KU LEUVEN CAMPUS BRUSSELS
FACULTY OF LAW
Academic year 2018-2019

Data protection in mobile wallets

Master's thesis, submitted by
Johan PEETERS
as part of the final examination for the degree of
MASTER OF INTELLECTUAL PROPERTY AND ICT LAW

Promoter: E. KINDT
Word count: 12251

KU LEUVEN CAMPUS BRUSSELS
FACULTY OF LAW
Academic year 2018-2019

Data protection in mobile wallets

Master's thesis, submitted by
Johan PEETERS
as part of the final examination for the degree of
MASTER OF INTELLECTUAL PROPERTY AND ICT LAW

Promoter: E. KINDT
Word count: 12251

I confirm that this thesis is my own work, that all ideas contained in the thesis are expressed in my own words and that I have not literally or quasi-literally taken anything over from other texts, except for fragments cited between quotes for which I provided full and accurate bibliographical data.

Johan Peeters

Abstract

The rise of mobile wallets in recent years resulted in increased security and privacy risks. The objective of this thesis is to analyse how the European legal framework deals with them. After providing an overview of the stakeholders and the current security measures in mobile wallets, the security and privacy risks will be discussed. The thesis will give an overview of PSD2 and point at the relevant changes in the light of the legal vacuum where mobile wallet issuers were operating in before. The obligations to apply enhanced security measures and strong consumer authentication are ought to result in increased protection of payment data, but conflicts with GDPR on different issues are arising too. In this context, examples will be given, and possible solutions examined. The layered approach of the EU legislator makes it challenging to predict whether the mobile wallet users' data are sufficiently protected now. While the RTS will come into force in a few months, the interaction with GDPR will only become more apparent in the following years.

Do you spend your day

Second guessing faith?

Looking for a way

To live so divine

Drop your sad pretence

You'll be doing fine

You will flourish like a rose in June

You will flourish like a rose in June

Belle & Sebastian

Table of contents

List of abbreviations

AIS: Account Information Service

AISP: Account Information Service Provider

API: Application Programming Interface

ASPSP: Account Servicing Payment Service Provider

BEUC: European Consumer Organisation

EBA: European Banking Authority

ECB: European Central Bank

EDPB: European Data Protection Board

EDPS: European Data Protection Supervisor

ENISA: European Union Agency for Network and Information Security

EPC: European Payment Council

GDPR: General Data Protection Regulation

MNO: Mobile Network Operator

NFC: Near Field Communication

PAN: Primary Authorisation Number

PIS: Payment Initiation Service

PISP: Payment Initiation Service Provider

PSD2: Payment Services Directive 2

PSP: Payment Service Provider

PSR: Payment Systems Regulator

RTS: Regulatory Technical Standards

SE: Secure Element

Secure Pay: European Forum on the Security of Retail Payments

TSM: Trusted Service Manager

TTP: Trusted Third Party

Working Party 29: Article 29 Data Protection Working Party

Introduction

The widespread availability of mobile internet in the EU led to the rise of online mobile services in the field of e-commerce. Being part of this development, mobile wallet providers offer customers an efficient possibility of making their purchases online. Data security and trust are, therefore, indispensable.

The main research question is: How does the EU legal framework deal with the security and privacy risks of mobile wallets?

Therefore, related sub-questions are the following:

1. What security and privacy risks do mobile wallets pose?
2. What are the personal data processed in mobile wallets?
3. What is the EU legal framework on data protection in mobile wallets?

In the first chapter, I will explain the basic concept of mobile wallets, and I will contrast them with traditional payment cards. Starting from the traditional payment card network structure, I will set the scene of the relevant stakeholders in mobile wallets and describe the security measures in mobile payments. At the end of the first chapter, I will elaborate on the risks that mobile wallets pose.

Chapter two provides an overview of the legal framework concerning payment services, more in particular, the revised Payment Services Directive (PSD2). I will give an introduction to the context and touch briefly on the interoperability standards created through self-regulation. I will describe critically the introduction of new types of services and the obligation for Payment Service Providers (PSPs) to apply strong customer authentication and to enhance security measures. I will analyse whether PSD2 brought a solution for mobile wallets.

In the third chapter, I will pick out some of the data protection issues that can be raised in mobile wallets. The chapter starts with defining the relationship between PSD2 and the General Data Protection Regulation (GDPR). Furthermore, I will analyse what personal data are processed in mobile wallets and how they can be collected legitimately. In this chapter, questions of compatibility

between PSD2 and GDPR will be raised. This is, for instance, the case in the part where I analyse whether the notion "*explicit consent*" has the same meaning in PSD2 and GDPR. Lastly, I will pay special attention to the data minimisation and the purpose limitation principles. I will analyse whether these principles are implemented in PSD2 and what the consequences are for mobile wallets.

Since this thesis focusses on mobile wallets related to payment accounts, I will not address the business of electronic money issuers. Given the quantitative limitation, I cannot provide an exhaustive overview of all the possible data protection issues, nor is it possible to go into detail of cybersecurity.

1. How do mobile wallets work, and what are the risks?

a. Concept

Digital wallets are computer software applications that store financial and/or other personal data. Financial data, in this context, refer primarily to debit and credit card data that are necessary to perform payment transactions. The storage of financial data is an essential function of digital wallets that allows users to purchase goods and services online or send money to other digital wallet users.[1]

There exist enormous varieties of digital wallets, and this includes the mobile wallets. The mobile wallets are run on mobile devices, such as smartphones, tablets and smartwatches. In that respect, they differ from web-based wallets.[2] Examples of mobile wallets are Apple Pay, Android Pay and Samsung Pay. An additional function of most mobile wallets is that they can be used to execute contactless transactions at merchants' payment terminals.

A distinguishing feature of digital wallets is their ability to store not only financial data, but to aggregate information related to other personal documents, such as driver's license, users' health card, loyalty cards, flight tickets, and other ID related documents. Virtually any type of personal data can be included in digital wallets. In that sense, they are digital analogues of physical wallets, used traditionally to store different forms of cards and documents.[3] Implementation of digital wallets within broader operational mobile systems allows them to use additional information accessible through mobile devices, such as real-time geolocation data and users' home address. In the context of this thesis, a mobile wallet is thus a service that allows wallet holders to access, manage and use mobile payment services, as well as other personal data.[4]

Mobile wallets should be differentiated from other mobile services with similar but limited functions such as banking applications, banking web-services, and digital-currencies wallets. While the first two services function as an access portal to personalised bank accounts, designed by real banks[5],

[1] ENISA, *Security of mobile payments and digital wallets*, 7.
[2] A. LEVITIN, *The promise and perils of digital wallets*, 15.
[3] E.g. N. VANDEZANDE, *Mobile wallets and virtual alternative currencies*, 5.
[4] EPC, *White paper mobile wallet payments*, 16.
[5] Historically, they have been regulated tighter than mobile wallets, cf. N. VANDEZANDE, *Mobile wallets and virtual alternative currencies*, 7.

the latter stands for new forms of storages for keys representing ownership of electronic money such as Bitcoin.[6]

Mobile wallets and traditional payment cards

Mobile wallets differ from traditional debit cards (e.g. Maestro and Bancontact/Mistercash) and credit cards (e.g. Visa and Mastercard) since they function as a mediating service that connects the initial payment with the specific debit or credit card. Before carrying out a transaction, customers open the application and pick the most relevant payment card. This is advantageous for customers as they need to enter their data only once. The payment process becomes faster.[7]

Another difference with traditional payment cards lies in the range of possible technologies that can be used for transmitting payment authorisation. Depending on the equipment of the device, users of mobile wallets can choose between proximity technology such as Near Field Communication (NFC)[8], Quick Recognition (QR) Code, Bluetooth, apps on the internet, text messaging (SMS) and chip technology.[9] Since different companies and developers provide all those additional services, this opens a host of questions related not only to data privacy but also to vulnerabilities to hacker attacks.

Finally, mobile wallets differ from traditional payment cards as they establish two-way communication between customers and merchants. Apart from the payment function, mobile wallets can be used for advertising and customer service.[10] This can potentially be beneficial for both customers and merchants. Customers may benefit from less administration. By keeping purchase records digitally, returns and reimbursements can be facilitated. Targeted advertising can also be beneficial for customers, e.g. when they get instant information about promotions on products they are looking for. Merchants can potentially benefit from mobile wallets as they enable an integrated retail platform, thus combining the payment process with advertising, search functions, shipping, returns procedures and customer loyalty.[11] All those elements allow customer

[6] ENISA, *Security of mobile payments and digital wallets*, 7.
[7] A. LEVITIN, *The promise and perils of digital wallets*, 37.
[8] NFC is a short-range high frequency wireless communication technology, which enables the contactless exchange of data between devices. This technology works in combination with the Secured Element (SE) in the mobile device. Users download their payment credentials to the SE, where they stay safe. (B. GEVA, *Mobile payments*, 281-282)
[9] ENISA, *Security of mobile payments and digital wallets*, 7-8.
[10] A. LEVITIN, *The promise and perils of digital wallets*, 4.
[11] *Ibid.*, 37-38 and 50.

binding. However, this also raises many specific issues related to data protection, which will be further elaborated on.

In the following section, I will first elaborate on the traditional framework of payment cards (section b). Secondly, I will contrast those services and involved stakeholders with those implicated in mobile wallets (section c). Finally, security and privacy risks of mobile wallets will be discussed in the section "d".

b. Stakeholders and security measures in a traditional payment card network structure

Mobile wallets are built on the traditional (i.e. offline) payment card network structure.
In a traditional four-party scheme[12], the following parties are involved: customers (payers), merchants (payees), customers' banks (issuers), merchants' banks (acquirers) and payment card networks (schemes, e.g. Visa and Mastercard for credit cards and Bancontact for debit cards).

The customer's bank is called the issuer as it issues the customer a payment card that contains the payment authorisation data. When customers want to buy goods or services from the merchant, they pay through the payment terminal of the merchant. Through this terminal, the payment authorisation data are transferred to the merchant's bank, which is also called the acquirer as it acquires the payment right on the transaction from the merchant. The merchant's bank then presents the transaction to the payment card network. Finally, the payment card network sends an authorisation request to the customer's bank. The latter verifies the credit or debit available on the account and sends an answer, either an approval or a denial, to the acquirer. The acquirer passes this information to the merchant to finalise the purchase.[13]

In the aforementioned system, the payment card network functions as a clearinghouse between the issuer and the acquirer. It streamlines the rules and offers necessary infrastructure. Those

[12] In some cases, three parties are sufficient. This is the case when a bank provides the possibility of direct payments to the merchant through a safe home banking website. Also, American Express uses the three-party model. (M. TRUYENS, *Elektronische betalingen*, 171.)
[13] A. LEVITIN, *The promise and perils of digital wallets*, 11.

rules bind the merchant through its incorporation in the contract between the merchant and the acquirer.[14]

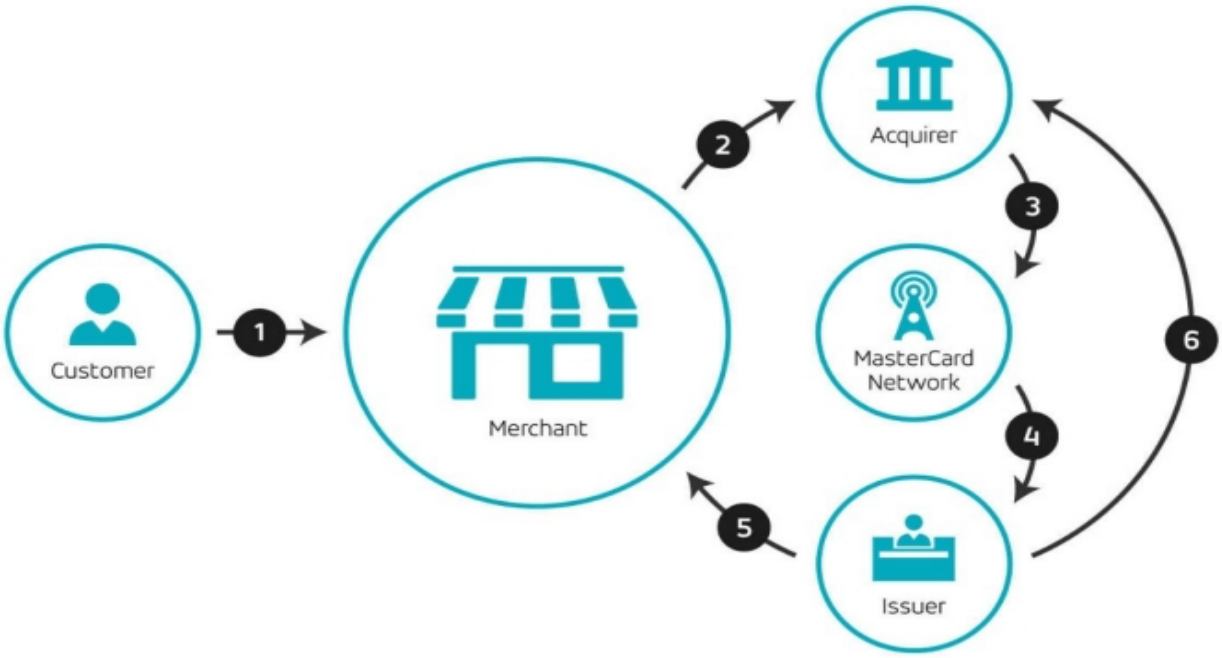

Figure 1[15]

Traditionally, issuers and acquirers were banks. Nowadays, other companies, e.g. PSPs can also issue payment instruments for customers or provide payment gateways for merchants. By pulling funds directly from the customers' bank account and thus passing by the schemes' fees, the overall cost of transactions can be reduced. This is potentially beneficial for merchants and could lead to lowering prices for customers.

