Merchant Payments Ecosystem

GDPR
in Financial Services: The World of Controllers or Processors?

October 25, 2018

Organized by

MODERATOR & PRESENTER:

Nadja van der Veer, Co-Founder / Payments Lawyer, PaymentCounsel

Nadja van der Veer is a payments lawyer with over 10 years of experience in the international Payments industry and a legal expert in rules and regulations involving PSD, GDPR, AML and CDD and Card Schemes. Having worked for a PSP and an acquirer, she has a broad perspective on all legal and business aspects of (Card and Alternative) Payment processing in the global e-Commerce industry. As Co-Founder of PaymentCounsel (www.paymentcounsel.com) and one of the Managing Partners of Pytch Ventures (www.pytchventures.com) she consults Merchant Acquirers, Payment Services Providers (PSPs/MSPs), other FinTech companies and Merchants in their start-up phases that want to expand their business internationally, while mitigating risk. Together with her partners, they understand all aspects of this sector intimately and aim to share their expertise with their partners with full transparency and simplicity. Nadja is an Executive Board Member of the European Women Payments Network (www.ewpn.eu), which aims to provide a support system to women in the industry through different initiatives like networking events and programmes.

PRESENTER & PANELIST:

Derek Fattal, Senior Corporate Counsel, Bluesnap

Derek Fattal has served as Senior Legal Counsel for US-based online payments company BlueSnap Inc., for the last seven years, and previously worked with the company in its ‘start-up phase’ as Director of Marketing prior to an initial ‘exit’ in 2011. He took charge of BlueSnap’s project relating to GDPR compliance which involved the company having to fine tune over 50 vendor and payment service provider relationships over an 18-month period.

Originally a London-based commercial litigation solicitor, Derek sidestepped the legal profession to work extensively in Internet media, including senior management positions with national newspapers in Israel, where he is still based at BlueSnap’s research and development headquarters. BlueSnap has subsidiaries in the UK - where it is an FCA-regulated payments institution - Canada and Australia. The company serves thousands of merchants across the globe.

PRESENTER & PANELIST:

Nasim Jenkouk, Member of the Payment & FinTech practice group, Aderhold law firm

Nasim Jenkouk is a member of the Payment and FinTech practice group at Aderhold law firm (Munich), advising national and international companies in the payment and FinTech sector on all legal issues related to IT, data protection, payments and anti-money-laundering law. She also has many years of experience with national and international companies from the sectors IT, e-commerce and consumer goods, and, in addition to IT law, she has a deep expertise in the areas of commercial law and intellectual property law.

Nasim Jenkouk studied law at the University of Cologne. She completed her legal traineeship inter alia in Berlin and San Francisco (USA). She has been admitted to the German Bar in 2012. Prior to joining Aderhold, she worked for the IP / IT practice group at Pinsent Masons Germany LLP in Munich. In addition, she works on a doctorate thesis in an arbitration law topic. In the course of her doctoral studies, she completed a research residence semester as a visiting scholar at the National Law School of India University, Bangalore.

GDPR in Financial Services

The World of Controllers or Processors?

Nadja van der Veer // Co-Founder / Payments Lawyer, PaymentCounsel

Controller or Processor?

which, alone or jointly with others, determines the purposes and means of the processing of personal data

Controllers

which processes personal data on behalf of the controller

Processors

Market players

Controllers

Processors

UK ICO Guidance

Differences (2014 report)

"…the data controller exercises overall control over the '**why**' and the '**how**' of a data processing activity.

The definition provides flexibility, for example it can allow one data controller to mainly, but not exclusively, control the purpose of the processing with another data controller.

It can also allow another data controller to have some say in determining the purpose whilst being mainly responsible for controlling the manner of the processing.Many business relationships work this way."

Which organisation decides...

