DOES THE SAME WORD MEAN THE SAME THING?

AN EXPLORATION OF THE NOTION OF CONSENT IN PSD2 AND GDPR

Master Thesis – Law & Technology

Alja Poklar
Student number: 1277868, ARN:114408
2018/2019
August 2019
Supervisor: Mara Paun
Second supervisor: Inge Graef

Contents

1. Chapter 1 (Introduction)

1.1. Background

"Those who expect moments of change to be comfortable and free of conflict have not learned their history."[1] The words of the American historian Joan Wallach Scott can be translated to many areas of modern society. The vast development of the new technologies has introduced many changes. The recent digitalization has changed the way business is conducted. More particular, the technological transformation discussed in this thesis has changed the playing field of the financial payment services as we knew it.[2] Consequently, the industry players and regulators need to align to these changes as well.[3] In response, big steps have been made by the EU regulators in enacting legislations that aim to govern technology. From the implementation of the EU Regulation on data protection ("GDPR") to the evolution of the EU Second Payment Service Directive ("PSD2"), change is everywhere.[4]

Digital business, particularly in banking and financial industry is facing developments in terms of the extended ecosystem.[5] In a response to the new players that have entered the financial-payment market in the past years and were previously not part of the regulated payment infrastructure, the Payment Service Directive had to be revised.[6] This lead to the adoption of PSD2 which among other, accommodated those developments and introduced new roles, such as the Third Party Providers.[7] PSD2 mandates the banks to provide access to accounts to regulated third party providers. Based on the payment data, these providers deliver new and innovative services. This implied that payment services are no longer only executed by banks. PSD2 lists three types of such providers, in particular financial technology companies[8]: Account Information Service Provider, Payment Initiation Service Provider and Account Servicing Payment Service Provider.[9] Payment Initiation Service Provider initiates payment order in the customer's bank at the request of the customer.[10] Account information service provider displays

[1] Coy H. Johnston, *Careers in Criminal Justice* (2nd edition, SAGE Publications, 2018)
[2] Thomas F. Dapp, 'Fintech reloaded – Traditional banks as digital ecosystems' (Deutsche Bank Research , 9 June 2019) < https://www.dbresearch.com/PROD/RPS_EN-PROD/PROD0000000000451937/Fintech_reloaded_%D0_Traditional_banks_as_digital_ec.PDF> accessed 25 May 2019
[3] Simon Grima, 'The Payment Services Directive 2 and Competitiveness: The Perspective of European Fintech Companies' (2018) XXI(2):5-24 European Research Studies
Journal <https://www.researchgate.net/publication/323114264_The_Payment_Services_Directive_2_and_Competitiveness_The_Perspective_of_European_Fintech_Companies> accessed 10 June 2019
[4] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC *OJ L 337*
Regulation (EU) 2016/679 of the European Parliament and of the Council of 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 (General Data Protection Regulation) *OJ L 119*
[5] Bruno Cambounet, 'PSD2 and Open Banking: Defining your role in the digital ecosystem' (Finextra, 2016) < https://www.euroforum.nl/media/filer_public/2017/02/16/axway_finextra.pdf>
[6] Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC *OJ L 319*
[7] To be more extensively discussed in Chapter 2.
[8] For instance, technology start-ups that are developing innovative services, leading to new business opportunities. They are associated with innovative ideas which cause disruption in the financial industry, contrary to the banks and their services.
[9] Preamble 4 Directive (EU) 2015/2366
[10] European Commission, 'Payment Services Directive (PSD2): Regulatory Technical Standards (RTS) enabling consumers to benefit from safer and more innovative electronic payments' (Fact Sheet, 2017) <https://europa.eu/rapid/press-release_MEMO-17-4961_en.htm> accessed June 2019

consolidated information on one or more payment accounts available within online bank in its own application.[11]

This thesis will discuss the main legal challenges in relation to the data protection, particularly linked to the GDPR and data protection provisions in PSD2, posed by the concept of Open Banking governed by the revised Payment Directive. Open Banking is a relatively new concept that is now framed by the PSD2 with a high potential for growth.[12] It gives the financial industry and nonbank entities the possibility to exploit financial transaction data.[13] The literature sees this concept as one of the key aspects of a revised PSD2.[14] Among many advantages this business model brings to the customers, banks and to the third party providers, it nevertheless comes with several legal issues.[15] The benefits of a new business model, such as cost efficacy, customer friendliness and transparency should not outweigh the violation of customer privacy.[16] As the financial data which holds many personal information about an individual is now also available to nonbank third party providers which contrary to banks still do not enjoy high level of trust by the customers, their access to data needs to be strictly regulated by the relevant legislations, namely the PSD2 and the GDPR. The customers' personal data needs to be protected as any privacy violation might result in the serious consequences to the parties involved.[17] However, the high level of protection can only be ensured if relevant legislations are complementary to each other, with no inconsistencies making their compliance burdensome.

Ensuring the compliance with a new legislation is often challenging. In the EU, national divergencies in implementation can make the compliance even more challenging.[18] Moreover, compliance issues become more substantial when the understanding of the content of the related legislations is not clear or even found contradicting. Concretely, the available literature has already acknowledged the issue of the overlap between the PSD2 and the GDPR.[19] Due to the lack of clearance on the sensitive topics, such as on the topic of data protection, several member states such as the Netherlands and Spain, missed the transposition deadline for PSD2 of 13 January 2018.[20] This was due to the conflict of interest between the third party providers and banks as well as the discussions on sensitive topics such as processing of payment data.[21] The

[11] Relevant payment services are set out in Annex 1 to PSD II

[12] 'PSD2 and Open Banking. Revolution or evolution? ' (KPMG, March 2019) <https://assets.kpmg/content/dam/kpmg/pl/pdf/2019/04/pl-Raport-PSD2-i-Open-Banking-ENG.pdf> accessed April 2019

[13] The concept of Open Banking will be discussed in detail in the second chapter.

[14] Olly Jackson, 'PSD2 gives banks chance to evolve' (2018) International Financial Law Review < https://search.proquest.com/openview/d6d3e565ec450c842538ddaa1b312b83/1?pq-origsite=gscholar&cbl=36341> Accessed July 2019

[15] Alessio Botta, Nunzio Digiacome, 'PSD2: Taking advantage of open banking disruption' (McKinsey & Company, 2018) < https://www.mckinsey.com/industries/financial-services/our-insights/psd2-taking-advantage-of-open-banking-disruption >Accessed July 2019

[16] Annette Mackenzie, 'The FinTech Revolution' (2015) 26(3) London Business School < https://onlinelibrary.wiley.com/doi/abs/10.1111/2057-1615.12059>Accessed July 2019

[17] Gaurav Bansal, 'Trust violation and repair: The information privacy perspective; (2015) Volume 71 Decision Support System < https://www.sciencedirect.com/science/article/pii/S0167923615000196>Accessed July 2019

[18] Ioannis Dimitrakopoulos, 'Conflicts between EU law and National Constitutional Law in the Field of Fundamental Rights' (European judicial training network) < http://www.ejtn.eu/PageFiles/17318/DIMITRAKOPOULOS%20Conflicts%20between%20EU%20law%20and%20National%20Constitutional%20Law.pdf> Accessed July 2019

[19] Niels Vandezande, 'Reconciling Consent in PSD2 and GDPR' (Web Fraud Prevention, Identity Verification & Authentication Guide 2018/2019, December 2018) < https://www.thepaypers.com/reports/web-fraud-prevention-identity-verification-authentication-guide-2018-2019/r776368> accessed 25 May 2019

[20] 'PSD2 licensing: solving the puzzle of becoming a Third Party Provider' (Blog, Innopay) <https://www.innopay.com/en/publications/psd2-becoming-a-third-party-provider> accessed 10 June 2019

[21] Tycho Van Ewijk and Josje Fiolet, 'PSD2 licensing: solving the puzzle of becoming a Third Party Provider' (Innopay, blog) < https://www.innopay.com/en/publications/psd2-becoming-a-third-party-provider> accessed July 2019

lack of clarity in the interpretation of the terms within the legislations was listed as one of the main reasons for a late adoption.[22]

With the data protection being a fundamental right, it has to be ensured that this right is respected in the legislations across different sectors. The PSD2, a legislation enabling the business model which allows for an increased personal data sharing with the third party providers and which could potentially undermine the privacy and data protection of customers, should not be an exception.[23] This model allows for the processing of a vast amount of personal data. With the advance of the technology that enables more efficient collection, storage and the interpretation of personal data, the amount is expected even to increase in the future. The advantages that the services enabled under the Open Banking are brought to the customers might undermine the concerns commonly raised by the customers in regard to the processing of personal data under the new business model.[24]

The PSD2 adds third party payment service providers to the EU's legal framework on payment services.[25] This means that traditional payment service providers will need to share certain data with those third party providers. Much of that data is very personal in nature and it therefore constitutes personal data in the sense of the EU's data protection framework set by the GDPR. This results in a conflict between on the one hand a requirement for a seamless sharing of personal data and on the other hand, the requirement to allow for such sharing under very strict conditions, resulting in a compliance conundrum.[26] The experts acknowledged that even after the entry into force of both legal frameworks, several uncertainties remain.[27] In this thesis, one particular matter will be examined, namely that of consent. From a data protection perspective, a GDPR requires that the personal data is processed on one of the legitimate bases listed in the legislation. The GDPR refers to a number of these, one of them being the consent of the data subject.[28] PSD2 in its article dedicated to data protection mandates that (explicit) consent is necessary in order to provide services in the case of Open Banking to the customers.[29] However, the PSD2 does not define the concept of the "explicit consent" and clarifies whether it has the same meaning as in the GDPR.[30] The expert opinion on this topic differs. This results in a lack of clarity surrounding adequate levels of consent for a third party payment providers to obtain in order to deliver their services. The bank sector was one of the industries which called for the need to ensure a consistent consent framework.[31] It is important to note that non-compliance carries heavy fines.[32] In order to avoid fines, banks will need to have correct procedures in place to comply with both legislations. This is currently not an easy task, given that they are not

[22] Ibid.
[23] P.T.J. Wolters and B.P.F. Jacobs, 'The security of access to accounts under the PSD2' (2018) 11(40) Computer Law & Security Review: The International Journal of Technology Law and Practice https://doi.org/10.1016/j.clsr.2018.10.005 accessed July 2019
[24] Ibid.
[25] They will be described in the next chapter.
[26] Niels Vandezande, 'Reconciling Consent in PSD2 and GDPR' (Web Fraud Prevention, Identity Verification & Authentication Guide 2018/2019, December 2018) < https://www.thepaypers.com/reports/web-fraud-prevention-identity-verification-authentication-guide-2018-2019/r776368> accessed 25 May 2019
[27] EDPB, 'Letter regarding PSD2 directive' (EDPB, 84-2018, 5 July 2018) < https://edpb.europa.eu/news/news/2018/letter-regarding-psd2-directive_en> accessed February 2019
[28] Article 6 (1) (a) GDPR
[29] Article 66, 67 and 94 PSD2
[30] Article 94 (2)
[31] European Banking Federation, 'European banking federation's comments on the article 29 working party guidelines on con sent (WP259)' (EBF_030527) <https://www.ebf.eu/wp-content/uploads/2018/01/EBF_030527-EBF-comments-on-WP29-Guidelines-on-consent-wp259-1.pdf> accessed 15 June 2019
[32] Non-compliance with the GDPR can lead to fines of up to 20M EUR, or up to 4 million of an undertaking's total worldwide annual turnover, whichever is higher. As per PSD2, member states are free to determine fines that may be imposed by national authorities.

aligned. Without any guidance, financial institutions alone, need to assess the interplay of all the conflicting provisions to act properly and mitigate the potential risks.[33] They will need to stand behind their decisions as to why they adopted specific interpretations or took certain positions. They will also need to assess the operational implications of such decisions and develop processes and records that demonstrate their compliance with the GDPR, including the strict requirement for the consent. Moreover, the customers opening their bank accounts to nonbank third parties also expect a high level of protection of their payment data. The clarification of the meaning of the 'explicit consent' as per PSD2 is necessary to determine the appropriate legal basis and the obligations expected to be fulfilled by the involved parties under the legislation.

Therefore, it is important to explore to what extent is the framework for the consent under the data protection provision under PSD2 aligned with the GDPR.[34] The relevance of this topic is confirmed by the fact that the guidelines on the PSD2 and the GDPR are included on the agenda of EDPB for the activities for 2019-2020.[35]

1.2. The PSD2

PSD2 which has replaced PSD1[36] is a sector specific directive that regulates payment services environment. As a directive, its transposition into a national law is required. The aim of the PSD2 is to ensure "continuity in the market, enabling existing and new service providers, regardless of the business model applied by them, to offer their services with a clear and harmonised regulatory framework while not compromising the security of payment transactions and customer protection against demonstrable risk of fraud."[37] A key to the introduction of a revised directive has been the opening of the EU market to "companies offering consumer or business oriented payment services based on access to information about the payment account."[38] This means that the PSD 2 provides a legal basis for third parties or non-bank legal persons to provide payment services. An example would be a Dutch iDEAL.[39] It is interesting to note that more than 55% of the internet payments in the Netherlands are made by the payment initiation service providers, one type of the non-banks discussed later in the text.[40] As discussed later in the text, many concerns about the data protection have been raised among privacy experts and industry since the adoption of the revised Directive.[41]

[33] Kristof Van Quathem and Sophie Bertin, 'GDPR and PSD2: a compliance burden for financial institutions' (Thomson Reuters, 18 April 2018) <https://www.cov.com/-/media/files/corporate/publications/2018/04/gdpr_and_psd2_a_compliance_burden_for_financial_institutions.pdf> accessed July 2019

[34] Ibid.

[35] EDPB, 'EDPB work program 2019-2020' (12 February 2019) < https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-02-12plen-2.1edpb_work_program_en.pdf> accessed April 2019

[36] Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC (Text with EEA relevance) OJ L 319 'PSD2 and GDPR: An awkward match?' (Deloitte Touche Tohmatsu Limited, 2018) https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/legal/deloitte-nl-psd2-and-gdpr-an-awkward-match.pdf Accessed January 2019

[37] Recital 33 of PSD2

[38] European Commission (EC), Revised rules for payment services in the EU (Summary of legislation, 32015L2366, March 2018) <https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32015L2366

[39] https://www.ideal.nl/en/partners/

[40] European Commission (EC), Payment Service directive; frequently asked questions (Fact sheet, MEMO/15/5793, January 2018) < http://europa.eu/rapid/press-release_MEMO-15-5793_en.htm> accessed May 2018

[41] Evelin Austin, 'The four year legal battle for the protection of your data' (Bits of Freedom in EDRi, 24 May 2018) < https://edri.org/four-year-battle-protection-of-your-data-gdpr/> Accessed June 2019

1.3. The GDPR

The data protection part will be based on the assessment of the current legislation, particularly the GDPR which was adopted in 2016 and it remains one of the most lobbied EU legislations.[42] The GDPR replaced the outdated Data Protection Directive ("DPD") and it is a general legislation.[43] The GDPR came into effect in May 2018. As a regulation, it is directly applicable in all member states. One of the general aims of the regulation is to give natural persons of the EU better control over their personal data.[44] However, as noted, the businesses process an increased amount of personal data. The advance of technology and the adoption of the new legislation as a response to the new developments, such as the PSD2 create more opportunities in regard to personal data processing.[45] Nevertheless, the legislations and businesses must ensure that the processing is compliant with the increased requirements from the data protection legislation, such as the GDPR. The financial sector is not an exception.

It is important to clarify whether explicit consent under PSD2 is understood as per the GDPR primary to determine the correct legal basis for data processing. As explained below, the payment data is specific as it holds many sensitive information of individual which is subject to the stricter data protection requirements.