In an online context, another stakeholder needs to be mentioned, the Internet service provider. It is responsible for operating the Internet network and securely routing messages. In more complex scenarios, the Trusted Third Party (TTP), is involved. This party obtains a certificate, issued by a certificate authority. The certification leads to a higher level of authentication and, thus, trust.

[14] *Ibid.*
[15] www.mastercard.co.uk/en-gb/merchants/start-accepting/payment-process.html.

To secure the use of payment cards offline, the merchant is obliged to control the signature at the card. As this may easily lead to fraud, payment cards have since long been equipped with a PIN code.[16]

In recent years, EMV Chips[17] have been introduced on payment cards. Unlike magnet stripes on payment cards, these chips have higher security standards that prevent skimming-fraud related to payment cards.[18] Most networks tie the liability claims to the use of EMV chips.[19] Another comprehensive tool in the prevention of fraud is statistical analyses of payment transactions.[20]

In a traditional card transaction online, the authorisation data, together with the card verification number/code (CVV/CVC), is sent to the merchant. This is the number at the backside of the payment card. The same number is used for every transaction, which creates risks if the number is compromised. In some cases, banks add an extra security layer, 3D-security, which mostly requires a card reader. After entering the PIN code, the card reader generates a code that has to be inserted to complete the payment. Also, in this case, most payment card networks oblige merchants to apply 3D-security authentication.[21]

Most of the payment card networks require both issuers and acquirers, and through the contracts with the acquirers also the merchants, to comply with the PCI DSS (Payment Card Industry Data Security Standard).[22] This standard consists of twelve primary obligations, e.g. installing and maintaining a firewall, restricting access to cardholder data to authorised personnel, maintaining an information security policy and encrypting[23] the transmission of cardholder data over open and public networks.

[16] M. TRUYENS, *Elektronische betalingen*, 187.
[17] Named after Europay, MasterCard and Visa.
[18] Skimming stands for obtaining payment card information, e.g. by copying or using more sophisticated means during the transaction.
[19] M. TRUYENS, *Elektronische betalingen*, 187-188.
[20] *Ibid.*, 188.
[21] *Ibid.*, 189.
[22] www.pcisecuritystandards.org.
[23] Encryption means that a mathematical algorithm is used to scramble the payment card data, so that only key owners can read the data. (A. LEVITIN, *The promise and perils of digital wallets*, 23.)

c. Stakeholders and security measures in payments through mobile wallets

In mobile wallet services, additional stakeholders are involved while some of the traditional stakeholders may take up a new role.[24]

The mobile wallet issuer delivers mobile wallet functionalities to both customers and merchants. This role can be assumed by new players, e.g. technology companies like Apple, which aim to strengthen their brand position in mobile services. However, also existing stakeholders, e.g. PSPs including banks can take up this role to widen their financial services.[25]

The Mobile Network Operator (MNO) takes over the role of the internet service provider. Next to that, it can also offer mobile wallets.[26]

The Secure Element (SE) issuer comes into play in the case where a dedicated application, authentication application or credentials on the mobile device is/are involved. [27] The application or credentials are stored confidentially on the mobile device in a SE, i.e. a chip with a secure microcontroller.[28]

The mobile wallet gateway provider operates the mobile wallet gateway service that establishes a link between the mobile wallet and a payment gateway for mobile payments transactions. This service may be operated directly by the mobile wallet issuer or a TTP.[29]

TTPs appear in various forms:

- As a Trusted Service Manager (TSM), acting on behalf of the SE issuer or the mobile payment service issuer in order to guarantee that payment credentials are securely transmitted;
- As a payment gateway provider, facilitating the transfer of information between the payment portal and the customer's or merchant's PSP;

[24] EPC, *White paper mobile wallet payments*, 23.
[25] *Ibid.*, 24.
[26] *Ibid.*, 23-24.
[27] *Ibid*.
[28] ENISA, *Security of mobile payments and digital wallets*, 8.
[29] EPC, *White paper mobile wallet payments*, 24.

- As the operator of a common infrastructure in cases when an alias is used for remote payments.[30]

Other stakeholders in the mobile wallet paying schemes are SE manufacturers, application developers and mobile device manufacturers, etc.[31]

In terms of security measures, it should be noted that mobile wallets do not change the basic design of the system used in the traditional payment card network structure. However, they differ from that structure as they can transmit payment authorisation data through a range of communication technologies and as they can change the nature of the data.[32]

Depending on the equipment of the device, mobile wallets can choose between NFC technology, QR Code, Bluetooth, Internet, SMS and chip technology.[33] Chip transactions, for instance, can only be performed by mobile wallets that are equipped with a chip in the mobile device. Moreover, these transactions can only be performed in the physical presence of the merchant.[34]

Mobile wallets also change the format of the data.[35] Before sending the payment authorisation data to the merchant, mobile wallets encrypt and, depending on the wallet, tokenise the data themselves. The merchant, thus, does not have direct access to any customer data.

Tokenisation, mentioned above, was developed as a supplemental security measure, aside of encryption. The process of tokenisation replaces the data with a token, i.e. randomly generated substitute data. The creation of one-time account identifiers leads to more secure transactions as it becomes more challenging to engage in credit card fraud. In contrast to encryption, no algorithmic transformations are used.[36]

Tokenisation, additionally, reduces the number of parties that own and store the data. Only the issuer remains in possession of the original data while the merchant sends the encrypted data, together with the card verification code, to its acquirer. The acquirer forwards both the encrypted

[30] *Ibid*.
[31] *Ibid*.
[32] A. LEVITIN, *The promise and perils of digital wallets*, 18.
[33] ENISA, *Security of mobile payments and digital wallets*, 7-8.
[34] A. LEVITIN, *The promise and perils of digital wallets*, 29.
[35] *Ibid.*, 20.
[36] *Ibid.*, 29.

data and the code to the card network and the issuer for authorisation. The acquirer tokenises the data and returns it to the merchant. The merchant therefore only retains the tokenised data which, in the form of a randomised number, becomes useless to potential hackers.[37] At the same time, merchants also cannot use the data for further advertising or other related personalised services. This technology reinforces data protection and increases the security of payments. The use of tokenisation, however, is not a necessary element in the PCI DSS.

d. Privacy and security risks of mobile wallets

Data privacy relates to the control that an individual has over his or her personal information. Data security stands for the tools, technology, protocols being integrated into the system in order to protect the confidentiality, integrity and availability of personal data.[38]

The entire mobile payment process is susceptible to both privacy and security risks since it constitutes a complex ecosystem with varied market participants, each with their business practices.

In its report on the security of mobile payments and mobile wallets, the European Union Agency for Network and Information Security (ENISA) identifies critical security threats of mobile wallets and provides guidelines and defines minimum measures to assist mobile payment developers and mobile payment providers in implement security.[39]

The report identifies several vulnerabilities in every stage of the use of mobile wallets, namely:

- Tampering with the wallet app in the app store. In this scenario, the attacker downloads the app from the store, unpacks it, patches the relevant routines and then repackages and uploads it back to the store;
- Theft of credit card data through an infected phone camera at the enrolment phase;
- Authentication of the user with weak or stolen passwords;

[37] M. TRUYENS, *Elektronische betalingen*, 193-194.
[38] ENISA, *Privacy and Data Protection by Design*, 6.
[39] ENISA, *Security of mobile payments and digital wallets*, 47p.

- Authentication of the user with fingerprint biometrics only. This technique can be bypassed by lifting the latent fingerprints from the device. When the device gets stolen, the wallet app can be exploited;
- Theft of credit card data through unsecured WIFI hotspots, phishing emails or at an infected merchant's POS terminal (the latter is technically called "*Man-in-the-Middle attacks*");
- Theft of look-up tables at the token service provider;
- Involvement of third parties in the wallet app to perform payments. A malicious application could be installed on the device to access the third-party app. The 2018 incident at Ticketmaster (*infra*) shows that the compromise of third-party apps can lead to a widespread data breach;
- Distributed Denial of Service (DDoS) attacks make the service unavailable, typically due to excessive requests;
- Increasing theft of mobile devices given the rise of mobile wallets.[40]

In June 2018, the Ticketmaster's UK branch was a victim of an attack. Digital skimmers were placed on several websites of this popular distributor of concert and festival tickets. This was caused by an infected chatbot app, developed by Ibenta, a third-party functionality supplier. Five percent of the customers, over ten thousand people, were victim of theft of their data, including credit card data.[41]

Aside from the risks related to unauthorised payments, mobile wallets also create risks concerning unauthorised use of personal data relating to the individual.

In his article on the promise and perils of digital wallets[42], LEVITIN mentions the loss of privacy for customers as the key difference between traditional payment cards and digital wallets. He argues that by payments made through payment cards, merchants only get in possession of customers' purchase-related information at their shop. Financial institutions, on the other hand, can mine the information from transactions at multiple merchants (including the type of industry and the location of the shops), which can already be enough to build a profound profile of the user. However, this profile is not complete since it relies on incomplete information.

[40] *Ibid.*, 26-29.
[41] www.techpulse.be/nieuws/225830/datalek-ticketmaster-bank-stelt-dat-bedrijf-al-maanden-op-de-hoogte/.
[42] A. LEVITIN, *The promise and perils of digital wallets*, 43-46.

Mobile wallets provide far more possibilities for financial institutions to build an integrated portrait of customers' spending behaviour. The abovementioned data can be combined, not only with transactions data from other payment cards, by multiple banks, but also with data on the customer past web browsing and his geolocation.[43] This leads to an enhanced privacy risk to customers.

Also, LEVITIN underlines that the collected data are beyond the control of customers as it can be shared with the other players in the ecosystem, e.g. retailers and app developers and sold to third parties, e.g. advertisers without their knowledge.[44]

As we could see from the previous discussion, mobile wallets represent new forms of payment that profoundly reconceptualises the idea of financial transactions. Traditional modes of card payments, although susceptible to risks, were still limited to a single bank account and contained only a limited amount of information. The unprecedented ability to gather a large number of various data into a single user-profile, which now characterises mobile wallets, brings new risks related not only to financial security but also to data privacy and data security. Even though many governmental and inter-governmental organisations have identified those risks, the legislative measures related to the development and regulation of mobile wallets are still nascent.

[43] *Ibid.*, 43-46.
[44] *Ibid.*, 46.