- to collect in the first place & the legal basis for doing so
- which items to collect
- the purpose
- which individuals to collect about
- whether to disclose the data & to who
- how long to retain

> *All decisions that can only be taken by controller as part of its overall control of the data processing operation*

Processors on the other hand...

> *Within the terms of the agreement with the controller, a processor may decide:*

- what IT systems to use
- how to store
- detail of security
- means used to transfer
- means used to retrieve
- methods for ensuring a retention schedule is adhered to
- means used to delete

Controller vs Processor

Taking all over-arching decisions,

- what the data will be used for
- what the content of the data is

Freedom to use its technical knowledge to decide how to carry out certain activities on controller's behalf

Example used:

Bank hiring IT services firm

Example payment services

> *A merchant works in co-operation with a 3rd party payment company.*

ICO: payment company not processor because it:

- Decides which info it needs to process payment correctly
- Exercises control over other purposes (example: direct marketing)
- Has legal requirements to meet
- Has own T&Cs that apply directly to merchant's customers

WP29/ EU DPB Guidance

SWIFT Opinion

> *A number of responsibilities that the organisation had taken up with regard*
> *to its processing operations, which were determined by WP29 as going*

"…beyond the set of instructions and duties incumbent
on a processor and cannot be considered compatible
with its claim to be just a processor."

What where they? (I)

- Decide autonomously on level of information provided to financial institutions in relation to processing.
- Determine purposes and means by developing, marketing and changing the existing or new SWIFT services and processing of data.
- Negotiate and terminate with full autonomy its services agreements and draft/ change its various contractual documents and policies.

What where they? (II)

Provide added value for processing such as storage and validation of personal data and protection of personal data with high security standard.

Take critical decisions with respect to processing such as security standard and the location of its operation centres.

Negotiate and terminate with full autonomy its services agreements and draft/ change its various contractual documents and policies.

Does this not apply to many financial institutions?

- Ability to compose services
- Added value for processing (fraud services, BI)
- Take critical decisions
- Develop software with ability to impose requirements on merchants
- Negotiate/ terminate/ draft/ change contracts & policies

WP29 Opinion 2010

"…the discretion of a controller over determining the purpose are characterized as the ability to have level of influence and margin of manoeuvre…"

Example 10

A bank (*PSP/Acquirer*) uses a financial messages carrier (*SWIFT/ Schemes*) in order to carry out financial transactions.

Both the bank and the carrier agree about the means of processing where the processing is carried out at a first stage by the financial institution and only at a later stage by the carrier.

Verdict: Joint Controllers

“However, even if at micro level each of these subjects pursues its own purpose, at macro level the different phases and purposes and means of the processing are closely linked.”

“In this case, both the bank and the message carrier can be considered as joint controllers.”

GDPR - Controllers or Processors

Derek Fattal // Senior Corporate Counsel, Bluesnap

GDPR - Controllers & Processors

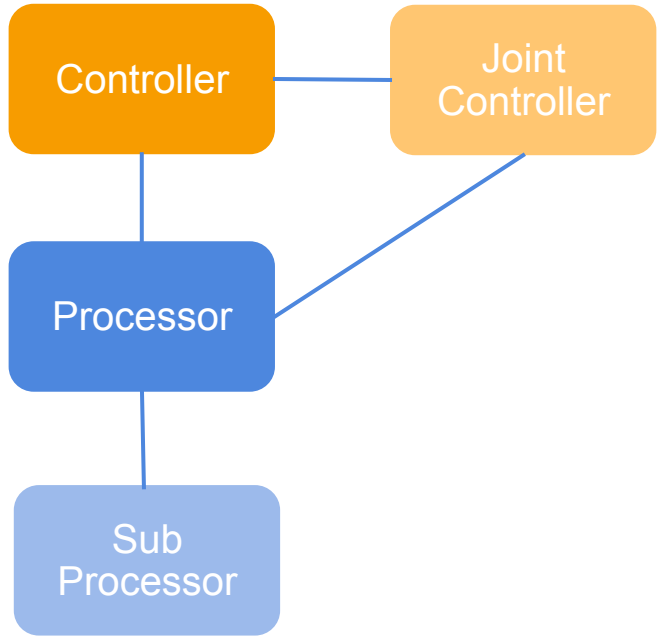
Controller Art.4(7)…body which alone or jointly with others determines the purposes and means of the processing of personal data