1.4. Hierachy of rules

Unlike PSD2, the GDPR as a general legislation applies to all businesses in the EU processing personal data, not just financial sector. The GDPR does not refer to the PSD2, whereas the intersection of PSD2 with the data protection has been recognized by the revised Payment Service Directive. The preamble as well as the legislative text of the PSD2 contain references to data protection.[46] PSD2 provides an entire chapter fully dedicated to data protection.[47] This chapter is however based on the DPD and does not acknowledge the enforcement of the future regulations, such as the GDPR. Nevertheless, the compliance with GDPR is required since the entry of GDPR into force in May 2018 therefore all references to the DPD are interpreted as referring to the GDPR.[48] The hierarchy of rules has not been clear and the implementation of certain provisions of PSD2 into a national legislation has therefore resulted in a topic of heated discussions between Data Protection Authorities ("DPA") and national legislators.[49] As observed by the DPAs, the GDPR has not been taken in consideration adequately in the course of the national implementation of PSD2.[50] For instance, due to the unclear hierarchy of rules as to which legislation prevails, the disagreement arose whether the Dutch National Bank (financial supervisor) or DPA (data protection supervisor) should monitor the compliance with data

[42] European Data Protection Supervisor; 'History of data protection regulation' < https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en> accessed April 2019
[43] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
[44] Recital 7 GDPR
[45] 'The main differences between DPD and the GDPR and how to address those moving forward' (Seeunity, White paper British legal technology forum) <https://britishlegalitforum.com/wp-content/uploads/2017/02/GDPR-Whitepaper-British-Legal-Technology-Forum-2017-Sponsor.pdf> accessed April 2019
46 Preamble 90 of PSD2
[47] Article 94 PSD2
[48] Article 94(2) GDPR
[49] 'Advies Implementatiebesluit herziene richtlijn betaaldiensten' (Dutch Data Protection Authority, 20 December 2017) < https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/20171220_advies_aan_min_fin_implementatiebesluit_psd2.pdf > accessed January 2019
[50] 'PSD2 and GDPR: An awkward match?' (Deloitte Touche Tohmatsu Limited, 2018) https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/legal/deloitte-nl-psd2-and-gdpr-an-awkward-match.pdf Accessed January 2019

protection rules required by the PSD2. The call for a further clarification has been requested on an EU level.[51] Yet, it has to be noted that when it comes to data processing operations, the GDPR has to be fully considered. Due to the lack of clarity and confusion as to what legislation to comply with, some banks even considered not to fully implement PSD2 as GDPR imposes higher penalties for non-compliance.[52] Since the GDPR also applies to the payment sector, several tensions have been identified in relation to the compliance to both regulations, the interpretation of the notion of consent being one of them.[53] The Forum on "PSD2 & GDPR" was held in February 2018 with the goal to discuss the alignment of PSD2 and GDPR for harmonized implementation in Europe.[54]

Consent, as one of the listed lawful grounds for processing of personal data, being subject to the strict requirements under GDPR plays an important role also in PSD2. The tension between these two regulations has been acknowledged in several industry sources.[55] Firstly, the lack of clarity leaves uncertainly whether the (explicit) consent which is required to be given by customers in order for the third party payment provider to access bank accounts under PSD2 can be understood as a data protection consent under GDPR. This is important because GDPR imposes strict requirements to be met when consent is chosen as a legitimate ground. Moreover, if the required 'explicit consent' under the data protection clause in PSD2 is not a legitimate ground for personal data processing, what would be another appropriate legal basis and how could the consent from PSD2 be then understood.[56] It can be argued that since the PSD2 does not give a specific definition to the notion of consent it cannot be *lex specialis* to the GDPR.

1.5. Sate of the art and novelty

Much has been written about the interaction between PSD2 and GDPR in the literature. However, the PSD2 has been introduced in a fairly narrow manner, particularly as a game changing Directive in the payment services, changing the banking as we know it.[57] The broader problem of the tension between the two legislations has been acknowledged in several documents, however, the particular issue of the consent has not been discussed in depth yet. Therefore, this thesis aims to fulfill this gap. The subject of this thesis is of great importance for all actors willing to exploit the opportunities that are created by technology and translated into the legislation (PSD2), while paying a respect to the human rights of their customers (GDPR and PSD2). From the human rights perspective, it is essential that customers know exactly what they consent to and whether they are entitled with the rights from the GDPR.

[51] Ibid.
[52] Arun Krishnakumar, 'GDPR vs PSD2 – Banks may abandon PSD2 due to conflicting policies' (Daily Fintech, 4 August 2017) < https://dailyfintech.com/2017/08/04/gdpr-vs-psd2-banks-may-abandon-psd2-due-to-conflicts/> Accessed December 2018
[53] 'PSD2 and GDPR: An awkward match?' (Deloitte Touche Tohmatsu Limited, 2018) https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/legal/deloitte-nl-psd2-and-gdpr-an-awkward-match.pdf Accessed January 2019
[54] PSD2 and GDPR Forum (Amsterdam, 2018) http://www.psd2gdpr.com/ accessed February 2019
[55] Arun Krishnakumar, 'GDPR vs PSD2 – Banks may abandon PSD2 due to conflicting policies' (Daily Fintech, 4 August 2017) < https://dailyfintech.com/2017/08/04/gdpr-vs-psd2-banks-may-abandon-psd2-due-to-conflicts/> Accessed December 2018
Christian F. McDermott, 'GDPR & PSD2: Squaring the Circle' (Latham & Watkins LLP, 13 August 2018) https://www.globalprivacyblog.com/legislative-regulatory-developments/gdpr-psd2-squaring-the-circle/ accessed January 2019
Mounaim Cortet and Tom Rijks and Shikko Nijland, 'PSD2: The digital transformation accelerator for banks' (2016) 10(1) Journal of Payments Strategy & Systems.< https://www.econbiz.de/Record/psd2-the-digital-transformation-accelerator-for-banks-cortet-mounaim/10011566458> accessed June 2019
Deloitte, 'PSD2 and GDPR: An awkward match?' (Deloitte Touche Tohmatsu Limited, 2018) https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/legal/deloitte-nl-psd2-and-gdpr-an-awkward-match.pdf Accessed January 2019
[56] Article 95 (2) PSD2
[57] 'PSD2 – a game changing regulation' (PwC) < https://www.pwc.co.uk/industries/banking-capital-markets/insights/psd2-a-game-changing-regulation.html> accessed march 2019

1.6. Research question

The research focuses on the provisions from PSD2 that require banks to open up their customers' payment account to the third parties.[58] Accessing bank data by the third-party providers is also one of the main novelties introduced by the PSD2. While it creates new opportunities to develop services for consumers, it also raises several legal questions. Many unclarities remain when it comes to the processing of payment data. As financial data holds a wealth of information about an identifiable customer it is considered to be a personal data as per the GDPR, meaning that the data protection legislation becomes applicable. According to the GDPR, personal data needs to be processed on at least one of the legitimate bases. PSD2 in its Data Protection provision mandates that "Payment service providers shall only access, process and retain personal data necessary for the provision of their payment services, with the 'explicit consent' of the customer". [59]

This means that the notion of the "explicit consent" is one of the key elements for the GDPR related to the PSD2 and third party providers. As the notion of consent appears in both related legislations, the main focus of the thesis is to analyse the meaning of the notion of the consent (to the processing of personal data) as understood under the GDPR and the PSD2. The main goal is to explore the extend of the consistency in the interpretation and understanding of the notion of consent in both legislations and what does it mean for the protection of the personal data of the customers.

Therefore, the research question of this thesis is as following:

To what extent do PSD2 and the GDPR overlap in the understanding of the notion of (explicit) consent to the processing of personal data?

1.7. Sub-questions

In order to properly answer the research question, the following questions should also be answered:

1. *What is the interaction between the Open Banking under PSD2 and the GDPR?*

2. *What is the significance of the data protection consent and its drawbacks, namely in the situation of Open Banking?*

3. *How should be the consent understood in PSD2? To what extend is it in line with the GDPR?*

1.8. Methodology

The thesis will be based on the traditional/doctrinal research method relying upon traditional sources of legal and policy documents, case law as well as on the relevant literature study. The focus of the research is on the analysis of the notion of consent as found in the GDPR and PSD2. The main aim is to analyze the interpretation of consent in the processing of personal data in a

[58] Article 66-69 and 95(2) PSD2
[59] Article 95(2) PSD2

financial sector, as specified in the relevant provisions of the PSD2 and compare it with a data protection consent under the GDPR. The findings are mainly based on the analysis of mainly legal and policy documents at the European level.

A systematic search will be conducted through databases of Tilburg University, and other online databases such as Google Scholar, ScienceDirect, Hein Online and Social Science Research Network.

1.9. Structure

This thesis is divided into four chapters and a conclusion, which will follow the sub-research questions and answering them. After the introductory chapter, the second chapter will introduce the concept of the Open Banking under the PSD2, as this new business model allows the processing of personal data which is governed by the data protection legislation. The chapter will introduce the third party providers and their services. Part of this chapter will explain the reasons why the payment data can be considered personal data and even sensitive data within the data protection meaning and what are the consequences of the abuse of such data on individual. The chapter also explores the level of trust the new entities to the payment market enjoy compared to the traditional parties such as banks.

The third chapter will discuss the data protection provision under PSD2 and the meaning of the 'explicit consent' from this Directive. Based on the finding, this notion will be weighed against the notion of consent under the GDPR.

The fourth chapter will look at the development of the notion of consent in the data protection meaning. The chapter further elaborates on the notion of consent under the GDPR and examines the conditions that need to be fulfilled for a consent to be considered valid. Furthermore, the problems with the data protection consent as a legal basis will be identified and applied to the case of Open Banking.

2. Chapter 2

2.1. The rationale for the adoption of PSD2

The aim of the PSD2 to open up the payment market is realised through the creation of the third party payment providers which among other gap the bridge between retailers and the banks.[60] This chapter introduces the historical development of the third party payment providers which were recently included in the scope of the PSD2. The chapter further elaborates more on the concept of the Open Banking under PSD2. As discussed in the next sections, the concept of the Open Banking allows for the extensive processing of personal data, which is held in the bank accounts by the parties that were previously not the part of the EU regulatory framework. Therefore, the chapter explores the level of the trust these new actors enjoy among customers compared to the traditional financial institutions from the data protection point of view. The chapter also describes the possible consequences that the abuse of the financial data by the third party payment providers has on the customers.

The financial developments during the late 90s and the beginning of the new century brought new actors to the payment market.[61] On the one hand, institutions began to pursue the activity of issuing the electronic money which fall under the scope of the EU e-money Directive while at the same time, there was a development of the institutions other than credit institutions which also enabled payment services.[62] These institutions, namely payment institutions, were covered under the first Directive of payment services. By bringing this new category under the EU legislation, the EU regulator aimed at opening up the payment market to the new institutions, particularly those active in a high-tech sector, such as telecommunications.

Since the adoption of the PSD1, new types of the payment service providers have emerged, particularly "payment initiation services" and "account information services".[63] Even though the significance of these new services was becoming evident, neither service fall under the category of a payment institution as per PSD1. Mainly due to the fact, that they did not manage the customer's payment account.[64] PSD1 did not explicitly state that access to the account is a requirement for the applicability of the Directive. However, according to the article 3(j), the PSD1 limited the access to accounts to non-banks and excludes the use of the technical service providers.[65]

[60] Steve Mansfield Devine, 'Open banking: opportunity and danger' (2016) Volume 2016, Issue 10 Computer Fraud & Security <https://reader.elsevier.com/reader/sd/pii/S136137231630080X?token=AE4968C27B69442FD2C16C239A9EA10E6FF61DA0F640D3BE53C802A18B24A8784C55151A715615A976E36120000484E3> accessed April 2019

[61] Richard J. Sullivan and Zhu Wang, 'Nonbanks in the Payments System: Innovation, Competition, and Risk' (Conference summary, KANSAS CITY, 2017) < https://pdfs.semanticscholar.org/41ad/051c62d02ae658ff36b02cb6a93866c3d298.pdf> accessed June 2019

[62] Markos Zachariadisa and Pinar Ozcan, 'The API Economy and Digital Transformation in Financial Services: The Case of Open Banking' (Swift Institute, 2017) https://www.swiftinstitute.org/wp-content/uploads/2017/07/SIWP-2016-001-ImpactOpen-APIs-FINAL.pdf accessed June 2019

[63] Marry Donelly, 'Payments in the digital market: Evaluating the contribution of Payment Services Directive II' (2016) 32(6) Computer Law & Security Review < https://www.sciencedirect.com/science/article/pii/S0267364916301170?via%3Dihub> accessed July 2019

[64] Ibid.

[65] European Commission (EC), Your questions on PSD Payment Services Directive 2007/64/EC Questions and answers (2011) < https://ec.europa.eu/info/system/files/faq-transposition-psd-22022011_en.pdf> accessed June 2019

Innovations in the area of technology and digitalisation result in an important strategic competitive consequences for the market players, as they shape the competitive environment and market dynamic in a specific industry.[66] As a result of the digitalisation, new actors, such as financial technology companies ("Fin Tech") or so called third party payment service providers entered the market of the payment services, which was previously exclusively reserved for banks. Considering that the financial industry is among one of the most regulated and complex industries where the innovation is rarely implemented, any such advance of technology poses significant regulatory challenges.[67] Several legal issues arise in regard to the consumer protection and security as well as data protection, in particular regarding protection of the payment service users' data in accordance with the European Union data protection rules.

On the one hand, it was clear that the lack of regulation made customers highly vulnerable for the potential abuse, for instance in the situation when the non-bank entities are able to access the customer bank accounts. On the other hand, it is also the lack of the regulation of these entities that hindered the innovation in the area of the payment services on an EU level.[68] Therefore, in order to address this challenge steaming from the developments in electronic payments and services, the European regulator adopted a revised Payment Service Directive ("PSD2") which had to address these issues.[69] The Directive aims to provide consumers with "adequate protection for their payment and account data as well as legal certainty about the status of account information service providers."[70]

The revised Directive has expanded its scope, changed the rights and obligations of the parties and the allocation of liability for unauthorized payment transactions.[71] The PSD2 introduced the new security and authentication requirements in the online context.[72] Part of the realization of this aim is to provide the sharing of customer data to new service providers.

A key part is to establish a playing field for the third party service payment providers, particularly account information service providers and payment initiation service providers.

The next sections will describe the concept of the Open Banking and the types of the third party payment service providers under the PSD2.

2.2. PSD2 and the concept of Open Banking

One of the most important parts of the PSD2 are the provisions related to access to accounts or so-called Open Banking.[73] Technological progress in the financial area challenged the self-

[66] Michael Eugene Porter, The Competitive Advantage: Creating and Sustaining Superior Performance, (Free Press, New York, 2nd edition, 1985) < https://www.albany.edu/~gs149266/Porter%20(1985)%20-%20chapter%201.pdf> accessed February 2019
[67] Steve Mansfield Devine, 'Open banking: opportunity and danger' (2016) Volume 2016, Issue 10<https://reader.elsevier.com/reader/sd/pii/S136137231630080X?token=AE4968C27B69442FD2C16C239A9EA10E6FF61DA0F640D3BE53C802A18B24A8784C55151A715615A976E36120000484E3> accessed April 2019
Stephen A. Lumpkin, 'Regulatory Issues Related to Financial Innovation' (OECD Journal: Financial Market Trends 2009) < https://www.oecd.org/finance/financial-markets/44362117.pdf> accessed February 2019
[68] 'Introducing the Open Banking standard' (Open Data Institute, 2016) < https://theodi.org/> accessed May 2019
[69] Preamble 6 PSD2.
[70] Recital 28 PSD2
[71] European Commission, 'Proposal for a Directive of the European parliament and of the council on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC' (COM/2013/0547 final - 2013/0264 (COD)) < https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52013PC0547> accessed June 2019
[72] Recital 33 PSD2
[73] Article 66-68, 95 PSD2

evident control of banks over payment accounts of their customers. In practice, mainly two kinds of new non-banking payment services emerged: payment initiation service and account information service.

Open banking is a new concept in the field of financial services.[74] The business model of Open Banking itself is a concept where internal recipes are shared with some third party eventually helping an organization to be more effective in creating and capture a value around the existing business model.[75]

In a financial field, the PSD2 dictates that banks are obliged to come up with a mechanism to enable the third party payment providers to access customer bank accounts. The third party payment providers can access the information on the payment account given that the customer has provided an explicit consent.[76] According to the Article 4 of the PSD2, these services can be divided into two types: account information services and payment initiation services. The PSD2 imposes a requirement on these actors to be registered or licensed by the competent authorities in their Member States.[77]

The *payment initiation service provider* provides payment services by establishing a "software bridge between the website of the merchant and the online banking platform of the customer."[78] The payment initiation services are seen as a cheaper alternative to the use of credit cards, allowing customers to shop online without the need for a credit card.

In response to the technological developments, many complementary services have recently emerged in the payment market. Companies, such as Facebook, Apple or Google take advantage of the ability to access the account to provide *account information services.* Those services "provide the customer with consolidated online information on one or more payment accounts held with one or more other payment service providers and accessed via online interfaces of the account servicing payment service provider."[79] The payment service user is in that way able to have an overall view of its financial situation immediately and at any time.

BillGuard is listed as an example of the account information service provider that uses payment data to detect fraudulent transactions and unnecessary spending. [80] The company uses algorithm to process the collected transaction information with the goal to find anything that could potentially indicate fraud or unnecessary spending patterns. However, the company also relies on the services delivered by the other companies which means that the customer payment data is shared with more companies than primary third party service provider.

[74] BEUC, 'Consumer-friendly Open Banking (BEUC-X-2018-082 , 20 September 2019) <https://www.beuc.eu/publications/beuc-x-2018-082_consumer-friendly_open_banking.pdf> accessed April 2019
[75] Henry Chesbrough, 'Business model innovation: it's not just about technology anymore' (2007) 24(3) Strategy&Leadership < https://www.emerald.com/insight/content/doi/10.1108/10878570710833714/full/html> accessed July 2019
[76] Article 66-68, 95(2) PSD2
[77] Article 5(1) PSD2
EBA, 'Guidelines on authorisation and registration under PSD2' (Consultation Paper, 2016) 18 <https://eba.europa.eu/documents/10180/1646245/Consultation+Paper+on+draft+Guidelines+on+authorisation+and+registration+under+PSD2+%28EBA-CP-2016-18%29.pdf/b8d49c1c-be4f-4b36-a5ce-e6710e00383c> accessed March 2018
[78] Recital 27 PSD2
[79] Recital 28 PSD2
[80] BillGuard, <https://www.billguard.com/ >

A market analysis shows the great potential of FinTech companies in delivering individually tailored financial solutions. The research has shown the value of FinTech investments of US$112 billion in 2018.[81] However, despite the success and the growth of these companies offering financial services, one can question whether companies have already gained the same level of trust as did the traditional banks did in the last centuries.