2. EU mobile payments legislation

a. No specific set of regulations for mobile payments

There does not exist a specific set of regulations for mobile payments. The regulation is layered.[45] Mobile payment operators have to comply with payments regulation (PSD2 and Electronic Money Directive 2[46]), consumer regulation (Consumer Right Directive[47], e-Commerce Directive[48] and Unfair Commercial Practices Directive[49]), privacy regulation (GDPR and e-Privacy Directive) and technology regulation (common standards and interoperability[50]). On top of that, mobile payment operators have to comply with the regulation on finance, competition, tax, intellectual property, etc. Since this thesis focusses on the privacy aspects of mobile wallets, most of those instruments are outside its scope. This thesis deals only with PSD2 and the privacy regulation.

b. Context and scope of PSD2

The adoption of PSD2 in 2015 was part of a package of legislative measures on payment services.[51] The European Commission initiated the revision in 2012. In its green paper "*Towards an integrated European market for card, internet and mobile payments*"[52] it laid down the base. The fact that some of the innovative payment services did not fall in the scope of PSD due to too broad exemptions and diverging implementations by the Member States, led to incongruences.[53] The

[45] S. DE BROUWER, *Navigating the labyrinth*, 46.
[46] Dir.EP and Council no. 2009/110/EC, 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC, *O.J.L.* 10 October 2009, 267, 7-17.
[47] Dir.EP and Council no. 2011/83/EU, 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, *O.J.L.* 22 November 2011, 304, 64–88.
[48] Dir.EP and Council no. 2000/31/EC, 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, *O.J.L.* 17 July 2000, 178, 1–16.
[49] Dir.EP and Council no. 2005/29/EC, 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No. 2006/2004 of the European Parliament and of the Council, *O.J.L.* 11 June 2005, 149, 22–39.
[50] The European Commission encourages the set-up of common standards and interoperability in order to reduce fragmentation. (Green Paper (Comm.) *Mobile payments*, 16.) For a detailed overview of SEPA-interoperability standards: S. DE BROUWER, *Navigating the labyrinth*, 54 and the website of the EPC.
[51] Another important piece of legislation in this package is the Interchange Fee Regulation. (Reg.EP and Council no. 2015/751/EU, 29 April 2015 on interchange fees for card-based payment transactions, *O.J.L.* 19 May 2015, 123, 1-15)
[52] Green Paper (Comm.) *Mobile payments*, 25p.
[53] For instance, under PSD1, providers of electronic communications' networks or services, including MNOs, were not covered where they acted as intermediaries, no matter the kind or value of purchases. Since those payment activities

European Commission concluded from the consultations of the field that these incongruences brought uncertainty for customers that were increasingly paying online, e.g. through their smartphone. This also led to competitive distortions, which hindered innovation.[54]

The scope of the revised PSD is still the provision of payment services[55], such as cash withdrawal and placement, transactions funded by payment account or credit line, the issuance of payment instruments and money remittance. A list of payment services is provided in the annex of the directive. Paper-based transactions like cash and cheque transactions are explicitly excluded.[56] Unlike PSD1, PSD2 applies to payments in all currencies, and, moreover, also when only one actor is based in the EEA (the so-called "*one-leg in*" transactions).[57]

One of the main objectives was the creation of a level playing field for PSPs. Therefore, PSD2 limits the exemptions and introduces two new payment institutions: Payment Initiation Service Providers (PISPs) and Account Information Service Providers (AISPs). These new services currently fall under the prudential regime[58], though it is a lighter one[59], in line with the risks they represent.[60] The fact that providers of these services have to comply with transparency obligations leads to more customer protection.[61]

A Payment Initiation Service (PIS) is defined as "*a service to initiate a payment order at the request of the payment service user with respect to a payment account held at another PSP*"[62], the Account Servicing Payment Service Provider (ASPSP)[63]. Customers with a payment account that is accessible

---

often comprise significant payment volumes and values and offer to customers a range of different products and services, was it against the *ratio legis* that these fell outside the scope of PSD.

[54] Rec. 4 PSD2.

[55] Art. 2, (1) PSD2.

[56] Art. 3, (a) and (g) PSD2.

[57] However, with a lower degree of transparency obligations for the non-EU actor (art. 2, art. 3 and art. 4 PSD2).

[58] They need an authorisation of the competent authority in their home Member State (art. 5, (1) PSD2) and have to comply with minimum capital requirements.

[59] As they do not hold the funds of customers. For PISPs, there is an initial capital requirement of € 50,000 (art. 7, (b) PSD2). For AISPs there is none.

[60] C. RIEFA, *Electronic payments*, 156.

[61] Other issues of consumer protection aimed at by PSD2 are the increase of information requirements and the allocation of obligations and liabilities to the involved stakeholders, and the prohibition of surcharging. For further information: C. RIEFA, *Electronic payments*, 167-172.

[62] Art. 4, (15) PSD2.

[63] A payment account means an account held in the name of one or more payment service users which is used for the execution of payment transactions (art. 4, (12) PSD2). Thus, an ASPSP is typically a bank, that opens accounts for their clients to enable them to receive and initiate payments. (T. THYS, S. VAN RAEMDONCK and K. DESMET, *GDPR, PSD2 and the repurposing of data*, 185.)

online have the right to use a PIS.[64] This service provides merchants and customers with the possibility to initiate internet payments based on a credit transfer. Such services operate between merchants and customers' banks. Through this service, customers can shop online without a payment card.[65] This could imply a low-cost solution for both merchants and customers.[66] Many digital (both mobile and web-based) wallets offer this kind of service.[67]

To execute the payment, the PISP accesses its users' bank account, with the identity and security information (the credentials) of its users. To ensure the availability of the funds, the PISP has to ask the ASPSP confirmation before the execution of the payment, which can only result in a simple yes or no answer.[68]

The PISP can only execute a payment with explicit consent of the customer.[69] The form of the explicit consent needs to be agreed between the payer and the PSP.[70] Consent can always be withdrawn for future payments.[71]

PISPs may, at no time, hold the payer's funds in connection with the service, store sensitive payment data[72] of the service user, request any other data beyond what is necessary to provide the service, use, access or store any data for purposes other than providing the PIS or modify the amount, payee or any other feature of the transaction.[73] Every time a payment is initiated, the provider must identify itself to the payer's ASPSP and must communicate with this service and with the payer and payee securely.[74]

[64] Art. 66, (1) PSD2.
[65] Rec. 29 PSD2.
[66] P.E. BERGER, I. VAN BIESEN and S. LIEBAERT, *De impact van PSD II*, 125.
[67] S. DE BROUWER, *Navigating the labyrinth*, 51.
[68] Art. 65 PSD2.
[69] Art. 64, (1) PSD2.
[70] Art. 64, (2) and (4) PSD2.
[71] Art. 64, (3) PSD2.
[72] Art. 4, (32) PSD2: Sensitive payment data means data, including personalised security credentials which can be used to carry out fraud. For the activities of PISPs and AISPs, the name of the account owner and the account number do not constitute sensitive payment data. According to the ECB, sensitive payment data include "*data enabling a payment order to be initiated, data used for authentication, data used for ordering payment instruments or authentication tools to be sent to customers, as well as data, parameters and software which, if modified, may affect a legitimate party's ability to verify payment transactions or control the payment account*". (ECB, *Draft recommendations for the security of mobile payments*, 5.)
[73] Art. 66, (3), (a), (e), (f) and (g) PSD2.
[74] Art. 66, (3), (d) PSD2.

They must ensure that personalised security credentials[75] are not made accessible to parties beyond the service user, and the security credentials issuer, and that these are transmitted through safe and efficient channels, to ensure that any other information obtained about the user is only provided to the payee and then only with the user's explicit consent.[76]

Service providers also have informational obligations. They must provide the payer and, where applicable, the payee with a confirmation of the successful initiation of the payment order, a reference enabling the transaction to be identified and information on the amount of the payment and any applicable charges.[77]

As PSD2 establishes a right for PISPs to access their users' payment accounts, there is no contract necessary between the PISP and the ASPSP. Member States have to ensure this right to access in an objective, non-discriminatory and proportionate way.[78] Rules restricting access can go no further than necessary to safeguard the users against specific risks, such as settlement risk, operational risk and business risk, and to protect the financial and operational stability of the payment system. Rules that discriminate between PSPs are prohibited.[79]

BERGER et al. point at the fact that during the trialogue legislative negotiations, the European Parliament intended to amend the proposal by explicitly excluding digital wallets from the scope of the revised directive. The amendment was not accepted. The authors believe that this may raise confusion as to whether mobile wallets are currently in- or excluded from the scope. They conclude that mobile wallet issuers are only considered PISPs when they can connect with an account. Otherwise, they are regarded as technical service providers and thus exempted from the scope of PSD2.[80]

An Account Information Service (AIS) is defined as "*an online service to provide consolidated information on one or more payment accounts held by the payment service user with either another*

[75] Art. 4, (31) PSD2: Personalised security credentials means personalised features provided by the PSP to a payment service user for the purposes of authentication.
[76] Art. 66, (3), (b) and (c) PSD2.
[77] Art. 46 PSD2.
[78] Art. 35 and art. 36 PSD2.
[79] Art. 35 PSD2.
[80] P.E. BERGER, I. VAN BIESEN and S. LIEBAERT, *De impact van PSD II*, 126.

PSP or with more than one PSP"[81]. It enables payment service users to have an overall, immediate view of their financial situation at any given moment through an online interface.[82] This access should not be blocked nor hindered by the ASPSP and should be provided proportionately.

The AISP has the right to access payment accounts, though to a lesser extent than the PISP, namely only with an explicit consent of the customer and only when the information is necessary for the service.[83] AISs are less relevant in the context of mobile wallets.

The controversy of the expansion lies in the concern of banks that non-financial market players are taking over a part of their market share. Payment services are the primary source of income for banks.[84] However, no legal restriction stops banks from providing PISs and AISs themselves. This would allow banks to obtain more personal data of their clients, originating from their competitors. As a result, banks can keep, and even enforce their competitive advantage in this highly data-driven industry.[85] Still, the concern revolves around the fact that banks are lacking the data-handling technology that some Fintechs dispose of and banks are highly cost-driven organisations.[86]

Moreover, banks are concerned that mandatory access to TPPs could lead to increased security incidents and data breaches. The abovementioned 2018 Ticketmaster data breach shows that a collaboration with third parties enhances risks.

c. Security and safety of payments under PSD2

i. Introduction

An essential driver of the European Commission for the reform was the enhancement of payment security and customer trust. It is argued that without safe, secured, and vital payment services, a payments market can hardly exist.[87] Since banks are now obliged to ensure that third party PSPs

[81] Art. 4, (16) PSD2.
[82] Rec. 28 PSD2.
[83] Art. 67 PSD2.
[84] P.E. BERGER, I. VAN BIESEN and S. LIEBAERT, *De impact van PSD II*, 127.
[85] T. THYS, S. VAN RAEMDONCK and K. DESMET, *GDPR, PSD2 and the repurposing of data*, 184.
[86] F. ZUNZUNEGUI, *Digitalisation of Payment Services*, 23.
[87] Rec. 7 PSD2: In recent years, the security risks relating to electronic payments have increased. This is due to the growing technical complexity of electronic payments, the continuously growing volumes of electronic payments

have access to their clients' payment accounts, banks are exposed to new risks in terms of data security and data protection. Liability issues in case of non-authorised transactions will arise.[88] PSD2 introduces legal requirements for security measures and authentication.

Like in other recent EU (technology) legislation[89], the technology neutrality principle is embedded in the provisions of PSD2. Technology neutral legislation is legislation drafted without aiming at a specific type of technology. The same regulatory policy should be applied to all kinds of technology.[90] Also, in PSD2, the European legislator does not want to preclude any technology, to prevent the disruption of innovation in payment services.[91]

Although PSD2 is not a regulation, it harmonises to no small extent. An important factor contributing to this is the involvement of the European Banking Authority (EBA)[92]. The EBA was mandated to develop guidelines on security measures and Regulatory Technical Standards (RTS) in collaboration with the European Central Bank (ECB) and after consulting all relevant stakeholders.[93] These guidelines bind the supervising competent authorities of the Member States.[94]

ii. Incident assessment and reporting

In terms of security measures, PSPs are firstly obliged to establish and maintain effective incident management procedures, in line with the risks embedded.[95] Secondly, major operational or security incidents need to be reported to the competent authority without undue delay. Where the incident has or may have an impact on the financial interests of the user, the PSP must inform the latter, without undue delay, of the incident and of all the measures they can take to mitigate the adverse

worldwide and emerging types of payment services. Users of payment services should therefore be adequately protected against such risks. Payment services are essential for the functioning of vital economic and social activities.