Processor Art.4(8)…body which processes personal data on behalf of the Controller

Sub-Processor Art.28(2),(4)...The Processor must not appoint a Sub-processor without the prior written consent of the Controller

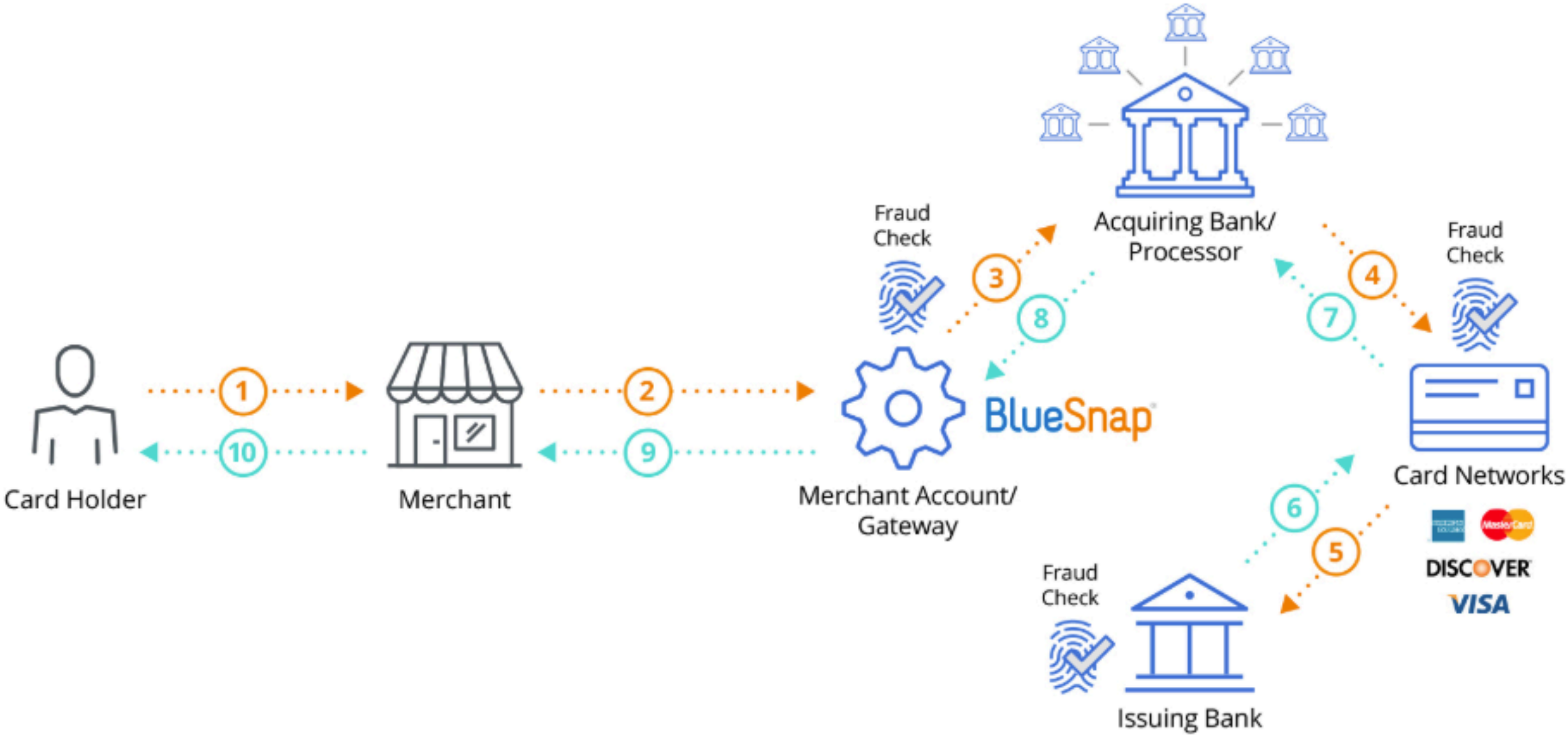
Joint Controllers Rec.79; Art.4(7), 26 … Where two or more Controllers jointly determine the purposes and means of the processing of personal data, they are Joint Controllers