2.3. Trust in banks and trust in applications

The financial services industry is built on trust.[82] Characteristics, such as honesty, reliability, competence, quality and credibility are closely linked to the consumer trust.[83] In a banking sector specifically, the customer trust is dependent primary on bank's reliability, observance of regulations, commitment, etc.[84] Traditional banks have long seen trust as their core strength.[85] This has been due to the visibility and familiarity of their brands and branches.[86]

The high perceived trust that is known for the banking sector can also be explained by the fact that the relationship between bank and customer is of contractual nature.[87] Moreover, as the traditional financial institutions, such as banks, have always been subject to tight rules and regulations they gained a trust of their customers, also in relation to the use of personal data.[88]

On the other hand, in case the trust given to the banks is broken, the negative consequences are perceived worse than are in the other industries, as banks are entrusted with safeguarding customer's money and sensitive financial data. [89]

The next sections explore the level of perceived trust the newcomers to the payment service market, such as account information service providers and payment initiation providers enjoy by the customers compared to the traditional financial institutions.
Traditionally, payment services were provided by banks. However, during the last years there has been a trend of non-bank third party providers who make use of their companies' business network to make transactions that were similar to payment transactions.[90] The introduction of non-bank third party providers not only affected the dominant position of banks. However, it has also raised the question of trust and the willingness of customers to share personal financial data with parties other than banks. It is generally argued that third party payment providers are less

[81] 'Global FinTech investment more than doubled to $112 billion' (Consultacy, 21 February 2019) < https://www.consultancy.eu/news/2390/global-fintech-investment-more-than-doubled-to-112-billion> accessed June 2019
[82] John "Skip" Benamati & Mark A. Serva, 'Trust and distrust in online banking: Their role in developing countries' (2007) 13(2) Information Technology for Development < https://www.tandfonline.com/doi/pdf/10.1002/itdj.20059?needAccess=true> accessed June 2019
[83] Raija Anneli Järvinen, 'Consumer trust in banking Consumer trust in banking relationships in Europe' (2014) 32(6) International Journal of Bank Marketing < https://www.researchgate.net/publication/265969491_> Accessed July 2019
[84] R V Casielles Alvarez, 'Trust as a key factor in successful relationships between consumers and retail service providers' (2005) 25(1) The Service Industries Journal < https://www.tandfonline.com/doi/abs/10.1080/0264206042000302423> Accessed July 2019
[85] 'Customer trust: without it, you're just another bank' (EY, 2016) < https://www.ey.com/Publication/vwLUAssets/ey-customer-trust-without-it-you-re-just-another-bank/$FILE/ey-customer-trust-without-it-you-re-just-another-bank.pdf> Accessed July 2019
[86] Ibid.
[87] Raija Anneli Järvinen, 'Consumer trust in banking Consumer trust in banking relationships in Europe' (2014) 32(6) International Journal of Bank Marketing < https://www.researchgate.net/publication/265969491_> Accessed July 2019
[88] Ibid.
[89] Kyle Wooten, 'With consumers' trust comes great responsibility: Approaching data security in a fintech-friendly world' (Abrigo) <https://www.abrigo.com/blog/2018/08/27/with-consumers-trust-comes-great-responsibility-approaching-data-security-in-a-fintech-friendly-world/> accessed May 2019
[90] 'Financial Services technology 2020 and beyond' (PwC) <https://www.pwc.com/gx/en/financial-services/assets/pdf/technology2020-and-beyond.pdf> Accessed May 2019

reliable than banks which was an important element of trust in banking sector.[91] However, this generalization is not reflected in the PSD2. The PSD2 works from the assumption that third party payment providers can be trusted.[92] It is interesting to observe the level of trust towards the non-bank third party providers entrusted with the financial data as they are commonly linked to the non-compliance with regulations which was listed as one of the main elements of trust by customers towards the traditional banks.[93] Moreover, as banks are under PSD2 obliged to grant an access and provide online interface to the third party providers without any contractual relationship, the lack of contractual relationship might raise additional trust issues among the customers.[94]

Generally, bank accounts of individuals contain vast amount of information about the balance and all incoming and outgoing transactions.[95] Detailed conclusions can be drawn from financial data about individual's personal life. If the data can be linked to an identified or identifiable natural person then it is considered personal data under GDPR and the processing must adhere to the requirement of this legislation.[96]

The possibility of finance startups or companies, such as Facebook or Google, to access the customer's record of a lifetime's spending, shopping habits and borrowing patterns is considered a "treasure trove".[97] Many companies discuss the numerous opportunities offered by the Open Banking. For instance, the insurance companies see the potential in data mining to get relevant insights in consumer behavior, such as spending on health care or the car insurance.[98] More specifically, if the insurance company gets a license and becomes a third party provider under PSD2 then it gets an access to the payment information of the customer. The insurance company can then analyze this payment information and use it to offer personalized products and services, making a better price offer based on the found patterns indicating risks, etc.[99]

However, the research performed by De Nederlandse Bank (DNB) in 2015 has shown that the Dutch customers have a negative attitude towards the commercial use of payment data by the non-banks. [100] The research concludes that the use of payment data is more acceptable for the purposes other than commercial, such as legal obligations or security. Another more recent research has shown that 75% of consumers are "very" or "extremely" concerned about the data

[91] KPMG, 'PSD2 and Open Banking. Revolution or evolution? ' (March 2019) <https://assets.kpmg/content/dam/kpmg/pl/pdf/2019/04/pl-Raport-PSD2-i-Open-Banking-ENG.pdf> accessed April 2019
[92] P.T.J. Wolters and B.P.F. Jacobs, 'The security of access to accounts under the PSD2' (2018) 11(40) Computer Law & Security Review: The International Journal of Technology Law and Practice https://doi.org/10.1016/j.clsr.2018.10.005 accessed March 2019
[93] 'Outrageous abuse of privacy:New York orders inquiry into Facebook data use' (Guardian, 23 February 2019) <https://www.theguardian.com/technology/2019/feb/22/new-york-facebook-privacy-data-app-wall-street-journal-report> accessed February 2019
[94] Article 66 (5) PSD2
[95] European Banking Authority, 'Consultation on RTS specifying the requirements on strong customer authentication and common and secure communication under PSD2' (Consultation Paper, 2016) 11 <https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2?p_p_auth=OtosFYa3&p_p_id=169&p_p_lifecycle=0&p_p_state=maximized&p_p_col_pos=1&_169_struts_action=%2Fdynamic_data_list_display%2Fview_record&_169_recordId=1616509> accessed May 2019
[96] Article 4 GDPR
[97] Rowland Manthorpe, 'To change how you use money, Open Banking must break banks' (Wired, 16 October 2017) https://www.wired.co.uk/article/psd2-future-of-banking accessed March 2019
[98] Ibid.
[99] Innopay, 'Insurance and the Open Banking wave: seven use cases' (Blog) <https://www.innopay.com/en/publications/insurance-and-open-banking-wave-seven-use-cases> accessed march 2019
[100] ING, 'ING and the use of customer data' <http://www.ing.com/About-us/ING-and-the-use-of-customer-data.htm>

protection when sharing their personal data with the payment application.[101] Moreover, customers indicated that banks are the most trusted institution to ensure the security of customers' personal information, compared to non-bank's companies, such as Amazon, PayPal and Facebook.

It appears that for the banks as already trusted institutions, the misuse of personal data and lack of its security may be judged by many according to different standards compared with the misuse of data by a non-bank third party provider. This could be seen as one of the reasons why traditional banks invest a lot of resources in protecting personal data and securing their systems and processes.[102]

It is important to note, that banks can also become a provider of payment initiation services or account information services. Therefore, as observed in the literature, banks should take a comparative advantage to offer such services considering the high level of trust they already enjoy. Customers are willing to share more personal data with them than with non-bank third party providers.[103] Moreover, the opinion differs whether the customer or banks should be the one in charge of the financial data held on the payment account. On the one hand, FinTech industry argues that the customer must be in charge to freely use his or her payment data whereas banks want to keep the monopoly over such data, as they can ensure the adequate protection against the potential threat of the security and privacy violations.

Contrary to banks, newcomers in a financial market still enjoy a great amount of distrust by the general public. According to the survey, only 3% of the respondents would trust their transaction data to the Google, and only 2% to Facebook, even in exchange for a more tailored financial offer which are offered by the account information service provider.[104] Companies such as Facebook, that have now possibility to obtain access to the payment accounts were previously already linked to the severe privacy violations that could be understood as yet another reason why the average bank user is less likely to share such personal data with them.[105]

2.4. Consequences of the abuse of payment data on the individual

The violation of data protection rules for the payment data can have a great impact on the consumers and their rights. The violation can take different forms, such as a personalized advertising, price discrimination through detailed profiling, fraud via identity theft and social engineering.[106] It is noted that the majority of the services provided by account information

[101] ATKearney, 'Key findings from the consumer Digital Behavior Study' (April 2018) https://www.atkearney.com/financial-services/the-consumer-data-privacy-marketplace/the-consumer-digital-behavior-study accessed May 2019
[102] Deutshe Bank, 'Fintech reloaded- Traditional banks as digital ecosystem' (Deutche Bank, 9 June 2015) <https://www.dbresearch.com/PROD/RPS_EN-PROD/PROD0000000000451937/Fintech_reloaded_%D0_Traditional_banks_as_digital_ec.PDF>accessed May 2019
[103] 103 ATKearney, 'Key findings from the consumer Digital Behavior Study' (April 2018) https://www.atkearney.com/financial-services/the-consumer-data-privacy-marketplace/the-consumer-digital-behavior-study Accessed May 2019
[104] KPMB, 'PSD and Open Banking' (March 2019) https://assets.kpmg/content/dam/kpmg/pl/pdf/2019/04/pl-Raport-PSD2-i-Open-Banking-ENG.pdf accessed April 2019
[105] 'Outrageous abuse of privacy:New York orders inquiry into Facebook data use' (Guardian, 23 February 2019) <https://www.theguardian.com/technology/2019/feb/22/new-york-facebook-privacy-data-app-wall-street-journal-report> accessed February 2019
[106] Jathan Sadowski, 'Companies are making money from our personal data – but at what cost?' (Guardian,31 August 2016) <https://www.theguardian.com/technology/2016/aug/31/personal-data-corporate-use-google-amazon> accessed March 2019

service providers even constitute profiling under the GDPR and would involve automated decision making in the sense of article 22 GDPR.[107]

This type of processing is considered to be high-risk for an individual.[108] Financial data holds very detailed personal information and can tell a lot about the actual behavior of people and depicts choices they make during their life. It is suggested that due to their sensitive nature, this type of data should be qualified as a special category of data, subject to stricter requirements.[109] In my opinion, this is relevant for the situation with PSD2 that opens up many opportunities for exploit such data.[110]

The financial data held on the bank accounts has always been of a great value for the further exploitation. The debates about its potential use reach back to the 1990s when the idea of the open network in a bank system first arose.[111] However, even before the existence of the third parties providers, financial institutions themselves aimed to match their customers to financial products and services by analyzing the bank transaction activities. In order to better target the customers, banks use a demographic and lifestyle segmentation systems.[112] By finding out the age of the customer, marital status or income the customer's bank database is divided into categories, such as elite suburbs, urban core or rustic living.[113] The purpose of this categorization is to link the specific customer group to the product or service. It can draw precise conclusions about an individual's private life. [114]

The abuse of such data can have significant (negative) consequences.[115]. The abuse can be seen from the perspective as to how valuable this data is for the business models of the companies. The scope of the abuse or violation differs from the situation where companies do not ask for consent or try to get a silent consent to cases where when the data is processed for the purposes other than those that was collected.[116] In sum, customers often live in dark and do not know how much data the company collected and what are the exact purposes are.[117]

Payment data is especially valuable because it tells more about an individual than online searching history.[118] The spending pattern can for instance indicate the individual's sexual preference. The fact that an individual spends their money on visiting places that are known for

[107] 'Beuc's Recommendations to the EDPB on the interplay between the GDPR and PSD2' (Recommendations, BEUC-X-2019-021, 11 April 2019) <https://www.beuc.eu/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf> accessed June 2019
[108] Information Commissioner's Office, 'Rights related to automated decision making including profiling' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/> accessed April 2019
[109] Dutch Data Protection Authority, 'Investigation into the combining of personal data by Google' (Report, 2013) < https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/en_rap_2013-google-privacypolicy.pdf> accessed August 2019
[110] 'Beuc's Recommendations to the EDPB on the interplay between the GDPR and PSD2' (Recommendations, BEUC-X-2019-021, 11 April 2019) <https://www.beuc.eu/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf> accessed June 2019
[111] IFI CLAIMS Patent Services, 'Apparatus and method for granting access to network-based services based upon existing bank account information' < https://patents.google.com/patent/US6910020B2/en> Accessed May 2019
[112] 'System and method for matching customers to financial products, services, and incentives based on bank account transaction activity' (US Patents) <https://patents.google.com/patent/US7954698B1/en> accessed April 2019
[113] Ibid.
[114] 'Data Protection Guidelines for Banks' (Malta bankers, May 2018) <https://idpc.org.mt/en/Documents/Data%20Protection%20guidelines%20for%20banking.pdf> accessed February 2018
[115] Angela Stringfellow, 'The ultimate data privacy guide for banks and financial institutions' (Ngdata, 14 August 2018) https://www.ngdata.com/data-privacy-guide-for-banks-and-financial-institutions/> accessed January 2019
[116] 'Opinion 14/2011 on the definition of consent' (Article 29 Working Party, 01197/11/EN WP187, 13 July 2011) < https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf> accessed May 2019
[117] Ibid.
[118] 'What the GDPR will concretely change for payment service providers' (European Payment Council) < European Payment Council> Accessed May 2019

specific groups of people can indicate the possibility that they are part of this group. This information can then be sold further, for instance to the insurance company which would consider an individual having higher risk for certain diseases and increased the premium. The use of such private information would be considered a serious infringement of privacy, potentially leading to discrimination.

2.5. Conclusion

The first part of this chapter introduces the technical and digital innovations which led to the adoption of PSD2. One of the listed innovations was the entry of the third party providers, particularly payment initiation services and account information services, in the payment market. This has changed the banking industry as we knew it. A new business model, Open Banking which is built on the premises to open up bank accounts to the non-bank third parties, comes with several concerns. This consequently results in a lower level of trust these services enjoy compared to the traditional financial institutions by the customers. Importantly, detailed conclusions can be drawn from financial data about individual's personal life and their abuse can have a severe negative consequence on an individual.[119] As shown, customers are less likely to trust their payment data to non-bank third party providers than banks. One of the reasons for the lower level of trust to these providers could be the fact that they are less likely to observe regulations and the contract does not play as an important role in the service relationships as this is known in the banking sector.

This chapter confirms certain trends which show that people care about their payment data. Moreover, as discussed above, the concept of the Open Banking under PSD2 poses several risks to the customer's data. Therefore, the legislation enabling such companies to access customers' personal data must have included controls to protect consumers against the threats that come from the abuse of that data.

[119] Alessandro Acquisti et al., 'What is privacy worth?' (2013) 42 The Journal of Legal Studies <https://www.cmu.edu/dietrich/sds/docs/loewenstein/WhatPrivacyWorth.pdf> accessed July 2019

3. Chapter 3

3.1. Introduction

The aim of this chapter is to assess the notion of consent in the context related to the framework of the PSD2 and the GDPR. The PSD2 makes references to the "consent" and to the notion of the "explicit consent" in several provisions. The GDPR also makes reference to these two terms and there is no suggestion that the notions of consent in the PSD2 has the same meaning as in the GDPR.[120]

The main goal of this chapter and thesis as a whole is to come to the conclusion whether or not the definition of consent from the PSD2 can be understood as the consent within the meaning of the GDPR. This is important as in order to be complaint with the transparency obligations, controllers should make sure that they know what the applicable legal basis is/are for the processing of personal data. The value of the data protection consent will be further discussed in the fourth chapter.

The first part of the current chapter will examine the consent as per PSD2. The next part will present the findings on this topic from the literature. The chapter includes several insights on this topic.

Data subject's consent is one of the bases for lawful processing of personal data in the European data protection law. As argued in the literature, consent plays an important role as it signal the enhance power and control over data subject's personal information.[121] However, consent has its own drawbacks which especially in the area of internet based services makes it mostly theoretical. This implies that in certain situations, an individual cannot expect high level of data protection when processing relies on consent and therefore, a different legal basis should be used.[122]

3.2. Consent in PSD2

The text (including preamble) of the PSD2 refers to the notion of consent 31 times. The question becomes what is the significance of the notion of consent in this legislation.