[88] S. DE BROUWER, *Navigating the labyrinth*, 52.

[89] For instance: e-Commerce Directive.

[90] C. RIEFA, *Electronic payments*, 163-165. The author underlines that the application of this principle has not always been easy. Under PSD1, this has led to inconsistencies. PSD2 addresses them.

[91] Rec. 21 PSD2: The definition of payment services should be technologically neutral and should allow for the development of new types of payment services, while ensuring equivalent operating conditions for both existing and new PSPs.

[92] Established by Reg.EP and Council No. 1093/2010/EU, 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No. 716/2009/EC and repealing Commission Decision 2009/78/EC, *O.J.L.* 15 December 2010, 331, 12-47.

[93] Art. 15, art. 95 and art. 98 PSD2.

[94] M. DONNELLY, *Payments in the digital market*, 829.

[95] Art. 95, (1) PSD2.

effects of the incident.[96] Thirdly, PSPs have to transmit a security assessment of the measures and control mechanisms to the competent authority on a yearly basis.[97] The EBA was mandated to issue guidelines on both the security measures and incident reporting.[98]

The EBA had already built up expertise with the guidelines on the security of internet payments in 2014.[99] This was before the adoption of the revised PSD, given to the urgency where fraud risks had to be mitigated. It is worth to note, however, that, except for mobile payments conducted over mobile internet using a standard web browser via a mobile device, mobile payments are explicitly excluded from the scope of these guidelines. For the latter, there are the draft recommendations for the security of mobile payments, developed by the European Forum on the Security of Retail Payments (Secure Pay) of the ECB in 2013.[100] In this document, the minimum requirements for mobile payment services are laid down, based on three technologies: contactless payments (e.g. NFC technology), payments using a mobile payment application (e.g. mobile wallets) and payments using MNO's channels (e.g. SMS). In this proposed recommendation, mobile payment providers should act in accordance with the following guiding principles:

- Identify, assess and mitigate the risks embedded with their services;
- Implement strong authentication mechanism;
- Protect customer's data both in transit and at rest;
- Employ secure management for authorisation and monitor transactions in order to prevent fraud;
- Provide information on security issues to customers and engage in customer education.

However, these security requirements were difficult to apply as mobile payment providers are varied, and especially smaller companies have less expertise in security issues. Moreover, at the time of the issuance of these draft recommendations, PSD2 was not yet adopted, so some of the PSPs were not appropriately regulated.[101] The European Payment Council (EPC) was of the opinion that these proposed recommendations were too rigid and would hinder the development of mobile payments. It stated that an "*adequate balance between usability and security is critical for the success of any payment method*".[102]

[96] Art. 96 PSD2.
[97] Art. 95, (2) PSD2.
[98] Art. 95, (3) and art. 96, (3) PSD2.
[99] EBA, *Final guidelines on the security of internet payments*, 42 p.
[100] ECB, *Draft recommendations for the security of mobile payments*, 26 p.
[101] S. KASIYANTO, *Security issues of new innovative payments*, 175.
[102] EPC, *Comments on the draft recommendation for the security of mobile payments*, 1.

The EBA published its final report on security measures on 12 December 2017 and on incident reporting on 27 July 2017. The EBA now uses the proportionality principle as its general principle. All PSPs should comply with all the provisions set out in the guidelines, but the level of detail should be proportionate to the PSP's size and to the nature, scope, complexity and riskiness of the particular services that the PSP provides.[103] Relevant for this thesis is the fourth guideline, "*protection*", under which "*PSPs should ensure the confidentiality, integrity and availability of their critical logical and physical assets, resources and sensitive payment data of their PSUs whether at rest, in transit or in use. If the data include personal data, such measures should be implemented in compliance with the data protection framework*".[104]

iii. Strong customer authentication

As we have seen in the first chapter, more and more attacks involve customers security credentials. This means that a secure authentication system is indispensable. Authentication through single passwords has been proven weak and unsafe.

PSD2 introduces the obligation for PSPs to apply strong customer authentication mechanisms when initiating online payments or accessing payment accounts.[105] In case of an unauthorised payment, the payer can claim full reimbursement from his PSP if there was no strong customer authentication measure in place.[106]

Strong customer authentication is defined as an authentication based on the use of two or more elements categorised as knowledge (something only the user knows, e.g. a PIN code or a password), possession (something only the user possesses, e.g. a card or a mobile phone) and inherence (something the user is, e.g. biometric identification like fingerprint, iris or voice recognition). These elements must be independent of each other, in that the breach of one does not compromise the

[103] EBA, *Guidelines on the security measures under PSD2*, 17.
[104] *Ibid.*, 19.
[105] Art. 97, (1) PSD2. As such, strong customer authentication is not a new technique as it is already widespread in the brick-and-mortar shops, where customers are required to validate a transaction by typing their PIN codes on card readers.
[106] Art. 74, (2) PSD2.

reliability of the others.[107] The combination of these elements must lead to an authentication code, which can only be used once.

The independence of the elements focuses primarily on mobile app security.[108] When a mobile phone is used, both to give the instruction for the payment and to be part of the authentication mechanism, the risks are omnipresent. In its abovementioned "*Draft recommendations for the security of mobile payments*", the ECB recommended that when a mobile device is used as one of the strong customer authentication factors, i.e. something only the user possesses, security measures must be implemented at the mobile device level to ensure that the second factor cannot be easily breached due to the use of the mobile device.[109]

Particularly, for remote payment transactions, strong authentication needs to include elements that dynamically link the transaction to its specific amount and the beneficiary of the payment. Dynamically linking refers to the creation of a one-time-password. This is *de facto* three-factor authentication. The code is not valid when it does not correspond. This is to protect the integrity of the payment order[110], which means that it minimises the risks in case of fraud.[111]

PSPs have the right to use the procedure that is put in place by the banks but can also decide to use their own authentication procedures. This is in line with the goal of PSD2 to enhance the development of user-friendly means of payments.[112] When using their own authentication procedures, PSPs have to apply strong customer authentication too.

In accomplishment with its mandate[113], the EBA published its report on RTS on 23 February 2017. This document was in an amended version published by the European Commission on 13 April 2018 and will come into force in September 2019. Thus, the payment industry has 18 months to prepare for this new regulation.

---

[107] Art. 4, (30) PSD2.
[108] Rec. 6 RTS.
[109] ECB, *Draft recommendations for the security of mobile payments*, 5.
[110] P.T.J. WOLTERS and B.P.F. JACOBS, *The security of access to accounts under the PSD2*, 40.
[111] C. RIEFA, *Electronic payments*, 166.
[112] P.T.J. WOLTERS and B.P.F. JACOBS, *The security of access to accounts under the PSD2*, 38.
[113] Art. 98 PSD2. The EBA had to develop the requirements of the strong customer authentication and define the exemptions (based on the level of risk, the amount and/or recurrence of the transaction and the payment channel used for the execution of the transaction), the requirements of the security measures concerning the users' personalised security credentials and the requirements for common and secure open standards of communication between ASPSPs, PISPs, AISPs, payers and payees. This needs to be reviewed and updated by the EBA on a regular basis in order to take account of innovation and technological developments.

The RTS foresee in exemptions on the application of strong customer authentication. Among the exemptions[114] are low-value remote payments and contactless card payments.[115] This is to enhance the customer usability of those innovative techniques. Another exemption concerns the creation by the payer of a list of trusted beneficiaries.[116] One could wonder whether the PSP itself could be listed as a trusted beneficiary. If that is the case, the authentication will only have to be performed only once for all further payments through that PSP. This would lead to an extreme wide-ranging exemption, practically evading the strong customer authentication requirement.[117] The interpretation of these exemptions will become more clear in practise.

iv. Application Programming Interfaces

Application Programming Interfaces (APIs) are communication gateways between banks and TPPs. They constitute a set of protocols and communication tools between computer applications. Through APIs, customers can choose which data are shared with TPPs.[118]

Before the revision, PISPs used the screen scraping technique. Screen scraping is a form of direct access to the customers' account through the customers' interface with the use of their security credentials, such as the PIN code. PISPs logged in as if they were the users themselves. This is an important source for data mining and thus a risk for privacy. Leakage of customers' data brings liability, especially for banks. As soon as that the European legislator and the European Court of Justice started to attach more importance to data protection, banks were reluctant to allow those companies access to customers' accounts.[119]

[114] Other exemptions include low risk payments such as unattended payment terminals for transport fares and parking spots, etc.
[115] Art. 16 RTS. Low value remote payments up to € 30 (except when a cumulative value of € 100 is reached or for 5 recurrent payments of € 30), contactless card payments up to € 50 (except when a cumulative value of € 150 is reached or for 5 recurrent payments of up to € 50).
[116] Art. 13 RTS.
[117] EPC, *Interview with Scott McInnes*, question 2.
[118] F. ZUNZUNEGUI, *Digitalisation of Payment Services*, 26.
[119] *Ibid.*, 30.

To ensure the confidentiality of the messages, PSD2 states that PSPs and banks have to communicate securely with each other.[120] Screen scraping is no longer allowed.[121] Banks can choose whether to adapt their customer online banking interface, i.e. a more secure and sophisticated version of screen scraping[122], or to create a new dedicated interface (an API) that needs to contain all the necessary information for the PSPs.[123]

However, third party providers lobbied against the strict prohibition of the screen scraping technique.[124] They were worried that they would lose their right to access in case of malfunction of the dedicated interface. The EBA explicitly amended the RTS by adding that banks have to ensure that the dedicated interface offers the same level of availability and performance, including support, as the customers' online interface. Besides, as a result of the lobbying, a fall-back mechanism has to be created, which means that screen scraping can still be used in case of failure of the system.[125] Banks can only be exempted of this latter obligation if the dedicated interface complies with all the obligations, has been tested by the PSPs and has been used for at least three months and any problems have been resolved without undue delay.[126]

v. Intermediate conclusion

The question remains, however, whether PSD2 brought the solution for the complex mobile payment ecosystem.

DE BROUWER states that PSD2 brought a solution for mobile wallets, in the sense that one of the significant barriers, the resistance of banks to provide TPPs access to the bank accounts of their customers, has been removed by regulating those services.[127] This could promote the development

[120] Art. 66, (3), (b) and (d), art. 66, (4), (a) and art. 67, (2), (b) and (c).
[121] EBA, *Report on RTS*, 46.
[122] Art. 30, (1) RTS states that the interface must enable the providers to identify themselves, to request and receive information on one or more designated accounts and associated transactions and to initiate a payment order.
[123] Art. 31 RTS.
[124] P.T.J. WOLTERS and B.P.F. JACOBS, *The security of access to accounts under the PSD2*, 36.
[125] Art. 33, (4) RTS; EBA, *Report on RTS*, 110-112.
[126] Art. 33, (6) RTS.
[127] S. DE BROUWER, *Navigating the labyrinth*, 51.

of innovative mobile and internet payments. The processing of transaction data remains, however, fragile as it "*will only be as secure as its weakest link*".[128]

BOTT and MILKAU discuss in their article of 2014 whether mobile wallets and current accounts can be "*friends*" or whether they will remain "*foes*". They explain that the initiatives on finding innovative ways to exchange payment transactions came from merchants and companies (e.g. through coupons and rebates). Banks never had a monopoly on the so-called "*shopping experience*" and, by providing a secure and stable platform for the liquidity, they have always been the trusted partners of merchants and companies.[129]

BOTT and MILKAU underline, however, that coexistence and collaboration can only work when PSPs operate in a well-governed environment with clear rules set by regulators, providing a level playing field. The dynamics of cooperation and coexistence will be driven by convenience for customers. Security and trust are, therefore, indispensable.[130]

GIMIGLIANO concludes that the negative scope of PSD has improved but not extensively modified.[131] The author believes that regulatory consistency can be achieved by self-regulation, though she underlines that the original mandate of the EBA does not cover consumer and data protection issues.[132]

WOLTERS and JACOBS argue that PSD2 gave ultimately a higher priority to the development of the market for payment services than to security and privacy.[133] They refer, amongst others, to the fact that the screen scraping technique has not been abolished entirely after lobbying by the TPP field.