ICO (UK) Draft Guidelines Sept 2017 .. Affirms prior 2014 guidance deems payment services as Data Controllers



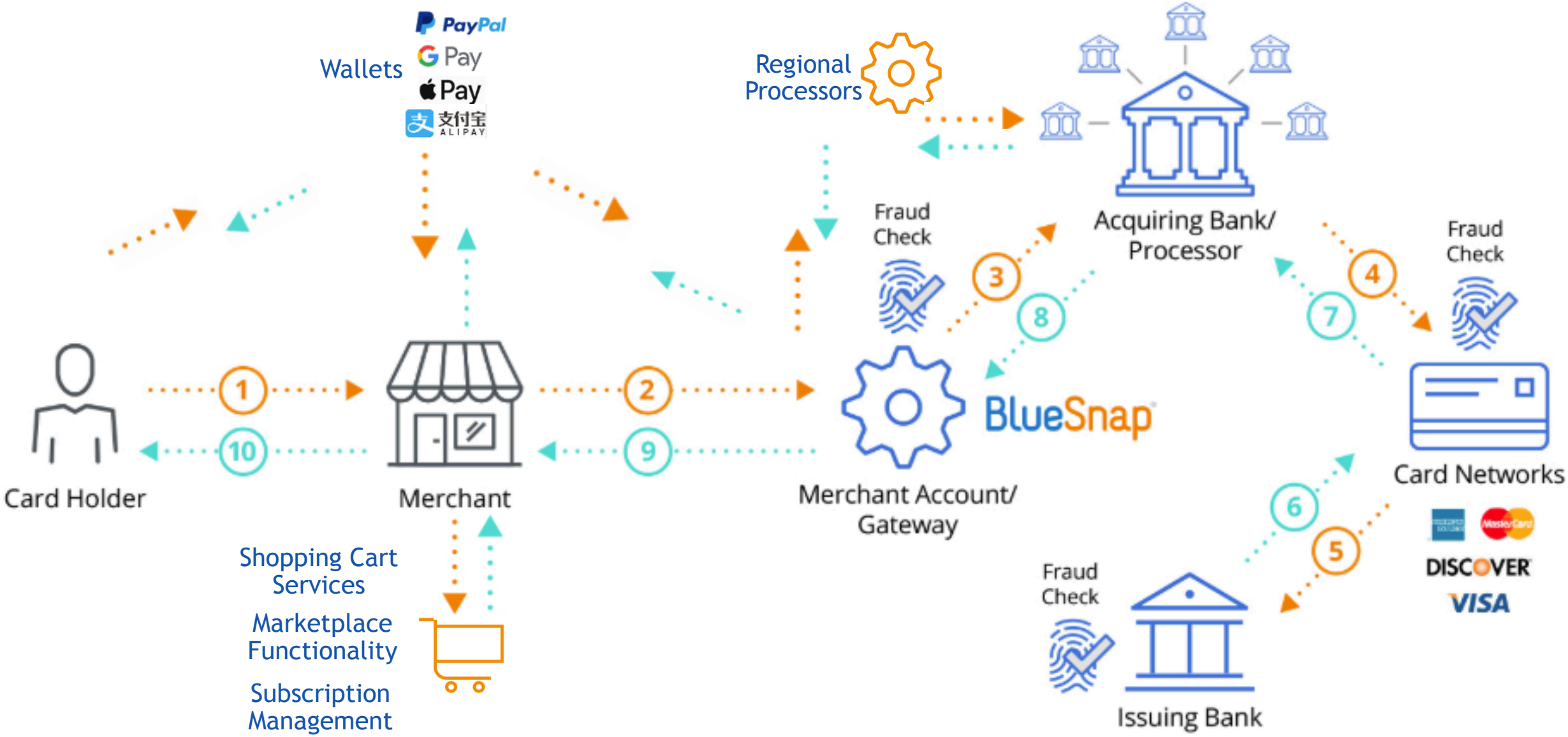
BlueSnap

Payments World - Controllers & Processors



BlueSnap

Real World - Controllers & Processors



BlueSnap

Liability Issues - Controllers & Processors

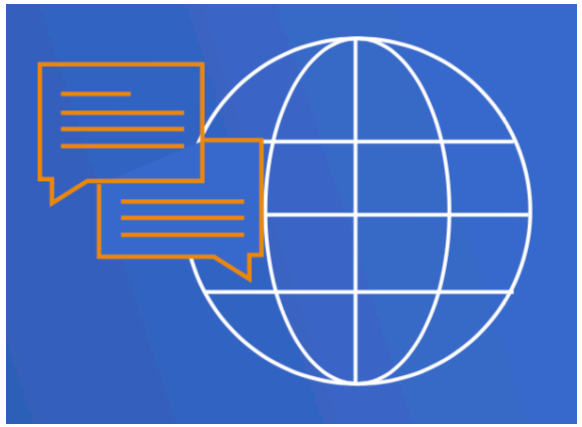
- Controller has overall responsibility to ensure that personal data is processed according to the principles set out in Art. 5
- Liability generally flows down the processing chain
  - Controllers liable for Processors & Sub-processors, Processors liable for Sub-processors
  - Under the GDPR Processors also assume liability
- Art. 82 – Unless it proves it has no responsibility for the event giving rise to damage:
  - Controller is liable for damage caused by Processing that infringes GDPR
  - Processor is liable for its failure to comply or act outside a Controller's lawful instructions

- Art.82(4) Liability to Data Subjects
  - Where there is more than one Controller or Processor involved in the same processing, **each Controller(s) or Processor(s)** maybe held **liable for the entire damage** caused by the processing to ensure effective compensation of the data subject
  - Only once data subject has been fully paid out for the damage suffered can a party seek compensation from another for their responsibility towards the damage
- Art. 82(6) Compensation claims - in home jurisdiction or Member State of respective Controller/Processor
    - Invites forum shopping, multiple defendants, jurisdictions with class actions

BlueSnap®

Issues - Controllers & Processors

- Rights of Data Subjects:
  - Art. 79 Claim against infringement of any GDPR rights
  - Art. 77 Issue complaints for infringement with supervisory authority
  - Art. 80 Can mandate a privacy rights organization to bring claims under the Regulation
- Art. 82(1)
  - **Any person** who has suffered damage under the Regulation can claim – includes special damages ie: financial loss, material and non-material damage
- Art. 83 Administrative Fines
  - Up to 4% of global turnover
- Lack of Privacy Certification regime
- Data Processing Agreements
  - Must indicate whether parties are Controllers or Processors
  - Contractual bargaining power
- Indemnity Issues
  - Controllers need high indemnity ceilings, Processors want to minimize