The PSD2 distinguishes between the notion of "consent" and the notion of the "explicit consent". Firstly, PSD2 refers to the "consent to execute the payment transaction" in several situations. For instance, this consent is used by a customer when paying at the automatic fueling stations or when booking a hotel room.[123] It is a consent which authorizes the banks to block the exact amount of funds that are needed for the execution of the payment transaction. Absence of such consent means that a payment transaction is unauthorized.[124] The PSD2 also lists the situations where the payer can revoke the consent or when the payment service provider can charge for

[120] 'Navigating the PSD2 and GDPR challenges faced by banks' (EY, 2018) <https://www.ey.com/Publication/vwLUAssets/ey-navigating-the-psd2-and-gdpr-challenges-faced-by-banks/$FILE/ey-navigating-the-psd2-and-gdpr-challenges-faced-by-banks.pdf> accessed May 2019
[121] Article 29 Working Party, 'Guidelines on consent under Regulation 2016/679' < https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051> accessed May 2019
[122] Bert-Jaap Koops , 'The Trouble with European Data Protection Law' (2014) International Data Privacy Law 250 < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2505692> accessed May 2019
[123] Preamble 75 PSD2
[124] Article 64 PSD2

revocation.[125] This type of consent is used for the purposes of identification and authorization of payment and is not linked to any processing of personal data by the payment service provider. It can even be referred as a "simple" consent linked to the authorization of a payment transaction. Such consent has been previously already included in PSD1 which however did not refer to the notion of the "explicit consent".

The same is applicable to the situation as per Article 65 PSD2 which states that based on the user 'explicit' consent, the bank must respond in a way of a simple confirmation or denial to the third party payment providers whether sufficient funds are available on the payer's account. This request does not include any information of either a qualitative or a quantitative nature and can therefore not be considered as a data protection consent as well.[126]

Secondly, in the context of the Open Banking, where the access to consumer's data is given to the third party providers, the PSD2 refers to the "explicit consent". More particularly, according to the article 66 and 67 PSD2, the customer is obliged to provide an explicit consent for payment to be executed by the account information service provider or for services based on the use of payment account information by the account information service providers. This consent may be given individually to each request for information or for each payment to be initiated.[127] However, this explicit consent can be understood as a contractual consent to the *service* and not the consent to the processing of personal data within the meaning of the GDPR. For instance, article 67 PSD2 specifically states that *services* by account information service providers can only be provided based on the explicit consent. There is no reference to the consent for the access to the payment account which can be translated as a data processing.

Nevertheless, the articles 66 and 67 refer to the data protection in certain points. For instance the third paragraph of article 66 mimics the data minimization principle when stating that payment initiation service provider shall not request from the user any data other than those necessary to provide payment initiation service. It can be argued that the two articles, however, do not refer to the consent within the data protection meaning. Some terms in the articles are even contradicting with the GDPR. For instance, the payment initiation service providers are not allowed to store *sensitive* payment data of the customer. Similarly, the account information service providers shall not request sensitive payment data linked to the payment accounts to provide their services. The problem arises as the term sensitive data under the PSD2 is not interpreted in line with the GDPR. The GDPR defines sensitive personal data (or special categories of data) as "data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual."[128] However, the PSD2 brings in additional definitions which is not found in the GDPR, such as "sensitive payment data". As noted by the Dutch data protection authority (Dutch DPA), this definition is rather inconsistent with the definition of "sensitive data" under

[125] Article 80 PSD2
[126] Marco Folcia and Gianmarco Zanetti and Sara Marcoli, 'The main regulatory change introduces: PSD2 in nutshell' (PwC) < https://www.pwc.com/it/en/industries/banking/assets/docs/psd2-nutshell-n03.pdf> accessed February 2019> accessed March 2019
[127] European Banking Authority, 'Consultation on RTS specifying the requirements on strong customer authentication and common and secure communication under PSD2' (Consultation Paper, 2016) 11 <https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2?p_p_auth=OtosFYa3&p_p_id=169&p_p_lifecycle=0&p_p_state=maximized&p_p_col_pos=1&_169_struts_action=%2Fdynamic_data_list_display%2Fview_record&_169_recordId=1616509> accessed May 2019
[128] Article 9 GDPR

the GDPR as the PSD2 defines "sensitive payment data" as data, including personalized security credentials which can be used to carry out fraud.[129] As extensively discussed in the second chapter, financial data which is held on the payment accounts can draw a detailed conclusion about an individual's personal life. An access to the bank account can reveal this type of information. Regulatory Technical Standard (RTS), Strong Customer Authentication (SCA) and Common and Secure Communication (SC) under the PSD2, leaves the discretion at the banks to determine which data is qualified as sensitive.[130] The Dutch DPA foresees that the use of a data protection impact assessment (DPIA) will be required for a proper classification.[131] The DPIA will help to map out and categories the type of data to be processed and whether or not this data fall in a category of sensitive data under GDPR. The question becomes whether financial data really "reveals" certain characteristics categorized as sensitive as per the GDPR, such as racial origin, political opinion, etc. The Dutch DPA is of opinion that payment data is of sensitive nature.[132] The financial data held on the bank account can for instance reveal that an individual is a member of certain political party. The executed transaction, such as membership fee or donations given to the political party can reveal political opinion.[133] With the help of DPIA it can be concluded that such data in itself should not be considered "high risk". However, in the context of Open Banking, where data can be combined with other data, processed via automated means, stored for a longer period and even shared with the third parties, constitutes a "risky nature" of processing this data.

The main problem with the inconsistent interpretation arises, as according to the data protection rules, sensitive data within the meaning of GDPR can only be processed on a limited legal basis.[134] Explicit consent would be the most appropriate one for the situation under the PSD2 when processing of that category of personal data takes place. At the same time, services provided by the account information providers in many cases constitute profiling and also in this case a prior explicit consent should be required.[135]

However, since the article 94 (2) PSD2, which requires explicit consent of the customers for the processing of payment data by the third party payment providers, makes an exemption on acquiring an explicit consent for the account information service providers, it results that processing of personal data under PSD2 would be circumventing the GDPR.It can even be argued that the processing of sensitive personal data by the account information service providers is unlawful as it is not necessarily based on the explicit consent. The data processor must therefore ensure that it adheres to the GDPR, regardless of the rules under PSD2. The exemption of the account information service providers from the rule on the explicit consent might even imply that this provision did not envisage 'explicit consent' as a legal basis but as an additional consent requirement outside the scope of GDPR.

[129] 'AP adviseert over wetgeving over invoering van richtlijn voor betaaldiensten (Dutch Data Protection Authority, 12 January 2019) < https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-adviseert-over-wetgeving-over-invoering-van-richtlijn-voor-betaaldiensten-psd2#subtopic-6852 > accessed January 2019
[130] Ibid.
[131] 'PSD2 and GDPR: An awkward match?' (Deloitte Touche Tohmatsu Limited, 2018) https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/legal/deloitte-nl-psd2-and-gdpr-an-awkward-match.pdf Accessed January 2019
[132] Dutch Data Protection Authority, 'Investigation into the combining of personal data by Google' (Report, 2013) < https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/en_rap_2013-google-privacypolicy.pdf> accessed August 2019
[133] Paul Voigt, *The EU General Data Protection Regulation: A practical guide (*Springer International Publishing, 2017)
[134] Article 9 GDPR
[135] Irish Data Protection Commissioner, 'Your rights in relation to automated decision making, including profiling (Article 22 of the GDPR)' <https://www.dataprotection.ie/en/individuals/know-your-rights/your-rights-relation-automated-decision-making-including-profiling> accessed August 2019

In order to avoid the risk of being non compliant, it should be clarified what type of data will be precisely processed under the PSD2 and whether they can be classified as sensitive data under the GDPR. Without further clarifications it is suggested, that banks take a precautionary approach and consider all data that is likely fall under the sensitive data category as sensitive data in order to avoid violating data protection rules, both under PSD2 and the GDPR. However, this might take a toll on businesses, as such approach is not only complex but also costly and not reliable or even not viable yet as banks are not able to filter out sensitive data.[136]

Pursuit to the article 94(2) on Data protection, "payment service providers shall only access, process and retain personal data necessary for the provision of their payment service, with the *explicit consent* of the payment service user." The GDPR also contains the requirement for those seeking to process personal data to obtain the 'explicit consent' of data subjects before doing so in certain circumstances – the explicit consent is linked to the situations where the data concerned qualifies as a special category of data or so called sensitive data. One way to interpret the data protection provision under the PSD2, is as the provision requires a consent being a *legal basis* for data processing by the payment service provider and hence interpreting the notion of the "explicit consent" taking the GDPR as the model to follow. As argued, such interpretation would ensure a high level of consumer protection.[137] It must be noted again that, according to the article 33(2) PSD2, the account information service providers are not subject to this particular data protection provision therefore, any type of the explicit consent is not a requirement for their services. As discussed below this is more problematic than in case of PISP which have limited access to the account information. The provision applies to the payment initiation service providers, as this is also evident from another provision on the "Access to payment account in the case of payment initiation services" which requires that "any other information about the payment service user, obtained when providing payment initiation services, is only provided to the payee and only with the payment service user's *explicit consent*."[138] Without any known reason, such wording is however missing from the similar provision concerning the account information service provider. As the account information services may be also used by the payment service providers to check whether the amount necessary for the execution of a card-based payment transaction is available on the customer's payment account, makes this exemption even more problematic.[139] Also based on that, it can be claimed that the account information service providers have unlimited access to the payment information, contrary to the limited access of payment initiation service providers, given that account information service providers are subject to less legal requirements under PSD2.

The main question then nevertheless remains whether the requirement of the "explicit consent" for the payment initiation service providers should be interpreted in the same way as per the GDPR. The literature has provided some opinions and guidelines on this issue.[140] The Directive itself does not provide any guidance as to the meaning of the explicit consent. Moreover, the

[136] 'Beuc's Recommendations to the EDPB on the interplay between the GDPR and PSD2' (Recommendations, BEUC-X-2019-021, 11 April 2019) <https://www.beuc.eu/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf> accessed June 2019
[137] Ibid.
[138] Article 66 PSD2
[139] Article 65 (1) PSD2
[140] Beuc's Recommendations to the EDPB on the interplay between the GDPR and PSD2' (Recommendations, BEUC-X-2019-021, 11 April 2019) <https://www.beuc.eu/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf> accessed June 2019
[140] 'PSD2 and GDPR: An awkward match?' (Deloitte Touche Tohmatsu Limited, 2018)

paragraph concerning the explicit consent was not previously part of the PSD1 therefore it is left to the expert to interpret the meaning of consent.[141]

Firstly, since the article 94(2) refers to the data protection legislation, it is argued that one could expect that in this situation the notion of the explicit consent is interpreted and held up to the same standards as in the GDPR, in case the same "data processing" situation takes place.[142] According to the Dutch Data Protection Authority, the explicit consent of the customer under PSD2 is in line with the GDPR.[143] Furthermore, as the GDPR contains additional rules on the use of explicit consent as a legal basis this would supplement PSD2. However, it also notes that as soon as the third party payment providers wants to process additional personal data than those necessary for the performance of payment initiation service, an additional consent is required that falls completely under the scope of the GDPR. Moreover, the Dutch DPA also argued that such consent by the customer is only pertained to the personal data of the customer that gave consent and not to the personal data of the silent party.[144]

The argument that the explicit consent should be understood in the data protection meaning can be supported by the fact that first paragraph of the same article allows for the processing of personal data for the prevention of fraud without having the consent of the customer. As a side note, it is believed that as a consequence of this rule the customer will lose track of what data is being processed, eventually leading to abuse.[145] Therefore, the existence of this rule helps to understand the second paragraph as a requirement for a data protection explicit consent.

However, the stakeholders who understand consent under the data protection provision of PSD2 as the data protection consent, nevertheless leave the room for the possibility that the processing might be also based on another legal ground under the GDPR, such as the processing necessary for the performance of a contract as per article 7(1)(b) of the GDPR. This is necessary, as it may be understood that an individual gives a consent to processing as a condition of service which makes consent less appropriate and even invalid.[146]

Nevertheless, this does not diminish the significance of the explicit consent as an additional legal basis required under PSD2. The explicit consent by the customer for the processing should be held up to the same standards as explicit consent under the GDPR. The consent must be informed, specific, unambiguous, etc. I agree with this argumentation, particularly, because I believe that there is a need for an explicit consent since sensitive data held in our payment accounts can only be processed when I explicitly agree with such processing. As observed in the guidelines, the Article 9(2) does not allow 'necessary for the performance of a contract' basis to be used as an exception for the processing of special categories of data.[147] Therefore, in my

[141] Article 94(2) PSD2
[142] 'Beuc's Recommendations to the EDPB on the interplay between the GDPR and PSD2' (Recommendations, BEUC-X-2019-021, 11 April 2019) <https://www.beuc.eu/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf> accessed June 2019
[143] 'PSD2 and GDPR: An awkward match?' (Deloitte Touche Tohmatsu Limited, 2018) https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/legal/deloitte-nl-psd2-and-gdpr-an-awkward-match.pdf Accessed January 2019
[144] Ibid.
[145] 'PSD2 and GDPR; friends or foes?' (Deloitte) < https://www2.deloitte.com/lu/en/pages/banking-and-securities/articles/psd2-gdpr-friends-or-foes.html> accessed May 2019
[146] 'PSD2 and GDPR: An awkward match?' (Deloitte Touche Tohmatsu Limited, 2018) https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/legal/deloitte-nl-psd2-and-gdpr-an-awkward-match.pdf Accessed January 2019
[147] European Data Protection Board, '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' (Guidelines, 9 April 2019)

opinion an explicit consent should always be required as a legal basis in the case of Open banking. By relying on this consent, it would be ensured that the processing of sensitive data (held on the bank account) is lawful as well as it will entitle the customer with all the rights linked to the consent, such as the right to revocation which was not part of the DPD.[148] Such control over the personal data by the customer is important considering all the negative consequences arising from the potential abuse of the personal data by the third party payment providers discussed in the second chapter. Moreover, I believe that the requirement of an (additional) consent as a legal basis should be further applied to the processing of personal data by the account information service provider which are now exempted from the data protection provision under the PSD2. This is important as the account information service provider in order to perform their services, process even more personal data and in even more intrusive way than payment initiation service provider, however, they are subject to less stringent regulation, as for unknown reasons, they are exempted from the data protection provision of PSD2. As many of their services constitute profiling under the GDPR and would involve automated decision making, the account information service provider should obtain an explicit consent by the customer for such processing and not be processed on some other legal basis.[149] On these points, the European Bank Authority has already raised concern about the amount of data that can be requested per communication session by the account information service provider even when the user is not actively requesting such information.[150] This goes against the requirements which are part of the data protection consent, such as giving the consent for a specific purpose only and data minimization. Moreover, according to the Authority for the Consumers and Markets ("ACM"), the account information service providers need to be transparent about their terms when providing their services.[151] The customer must be well informed before making the decision to use these services. This is less likely to be achieved without having informed consent in place as a legal basis for the processing of personal data.

Secondly, several stakeholders are of opinion that consent means different things in PSD2 and the GDPR.[152] In the absence of the requirement for the data protection consent as a legal basis for data processing under PSD2, such processing must be then based on at least one of the other legitimate grounds which results in different ramifications.[153] Without a lawful basis, the processing of personal data would be considered as unlawful. The opinion that consent means different things in PSD2 and GDPR is shared by the majority of the payment services industry as well as the European Data Protection Board ("EDPB") which argues that explicit consent referred to in Article 94(2) of PSD2 is an *additional contractual* and not a data protection

<https://edpb.europa.eu/sites/edpb/files/consultation/edpb_draft_guidelines-art_6-1-b-final_public_consultation_version_en.pdf> accessed April 2019

[148] L Curren and J Kaye, 'Revoking consent: a 'blind spot' in data protection law?' (2010) 26(273) Comp L & Sec Rev 2010 < https://scholar.google.com/scholar_lookup?title=Revoking%20consent%3A%20a%20%E2%80%98blind%20spot%E2%80%99%20in%20data%20protection%20law%3F&author=L%20Curren&author=J.%20Kaye&publication_year=2010&journal=Comp%20L%20%26%20Sec%20Rev&volume=26&pages=273-83>

[149] 'Beuc's Recommendations to the EDPB on the interplay between the GDPR and PSD2' (Recommendations, BEUC-X-2019-021, 11 April 2019) <https://www.beuc.eu/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf> accessed June 2019

[150] European Banking Authority, 'Single Rulebook Q&A' (2018) < https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4309> accessed March 2019

[151] 'ACM enforces competition with regard to payment service directive "PSD2"' (ACM Publication) < https://www.acm.nl/en/publications/acm-enforces-competition-regard-payment-service-directive-psd2> accessed May 2019

[152] .T.J. Wolters and B.P.F. Jacobs, 'The security of access to accounts under the PSD2' (2018) Computer Law & Security Review: The International Journal of Technology Law and Practice <https://scihub-dl.com/pdf/0/scihub-dl.com-39.pdf> accessed May 2019

'BEUC's Recommendations to the EDPB on the interplay between the GDPR and PSD2' (Recommendations, BEUC-X-2019-021, 11 April 2019) <https://www.beuc.eu/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf> accessed June 2019

[153] Inside Privacy, 'Overlap between GDPR and PSD2' (16 March 2018) <https://www.insideprivacy.com/financial-institutions/overlap-between-the-gdpr-and-psd2/> accessed December 2019

consent.[154] To support this argument the EDPB refers to Recital 87 of PSD2, which states that the Directive "should concern only contractual obligations and responsibilities between the payment service user and the payment service provider". Several national Data Protection Authorities agree in that the required consent should be seen as an additional protection imposed by PSD2 and not as a legal basis for the processing of personal data under the GDPR.[155]

Instead of consent, the EDPB proposes a contractual performance as the appropriate legal basis for the processing. The explicit consent under the PSD2 can then be understood more as a transparency obligation than data protection consent.[156] It can be argued that the PSD2 introduces a new type of "semi data protection consent." The aim of this type of consent, which does not constitute a legal basis, is to rather make a customer better informed about the purposes for which their personal data is processed. PSD2 however, does not list any requirement as to what information should be provided to customers. BEUC even made a following proposal on the explicit consent under PSD2, taking into account WP29 guidelines on consent:

> *'by ticking this box, I agree that company "XXX" will have access to the following financial data (list data for which the access is being requested) managed by the ASPSPs (bank) "YYY".*[157]

Moreover, the term "explicit" under PSD2 implies that the customer explicitly agrees to the processing in a manner that is distinguished from the other contractual matters. In that view, the meaning of the explicit part of the consent can be compared to the meaning of the explicit consent under the GDPR.