I see the point of the authors who question whether the security measures in PSD2 are sufficient. The business model of some of the TPPs is built on the collection of data and its further processing, e.g. for advertising purposes. However, I believe that the RTS, and especially the obligation to apply strong customer authentication, is a - solid - step forward in the protection of personal data. Before the revision, TPPs were operating in a legal vacuum. With strong customer authentication and API,

[128] *Ibid.*, 52.
[129] J. BOTT and U. MILKAU, *Mobile wallets and current accounts: friends or foes?*, 293.
[130] *Ibid.*, 297-298.
[131] G. GIMIGLIANO, *Mobilizing payments*, 85.
[132] *Ibid.*, 87.
[133] P.T.J. WOLTERS and B.P.F. JACOBS, *The security of access to accounts under the PSD2*, 29-41.

the (minimum) standard is set for the development of TPP businesses. The latter are now obliged to invest in security measures compliant to the state of the art, including incident reporting, and they are also subject to the supervision of both the financial and data protection authorities.

In this chapter, I gave an introduction to the revised PSD. I analysed the shortcomings of the repealed PSD in the context of mobile wallets, and I pointed at the changes. Aside from the introduction of two new regulated services, the enhanced security measures are of significant importance. In the following chapter, I will analyse where those assets also contributed to an enhanced data protection of the mobile wallet user.

3. Data protection in mobile wallets

a. Interaction between PSD2 and GDPR

The scope of GDPR is the processing of personal data in general. It is a horizontal legislation that is principally applicable to all sectors. Whereas, PSD2 focuses only on data processed by PSPs. It is a sector-specific legislation. Therefore, one could presume that PSD2 is *lex specialis* and prevails.[134]

A more in-depth view of other provisions in PSD2, however, may lead to a different conclusion. Article 94 PSD2 states in its first paragraph explicitly that the processing of personal data for PSD2 "*shall be carried out in accordance with (the repealed)[135] Directive 95/46/EC, the national rules which transpose Directive 95/46/EC and with Regulation (EC) No 45/2001.*" Moreover, recital 89 PSD2 states that the legislations mentioned above apply to the processing of personal data for the purposes of PSD2. Furthermore, recital 29 PSD2 states that the new rules should correspond to legal issues like the protection of the payment service users' data in accordance with GDPR.[136] THYS et al. conclude that as for the processing of personal data, both GDPR and PSD2 have to be applied "*on the same level*".[137]

This discussion is of significant importance for the interpretation of numerous provisions of PSD2. As we will see in the following chapters, compliance with both PSD2 and GDPR is not always straightforward and will need to be clarified further in the future.

b. What are the personal data processed in mobile wallets?

Mobile wallet issuers can collect various kind of data. The Payment Systems Regulator (PSR)[138] devises in its discussion paper "*Data in the payments industry*" payment data into two groups: on

[134] T. THYS, S. VAN RAEMDONCK and K. DESMET, *GDPR, PSD2 and the repurposing of data*, 185.
[135] Art. 94 GDPR states that references to the repealed Directive 95/46/EC shall be construed as references to GDPR.
[136] The EDPB is also of the opinion that the interpretation and the implementation of the articles in the PSD2 have to be made in the light of GDPR. (EDPB, *Letter PSD2*, 2.)
[137] See also T. THYS, S. VAN RAEMDONCK and K. DESMET, *GDPR, PSD2 and the repurposing of data*, 185.
[138] The PSR is formally established by the UK Financial Services (Banking Reform) Act 2013. It works independently from the UK Government and is funded by the industry.

the one hand data collected as part of the core payment service and on the other hand ancillary data that are not always necessary to process the payment but may be collected while processing.[139]

Data that form the core of a payment transaction are[140]:

- Data about the identity of payers: names, telephone numbers, email addresses;
- Sort codes and account numbers of both the payers and the payees;
- Reference information for payments;
- Date and time of payments;
- Primary Authorisation Numbers (PAN) for card transactions (cardholder number).

Ancillary data are[141]:

- The location where payments were made;
- Information about the channel through which payments were made;
- Information about the device: mobile device identification numbers, IP addresses and cookies for online payments;
- Usage data such as the frequency with which customers log on to their online/ mobile banking or payments accounts.

Some of these data constitute personal data. GDPR defines personal data as any information relating to an identified or identifiable natural person, the data subject.[142] If a natural person cannot be identified directly by this information, it does not mean that the information does not contain personal data. Data also qualifies as personal data if an individual can be singled out by this information, either by the controller or by another person to whom this information is disclosed. Thus, the qualification of personal data depends on the specific context of the processing.[143]

As we have seen in the first chapter, mobile wallets are applications on smart devices. The Article 29 Data Protection Working Party (Working Party 29) underlines in its opinion on apps on smart devices[144] that many data on mobile devices are personal data given the individual nature of mobile

[139] PSR, *Data in the payments industry*, 16-17.
[140] *Ibid.* 17.
[141] *Ibid.*
[142] Art. 4, (1) GDPR.
[143] This requires an assessment by the controller, taking into account the costs and time required for identification, taking into consideration the available technology at the time of the processing. (Rec. 26 GDPR; FRA, *Handbook on European data protection law*, 83.)
[144] Working Party 29, *Opinion on apps on smart devices*, 8-9.

devices. This means that not only data stored on the device that are personal by nature are considered personal data, but also data related to the device itself.[145] The Working Party 29 highlighted some examples of data accessible by applications on smart devices, which can constitute personal data: location data, contacts, unique device and customer identifiers (e.g. IMEI[146] and phone number), credit card and payment data, phone call logs, SMS or instant messaging, browsing history, e-mail, information society service authentication credentials, pictures, videos and biometrics (e.g. facial recognition and fingerprint templates).[147]

Some of the data as mentioned above are data by which persons can be identified directly (e.g. name) or indirectly (e.g. telephone number, credit card number, mobile device identification numbers, etc.). Whereas other data (e.g. date and time, location data and cookies), when combined with other data (e.g. information about the shops visited and purchases made), can be used to single out individuals based on their behaviour and habits. [148]

Also, not only data relating to the owner of the device are considered personal data, but also data relating to other individuals are. Examples are contact details in the address book and pictures. In the context of mobile payments, these also include the name and account number of beneficiaries.

Under GDPR, some data are classified as special categories of data (formerly called sensitive data).[149] Stricter requirements apply to those data. The use of mobile wallets does not usually result in the processing of special categories of data. It is generally accepted that data about the financial situation of users are not one of those. However, as we will see further in this chapter, the further processing of data obtained through mobile wallets can sometimes reveal sensitive information about people.

[145] ENISA, *Privacy and data protection in mobile applications*, 15.
[146] IMEI stands for International Mobile Equipment Identity. It is a number that identifies the device.
[147] Working Party 29, *Opinion on apps on smart devices*, 8; Working Party 29 refers to rec. 24 e-Privacy directive, that states: *"Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms"*.
[148] PSR, *Data in the payments industry*, 28.
[149]Non-limitative examples of these data are ethnic origin, political opinions, genetic and biometric data for the purposes of uniquely identifying a natural person, health, sexual orientation, etc. (art. 9, (1) GDPR)

Confusingly, PSD2 introduces the term "*sensitive payment data*". PSD2 defines sensitive payment data as data, including personalised security credentials which can be used to carry out fraud.[150] These data are personal since they identify an individual at the moment of the authentication. In its opinion on the proposal for PSD2, the European Data Protection Supervisor (EDPS) recommended to use the term payment data instead of sensitive payment data, but its recommendation did not make it.[151]

Security measures, such as pseudonymisation[152], encryption[153] and tokenisation[154] do not change the personal nature of data. They indirectly refer to the data subject and the controller disposes of the key to undo the security measure. In Apple Pay, for instance, the card number is replaced by a token during the card enrolment. Only this token is stored on the mobile device. During the payment, only the token is sent to the merchant. The PAN and CVV are never used. These are also not exposed to the application processor.[155] That is how Apple complies with the obligations in PSD2 not to store sensitive payment data on the device[156] and to ensure that personalised security credentials are not made accessible to parties beyond the service user and the security credentials issuer.[157] Although this can be seen as a profound security measure, and an example of privacy by design, tokenised data stay personal data.

[150] Art. 4, (32) PSD2; For PISPs and AISPs it does not include the name of the account owner and the account number.
[151] EDPS, *Opinion on a proposal on payment services*, 7.
[152] Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person (art. 4, (5) GDPR).
[153] Encryption means that a mathematical algorithm is used to scramble the payment card data, so that only key owners can read the data. (A. LEVITIN, *The promise and perils of digital wallets*, 23.)
[154] The process of tokenisation replaces the data with a token, i.e. randomly generated substitute data. The creation of one-time account identifiers leads to more secure transactions as it becomes more difficult to engage in credit card fraud. In contrast to encryption, no algorithmic transformations are used. (A. LEVITIN, *The promise and perils of digital wallets*, 29.)
[155] ENISA, *Security of mobile payments and digital wallets*, 12.
[156] Art. 66, (3), (e) PSD2.
[157] Art. 66, (3), (b) PSD2.

c. What stakeholders are involved?

Data protection in mobile wallets is sometimes complex as multiple transfers of data between different systems are involved. As from the moment one of the stakeholders act as a data controller, it has to comply with the corresponding obligations.[158]

Under GDPR, controllers determine the purposes and means of the processing, alone or jointly with other controllers.[159] Processors process on behalf of controllers.[160] The distinction is essential as controllers bear the primary responsibility for the compliance with GDPR.[161] The difference between them is functional, depending on the explicit or implicit legal competence or the factual influence.[162] The relation between them is contractual. In the contracts between controllers and processors, the responsibilities for compliance with GDPR are allocated.

Payers and payees in a P2P transaction are both data subjects. In the scenario where one of those parties is a legal person, GDPR does not apply to the processing of the data concerning that person.[163] Legal persons are currently protected under the e-Privacy Directive, but only on the condition that they are subscribers to a publicly available electronic communications service and only with regards to their legitimate interest.[164] In the proposed reform of the e-Privacy Directive, the protection of both natural and legal persons is extended. The new regulation will also be applicable to over-the-top communication service providers, e.g. providers of mobile wallet apps. This means that businesses that own a mobile device through which they make payments, will be better protected in the future. For instance, if none of the other limited grounds are applicable, information stored on the mobile device relating to those payments can only be processed by the provider with consent of the company.[165] However, discussion has already risen concerning the application of consent by legal persons. Recital 18 of the proposal states that "*consent should have*

[158] S. DE BROUWER, *Navigating the labyrinth*, 56.
[159] Art. 4, (7) GDPR: controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; Art. 26, (1) GDPR states that joint controllers are two or more controllers that jointly determine the purposes and means of processing. They are obliged to determine their respective responsibilities for compliance in a transparent manner.
[160] Art. 4, (8) GDPR: processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
[161] GDPR introduced also a liability regime for processors, e.g. when they process beyond the instructions from controllers.
[162] Working Party 29, *Opinion on the concepts of controller and processor*, 9-12.
[163] Rec. 14 and art. 4, (1) GDPR.
[164] Art. 1, (2) e-Privacy Directive.
[165] Art. 8 Proposal e-Privacy Regulation.

the same meaning and be subject of the same conditions as the data subject's consent (under GDPR)". The Working Party 29 asks for clarification on how the conditions for consent will be fulfilled, in particular how legal persons can be considered to be informed and when there is an expression of will.[166]