BlueSnap®

Suggested Approaches

- Look at the ‘big picture’ rather than Controller/Processor roles
  - Commit to security & privacy compliance
  - Risk of massive reputational damage through a data breach
  - Review data flows, map accurately, keep full records
  - Undertake due diligence & collect relevant information on your partners
- Dual Role - Payment companies can be Controllers in some instances and Processors in others
  - Be prepared to take on obligations of a Controller – even if you are a Processor
- Our Approach
  - For Merchants
    - Direct contracts and contracts with merchants, perform underwriting, AML checks, provide reporting -- acting as a **Controller**
  - For Shoppers:
    - Acting as a technical solution in a long flexible chain
    - No direct contact with shoppers, process is dictated by payment scheme owners, we connect the parties, move data along the chain -- acting as a **Processor**
- Conclusion

BlueSnap®

The Hate-Love Affair of PSD2 and GDPR

Interaction of the regulations with regard to data protection

Nasim Jenkouk // Member of the Payment & FinTech practice group, Aderhold law firm

GDPR and PSD2 - Basic Differences

GDPR

EU Regulation:

- Directly applicable and enforceable by law in all Member States
- National implementation act is not required
- Member States, however, issue national legislation that defines e.g. the competent national authorities

PSD2

EU Directive:

- Applicable to all Member States
- Sets out requirements and results that have to be achieved in every Member State
- National authorities have to create or adapt their national legislation to meet the EU Directive

Aderhold

GDPR and PSD2 - What are the objectives of GDPR and PSD2 ?

Both legislative acts are designed to protect consumers, however, from a different perspective.

GDPR

- Protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data
- Protection of fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data
- The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data

PSD2

Its main objectives are to:

- Contribute to a more integrated and efficient European payments market
- Improve the level playing field for payment service providers (including new players)
- Make payments safer and more secure
- Protect consumers

GDPR and PSD2 - Data protection references in the PSD2

PSD2

- Art. 67 section 2 (f) PSD2:

"not use, access or store any data for purposes other than for performing the account information service explicitly requested by the payment service user, in accordance with data protection rules;"

- Art. 94 PSD2:

"1. Member States shall permit processing of personal data by payment systems and payment service providers when necessary to safeguard the prevention, investigation and detection of payment fraud. The provision of information to individuals about the processing of personal data and the processing of such personal data and any other processing of personal data for the purposes of this Directive shall be carried out in accordance with Directive 95/46/EC, the national rules which transpose Directive
95/46/EC and with Regulation (EC) No 45/2001.
2. Payment service providers shall only access, process and retain personal data necessary for the provision of their payment services, with the explicit consent of the payment service user. ."

GDPR and PSD2 - What is an explicit consent?