Even though there are stakeholders who share the opinion that the explicit consent under the article 94(2) should be interpreted as a data protection consent, constituting a legal basis for data processing, as previously discussed, the EDPB has disagreed with this statement. As a result, the explicit consent must be seen as an additional requirement or a quest for a transparency on the top of the chosen legal basis. The literature proposes the contractual performance as the most appropriate one.

Despite the fact that some might question the necessity of the additional consent as a legal basis if there is already some other legal basis in place, it could be argued that explicit consent under PSD2 should be an additional legal basis besides the use of another legal ground. The main reason for this is that an under GDPR, explicit consent is the only possible legal ground for the situations of the processing of sensitive personal data or automated decision making processing which are situations also applicable to the concept of Open Banking. Without an explicit consent, the customer cannot have adequate level of control over their personal data as no other legal basis under GDPR does not directly involved an individual in the question whether or not processing can take place. For instance, the consent as a legal basis requires that the new consent or a new legal basis is obtained for any new or further processing while under the legal basis for the performance of the contract the processing is allowed as long as it is in the scope of the

[154] 'Letter regarding PSD2 directive' (EDPB, 84-2018, 5 July 2018) < https://edpb.europa.eu/news/news/2018/letter-regarding-psd2-directive_en> accessed February 2019
[155] 'The Netherlands tackles uncertainties around PSD2 consent and GDPR' (Medium, 20 November 2018) <https://medium.com/@touchtech/the-netherlands-tackles-uncertainties-around-psd2-consent-and-gdpr-e5beb31c4e16> accessed May 2019
[156] Christian F. McDermott, 'GDPR & PSD2: Squaring the Circle' (Latham & Watkins LLP, 13 August 2018) https://www.globalprivacyblog.com/legislative-regulatory-developments/gdpr-psd2-squaring-the-circle/ accessed January 2019
[157] 'BEUC's Recommendations to the EDPB on the interplay between the GDPR and PSD2' (Recommendations, BEUC-X-2019-021, 11 April 2019) <https://www.beuc.eu/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf> accessed June 2019

existing contract. This is problematic as it was observed that the services provided by the third party payment providers are vaguely defined.[158] It was also noted that as part of the service the personal data can be shared with parties other than primary service provider.[159] Therefore, consent would be considered a more appropriate legal basis to limit the scope of the services and hence processing of the financial data by third party payment providers and prevent the abuse. At the same time, I find a request for an additional contractual consent for the processing of personal data an innovative way to ensure adequate level of data protection when processing is based on some other legal basis. However, the legislator should better define what constitutes the valid contractual consent. Here I would suggest taking an explicit consent from the GDPR as an example.

If properly used, this contractual consent or as in this thesis referred to as a semi-data protection explicit consent is an additional requirement introduced by the PSD2 that can to the certain extend substitute the explicit data protection consent in situations when data is chosen to be processed on the other legal basis. This requirement can enhance data protection. I nevertheless believe that the explicit consent from the article 94 of the PSD2 should be understood as a data protection consent within the meaning of the GDPR. The PSD2 mentions "explicit consent" in situations where access to customers data is given.[160] It would logically follow that consent should be understood in a data protection meaning. This could be also supported by the Article 94 PSD2 which even refers to the data protection legislation (now GDPR). This paragraph was not included in PSD1. The possibility that the processing is based on some other legal bases under GDPR does not exclude that the explicit consent under PSD2 should be interpreted as per the GDPR.

However, my main concern related to the issue of consent is that the account information service providers are not part to the data protection article, so they are not subject to the explicit consent requirement, this either be interpreted as a contractual consent or data protection consent. Their processing will nevertheless need to be based on legal basis to comply with the GDPR. Importantly, when processing of a sensitive data, this being explicit consent.

Even though I like the opinion of some, that the legislator of the PSD2 intended to include a requirement for an explicit consent as an additional legal basis, I do not believe this is a case. This is because the legislator already refers to the data protection legislation which governs this matter in more details.

Following the argumentation of the EDPB it can be concluded that the notions of explicit consent is not the same for PSD2 and GDPR. This was also assumed by the BEUC.[161] Explicit consent under PSD2 can be understood as an additional requirement of a contractual nature and is not the same as consent within the meaning of the GDPR. Therefore, this implies that the third party payment providers as per payment initiation service providers will be required to obtain both PSD2 and the GDPR consent.

[158] T.J. Wolters and B.P.F. Jacobs, 'The security of access to accounts under the PSD2' (2018) Computer Law & Security Review: The International Journal of Technology Law and Practice <https://scihub-dl.com/pdf/0/scihub-dl.com-39.pdf> accessed May 2019
[159] BillGuard (https://www.billguard.com/) Yodlee (http://www.yodlee.com)
[160] Article 65-67 and article 94(2) PSD2
[161] 'BEUC's Recommendations to the EDPB on the interplay between the GDPR and PSD2' (Recommendations, BEUC-X-2019-021, 11 April 2019) <https://www.beuc.eu/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf> accessed June 2019

Many questions about the correct interpretation remain. My main question would be as to why the requirement for this additional contractual consent is included under the article on data protection and why did the legislator of the PSD2 leave so much room for interpretation of this notion and leave out of the scope the account information service providers.

3.3. Conclusion

The financial services industry has to adapt to new legislation such as PSD2 and GDPR. This chapter assessed the compliance burden caused by the conflict between PSD2 and GDPR, in regard to the notion of the 'explicit consent', being a requirement for the processing of personal data held on customer's bank accounts by payment initiation service providers. It is not clear from PSD2 whether this notion has the same meaning as per GDPR. Therefore, the interpretation is needed. It is argued by the majority, that the 'explicit consent' under PSD2 must be seen as an additional contractual requirement and not necessarily a legal basis for the processing of payment data. Question, such as why are the account information service providers left out of the data protection provision remains.

4. Chapter 4

4.1. Introduction

One of the key elements of the GDPR and related to the PSD2, also in terms of the potential conflict, is the notion of consent. The notion of 'explicit consent' plays an important role in the business model under the revised PSD2 as without an explicit consent payment data cannot be access, process and retain by a third party providers (as discussed in Chapter 3).[162]

Most parts of this chapter will shift focus from the PSD2 to the description of the role of consent and its significance in the data protection. The first part of this chapter will focus on the theoretical background of the notion of consent in data protection. The last part will explore the extend the 'explicit consent' for the processing of personal data is suitable in the case of Open Banking under PSD2.

4.2. Value of legal consent

The value of legal consent has been extensively discussed in the field of legal theory and ethics.[163] The majority of literature sees the value of consent in the light of autonomy or self-determination.[164] The ethical rationale underlying the doctrine of informed consent is rooted in the notions of freedom of choice, liberty, and autonomy.[165] The role of consent in that view is seen in the importance to respect a person's decision making even though such decision does not maximize his or her well-being.[166] The notion of consent has been a laudable and a necessary part of the any regulatory regime or legal domain as is it used to constitute legal acts.[167] For instance, consent is considered to be a possible as well as an appropriate device to legitimate large parts of the international law, signaling the state sovereignty.[168] Moreover, consent lies in the center of the contract law and it is linked to the ideal of freedom of contract. The agreement is valid only if parties freely consent to its terms and conditions.[169]

4.3. Role of consent in data protection and its effectiveness

The general values of consent, such as serving the right of autonomy or well-being have also been translated in the field of privacy and later in the field of data protection. In relation to privacy, consent is commonly discussed in terms of control over personal data and information self-determination.[170] Consent to the processing of personal data has been long seen as the most important mechanism that exists for the data subject being able to determine on how and when

[162] Article 94 PSD2
[163] UK Clinical Ethics Network, 'Ethical Issue- Consent' <http://www.ukcen.net/ethical_issues/consent/ethical_considerations1>
[164] Ibid.
[165] Christina Hultsch, 'Basic principles of European Union consent and data protection (Porter Wright Morris & Arthur LLP, 25 July 2011) https://www.technologylawsource.com/2011/07/articles/privacy-1/basic-principles-of-european-union-consent-and-data-protection/ accessed January 2019
[166] Charles E Harris et al., *Engineering Ethics* (5th Edition, Wadsworth, 2013)
[167] European Commission, 'Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on a comprehensive approach on personal data protection in the European Union' (2010) COM(2010) 609 final, 04.11.2010.
[168] Matthew Lister, ' The Legitimating Role of Consent in International Law' (2011) 11(2) Chicago Journal of International Law http://chicagounbound.uchicago.edu/cjil/vol11/iss2/25 accessed June 2019
[169] Alan Wertheimer, 'Consent in Contract Law" THE ETHICS OF CONSENT: THEORY AND PRACTICE' (2010) no.08-36 (Oxford University Press, Minnesota Legal Studies Research) <https://ssrn.com/abstract=1140256> accessed May 2019
[170] Bart Cluster et al., *Consent and Privacy* (The Routledge Handbook of the Ethics of Consent, 2018)

this data can be used.[171] As explained in the guidelines by the Article 29 Working Party, by consenting, a data subject itself authorizes the processing of their personal data. This signals enhanced power of the control over data subject's personal information and has been an important idea from a fundamental right perspective.[172] The consent which is in the literature often referred as a privacy self-management, gives a data subject influence over the processing of his or her personal information which implies that data subject can exercise his or her autonomy.[173] The control through consent is also evident in the possibility for data subject to withdraw his or her consent, preventing any further processing of the data subject's data by the controller.[174] The early literature saw the possibility for a revocation of a given consent as a new understanding of control of personal data.[175] Some scholar went even further in arguing that the consent requirements cannot be reduced or eliminated as they represent the last defense for an individual against the loss of control on their personal information processing.[176]

Yet, the more recent literature has raised many concerns in terms of consent being ineffective for privacy protection.[177] This follows from the observations that consent is in many situations uninformed and people are failing to exercise their right effectively.[178] To this end, the PSD2 marries the emphasis on a "semi-data protection consent" with a parallel focus on some other legal basis for the processing personal data which could enhance the users' privacy and could be a solution to address the drawbacks of the data protection consent. Moreover, the privacy is further enhanced with the duties of data controllers, regardless whether the consent is fully efficient.

The above mentioned importance of consent has been acknowledged by the legislation on privacy and the data protection in Europe as well as globally. Some European national legislation on privacy or data protection acknowledged the consent as one of the legal grounds for processing personal data in the seventies already.[179] Also in the United States, the case law recognized the informed consent as a privacy claim.[180] Although in that time discussion was not related to protection of personal data itself, the case law recognized the "interest in independence in making certain kinds of important decisions", as seen in the case discussing the invasion of one's bodily integrity.[181] On the level of the European Union, the reliance on consent as a criterion for legitimizing personal data processing operations has been included in the very beginning of the legislative process as well as in the latest adoption of DPD and finally the

[171] Edgar A Whitley, 'Informational privacy, consent and the "control" of personal data' (2009) 14(3) Information Security Technical Report <https://reader.elsevier.com/reader/sd/pii/S1363412709000363?token=801F05515C5B3A44704F5329A12E213E093F6B3ED273C87E27F75F80DC87AF3ED8FC44289FAF7383EA7B266D82648766> accessed May 2019
[172] Eleni Kosta, *Consent in European Protection Law* (Brill, 2013) p.30
[173] Article 29 Working Party, 'Guidelines on consent under Regulation 2016/679' < https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051> accessed May 2019
[174] Article 7(3) GDPR
[175] Edgard A. Whitley, 'Informational privacy, consent and control of personal data' (2009) 14(3) Information Security Technical Report <https://reader.elsevier.com/reader/sd/pii/S1363412709000363?token=801F05515C5B3A44704F5329A12E213E093F6B3ED273C87E27F75F80DC87AF3ED8FC44289FAF7383EA7B266D82648766> accessed May 2019
[176] Eugenia Politous et al., 'Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions' (2018) 4(1) Journal of Cyber Security < https://academic.oup.com/cybersecurity/article/4/1/tyy001/4954056> accessed August 2019
[177] Yvonne McDermott, 'Conceptualising the right to data protection in an era of Big Data' (2017) 1(7) Big Data & Society <https://journals.sagepub.com/doi/pdf/10.1177/2053951716686994> accessed July 2019
[178] T Matzner et al., 'Do it yourself data protection- Empowerment or Burden? (2016) Springer <http://www.philippmasur.de/documents/pubs/Matzner%20Masur%20et%20al._2016_Do-it-yourself%20data%20protection.pdf> accessed August 2019
[179] Article 29 Data Protection Working Party, 'Opinion 15/2011 on the definition of consent' (13 July 2011) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf> accessed May 2019
[180] Ruth R. Faden and Tom L. Beauchamp, *A History and Theory of Informed Consent* (Oxford University Press, 1986)
[181] Whalen v. Roe, 429 U.S. 589 (1977)

GDPR. [182] As observed in the next section, the popularity of consent in terms of self-determination and its effectiveness decreased over the years.

It can be argued that consent has played an important role in data protection as it is the only ground for legitimacy that focuses on the data subject's self-determination. From that it would reasonably follow that when processing is based on consent, an individual can be ensured that his personal data is processed in a manner in which he has given the consent.[183]

Based on the above mentioned it could be concluded that at least in theory, processing of personal data by third party payment providers based on the consent, if properly used, can ensure the adequate level of data protection. However, as it will be discussed in the next sections, in practice, the processing based on consent can be seen as problematic, also in the situation of Open Banking.

4.4. The notion of consent throughout the EU legislative history

The notion of consent has not always been an integral part of the data protection. Consent gained more significance when data protection shifted focus away from the control over the data processing technology itself to the protection of privacy of individuals.[184] This was eventually understood as the principle of informational self-determination which implies that an individual has control over their personal data. In the European data protection legislation, it was first intended to be used as a tool to stop an action that would otherwise be invasive.[185] Over the years, the main idea was that individuals get control over the data processing process. Therefore, in some cases consent became a precondition for personal data processing. Moreover, the Norwegian Data Act went even further to allow the individuals to refuse processing of their data for the purposes of a direct marketing or market research.[186] It was understood that an individual is best suited to protect his or her personal data and that data protection is all about an individual freedom of citizens.[187]

The rules on data protection from the 1980s finally put the emphasis on the participation and informational self-determination. The main reason behind this idea was the German Constitutional Court with its population census case in 1983.[188] As a result of this judgment, the population census was postponed, and the court proclaimed the right of information self-determination as a constitutional fundamental right. Under this right, an individual gets the ability to decide or to determine the use of his or her personal data. The literature sees the importance of this judgment for the further development of the data protection laws in Europe. As noted by Kosta, the right to information self-determination deriving from the German judgment influenced the national data protection legislations, placing an individual as an active

[182] Article 29 Data Protection Working Party, 'Opinion 15/2011 on the definition of consent' (13 July 2011) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf> accessed May 2019
[183] Articles 12-23 GDPR
Article 29 Working Party, 'Guidelines on consent under Regulation 2016/679' < https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051> accessed May 2019
[184] V. Mayer-Schönberger, *Generational development of data protection in Europe* (Cambridge: The MIT Press, 1997)
[185] Neil Manson and Onora O'Neill, *Rethinking informed consent in bioethics* (Cambridge University Press, Cambridge 2007)
[186] Ibid, page 223
[187] Ibid.
[188] BverfGE 65,1 of 15 december 1983 (Volkszählung)

participant in society.[189] It is argued that as a result of the new right to information self-determination, consent became an integral part of data protection law.[190] This was for instance evident in Norway and Finland which amended their legislation to accommodate the right to informational self-determination.[191] However, in practice an individual still remained a weaker party, unable to exercise the new right. Therefore, a new generation of the data protection rules took this into consideration. For instance, already DPD recognized the consent as a ground for a legitimate processing of personal data, including a sensitive data and a transfer of personal data to the third country with a weaker data protection. It can be argued that DPD implemented the right to informational self-determination through the consent which intended to be a powerful tool of applying control to data processing activities. DPD offered, at least in theory, several opportunities for data subjects to remain in control over their personal data.[192]

However, the increased control in the hands of the data subject was in many situations only illusional.[193] According to Kosta, the concept of consent in DPD was too vaguely defined, allowing for a (too) broad interpretation.[194] Moreover, the fact that the concept of consent had to be interpreted in each Member State according to their civil law, led to even more discrepancies in its interpretation. Consent as per DPD faced several other contextual problems. For instance, there were uncertainties about the amount and type of information to be provided in order for consent to be informed.[195] More control in hands of data subject does not mean that individuals will act to limit data processing or that such processing will decrease.