In mobile wallets, there are several controllers and processors. Mobile wallet issuers are considered controllers over the personal data necessary to provide the payment service to their customers. They determine if and how they provide this payment service within the context of the PSD2 framework. Once they get access to the account data, they are controllers over those data. Mobile wallet issuers are also considered controllers when they provide additional services, e.g. personalised advertising through which they get in possession of personal data. On the other side of a P2C payment transaction is the merchant. Merchants are considered controllers as for the registration of the payment transaction.[167] They store the purchase details, e.g. name, date and time for the fulfilment of the purchase and administration. TSMs are processors when they only operate on behalf of PSPs.[168] As we have seen in the first chapter, they guarantee that customers' payment credentials are securely transmitted. Other third parties are considered controllers when they are allowed by mobile wallet issuers to access users' data independently (e.g. advertising networks process geolocation data for behavioural advertising). [169]

Examples of processors in mobile wallets are app developers (they deliver apps on behalf of banks or other PSPs), OS and device manufacturers, etc. The latter are (joint) controllers where they process the users' data for their own purposes (e.g. user details at registration).[170]

An exciting discussion concerns the qualification of the relationship between PSPs and banks. As we have seen in the first chapter, PSD2 establishes a right for PISPs to access their users' payment accounts, without being obliged to enter into a contract with the bank.[171] Although banks have to allow PISPs to access the payers' accounts without being able to make any contractual reservation concerning data protection, they keep their obligations as a data controller and they even have to

[166] Working Party 29, *Opinion on the Proposed e-Privacy Regulation*, 28-29.
[167] SIMONT BRAUN, *Mobile wallets*, 1.
[168] *Ibid.*, 2.
[169] Working Party 29, *Opinion on apps on smart devices*, 9-10.
[170] *Ibid.*, 10-11.
[171] Art. 66, (5) PSD2.

demonstrate compliance. This question remains unsolved. At the end of this chapter, I will discuss a possible solution.

d. How are the data obtained?

Under GDPR, personal data shall be processed in a lawful, fairly and transparent manner.[172] To process personal data lawfully, the processing has to comply with one of the six legal grounds set out in article 6 GDPR.[173] Three legal grounds relevant for the thesis are consent[174], the necessity for the performance of a contract to which the data subject is party[175] and the necessity for the purposes of the legitimate interest of the controller or by a third party. [176][177]

In the context of mobile wallets, personal data will primarily be processed on the ground that it is necessary for the performance of the contract. This includes pre-contractual obligations.[178] The Working Party 29 stated in its opinion in 2014 that this needs to be interpreted strictly and has to be distinguished from a contractual condition. It stated that "*(…) the fact that some processing is covered by a contract does not automatically mean that the processing is necessary for its performance.*"[179] The European Data Protection Board (EDPB) worked further on this opinion in its recent "*Guidelines on the processing of personal data under article 6, (1), (b) GDPR in the context of the provision of online services to data subjects*". In the assessment of what is objectively necessary for the performance of a contract, the following questions can be posed:

- What is the nature of the service being provided to the data subject? What are its distinguishing characteristics?
- What is the exact rationale of the contract?

[172] Art. 5, (1), (a) GDPR; Fair processing relates to the specific obligations of the controller towards the data subject, e.g. the obligation to notify the subject of his data being processed and the obligation to comply with the rights of data subjects.
[173] However, the principle of lawful processing is not further defined. It may not preclude the existence of other legal grounds in other applicable laws or even fundamental rights.
[174] Art. 6, (1), (a) GDPR.
[175] Art. 6, (1), (b) GDPR.
[176] Art. 6, (1), (f) GDPR.
[177] Other legal grounds are necessity for compliance with a legal obligation of the controller, e.g. tax purposes (art. 6, (1), (c) GDPR), necessity for the protection of vital interests of either the data subject or another natural person (art. 6, (1), (d) GDPR) and necessity for the performance of a task carried out in the public interest or in the exercise of official authority (art. 6, (1), (e) GDPR).
[178] Art. 6, (1), (b) GDPR.
[179] Working Party 29, *Opinion on the notion of legitimate interests*, 16-17.

- What are the essential elements of the contract?
- What are the mutual perspectives and expectations of the parties to the contract? [180]

The assessment depends on the type of wallet. As seen in the first chapter, wallets differ from traditional payment cards since they establish two-way communication. Aside from to the payment function, some of the wallets provide additional services, e.g. the possibility of storing purchase records to facilitate returns and reimbursements and displaying personalised product suggestions. The assessment needs to be done separately for every service.[181] The payment function is undoubtedly an essential element for the performance of the contract between mobile wallet issuers and their users. After having received users' consent for the installation of the wallet app (assuming a valid contract), mobile wallet issuers do not have to ask for separate consent to disclose the users' name and bank account number to the recipient of the payment. When it comes to personalising content, the processing of personal data may constitute an essential or expected element of the contract. It depends not only on the contractual conditions but also on the way the mobile wallet is promoted to the users.[182] This could be, for instance, the case when the personalised offers are based on a profile that is created by the users themselves, provided the necessary safeguards are respected. Offering personalised advertising based on purchase or browsing history (behavioural advertising) through mobile wallets can, in my opinion, never be considered objectively necessary for the performance of the mobile wallet contract. Data protection is a fundamental right guaranteed by article 8 of the Charter of Fundamental Rights. Once personal data are out of control of the data subject, they cannot be regained.

If mobile wallet issuers want to offer additional services, they have to ask for consent. Consent has to be freely given, informed, specific and unambiguous.[183] Consent is not freely given if the data subject does not have a genuine choice. This is, for instance, the case when goods or services can only be obtained if the customer has to agree on disclosing his data for further use by third parties (e.g. marketing purposes).[184] Information to the data subject has to be given in a clearly distinguishable manner, i.e. in an intelligible and easily accessible form, using clear and plain language.[185] This means separate from other terms and conditions. Specific consent relates to the

[180] EDPB, *Guidelines art. 6, (1), (b) GDPR online services*, 9.
[181] *Ibid.*, 10.
[182] *Ibid.*, 13-14.
[183] Art. 4, (11) GDPR.
[184] FRA, *Handbook on European data protection law*, 145-146.
[185] Art. 7, (2) GDPR.

processing purpose. When the processing has multiple purposes, granular consent is required.[186] Unambiguous means that there cannot be any reasonable doubt that the data subject agreed with the processing of his or her data. It needs to be given using "*a statement or by a clear affirmative action*".[187] According to the Working Party 29, this means that pre-ticked boxes or opt-out boxes are not valid.[188] Consent can always be withdrawn without any detriment to the processing based on the consent.[189]

An exciting discussion concerns the interpretation of the condition "*explicit consent*" in PSD2. The second paragraph of article 94 states that "*PSPs 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*". As discussed above, the PSD2 provisions have to be interpreted in the light of GDPR. However, GDPR provides five other legal bases for the processing of personal data.

The question is, thus, whether PSPs could only process personal data based on explicit consent from the users. GONZALEZ FUSTER noticed this consistency problem in her article "*EU Data Protection and Future Payment Services*" in 2016. She underlined that it would be practically challenging to require freely given, fully and specifically informed consent, especially in the case of sophisticated data processing practices in mobile payments.[190]

In its letter to Ms. in 't Veld, member of the European Parliament, the EDPB has clarified that explicit consent under PSD2 and GDPR are different concepts.[191] According to the EDPB, the second paragraph of article 94 refers to contractual consent. Payment services are always provided on a contractual basis between the payment service user and the provider. The EDPB refers to recital 87 PSD2 that states: "*This directive should concern only contractual obligations and responsibilities between the payment service user and the PSP*". Compared to the legal bases of GDPR, this is similar to the necessity for the performance of a contract to which the data subject is party.[192] The EDPB concludes that explicit consent under PSD2 is an additional requirement of a contractual nature. This means that "*when entering a contract with a PSP under PSD2, data subjects must be made fully*

[186] Rec. 32 GDPR.
[187] Art. 4, (11) GDPR.
[188] Working Party 29, *Guidelines on consent under GDPR*, 16.
[189] Art. 7, (3) GDPR; The data subject must be informed of this right, prior to giving consent.
[190] G. GONZALEZ FUSTER, *EU data protection and future payment services*, 189-190.
[191] EDPB, *Letter PSD2*, 3-4.
[192] Art. 6, (1), (b) GDPR.

aware of the purposes for which their personal data will be processed and have to explicitly agree to these clauses. Such clauses should be clearly distinguishable from the other matters dealt with in the contract and would need to be explicitly accepted by the data subject".[193]

This leads to the conclusion that PSPs need explicit (i.e. contractual) consent to establish the contract, in which they do have to specify the purposes for the processing (and this needs to be done in contractual clauses, distinct from other contractual matters), but they can at the same time base the processing of personal data, not only on consent but also on one of the other legal grounds of GDPR, such as necessity for the performance of a contract and legitimate interest. When basing the processing on the performance of the contract, the PSP does not necessarily need to fulfil the requirements of explicit consent, such as strictly separating the consent from its terms and conditions.[194] There is also no obligation to inform the users of their right to withdraw consent. The notion "*explicit consent*" in PSD2 has thus to be seen as a transparency requirement and not a reference to the conditions for consent under GDPR.[195]

The Dutch supervisory authority for data protection acknowledges that PSD2 consent and GDPR consent are not the same. However, according to the Dutch supervisory authority, the same standards need to be applied to both as adhering different standards would be in breach of the guarantee of article 94, (2) PSD2. It refers to the guidelines of the Working Party 29 on consent and states that all supervisory authorities agreed on a uniform application of the notion of consent.[196] Not only does consent need to be obtained explicitly, separated from other clauses, but users also have the right to withdraw their consent.

e. Data minimisation and security measures

PSD2 mentions at several places that the processing of personal data must be in accordance with the data protection framework, but it does not contain a profound substance to those principles. At the time of reviewing PSD, the legislation process of GDPR was still going on. This can explain why

[193] EDPB, *Letter PSD2*, 4.
[194] T. THYS, S. VAN RAEMDONCK and K. DESMET, *GDPR, PSD2 and the repurposing of data*, 187.
[195] N. VANDEZANDE, *Reconciling consent in PSD2 and GDPR*, 114.
[196] AP, *Advies implementatiebesluit herziene richtlijn betaaldiensten*, 5-6.

there are so little provisions on data protection in PSD2. However, the EDPS stated in its opinion on the proposal for PSD2 that clarifying the applicable data protection legislation is essential but not sufficient. It recommended the addition of concrete safeguards in this regard, e.g. a provision stating that "*mobile operators responsible for the transmission of the transaction order should not have access to content information on the details of payments*".[197] In response to these concerns, few more principles were put under recital 89, though no provision was added. GONZALEZ FUSTER describes this as the "*missing data protection safeguards*".[198]

Recital 89 PSD2 states "*(…) in particular, where personal data is processed for the purposes of this Directive, the precise purpose should be specified, the relevant legal basis referred to, the relevant security requirements laid down in Directive 95/46/EC complied with, and the principles of necessity, proportionality, purpose limitation and proportionate data retention period respected. Also, data protection by design and data protection by default should be embedded in all data processing systems developed and used within the framework of this Directive.*"

The data minimisation principle means that data processing must be adequate, relevant and limited to what is necessary to fulfil the specific legitimate purpose for which they are processed.[199] The processing can only take place when the purpose cannot be fulfilled by other means.[200] This means that the data controller cannot collect more data than necessary.

The Working Party 29 stated in its opinion on apps on smart devices that app developers, when updating the app, should inform users appropriately and provide them opportunities to withdraw from processing by new features or from the entire application. Moreover, it recommends that third parties should not use unique device identifiers for advertising purpose or analytics.[201] Lastly, it advises OSs and device manufacturers to offer an API where app developers can only have access to those data that are necessary for the functionalities of their app.[202]

PSD2 does not provide profound substance to the data minimisation principle. It touches it only briefly in its article 65, which regulates the interaction between PISPs and banks.[203] It states in its

[197] EDPS, *Opinion on a proposal on payment services*, 3-4.
[198] G. GONZALEZ FUSTER, *EU data protection and future payment services*, 192-193.
[199] Art. 5, (1), (c) GDPR.
[200] FRA, *Handbook on European data protection law*, 125.
[201] Working Party 29, *Opinion on apps on smart devices*, 17.
[202] *Ibid.*, 17-18.
[203] G. GONZALEZ FUSTER, *EU data protection and future payment services*, 192-193.

third paragraph that the confirmation of the availability of the amount necessary for the execution of a card-based payment transaction is available on the payment account of the payer, shall consist only in a simple yes or no answer and not in a statement of the account balance. Also, that answer shall not be stored or used for purposes other than for the execution of the card-based payment transaction. Moreover, article 66, (3), (f) PSD2 states that PISPs can only request their users' data necessary to provide the payment service.