GDPR

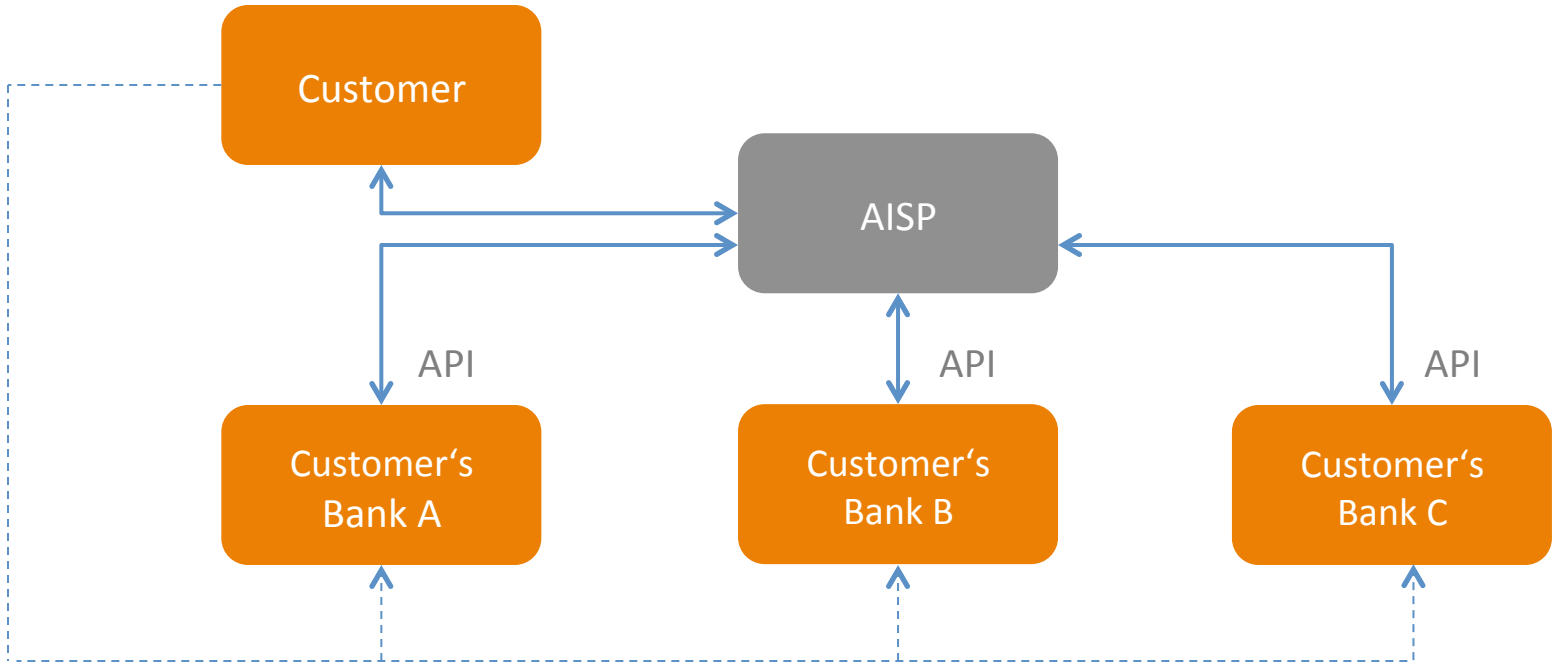
- Consent (Art. 6 section 1 (1) a) GDPR) is just one of several legal grounds to process personal data
- data can be lawfully processed if *"processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract"* (Art. 6 section 1 (1) b) GDPR GDPR)

PSD2

- *"Payment service providers shall only access, process and retain personal data necessary for the provision of their payment services, with the explicit consent of the payment service user"* (Art. 94 section 2 PSD2)

- EDPB: "Explicit consent" referred to in Art. 94 PSD2 and Art. 67 PSD2 shall be understood as a contractual consent. In terms of the GDPR, the legal basis for the processing of personal data is Art. 6 section 1 (1) b) GDPR, as long as the data are merely processed for the performance of the contract.
- Uncertainties remain with regard to the understanding of national authorities.

GDPR and PSD2 - What are silent party data?



Sometimes AISPs and PISPs can encounter the personal data of other people when seeking to deliver their services to customers.

GDPR and PSD2 - What about silent party data?

GDPR

- Art. 6 I 1 f) GDPR allows for the processing of personal data based on the legitimate interests pursued by a controller or by a third party.

EDPB: A lawful basis for the processing of silent party data by TTPs can be the legitimate interest of a controller or a third party (Article 6 section 1 (1) f) GDPR) to perform the contract with the service user.

GDPR and PSD2 - Outlook

- Even if the GDPR is an EU Regulation and has direct effect in all countries, national specialities need to be considered when dealing with the overlap between the GDPR and PSD2.
- Guidelines can only be understood as what they are: Guidelines.

Q&A

Panelists are addressing questions from the audience collected in advance.

If your question was not responded during the Q&A session, please feel free to contact the organizer at mpe@empiriagroup.eu with any further questions

Merchant Payments Ecosystem

Thank you for attending!

GDPR in Financial Services: The World of Controllers or Processors?

This webinar is a supportive initiative to:
MPE 2019, conference and exhibition, 19-21 February, 2019, Berlin
You can download the agenda at www.merchantpaymentsecosystem.com