The autonomy of individual plays an important role also in the recent legislation. Recital 7 of GDPR states that '[n]atural persons should have control of their own personal data.[196] With the adoption of the GDPR the notion of informational self-determination seems to have become more important as the GDPR added control for individuals with regards to their own personal data, such as data portability. Conditions for consent have been strengthened. It must be as easy to withdraw a consent as it is to give it.[197] However, it can be argued that information self-determination related to consent is not at the core of the GDPR, as the legislator encourages the data processing not only on the basis of consent but also on several other legal grounds. There is no legal basis 'better' or more important than others.[198] Therefore, the question arises in which situations is consent the most appropriate legal basis for the processing of personal data? In order to analyze whether consent is even an appropriate legal basis for the processing of personal data by the third party payment providers under PSD2, the requirements for the valid consent under the GDPR need to be examined first. After that, the section will identify the problems of consent as a legal basis and finally apply them to the third party payment providers.

[189] Eleni Kosta, *Consent in European Data Protection Law* (Brill Nijhoff, 2013) p. 52
[190] Ibid.
Article 29 Working Party, 'Opinion 15/2011 on the definition of consent'(2011) < https://www.pdpjournals.com/docs/88081.pdf> accessed June 2019
[191] Ibid. page 106
[192] Articles 7(a), 8(2)(a), 14, 15(1) and 26(1)(a) DPD
[193] Lee A Bygrave and Dag Wiese Schartum, *Consent, Proportionality and Collective Power in Reinventing Data Protection?* (Springer, 2009)
[194] Eleni Kosta, *Consent in European Data Protection Law* (Brill Nijhoff, 2013) p. 52
[195] This is addressed in more details in GDPR
[196] Recital 7 GDPR
[197] 'GDPR key changes' (EU GDPR Portal) < https://eugdpr.org/the-regulation/> accessed June 2109
[198] 'Lawful basis for processing' (UK Information Commissioner's Office) < https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/> Accessed July 2019

4.5. Conditions for a valid consent under the GDPR

The GDPR in article 4(11) lists several requirements that must be satisfied in order to grant consent. In order to be valid, the consent should be freely given, informed, specific, unambiguous, and in certain cases also explicit. Moreover, the GDPR provides that the data subject should give his or her indication of wishes by a statement or by a clear affirmative action. The analysis of the consent requirements is based on the GDPR as well as on the Article 29 Data Protection Working Party's guidelines on consent for the GDPR and their earlier Opinion.

Firstly, the consent must be freely given.[199] This means that consent reflects a data subject's genuine or a free choice.[200] Furthermore, the data subject should not fear severe disadvantages if they refuse to give consent. Any element of pressure on the data subject invalidates the consent.[201] This risk is also acknowledged in the GDPR which states that consent cannot be used as a legal basis in case of a clear imbalance between the data subject and the controller, such as in the some situations in the context of the employment relationship.

Secondly, the consent must be informed. The data subject must be informed about the processing and rights in a clear and transparent way, before making any decisions. The notion of informed consent was for the first time used in the context of medical research. The Nuremberg Code established the right to withdraw from medical research, effectively revoking any consent that was given or implied.[202] Some argued that the development of the data protection consent was first inspired by the informed consent used in medicine.[203]

Thirdly, the consent must be specific which is intrinsically linked to the requirement for the informed consent.[204] This implies that consent is specific when the data subject is provided with enough information about the use of personal data and processing methods. Moreover, the request for consent shall be separated from the other terms and conditions, concise, in an intelligible and easily accessible form, using clear and plain language.

Fourthly, the consent must be unambiguous. This is a new requirement, added by the GDPR.

According to the GDPR, unambiguous means that the data subject should not leave any doubt of his intentions for giving the consent. This can be achieved by for instance consenting with an active declaration, so it is obvious that the data subject has consented.

Finally, the consent is explicit when expressly confirmed by data subject, for instance in writing and there are no doubts about the intention. Explicit consent signals a higher level of control and data protection and even though not defined in the legislation, it is only used in specific circumstances under the GDPR.[205] As explained by the WP29, explicit consent is required in

[199] Article 4(11) GDPR
[200] Recital 42 GDPR
[201] Article 29 Working Party, 'Guidelines on consent under Regulation 2016/679' (WP259 rev.01, 10 April 2018) < https://iapp.org/media/pdf/resource_center/20180416_Article29WPGuidelinesonConsent_publishpdf.pdf> accessed March 2018
[202] Klaus Hoeyer, ' Informed consent: the making of a ubiquitous rule in medical practice' (2009) 169(2) Sage publication < http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.838.6147&rep=rep1&type=pdf> accessed February 2019
[203] Neil Manson and Onora Neill, 'Rethinking Informed Consent in Bioethics' (2007) 8(8) Cambridge: Cambridge University Press < https://heinonline.org/HOL/LandingPage?handle=hein.journals/selt3&div=20&id=&page=> accessed May 2019
[204] Article 29 Working Party, 'Guidelines on consent under Regulation 2016/679' (WP259 rev.01, 10 April 2018) < https://iapp.org/media/pdf/resource_center/20180416_Article29WPGuidelinesonConsent_publishpdf.pdf> accessed March 2018
[205] 'Explicit consent and how to obtain it – new GDPR consent guideline' (I-scoop) <https://www.i-scoop.eu/gdpr/explicit-consent/#What_is_explicit_consent_and_when_do_you_need_it> accessed April 2019

certain situations when there is a higher risk for data protection. Firstly, explicit consent legitimates the processing of special categories of personal data.[206] Secondly, the explicit consent is mentioned in relation to the automated individual decision-making.[207] Thirdly, explicit consent is used in the situations when data is transferred to third countries or international organizations in the absence of adequate safeguards.[208] Explicit consent should be a two-steps process where the controller provides with an explicit statement of a proposed action, its consequences and risks to the data subject. After that, the data subjects must explicitly state that they understand the information provided and will agree to the request.[209]

4.6. Problems with consent as a legal basis

Much has been written in the academic literature about the effectiveness of consent in the context of data processing.[210] The literature as well as society show a lot of skepticism and doubts about the use of consent.[211] As discussed earlier, consent legitimizes nearly any form of processing of personal data.[212] However, the literature argues that consent does not always provide people with meaningful control over their data.[213] According to the empirical and social science research, consent is undermined by the severe cognitive problems of the individuals which have effect on their ability to make informed, rational choices about the costs and benefits of consenting to the processing of their personal data.[214] In other words, people lack knowledge to adequately assess the consequences of consenting and therefore an uniform individual cannot make a rational decision when consenting to the data processing. This is problematic as it is shown that most people choose to ignore privacy notices or are even not proactive in changing the default privacy settings on the website. [215] This can be confirmed by a recent study conducted by BEUC.[216] Most of the customers from the study are not giving informed consent when they share their financial data as they do not read or understand what is written in terms and conditions.[217]

Moreover, structural problems, such as the increasing number of entities processing individual's personal data or uninformed changes to privacy notices and future aggregation of data, make consenting even of a well-informed and rational individual troublesome. Today, an average person does not have enough time and resources to manage his personal data. [218] Therefore, it

[206] Article 9 GDPR
[207] Article 22 GDPR
[208] Article 45 and 46 GDPR
[209] I-scoop, 'Explicit consent and how to obtain it – new GDPR consent guideline' <https://www.i-scoop.eu/gdpr/explicit-consent/#What_is_explicit_consent_and_when_do_you_need_it> accessed April 2019
[210] Bart W. Schermer and Bart Custers, 'The crisis of consent: how stronger legal protection may lead to weaker consent in data protection' (2014) 16(2) Ethics and Information Technology < https://link.springer.com/article/10.1007/s10676-014-9343-8> accessed March 2019
[211] Ibid.
[212] Daniel J. Solove, 'Privacy Self-Management and the Consent Dilemma' (1880) 126 Harv. L. Rev. (2013) < https://pdfs.semanticscholar.org/809c/bef85855e4c5333af40740fe532ac4b496d2.pdf> accessed December 2018
[213] Ibid.
[214] Ibid.
[215] Adam S. Chilton and Omri Ben-Shahar, 'Simplification of Privacy Disclosures: An Experimental Test' (Coase-Sandor Working Paper Series in Law and Economics No. 737, 2016) < https://chicagounbound.uchicago.edu/law_and_economics/774/ > accessed March 2019
Alessandro Acquisti and Jens Grossklags, 'What Can Behavioral Economics Teach Us About Privacy?' (2006) Digital Privacy < https://www.heinz.cmu.edu/~acquisti/papers/Acquisti-Grossklags-Chapter-Etrics.pdf> accessed January 2019
[216] 'Consumer-friendly open banking: access to consumer' financial data by third parties' (BEUC-X-2018-082, 20 September 2018) < https://www.beuc.eu/publications/beuc-x-2018-082_consumer-friendly_open_banking.pdf> accessed June 2019
[217] 'Beuc's Recommendations to the EDPB on the interplay between the GDPR and PSD2' (Recommendations, BEUC-X-2019-021, 11 April 2019) <https://www.beuc.eu/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf> accessed June 2019
[218] Bert-Jaap Koops , 'The Trouble with European Data Protection Law' (2014) International Data Privacy Law 250 < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2505692> accessed May 2019

could be argued that consent must be subject to a rigorous requirements under data protection law, such as consent being concise and intelligible, in order to protect individuals who are presumably unable to provide meaningful consent in many situations. As noted by Solove, it is difficult for the individuals to assess (future) harm as the privacy can be considered a long term issue, whilst most decisions to consent are tied to short-term benefits.[219]

If obtained in full compliance with the GDPR, consent is a tool that gives data subjects control over whether or not personal data concerning them will be processed. If not, the data subject's control becomes illusory and consent will be an invalid basis for processing.[220]

However, consent is not the only ground that legitimizes data processing. In certain cases, the processing should be based on some other grounds, such as when the processing is necessary for the performance of a contract.[221] The next part will examine whether or not the use of consent as a basis for processing personal data provides adequate data protection in Open Banking where the access to personal data (processing) by a third party payment provider is only allowed when the customer has given an explicit consent.

In this chapter it is examine what level of data protection can a customer expect if "explicit consent" is a legitimate basis for the processing of personal data by a third party payment provider as it could be interpreted under Article 94 PSD2 on Data Protection. It follows that without a valid consent, the processing is considered unlawful.[222] As an alternative interpretation of the same article, the necessity for the performance of a contract constitutes legal ground together with the requirement for "explicit consent" of the semi-data protection meaning or of contractual nature.

As confirmed by European Banking Authority, it is the obligation of the third party payment provider to obtain consent whereas banks are not obliged to double check whether consent was actually given.[223] With that, European Banking Authority finally clarified the question about the consent management in the case of Open Banking. As the third party payment providers are obliged to obtain consent it can be interpreted that they are the controllers as per the GDPR.[224]

As previously discussed, GDPR requires the consent to be "freely given, specific, informed and unambiguously." Therefore, these specific requirements from the GDPR supplement the specific rules on consent under PSD2. It could be argued that Article 94(2) PSD2 mimics the requirement for data minimization by emphasizing that payment service providers shall only process personal data *necessary* for the provision of their services.

[219] Daniel J. Solove, 'Privacy Self-Management and the Consent Dilemma' (1880) 126 Harv. L. Rev. (2013) < https://pdfs.semanticscholar.org/809c/bef85855e4c5333af40740fe532ac4b496d2.pdf> accessed December 2018.
[220] Article 29 Working Party, 'Guidelines on consent under Regulation 2016/679' (WP259 rev.01, 10 April 2018) < https://iapp.org/media/pdf/resource_center/20180416_Article29WPGuidelinesonConsent_publishpdf.pdf> accessed March 2018
[221] Article 6(b) GDPR
[222] 'CAPS Considerations on PSU Consent under PSD2' (CAPS, White paper, March 2018) <https://www.caps-services.com/documents/CAPS%20Considerations%20on%20PSU%20Consent%20under%20PSD2.pdf> accessed March 2018
[223] European Banking Authority, 'Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC' (EBA-Op-2018-04, 13 June 2018) <https://eba.europa.eu/documents/10180/2137845/Opinion+on+the+implementation+of+the+RTS+on+SCA+and+CSC+%28EBA-2018-Op-04%29.pdf/0f525dc7-0f97-4be7-9ad7-800723365b8e> accessed January 2019
[224] Andrew Clearwater and Brian Philbrook, 'Practical tips for consent under GDPR' (Iapp, 23 January 2018) < https://iapp.org/news/a/practical-tips-for-consent-under-the-gdpr/> accessed February 2019

Firstly, the third party payment providers are able to access a large range of data, therefore it is important that the consent is specific.[225] Secondly, the customers must agree with the processing separately form the other parts of agreement. The third party payment providers are not allowed to include the request for the consent inside broader request for the acceptance of the terms and conditions for the service.[226] This can be ensured by creating a separate window, such as a checkbox which also makes consent unambiguous. If the consent is made as a precondition of a service, consent is considered to be invalid.[227] As the Open Banking is all about the provision of payment services, performance of the contract can be used as a legal basis. In this case, the processing of personal data is necessary for the performance of the contract in which third party provider's obligations are strictly defined and consequently is also limited the processing of personal data for the provision of the service under the contract. The problem arises as PSD2 nor literature do not specify any contractual requirements governing the relationship between the third party provider and customer. It is clear however, that no contract is required between the third party provider and banks which are data controllers in case of Open Banking.[228] In the absence of detailed contract between customer and third party provider, the relationship could for instance be based on the acceptance of a simple terms and conditions which allows for a broad provision and change of services and consequently the unlimited processing. Therefore, it is uncertain whether consent or performance of the contract would better limit the processing of personal data under Open Banking.

As another consent requirement, the customer must agree with a specific processing purpose. The customer must be aware of the processing purpose and any further (even compatible) processing should be limited or prohibited. It is explained that the third party payment providers will only be allowed to provide the services that the payer decides to make use as agreed by the way of consent.[229] In order to provide these services and at the same time not processing more than necessary, PSD2 ensures that the third party payment providers will not have full access to the account of the payer. For instance, the payment initiation service provider will only be able to receive information from the payer's bank on the availability of funds (a yes/no answer). On the other hand, the account information service provider will receive from the customer's bank the information explicitly agreed by the payer and only to the extent they are necessary for the service previously agreed and provided to the customer. In that way it can be argued that PSD2 imposes limitations on the scope of the processing of customer's personal data by the third party payment providers. This could be understood as a general requirement and not the requirements steaming from the data protection explicit consent found PSD2. It is important to note, that a consent-based model alone anyway does not entirely guarantee the protection personal data, for instance when data collected for one purpose can be used for another purpose.[230]

[225] European Banking Authority, 'Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC' (EBA-Op-2018-04, 13 June 2018) <https://eba.europa.eu/documents/10180/2137845/Opinion+on+the+implementation+of+the+RTS+on+SCA+and+CSC+%28EBA-2018-Op-04%29.pdf/0f525dc7-0f97-4be7-9ad7-800723365b8e> accessed January 2019

[226] 'The Netherlands tackles uncertainties around PSD2 consent and GDPR' (Medium, 20 November 2018) <https://medium.com/@touchtech/the-netherlands-tackles-uncertainties-around-psd2-consent-and-gdpr-e5beb31c4e16> accessed May 2019

[227] 'What is valid consent?' (ICO) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/> accessed June 2019

[228] 'Open banking, open liability' (Ashurst, 2018) < https://www.ashurst.com/en/news-and-insights/legal-updates/open-banking-open-liability-accountability-issues-for-open-banking-apis/> accessed August 2019

[229] Ibid.

[230] Yvonne McDermott, 'Conceptualizing the right to data protection in an era of Big Data' (2017) 1(7) Big Data & Society <https://journals.sagepub.com/doi/pdf/10.1177/2053951716686994> accessed July 2019

Furthermore, consent must be informed. As indicated in the GDPR, the data subject must be provided with at least information about the identity of the controller and the intended purposes of the processing, the right to withdraw consent at any time prior to giving consent, etc.[231] This requirement translated to the Open banking situation imply that the customer must know the identity of third party payment provider, what data they wish to share, how frequently and the expiration period of the consent. As shown by the study conducted by BEUC, customers are not giving an informed consent when they share their financial data.[232] The risk remains that the customers will be presented with too much, often difficult and highly legalistic information in consent requests. That would mean that the consent lacks any practical meaning as most of the customers will just agree with something they have not read or understood. Therefore, the third party payment providers must ensure that the request for the consent is written in a clear and plain language.[233]

Moreover, the customer has the right to withdraw a consent and in so deny the access to his or her account.[234] It is on the customer and not on the bank to revoke the consent.[235] Bank as a data controller must act upon such customer's request, however, having no agreement in place with the third parties, might result in banks being unaware of existing consents which could undermine the customer's right link to consent.[236]

Another fear that would undermine the requirement for a freely given consent is that the customers do not really have a meaningful choice when given a consent request, left with a 'take it or leave it' scenario.[237] As a result, the use of consent as a legitimate basis for the processing might undermine customer's data protection as it might not reflect the individual's wishes.