In order to be compliant with these provisions, PISPs have to build the data minimisation principle in their authentication procedure. This alludes to data protection by design and data protection by default.[204] This is exactly what the European Commission stated in its green paper.[205]

In PSD2, both principles are reflected in the enhanced secure authentication procedures. PSPs have to apply strong customer authentication.[206]

As noted in the first chapter, PSPs have the right to use the procedure that is put in place by the banks but can also decide to use their own authentication procedures. WOLTERS and JACOBS argue that this multiplies the risks of attacks since more ways of authentication procedures imply an enhanced chance that one of them is compromised.[207]

Moreover, banks cannot verify whether their client gave consent to the access of his or her payment account, and to the disclosure of what specific data he or she has consented to disclose. According to the European Consumer Organisation (BEUC), this makes it impossible for banks to comply with their obligations in the context of GDPR to apply data minimisation and data security.[208] It states that the verification by banks of consent provided to PSPs would be an extra, necessary, layer of security. Also, the EDPB, that was not officially consulted during the development of the RTS, mentioned in its letter to Ms. in 't Veld that authentication and consent must not be confused. Authentication is a technical measure to ensure that the person who has given consent is the legitimate user.[209]

[204] *Ibid.*, 192-193.
[205] Green Paper (Comm.) *Mobile payments*, 19.
[206] Art. 97, (1) PSD2.
[207] P.T.J. WOLTERS and B.P.F. JACOBS, *The security of access to accounts under the PSD2*, 38.
[208] BEUC, *Recommendations to the EDPB on the interplay between the GDPR and PSD2*, 6.
[209] EDPB, *Letter PSD2*, 3-4.

WOLTERS and JACOBS argue in this regard that a possible solution could be to enable banks to require a digital signature from the user. [210] This can be passed on to the PSP and verified by the bank itself. The authors underline that this technology also guarantees the non-repudiation of the payment. As the RTS already implement measures to ensure the confidentiality, authenticity and integrity of the amount, it is an additional safeguard that will only lead to more data security.

In my opinion, this discussion shows that the position of banks towards their data protection obligations, on the one hand, and their obligation under PSD2 to work together with PSPs on the other hand remains unclear. Banks do not have many options to restrict access to the accounts. In the end, banks have to comply with their data security obligations, and they have to demonstrate it. A digital signature would contribute to data security and avoid a risk-averse approach by the banks.

f. Purpose limitation

The purpose limitation principle contains two significant elements.[211] Firstly, any processing of personal data must be done for a specific, well-defined purpose. A specific, well-defined purpose means that the purpose of the collection must be detailed enough to allow the data subject to distinguish the purposes included and not included.[212] The amount of information that needs to be provided is often dependent on the context. The Working Party 29 recommends a layered notice approach, i.e. making the information available in multiple levels of detail, allowing data subjects to find the information they want to read easily (and avoiding information fatigue).[213] This means that critical information which has the most impact on the data subject and could surprise them, is provided in a concise and user-friendly manner on the first layer, while more detailed information, e.g. through hyperlinks. The small screen of a mobile device does not dispose developers of this transparency obligation.[214] Moreover, the purpose must be explicit. Data subjects need to be able to rely on the limitative purpose description in order to trust the party with their personal data. This improves transparency and legal certainty. Lastly, the purpose must be legitimate and this at all

[210] P.T.J. WOLTERS and B.P.F. JACOBS, *The security of access to accounts under the PSD2*, 38.
[211] Art. 5, (1), (b) GDPR.
[212] Working Party 29, *Opinion on purpose limitation*, 15.
[213] Working Party 29, *Guidelines on transparency under GDPR,* 19.
[214] Working Party 29, *Opinion on apps on smart devices*, 23-24.

different stages and times. The purpose limitation principle is closely linked to the notion of consent. The Working Party 29 states that the combination of those two functions as a safeguard to the gradual widening (or blurring) of the purposes after the initial consent was given.[215] It refers to recital 32 GDPR according to which a granular consent is required when the processing has multiple purposes. For each purpose, the controller should provide a separate opt-in.[216]

Secondly, processing for additional purposes must be compatible with the initial purpose. Consequently, further processing requires a compatibility assessment.[217] The Working Party 29 stated in its opinion on purpose limitation that this goes beyond the formal (literal) statements of the provided purpose and the new purpose. It developed a substantive assessment based on the following key factors:

- The relationship between the purposes for which the personal data have been collected and the purposes of further processing (e.g. was the new purpose already implied or a logical next step in the processing?);
- The context in which the personal data have been collected and the reasonable expectations of the data subject as to their further use (e.g. was there initially profound freedom of choice?);
- The nature of the personal data and the impact of the further processing on the data subjects (e.g. does the processing involve special categories of data? May the further processing result in discrimination?);
- The safeguards adopted by the controller to ensure fair processing and to prevent any undue impact on the data subjects (e.g. anonymisation, increased transparency, a possibility to object).

As a result, the processing of personal data for purposes that are not compatible with the initial purpose, require a separate legal base.[218]

No profound provision on purpose limitation can be found in PSD2. The only obligation for PISPs that relate to this principle is the prohibition to use, access or store any data for purposes other

[215] Working Party 29, *Guidelines on consent under GDPR*, 12.
[216] *Ibid*.
[217] Working Party 29, *Opinion on purpose limitation*, 23-27. These criteria were incorporated in art. 6, (4) GDPR.
[218] The exemptions are processing of personal data for archiving in the public interest, scientific of historical research or statistical purposes.

than providing the PIS.[219] However, as we have seen in a previous section, the PSD2 provisions have to be interpreted in the light of GDPR. This raises the question of whether the data can now be used only for that service or whether the PISP can use the data for other purposes. The EDPB states that for further processing of personal data, unnecessary for the performance of the contract, the requirements of consent under GDPR have to be fulfilled.[220]

Mobile wallet issuers may want to offer targeted adverting as an additional service. For instance, everyone that already booked a flight on the internet will remember the advertising for hotels that appear on the screen after the booking. For many PSPs, targeted advertising is the way to keep their business alive. The question raises whether this complies with GDPR and PSD2.[221] Firstly, there is no direct link between the initial purpose (executing a payment transaction) and targeted advertising. Secondly, the context in which the data were collected and the reasonable expectations: Users would not expect their data to be used for targeted advertising. Moreover, users do not necessarily use all the functionalities of a mobile wallet. They also may perceive targeted advertising as an additional service. They would be expected to be asked for consent. Thirdly, concerning the nature of the data, financial data are not considered a special category of data. However, the same does not go for some of the data collected, in particular not for data concerning their visits to LGTB-friendly bars for instance. Although the mobile wallet issuer would not advertise based on the latter data, it will be perceived privacy-intrusive for the users. Lastly, mobile wallet issuers could argue that it would be sufficient to put the possible use of collected data for targeted advertising in their privacy notices. However, this would not change the surprising effect this unwanted additional service has on the users.

In my opinion, targeted advertising would not be compatible with the initial purpose. Consequently, the mobile wallet issuer has to ask for consent for this additional service.

This analysis made clear that mobile wallet issuers can come in possession of special categories of personal data. This is, in principle, prohibited.[222] Exemptions to this prohibition are listed in article 9, (2) GDPR. The most important is explicit consent of the data subject.[223] According to the Working

[219] Art. 66, (3), (g) PSD2.
[220] EDPB, *Letter PSD2*, 4.
[221] For a comparable analysis of a bank that would like to use these data for targeted advertising see: T. THYS, S. VAN RAEMDONCK and K. DESMET, *GDPR, PSD2 and the repurposing of data*, 193-195.
[222] Art. 9, (1) GDPR.
[223] Art. 9, (2), (a) GDPR.

Party 29, this is preferably a written and signed statement.[224] In an online context, explicit consent can be given "*by filling in an electronic form, by sending an email, by uploading a scanned document carrying the signature of the data subject, or by using an electronic signature*". Also, two stage verification can be used.[225] The necessity for the performance of the contract or necessity for legitimate purposes is not exempted.

VEALE and BINNS developed approaches for organisations that want to develop learning systems without becoming in possession of special categories of data.[226] One of the methods is the involvement of a TTP. The organisation collects non-sensitive data of its customers in order to train the model and, simultaneously, the TTP gathers data on the protected characteristics of those individuals. The third party performs an audit based on a comparison of the collected information. Both parties communicate through an API. The authors suggest different players for this role, from private firms to statutory antidiscrimination bodies.

In this case, mobile wallet users who make remote purchases will be directed to the portal of the TTP after the purchase, where they will be asked to give their sensitive data. In the case of wanted marketing based on their purchase history, they may be likely to collaborate. In case of unwanted marketing, this approach will, in my opinion, not be a solution.

[224] Working Party 29, *Guidelines on consent under GDPR*, 18.
[225] For instance, the combination of sending a mail and clicking on a received verification link in the response or filling out a verification code received by SMS.
[226] M. VEALE and R. BINNS, *Sensitive data*, 5-8.

Conclusion

The rise of mobile wallets in recent years resulted in increased security and privacy risks. Therefore, I analysed how the EU legal framework deals with them. The first result of the research was that the revised PSD, through the introduction of the payment initiating service, brought a solution for the legal vacuum that mobile wallet issuers were operating in. The obligation to take appropriate security measures, e.g. on incident reporting, and to apply strong customer authentication, brings mobile wallet issuers into an atmosphere of responsibility for and awareness of the protection of payment data of their users.

As the first result shows, payment data consist of both personal and non-personal data. Security measures, such as encryption and tokenisation, do not change the personal nature of payment data. The absence of profound data protection provisions in PSD2 implies the application of GDPR and e-Privacy Directive provisions on the processing of payment data.

In the light of these results, I analysed how GDPR could be applied on payment data. This led to the following conclusions. Firstly, the notion "*explicit consent*" is different in PSD2 and GDPR. In PSD2, it can instead be seen as a transparency requirement. The condition for PSPs to process payment data with the explicit consent of the user does not prevent PSPs from processing personal data based on other legitimate grounds. However, the necessity for the performance of a contract is limited to services that are essential for the contract. The personalisation of content e.g. through offering coupons and rebates could ultimately be legitimate though only based on a profile that is created by the users themselves. For additional services, consent is required but this needs to be given in accordance with the strict requirements of GDPR.

Secondly, the absence of profound data minimisation provisions in PSD2 leads to legal uncertainty, in particular for banks. In the scenario where PSPs exploit the legitimate possibility to use their own authentication process, banks do not have any control over the fulfilment of the consent requirements of their clients. As a result, banks are facing difficulties in demonstrating compliance with GDPR. The requirement of a digital signature could be a solution to this problem.

Thirdly, further processing by mobile wallet issuers is only possible as far as it is compliant with the assessment criteria under the purpose limitation principle. Targeted advertising is not compliant

with payment services offered by mobile wallets. Mobile wallet issuers should, in particular, be aware that special categories of data could be revealed.

The layered approach of the EU legislator makes it challenging to predict whether the mobile wallet users' data are sufficiently protected now. While the RTS will come into force in a few months, the interaction with GDPR will only become more apparent in the following years.

Further research should be done on data protection and data security issues arising from the incorporation of biometrics into the strong customer authentication process by mobile wallets. The use of biometric data complementary to the use of public key cryptography becomes more and more popular among PSPs. However, compliance with PSD2 and GDPR is not apparent. Questions concern for instance the storage of these data in the mobile device or in the cloud.

