and services of their bank
- Bank customers are denied access to third party products
- Access to customer data will allow for new and competitive services and products
- Bank APIs are an essential facility with mandatory open access for third parties
- Screen scraping is safe and legal

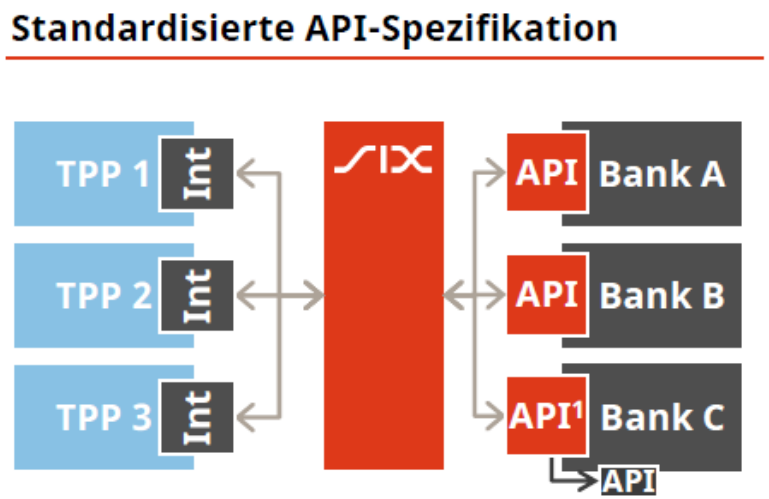
HKMA Open API Framework

- Sponsored by Hong Kong Monetary Authority (HKMA)
- Collaborative and phased approach among regulator, banks and TSPs
- Phases
  I. Product and Services Information
  II. Subscription for Products and Services
  III. Account Information
  IV. Transactions
- Recommended architecture, security and data standards
- Sound industry practices; banks may use and publish their own data dictionaries
- Definition of API functions and use cases

Main Challenges

- TSP Onboarding
  - Due Diligence
  - Common baseline; fair and transparent criteria
  - Business pre-requisites and risk management
- TSP monitoring and relationship management
- Commercial contract
  - Cost
  - Governance and reporting (incidents etc.)
  - Customer information and protection
  - **Data security and protection of personal data**
  - Liability and indemnity
  - Termination

Swiss approach



- SIX Banking Services to develop a baseline API for open access
- Centralized onboarding and management of TSPs
- Establishment of multilateral scheme rules
- Pilot phase with two participating TSPs
- Rollout Phase I: API access for account information services provided to SMEs
- Collection of industry experience and preparation of further phases / use cases