Certain situations require the consent to be explicit. This could be for instance, when processing of sensitive data is at stake. Compared to the general consent, the explicit consent must be collected in a precise and clear way.[238] According to the British ICO "the statement to obtain explicit consent must specify the nature of the data to be collected, the details of the automated decision and its effects or the details of the data that are going to be transferred and the risks of said transfer". The problem under Open Banking arises because payment and transaction details contain 'sensitive personal data' that should be only accessed if there is an explicit consent in place. Therefore, without a data protection explicit consent given by the customers, the third party payment providers should not be allowed to process such data. However, at the moment, banks are not able to filter out sensitive data and are therefore issued together with other personal data to the third party payment providers. This would imply that sensitive data that is held on the payment account is processed on the basis of the general data protection consent. As discussed in

[231] Recital 42, Article 7(3)GDPR
[232] 'Beuc's Recommendations to the EDPB on the interplay between the GDPR and PSD2' (Recommendations, BEUC-X-2019-021, 11 April 2019) <https://www.beuc.eu/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf> accessed June 2019
[233] 'Explicit consent and how to obtain it – new GDPR consent guideline' (Iscoop) <https://www.i-scoop.eu/gdpr/explicit-consent/#What_is_explicit_consent_and_when_do_you_need_it> accessed April 2019
[234] European Banking Authority, 'Single Rulebook Q&A' (2018) < https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4309> accessed March 2019
[235] Ibid.
[236] 'How to manage consent under PSD2' (iWelcome) < https://www.iwelcome.com/hubfs/Solution%20profile/iWelcome%20Solution%20Profile%20-%20PSD2%20-%20GDPR%20v1.pdf> accessed July 2019
[237] Bart W. Schermer and Bart Custers and Simone van der Hof, 'The crisis of consent: how stronger legal protection may lead to weaker consent in data protection' (2014) 16(2) Ethics Inf. Technology < https://philpapers.org/rec/SCHTCO-98> accessed April 2019
[238] 'GDPR: when do you need explicit consent from your clients?' (Signaturit, Blog, 22 March 2018) < https://blog.signaturit.com/en/gdpr-explicit-consent-from-your-clients> March 2019

Chapter 3, even though the PSD2 refers to the "explicit consent" it does not necessarily have the same meaning as the "explicit consent" under the GDPR.

To sum up, it is evident that there is a gap between the legal theory, which on the one hand presupposes an informed and rational customer who makes conscious decisions and on the other hand the current practice in which controllers have difficulty to offer fully compliant consent. This suggests that the consent has many drawbacks when used as a legal basis to process payment data under PSD2. The control linked to this notion, often times becomes illusionary. In some situations, such as when processing the sensitive data, it will not even count as valid consent. As this will be discussed in chapter 4, it is important that PSD2 clearly defines and even strengthens the requirements for the explicit consent in order to provide adequate protection to customers.

The general conclusion can be draw that the consent is not the "most appropriate" legal basis in many processing situations. As suggested in the literature the data protection law should shift the focus away from the debates on the most appropriate legal basis to the development of efficient and clear provisions for handling data, which can be deemed as "suitable safeguards".[239]

4.7. The most appropriate legal basis in case of Open Banking

The data subject should be always entitled to the data subject right under the GDPR, such as right to access or right to information, regardless of the legal basis. In such view, consent is not placed at the heart of the data protection law but instead the emphasis is on the importance of the processing in line with the data protection principles, such as purpose limitation. It can be claimed that the ramifications of consent which arguably give individual a great control over their data can be achieved also when processing is based on some other legal grounds. This might be the case under Open Banking where the third party payment providers are able to process payment data held on the customer's bank account. In this situation the consent is believed to be a condition for services provided by the third party payment providers. Therefore, for the processing necessary for the service, the more appropriate lawful basis would likely be "necessary for the performance of the contract" under Article 6(1)(b).[240]

In practice, I believe that the third party payment providers will more likely rely on this basis because if processing is based on consent, the third party payment providers are obliged to seek a new consent each time they introduce new purpose. "The necessary for the performance of a contract" legal basis is advised to be used in the situations when data such as contact information, purchase history or payment data is processed for the purposes for providing an online service.[241] As this is also true in the case under Open Banking, the third party payment providers can rely on this legal basis when processing payment data of the customers. By relying on this legal basis, the third party payment providers are authorized to process data that are

[239] Gabriela Zanfir-Fortuna, 'Forgetting About Consent: Why the Focus Should Be on 'Suitable Safeguards'' (2013) Data Protection Law < https://ssrn.com/abstract=2261973 or http://dx.doi.org/10.2139/ssrn.2261973> accessed May 2019

[240] Information Commisioner's Office, 'When is consent appropriate' (Guide) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/when-is-consent-appropriate/> accessed May 2019

[241] Charles-Albert Helleputte and Diletta De Cicco, 'Using Performance of a Contract as a Legal Basis for Processing in the context of Online Services' (Mayer Brown, 2 May 2019) <https://www.mayerbrown.com/en/perspectives-events/publications/2019/05/using-performance-of-a-contract-as-a-legal-basis-for-processing-in-the-context-of-online-services> accessed June 2019

necessary for the performance of the contract. In this light the question became whether processing of the so called "silent parties" can be based on the "the necessary for the performance of a contract" considering that silent party did not consent to such processing or did not request the service while their data is nevertheless processed. While the personal data of the customer using account information services can be processed on the basis of contractual performance under the GDPR, the EDPB explained that the GDPR might allow processing of personal data of the "silent party" based on the legitimate interests of a controller or third party. The opinion on this topic however differs. For instance, some claim that it is still not clear whether banks can allow the third party payment providers to have access to the personal data of the third parties that are for instance listed as the sender or recipient of a transaction or listed in the transaction comments. The EDPB provides some more clarifications.[242] In line with the applicable GDPR obligations, such as transparency, the EDPB noted that the silent party's personal data cannot be further processed in a manner incompatible with the original purposes for which the personal data was collected.[243] However, the issue arises on whether or not the third party payment providers can comply with the Article 21 GDPR which states that this that data subjects have the right to object to processing based on legitimate interests. The question is how the silent party can exercise this right as in the most cases will not be even aware of the ongoing processing. In order to limit the greater violation of the privacy of a larger group of silent parties, account information service providers should only process this data to the extent that this is truly necessary for the provision of the service.[244] They are not allowed to build a profile about the silent party.

In my opinion due to the existence of the technical limitations, we cannot expect that the third party payment providers or banks will filter out the "unnecessary" personal data in line with the data minimization principle from the GDPR.[245][246]

4.8. Conclusion

There has been much discussion around the notion of consent in the field of law and data protection in particular. Consent has gained importance as it has been linked to the enhance control of data subjects over their personal data or so called information self-determination. It legitimizes large parts of data processing, however, it is argued that it is largely theoretical, having no practical meaning. This is due to the fact that for instance, people are presented with too many consent requests, etc.

The identified limitations of consent can confirm the findings from chapter 3 that the legislator in article 94 PSD2 did not envisaged the 'explicit consent' as a legal basis but instead as a supplementary condition steaming from an 'explicit consent under the GDPR. I refer to it as a semi-data protection consent. That implies that processing must be based on one of the other

[242] VanDoorne, 'Forget PSD2: start cooperating ' https://www.vandoorne.com/globalassets/van-doorne-arno-voerman-forget-pds2-and-start-cooperating.pdf May 2019
[243] Latham & Watkins LLP, 'GDPR & PSD2: Squaring the Circle ' (13 August 2018) <https://www.latham.london/2018/08/gdpr-psd2-squaring-the-circle/> accessed June 2019
[244] .T.J. Wolters and B.P.F. Jacobs, 'The security of access to accounts under the PSD2' (2018) Computer Law & Security Review: The International Journal of Technology Law and Practice <https://scihub-dl.com/pdf/0/scihub-dl.com-39.pdf> accessed May 2019
[245] 'Financial Privacy & PSD2' (Privacy First, 7 January 2019) < https://www.privacyfirst.eu/focus-areas/financial-privacy/672-privacy-first-demands-psd2-opt-out-register.html>
[246] 'Beuc's Recommendations to the EDPB on the interplay between the GDPR and PSD2' (Recommendations, BEUC-X-2019-021, 11 April 2019) <https://www.beuc.eu/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf> accessed June 2019

remaining legal bases from the article 6 GDPR. It is commonly argued that performance of the contract would be the most appropriate one. This nevertheless, poses many other problems, as payment data consists of the sensitive data and Open Banking processes data via automated means, for which explicit consent as per GDPR would be still required.

5. Chapter 5 (Conclusion)

Changes in technology have changed the financial sector and their business models. One of the changes discussed in this thesis is the concept of Open Banking under the revised Payment Service Directive which opened up financial industry to the new servicers and providers that were previously not part of the payment markets. [247]

The new business model brought many advantages to the customers, for instance in the form of tailor made financial services, however, it has also raised several legal issues. Under the revised Payment Directive the third party payment providers, namely the payment initiation service providers and account information service provider are able to access customer bank accounts given the customer provided an explicit consent. The payment data holds many personal information about an identifiable person and should therefore be categorized as personal as per meaning of the GDPR. Considering that the abuse of such data can severely interfere with the fundamental right of an individual, the protection of the users' personal data has been an important part of the revised Directive.

As a general obligation, the governance of the personal data falls under the scope of the GDPR. Nevertheless, PSD2 itself refers to the data protection in a provision which requires the payment initiation service providers to access the payment accounts only when customer has provided an explicit consent for such access. The lack of the coordination between the regulators when drafting these two legislations is evident. For instance, it is not clear whether or not the notion of the explicit consent should be understood in a same way as the notion of the explicit consent under the GDPR. The expert opinion on this topic differs. However, as argued by the EDPB, a leading authority in the area of the data protection, the explicit consent in PSD2 does not have the same meaning as the explicit consent under the GDPR. It is believed that the legislator of PSD2 intended to include an additional contractual type of consent, different than the one from the GDPR. Therefore, the explicit consent under PSD2 does not constitute a legal basis for the processing of personal data. The third party payment provider must therefore base processing on another legal basis, the GDPR consent being one of them. It was assessed that the performance of the contract would be the most appropriate legal basis for the processing of personal data for the provision of the services by the third party payment providers. The processing of personal data by the silent party might be allowed based on the legitimate interest of the data control and third party.

The thesis identified several problems with such interpretation of the notion of explicit consent. Firstly, as the explicit consent within a data protection meaning is not required, the processing of payment data which might include sensitive personal data as per the GDPR meaning held on the bank account should also not be allowed on another legal basis. The exception for the processing of such data is allowed namely that the customer explicitly consented. Moreover, the processing based on the contractual performance is allowed to the extent that the personal data is necessary for the performance of the contract. As the services provided by the payment initiation service providers are broadly defined, the processing by the third party payment providers might go beyond what is necessary. This violates the data protection principles, such as principle of data minimization and purpose limitation principle. The processing based on consent would limit the

[247] 'Revised Rules for payment services in the EU' (EU Publication Office, Document 32015L2366, 8 March 2017) https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32015L2366 > accessed June 2019

scope as for instance, the third party payment providers would be obliged to ask for consumer consent every time processing would be done for a new purpose. Another discussed issue related to the data protection provision and consent under PSD2 was that the account information service provider which in order to provide their financial services extensively process personal data are not bound to ask for any consent. For the realization of their services, the account information service providers ask for the help of other parties which result in seamless sharing of personal data.

I see the benefits of the semi-data protection consent in PSD2 as an addition to the one legal basis from the GDPR to make customer better aware of when and for what purposes their data is processed. This is especially true as also the data protection consent has its drawbacks. Nevertheless, it has to be assessed to what extent does payment data include sensitive data and whether automated decision making is present so such processing would be only based on the explicit consent as a legal ground. Moreover, considering the intrusiveness of the processing of personal data by account information service providers, they should be subject to the data protection provision under PSD2, whatever its interpretation to be.

6. Bibliography

TABLE OF CASES

BverfGE 65,1 of 15 December 1983 (Volkszählung)

TABLE OF LEGISLATION

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data *OJ L 281*

Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC (Text with EEA relevance) *OJ L 319*

Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and

Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance) *OJ L 337*

Regulation (EU) 2016/679 of the European Parliament and of the Council of 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 (General Data Protection Regulation) (Text with EEA relevance *OJ L 119*

SECONDARY SOURCES

--, 'Advies Implementatiebesluit herziene richtlijn betaaldiensten' (Dutch Data Protection Authority, 20 December 2017) < https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/20171220_advies_aan_min_fin_implementatiebesluit_psd2.pdf > accessed January 2019

--, 'Apparatus and method for granting access to network-based services based upon existing bank account information' (IFI CLAIMS Patent Services)< https://patents.google.com/patent/US6910020B2/en> Accessed May 2019

--, 'BEUC's Recommendations to the EDPB on the interplay between the GDPR and PSD2' (Recommendations, BEUC-X-2019-021, 11 April 2019) <https://www.beuc.eu/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf> accessed June 2019

--, 'CAPS Considerations on PSU Consent under PSD2' (CAPS, White paper, March 2018) <https://www.caps-services.com/documents/CAPS%20Considerations%20on%20PSU%20Consent%20under%20PSD2.pdf> accessed March 2018

--, 'Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on a comprehensive approach on personal data protection in the European Union' (2010) COM(2010) 609 final, 04.11.2010

--, 'Consultation on RTS specifying the requirements on strong customer authentication and common and secure communication under PSD2' (European Banking Authority ,Consultation Paper, 2016) 11 <https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2?p_p_auth=OtosFYa3&p_p_id=169&p_p_lifecycle=0&p_p_state=maximized&p_p_col_pos=1&_169_struts_action=%2Fdynamic_data_list_display%2Fview_record&_169_recordId=1616509> accessed May 2019

--, 'Customer trust: without it, you're just another bank' (EY, 2016) < https://www.ey.com/Publication/vwLUAssets/ey-customer-trust-without-it-you-re-just-another-bank/$FILE/ey-customer-trust-without-it-you-re-just-another-bank.pdf> Accessed July 2019

--, 'Data Protection Guidelines for Banks' (Malta Bankers' Association, May 2018) <https://idpc.org.mt/en/Documents/Data%20Protection%20guidelines%20for%20banking.pdf> accessed February 2018

--, 'EDPB work program 2019-2020' (EDPB, 12 February 2019) < https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-02-12plen-2.1edpb_work_program_en.pdf> accessed April 2019

--, 'European banking federation's comments on the article 29 working party guidelines on con sent (WP259)' (EBF_030527) <https://www.ebf.eu/wp-content/uploads/2018/01/EBF_030527-EBF-comments-on-WP29-Guidelines-on-consent-wp259-1.pdf> accessed 15 June 2019

--, 'Financial Services technology 2020 and beyond' (PwC) <https://www.pwc.com/gx/en/financial-services/assets/pdf/technology2020-and-beyond.pdf> Accessed May 2019

--, 'Fintech reloaded- Traditional banks as digital ecosystem' (Deutche Bank, 9 June 2015) <https://www.dbresearch.com/PROD/RPS_EN-PROD/PROD0000000000451937/Fintech_reloaded_%D0_Traditional_banks_as_digital_ec.PDF>accessed May 2019

--, 'GDPR key changes' (EU GDPR Portal) < https://eugdpr.org/the-regulation/> accessed June 2019

--, 'Global FinTech investment more than doubled to $112 billion' (Consulatncy,21 February 2019) < https://www.consultancy.eu/news/2390/global-fintech-investment-more-than-doubled-to-112-billion> accessed June 2019

--, 'Guidelines on authorisation and registration under PSD2' (European Banking Authority ,Consultation Paper, 2016) 18 <https://eba.europa.eu/documents/10180/1646245/Consultation+Paper+on+draft+Guidelines+on+authorisation+and+registration+under+PSD2+%28EBA-CP-2016-18%29.pdf/b8d49c1c-be4f-4b36-a5ce-e6710e00383c> accessed March 2018

--, 'Guidelines on consent under Regulation 2016/679' (Article 29 Working Party) < https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051> accessed May 2019

--, 'History of data protection regulation' (European Data Protection Supervisor) < https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en> accessed April 2019

--, 'How to manage consent under PSD2' (iWelcome) < https://www.iwelcome.com/hubfs/Solution%20profile/iWelcome%20Solution%20Profile%20-%20PSD2%20-%20GDPR%20v1.pdf> accessed July 2019

--, 'Introducing the Open Banking standard' (Open Data Institute, 2016) < https://theodi.org/> accessed May 2019

--, 'Key findings from the consumer Digital Behavior Study' (ATKearney ,April 2018) https://www.atkearney.com/financial-services/the-consumer-data-privacy-marketplace/the-consumer-digital-behavior-study Accessed May 2019