Bibliography

Legislation

Reg.EP and Council no. 2016/679/EU, 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC, *O.J.L.* 4 May 2016, 119, 1–88.

Del.Reg.Comm. no. 2018/389, 27 November 2017 supplementing Directive (EU) no. 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication, *O.J.L.* 13 March 2018, 69, 23–43.

Dir.EP and Council no. 2002/58/EC, 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, *O.J.L.* 31 July 2002, 201, 37–47.

Dir.EP and Council no. 2015/2366/EU, 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation 1093/2010/EU, and repealing Directive 2007/64/EC, *O.J.L.* 23 December 2015, 337, 35–127.

Proposal (Comm.) for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC, 10 January 2017, COM(2017)10 final - 2017/0003 (COD).

Green Paper (Comm.). *Towards an integrated European market for card, internet and mobile payments*, 11 January 2012, COM(2011)941 final.

AUTORITEIT PERSOONSGEGEVENS (AP) (THE NETHERLANDS), *Advies implementatiebesluit herziene richtlijn betaaldiensten*, 20 December 2017, https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/20171220_advies_aan_min_fin_implementatiebesluit_psd2.pdf.

Literature

BERGER, P.E., VAN BIESEN, I. and LIEBAERT, S., “De impact van de nieuwe richtlijn betalingsdiensten (PSD II) op de Europese betaalmarkt”, *Tijdschrift voor Belgisch Handelsrecht* 2017, 123-134.

BOTT, J. and MILKAU, U., “Mobile wallets and current accounts: friends or foes?”, *Journal of Payments Strategy & Systems* 2014, 289-299.

DE BROUWER, S, “Navigating the labyrinth of laws applicable to mobile payments: some aspects”, in DAEMS, H., DE MEULENEERE, I., HOUSSA, C. and RAGHENO, N. (eds.), *Digital finance / La finance numérique*, *s.l.*, Anthemis, 2015, 43-57.

DONNELLY, M., “Payments in the digital market: Evaluating the contribution of Payment Services Directive II”, *Computer Law & Security Review* 2016, 827-839.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS AND COUNCIL OF EUROPE (FUNDAMENTAL RIGHTS AGENCY - FRA), *Handbook on European data protection law*, Luxemburg, Publications Office of the European Union, 2018, 399 p.

GEVA, B., "Mobile payments and Bitcoin: concluding reflections on the digital upheaval in payments", in GIMIGLIANO, G. (ed.), *Bitcoin and mobile payments: Constructing a European Union framework*, London, Palgrave Macmillan UK, 2016, 271-287.

GIMIGLIANO, G., "Mobilizing payments within the European Union framework: A legal analysis", in GIMIGLIANO, G. (ed.), *Bitcoin and mobile payments: Constructing a European Union framework*, London, Palgrave Macmillan UK, 2016, 73-88.

GONZALEZ FUSTER, G., "EU data protection and future payment services", in GIMIGLIANO, G. (ed.), *Bitcoin and Mobile Payments: Constructing a European Union Framework*, London, Palgrave Macmillan UK, 2016, 181-201.

KASIYANTO, S., "Security issues of new innovative payments and their regulatory challenges", in GIMIGLIANO, G. (ed.), *Bitcoin and mobile payments: Constructing a European Union framework*, London, Palgrave Macmillan UK, 2016, 145-179.

LEVITIN, A., "Pandora's digital box: the promise and perils of digital wallets", *University of Pennsylvania Law Review*, 2018, 305-394.

RIEFA, C., "Directive 2009/110/EC on the taking up, pursuit and prudential supervision of the business of electronic money institutions and Directive 2015/2366/EU on the control of electronic payments in the EU", in LODDER, A. and MURRAY, A. (eds.), *EU Regulation of E-commerce. A commentary*, Cheltenham, Edward Elgar Publishing Limited, 2017, 146-176.

SIMONT BRAUN, "Mobile wallets and mobile contactless payments – a closer look at data protection", 2015*, www.simontbraun.eu/images/pdf/News/NFC_News_II_versie_ 21mei_2015_2_2.pdf*.

THYS, T., VAN RAEMDONCK, S. and DESMET, K., "GDPR, PSD2 and the repurposing of data: no big deal?", *Bank- en financieel recht*, 2018, 184-196.

TRUYENS, M., "Elektronische betalingen: een praktische verkenning van het juridische landschap" in INSTITUUT VOOR BEDRIJFSJURISTEN (ed.), *Let's go digital – Le juriste face au numérique - De digitale uitdaging van de jurist*, Brussels, Bruylant, 2015, 169-197.

VANDEZANDE, N., *Mobile wallets and virtual alternative currencies under the EU legal framework on electronic payments,* ICRI Working Paper Series 16, 2013, 28 p.

VANDEZANDE, N., "Reconciling consent in PSD2 and GDPR", in THE PAYPERS, *Web fraud prevention, identity verification & authentication guide*, www.thepaypers.com/reports/web-fraud-prevention-identity-verification-authentication-guide-2018-2019/r776368, 2018, 113-114.

VEALE, M. and BINNS, R., "Fairer machine learning in the real world: Mitigating discrimination without collecting sensitive data", *Big Data & Society* 2017, 1-17.

WOLTERS, P.T.J. and JACOBS, B.P.F., "The security of access to accounts under the PSD2", *Computer Law & Security Review* 2019, 29-41.

ZUNZUNEGUI, F., *Digitalisation of payment services*, Ibero-American Institute for Law and Finance Working Paper Series 5, 2018, 33 p.

European Reports

ARTICLE 29 DATA PROTECTION WORKING PARTY (Working Party 29), *Guidelines on consent under Regulation 2016/679*, 10 April 2018, 17/EN, WP 259 rev01, https://ec.europa.eu/newsroom/article29/ document.cfm?action=display&doc_id=51030.

ARTICLE 29 DATA PROTECTION WORKING PARTY (Working Party 29), *Guidelines on transparency under Regulation 2016/679*, 11 April 2018, 17/EN, WP206 rev.01, https://ec.europa.eu/ newsroom/article29/document.cfm?action=display&doc_id=51025.

ARTICLE 29 DATA PROTECTION WORKING PARTY (Working Party 29), *Opinion 01/2017 on the proposed regulation for the e-Privacy Regulation (2002/58/EC)*, 4 April 2017, 17/EN, WP 247, http://ec.europa.eu/newsroom/document.cfm?doc_id=44103.

ARTICLE 29 DATA PROTECTION WORKING PARTY (Working Party 29), *Opinion 02/2013 on apps on smart devices*, 27 February 2013, 00461/13/EN, WP 202, https://ec.europa.eu/justice/article-29/ documentation/opinion-recommendation/files/ 2013/wp202_en.pdf.

ARTICLE 29 DATA PROTECTION WORKING PARTY (Working Party 29), *Opinion 01/2010 on the concepts of "controller" and "processor"*, 16 February 2010, 00264/10/EN, WP 169, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/ 2010/wp169_en.pdf.

ARTICLE 29 DATA PROTECTION WORKING PARTY (Working Party 29), *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, 9 April 2014, 844/14/EN, WP217, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/ files/2014/wp217_en.pdf.

ARTICLE 29 DATA PROTECTION WORKING PARTY (Working Party 29), *Opinion 03/2013 on purpose limitation*, 2 April 2013, 00569/13/EN, WP 203, https://ec.europa.eu/justice/article-29/documentation/ opinion-recommendation/files/2013/wp203_en.pdf.

EUROPEAN CONSUMER ORGANISATION (BEUC), *BEUC's recommendations to the EDPB on the interplay between the GDPR and PSD2*, 11 April 2019, https://www.beuc.eu/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf.

EUROPEAN BANKING AUTHORITY (EBA), *Final guidelines on the security of internet payments*, 19 December 2014, EBA/GL/2014/12_Rev1, https://eba.europa.eu/documents/10180/ 934179/EBA-GL-2014-12+%28Guidelines+on+the+security+of+internet+payments%29_Rev1.

EUROPEAN BANKING AUTHORITY (EBA), *Final report. Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2)*, 12 December 2017, EBA/GL/2017/17, https://eba.europa.eu/documents/10180/2060117/Final+report+on+EBA+Guidelines+on+the+security+measures+for+operational+and+security+risks+under+PSD2+%28EBA-GL-2017-17%29.pdf.

EUROPEAN BANKING AUTHORITY (EBA), *Final report. Guidelines on major incident reporting under Directive (EU) 2015/2366 (PSD2)*, 27 July 2017, EBA/GL/2017/10, https://eba.europa.eu/documents/10180/1914076/Guidelines+on+incident+reporting+under+PSD2+%28EBA-GL-2017-10%29.pdf.

EUROPEAN BANKING AUTHORITY (EBA), *Final Report. Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2)*, 23 February 2017, EBA/RTS/2017/02, https://eba.europa.eu/documents/10180/1761863/Final+draft+RTS+on+SCA+and+CSC+under+PSD2+%28EBA-RTS-2017-02%29.pdf.

EUROPEAN CENTRAL BANK (ECB), *Draft recommendations for the security of mobile payments*, 20 November 2013, https://www.ecb.europa.eu/paym/cons/pdf/131120/recommendationsforthesecurityofmobilepaymentsdraftpc201311en.pdf.

EUROPEAN DATA PROTECTION BOARD (EDPB), *Guidelines 2/2019 on the processing of personal data under article 6(1)(b) GDPR in the context of the provision of online services to data subjects*, 9 April 2019, https://edpb.europa.eu/sites/edpb/files/consultation/ edpb_draft_guidelines-art_6-1-b-final_public_consultation_version_en.pdf.

EUROPEAN DATA PROTECTION BOARD (EDPB), *Letter regarding the PSD2 directive*, 5 July 2018, https://edpb.europa.eu/sites/edpb/files/files/news/psd2_letter_en.pdf.

EUROPEAN DATA PROTECTION SUPERVISOR (EDPS), *Opinion on a proposal for a directive of the European Parliament and of the Council on payment services in the Internal Market amending Directives 2002/65/EC, 2006/48/EC and 2009/110/EC and repealing Directive 2007/64/EC, and for a regulation of the European Parliament and of the Council on interchange fees for card-based payment transactions*, 5 December 2013, https://edps.europa.eu/sites/edp/files/publication/13-12-05_opinion_payments_en.pdf.

EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA), *Security of mobile payments and digital wallets*, 19 December 2016, https://www.enisa.europa.eu/publications/mobile-payments-security.

EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA), *Privacy and data protection by design – from policy to engineering*, 12 January 2015, https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design.

EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA), *Privacy and data protection in mobile applications. A study on the app development ecosystem and the technical implementation of GDPR*, 29 January 2018, https://www.enisa.europa.eu/ publications/privacy-and-data-protection-in-mobile-applications.

EUROPEAN PAYMENTS COUNCIL (EPC), *White paper mobile wallet payments*, 21 January 2014, EPC 163-13, https://www.europeanpaymentscouncil.eu/sites/default/files/KB/files/EPC163-13%20v2.0%20White%20Paper%20Mobile%20Wallet%20Payments.pdf.

EUROPEAN PAYMENTS COUNCIL (EPC), *Comments on the draft recommendation for the security of mobile payments developed by the European Forum on Security of Retail Payments*, 29 April 2014, https://www.europeanpaymentscouncil.eu/news-insights/insight/epc-comments-draft-recommendations-security-mobile-payments-developed.

EUROPEAN PAYMENTS COUNCIL (EPC), *The European Commission's final RTS: Some issues remain unclear. Interview with Scott McInnes*, 6 December 2017, https://www.europeanpaymentscouncil.eu/news-insights/insight/european-commissions-final-rts-some-issues-remain-unclear.

PAYMENT SYSTEMS REGULATOR (PSR) (UK), *Discussion paper: Data in the payments industry*, June 2018, DP 18/1, https://www.psr.org.uk/sites/default/files/media/PDF/PSR-Discussion-paper-Data-in-the-payments-industry-June-2018.pdf.

Websites

www.pcisecuritystandards.org.

www.europeanpaymentscouncil.eu.

www.psr.org.uk.