--, 'Letter regarding PSD2 directive' (EDPB, 84-2018, 5 July 2018) < https://edpb.europa.eu/news/news/2018/letter-regarding-psd2-directive_en> accessed February 2019

--, 'Navigating the PSD2 and GDPR challenges faced by banks' (EY, 2018) <https://www.ey.com/Publication/vwLUAssets/ey-navigating-the-psd2-and-gdpr-challenges-faced-by-banks/$FILE/ey-navigating-the-psd2-and-gdpr-challenges-faced-by-banks.pdf> accessed May 2019

--, 'Open banking, open liability' (Ashurst, 2018) < https://www.ashurst.com/en/news-and-insights/legal-updates/open-banking-open-liability-accountability-issues-for-open-banking-apis/> accessed August 2019

--, 'Opinion 14/2011 on the definition of consent' (Article 29 Working Party, 01197/11/EN WP187, 13 July 2011) < https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf> accessed May 2019

--, 'Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC' (EBA-Op-2018-04, 13 June 2018)

--, 'Outrageous abuse of privacy: New York orders inquiry into Facebook data use' (Guardian, 23 February 2019) <https://www.theguardian.com/technology/2019/feb/22/new-york-facebook-privacy-data-app-wall-street-journal-report> accessed February 2019

--, 'Overlap between GDPR and PSD2' (Inside Privacy, 16 March 2018) <https://www.insideprivacy.com/financial-institutions/overlap-between-the-gdpr-and-psd2/> accessed December 2019

--, 'Payment Service directive; frequently asked questions (European Commission, Fact sheet, MEMO/15/5793, January 2018) < http://europa.eu/rapid/press-release_MEMO-15-5793_en.htm> accessed May 2018

--, 'Payment Services Directive (PSD2): Regulatory Technical Standards (RTS) enabling consumers to benefit from safer and more innovative electronic payments' (European Commission, Fact Sheet, 2017) <https://europa.eu/rapid/press-release_MEMO-17-4961_en.htm> accessed June 2019

-- 'Proposal for a Directive of the European parliament and of the council on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC' (COM/2013/0547 final - 2013/0264 (COD)) < https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52013PC0547> accessed June 2019

--, 'PSD2 – a game changing regulation' (PwC) https://www.pwc.co.uk/industries/banking-capital-markets/insights/psd2-a-game-changing-regulation.html accessed march 2019

--, 'PSD2 and GDPR: An awkward match?' (Deloitte Touche Tohmatsu Limited, 2018) <https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/legal/deloitte-nl-psd2-and-gdpr-an-awkward-match.pdf> accessed May 2019

--, 'PSD2 and GDPR; friends or foes?' (Deloitte) < https://www2.deloitte.com/lu/en/pages/banking-and-securities/articles/psd2-gdpr-friends-or-foes.html> accessed May 2019

--, 'PSD2 licensing: solving the puzzle of becoming a Third Party Provider' (Innopay Blog) https://www.innopay.com/en/publications/psd2-becoming-a-third-party-provider accessed 10 June 2019

--, 'Revised Rules for payment services in the EU' (EU Publication Office, Document 32015L2366, 8 March 2017) https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32015L2366 > accessed June 2019

--, 'Rights related to automated decision making including profiling' (ICO) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/> accessed April 2019

--, 'The main differences between DPD and the GDPR and how to address those moving forward' (Seeunity, White paper British legal technology forum) https://britishlegalitforum.com/wp-content/uploads/2017/02/GDPR-Whitepaper-British-Legal-Technology-Forum-2017-Sponsor.pdf accessed April 2019

--, 'The Netherlands tackles uncertainties around PSD2 consent and GDPR' (Medium , 20 November 2018) <https://medium.com/@touchtech/the-netherlands-tackles-uncertainties-around-psd2-consent-and-gdpr-e5beb31c4e16> accessed May 2019

--, 'What the GDPR will concretely change for payment service providers' (European Payment Council) < European Payment Council> Accessed May 2019

--, 'When is consent appropriate' (ICO Guide) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/when-is-consent-appropriate/> accessed May 2019

--, 'Your questions on PSD Payment Services Directive 2007/64/EC' (European Commission (EC), 2011) < https://ec.europa.eu/info/system/files/faq-transposition-psd-22022011_en.pdf> accessed June 2019

Acquisti A and Grossklags J, 'What Can Behavioral Economics Teach Us About Privacy?' (2006) Digital Privacy < https://www.heinz.cmu.edu/~acquisti/papers/Acquisti-Grossklags-Chapter-Etrics.pdf> accessed January 2019

Acquisti A et al., 'What is privacy worth?' (2013) 42 The Journal of Legal Studies <https://www.cmu.edu/dietrich/sds/docs/loewenstein/WhatPrivacyWorth.pdf> accessed July 2019

Austin E, 'The four year legal battle for the protection of your data' (Bits of Freedom in EDRi, 24 May 2018) < https://edri.org/four-year-battle-protection-of-your-data-gdpr/> Accessed June 2019

Alvarez R, 'Trust as a key factor in successful relationships between consumers and retail service providers' (2005) 25(1) The Service Industries Journal < https://www.tandfonline.com/doi/abs/10.1080/0264206042000302423> Accessed July 2019

Austin E, 'The four year legal battle for the protection of your data' (Bits of Freedom in EDRi, 24 May 2018) < https://edri.org/four-year-battle-protection-of-your-data-gdpr/> Accessed June 2019

Bansal A, 'Trust violation and repair: The information privacy perspective; (2015) Volume 71 Decision Support System < https://www.sciencedirect.com/science/article/pii/S0167923615000196>Accessed July 2019

Benamati J and Serva M, 'Trust and distrust in online banking: Their role in developing countries' (2007) 13(2) Information Technology for Development < https://www.tandfonline.com/doi/pdf/10.1002/itdj.20059?needAccess=true> accessed June 2019

Botta A, 'PSD2: Taking advantage of open banking disruption' (McKinsey & Company, 2018) < https://www.mckinsey.com/industries/financial-services/our-insights/psd2-taking-advantage-of-open-banking-disruption >Accessed July 2019

Bygrave LA and Schartum DW, *Consent, Proportionality and Collective Power in Reinventing Data Protection?* (Springer, 2009)

Cambounet B, 'PSD2 and Open Banking: Defining your role in the digital ecosystem' (Finextra, 2016) < https://www.euroforum.nl/media/filer_public/2017/02/16/axway_finextra.pdf>

Chesbrough H, 'Business model innovation: it's not just about technology anymore' (2007) 24(3) Strategy&Leadership < https://www.emerald.com/insight/content/doi/10.1108/10878570710833714/full/html> accessed July 2019

Chilton AS and Ben-Shahar O, 'Simplification of Privacy Disclosures: An Experimental Test' (Coase-Sandor Working Paper Series in Law and Economics No. 737, 2016) < https://chicagounbound.uchicago.edu/law_and_economics/774/ > accessed March 2019

Clearwater A and Philbrook B, 'Practical tips for consent under GDPR' (Iapp, 23 January 2018) < https://iapp.org/news/a/practical-tips-for-consent-under-the-gdpr/> accessed February 2019

Cluster B et al., *Consent and Privacy* (The Routledge Handbook of the Ethics of Consent, 2018)

Curren L and Kaye J, 'Revoking consent: a 'blind spot' in data protection law?' (2010) 26(273) Comp L & Sec Rev 2010 < https://scholar.google.com/scholar_lookup?title=Revoking%20consent%3A%20a%20%E2%80%98blind%20spot%E2%80%99%20in%20data%20protection%20law%3F&author=L%20Curren&author=J.%20Kaye&publication_year=2010&journal=Comp%20L%20%26%20Sec%20Rev&volume=26&pages=273-83

Dapp T F, 'Fintech reloaded – Traditional banks as digital ecosystems' (Deutsche Bank Research , 9 June 2019) < https://www.dbresearch.com/PROD/RPS_EN-PROD/PROD0000000000451937/Fintech_reloaded_%D0_Traditional_banks_as_digital_ec.PDF> accessed 25 May 2019

Devine SM, 'Open banking: opportunity and danger' (2016) Volume 2016, Issue 10 Computer Fraud & Security <https://reader.elsevier.com/reader/sd/pii/S136137231630080X?token=AE4968C27B69442FD2C16C239A9EA10E6FF61DA0F640D3BE53C802A18B24A8784C55151A715615A976E36120000484E3> accessed April 2019

Dimitrakopoulos J, 'Conflicts between EU law and National Constitutional Law in the Field of Fundamental Rights' (European judicial training network) < http://www.ejtn.eu/PageFiles/17318/DIMITRAKOPOULOS%20Conflicts%20between%20EU%20law%20and%20National%20Constitutional%20Law.pdf> Accessed July 2019

Donelly M, 'Payments in the digital market: Evaluating the contribution of Payment Services Directive II' (2016) 32(6) Computer Law & Security Review < https://www.sciencedirect.com/science/article/pii/S0267364916301170?via%3Dihub> accessed July 2019

Folcia M et al., 'The main regulatory change introduces: PSD2 in nutshell' (PwC) < https://www.pwc.com/it/en/industries/banking/assets/docs/psd2-nutshell-n03.pdf> accessed February 2019> accessed March 2019

Grima S, 'The Payment Services Directive 2 and Competitiveness: The Perspective of European Fintech Companies' (2018) XXI(2):5-24 European Research Studies Journal <https://www.researchgate.net/publication/323114264_The_Payment_Services_Directive_2_and_Competitiveness_The_Perspective_of_European_Fintech_Companies> accessed 10 June 2019

Harris C et al., *Engineering Ethics* (5th Edition, Wadsworth, 2013)

Helleputte CA and Cicco D, 'Using Performance of a Contract as a Legal Basis for Processing in the context of Online Services' (Mayer Brown, 2 May 2019) <https://www.mayerbrown.com/en/perspectives-events/publications/2019/05/using-performance-of-a-contract-as-a-legal-basis-for-processing-in-the-context-of-online-services> accessed June 2019

Hultsch C, 'Basic principles of European Union consent and data protection (Porter Wright Morris & Arthur LLP, 25 July 2011) https://www.technologylawsource.com/2011/07/articles/privacy-1/basic-principles-of-european-union-consent-and-data-protection/ accessed January 2019

Jackson O, 'PSD2 gives banks chance to evolve' (2018) International Financial Law Review < https://search.proquest.com/openview/d6d3e565ec450c842538ddaa1b312b83/1?pq-origsite=gscholar&cbl=36341> Accessed July 2019

Järvinen RA, 'Consumer trust in banking Consumer trust in banking relationships in Europe' (2014) 32(6) International Journal of Bank Marketing < https://www.researchgate.net/publication/265969491_> Accessed July 2019

Koops BJ, 'The Trouble with European Data Protection Law' (2014) International Data Privacy Law 250 < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2505692> accessed May 2019

Kosta E, *Consent in European Protection Law* (Brill, 2013) p.30
KPMG, 'PSD2 and Open Banking. Revolution or evolution? ' (March 2019) <https://assets.kpmg/content/dam/kpmg/pl/pdf/2019/04/pl-Raport-PSD2-i-Open-Banking-ENG.pdf> accessed April 2019

Krishnakumar A, 'GDPR vs PSD2 – Banks may abandon PSD2 due to conflicting policies' (Daily Fintech, 4 August 2017) < https://dailyfintech.com/2017/08/04/gdpr-vs-psd2-banks-may-abandon-psd2-due-to-conflicts/> Accessed December 2018

Latham & Watkins LLP, 'GDPR & PSD2: Squaring the Circle ' (13 August 2018) <https://www.latham.london/2018/08/gdpr-psd2-squaring-the-circle/> accessed June 2019

Lister M, ' The Legitimating Role of Consent in International Law' (2011) 11(2) Chicago Journal of International Law http://chicagounbound.uchicago.edu/cjil/vol11/iss2/25 accessed June 2019

Lumpkin S, 'Regulatory Issues Related to Financial Innovation' (OECD Journal: Financial Market Trends 2009) < https://www.oecd.org/finance/financial-markets/44362117.pdf> accessed February 2019

Mackenzie A, 'The FinTech Revolutiom' (2015) 26(3) London Business School < https://onlinelibrary.wiley.com/doi/abs/10.1111/2057-1615.12059>Accessed July 2019

Manson N and O'Neill O, *Rethinking informed consent in bioethics* (Cambridge University Press, Cambridge 2007)

Manthorpe R, 'To change how you use money, Open Banking must break banks' (Wired, 16 October 2017) <https://www.wired.co.uk/article/psd2-future-of-banking> accessed March 2019

Matzner T et al., 'Do it yourself data protection- Empowerment or Burden? (2016) Springer <http://www.philippmasur.de/documents/pubs/Matzner%20Masur%20et%20al._2016_Do-it-yourself%20data%20protection.pdf> accessed August 2019

McDermott CF, 'GDPR & PSD2: Squaring the Circle' (Latham & Watkins LLP, 13 August 2018) https://www.globalprivacyblog.com/legislative-regulatory-developments/gdpr-psd2-squaring-the-circle/ accessed January 2019

McDermott Y, 'Conceptualising the right to data protection in an era of Big Data' (2017) 1(7) Big Data & Society <https://journals.sagepub.com/doi/pdf/10.1177/2053951716686994> accessed July 2019

Mounaim Cortet and Tom Rijks and Shikko Nijland, 'PSD2: The digital transformation accelerator for banks' (2016) 10(1) Journal of Payments Strategy & Systems.< https://www.econbiz.de/Record/psd2-the-digital-transformation-accelerator-for-banks-cortet-mounaim/10011566458> accessed June 2019

Politous E et al., 'Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions' (2018) 4(1) Journal of Cyber Security < https://academic.oup.com/cybersecurity/article/4/1/tyy001/4954056> accessed August 2019

Porter ME, The Competitive Advantage: Creating and Sustaining Superior Performance, (Free Press, New York, 2nd edition, 1985) < https://www.albany.edu/~gs149266/Porter%20(1985)%20-%20chapter%201.pdf> accessed February 2019

Quathem K and Bertin S, 'GDPR and PSD2: a compliance burden for financial institutions' (Thomson Reuters, 18 April 2018) <https://www.cov.com/-/media/files/corporate/publications/2018/04/gdpr_and_psd2_a_compliance_burden_for_financial_institutions.pdf> accessed July 2019

Stringfellow A, 'The ultimate data privacy guide for banks and financial institutions' (Ngdata, 14 August 2018) https://www.ngdata.com/data-privacy-guide-for-banks-and-financial-institutions/> accessed January 2019

Sullivan RJ and Wang Z, 'Nonbanks in the Payments System: Innovation, Competition, and Risk' (Conference summary, KANSAS CITY, 2017) < https://pdfs.semanticscholar.org/41ad/051c62d02ae658ff36b02cb6a93866c3d298.pdf> accessed June 2019

Van Ewijk T and Fiolet J, 'PSD2 licensing: solving the puzzle of becoming a Third Party Provider' (Innopay, blog) < https://www.innopay.com/en/publications/psd2-becoming-a-third-party-provider> accessed July 2019

Vandezande N, 'Reconciling Consent in PSD2 and GDPR' (Web Fraud Prevention, Identity Verification & Authentication Guide 2018/2019, December 2018) < https://www.thepaypers.com/reports/web-fraud-prevention-identity-verification-authentication-guide-2018-2019/r776368> accessed 25 May 2019

Voerman A, 'Forget PSD2: start cooperating ' (VanDoorne,) https://www.vandoorne.com/globalassets/van-doorne-arno-voerman-forget-pds2-and-start-cooperating.pdf May 2019

Wertheimer A, 'Consent in Contract Law" The ethics of consent: theory and practice' (2010) no.08-36 (Oxford University Press, Minnesota Legal Studies Research) <https://ssrn.com/abstract=1140256> accessed May 2019

Whitley EA, 'Informational privacy, consent and the "control" of personal data' (2009) 14(3) Information Security Technical Report <https://reader.elsevier.com/reader/sd/pii/S1363412709000363?token=801F05515C5B3A44704F5329A12E213E093F6B3ED273C87E27F75F80DC87AF3ED8FC44289FAF7383EA7B266D82648766> accessed May 2019

Wolters PTJ and Jacobs BPF, 'The security of access to accounts under the PSD2' (2018) 11(40) Computer Law & Security Review: The International Journal of Technology Law and Practice https://doi.org/10.1016/j.clsr.2018.10.005 accessed July 2019

Wooten K, 'With consumers' trust comes great responsibility: Approaching data security in a fintech-friendly world' (Abrigo) <https://www.abrigo.com/blog/2018/08/27/with-consumers-trust-comes-great-responsibility-approaching-data-security-in-a-fintech-friendly-world/> accessed May 2019

Zachariadisa M and Ozcan P, 'The API Economy and Digital Transformation in Financial Services: The Case of Open Banking' (Swift Institute, 2017) https://www.swiftinstitute.org/wp-content/uploads/2017/07/SIWP-2016-001-ImpactOpen-APIs-FINAL.pdf accessed June 2019

Zanfir-Fortuna G, 'Forgetting About Consent: Why the Focus Should Be on 'Suitable Safeguards'' (2013) Data Protection Law < https://ssrn.com/abstract=2261973 or http://dx.doi.org/10.2139/ssrn.2261973> accessed May 2019