PERSONAL DATA PROCESSING BY THIRD PARTY PROVIDERS IN ONLINE PAYMENT TRANSACTIONS UNDER GDPR AND PSD2

AN IN-DEPTH LEGAL ANALYSIS FOR GDPR AND PSD2 COMPLIANCE

Master Thesis – Law and Technology
Hasan Özgür
Student Number: 2052737
2020-2021
June 2021
Supervisor: Mara Păun
Second Supervisor: Paul De Hert

TABLE OF CONTENTS

1. CHAPTER 1 - Introduction

1. Background

In the last decades, humanity witnessed incredible changes in many different parts of daily life thanks to technology. Wide usage of the telephone, radio, television, mobile phone, internet, and the other latest digital technologies, particularly in the payment services, disrupted the *status quo*, created new realities, and forced incumbent and potential new players to adopt the latest developments.[1] As a result of the latest technological developments in the payment sector and the boost in e-commerce, providers of payment services have to provide their services faster, better, and more user-friendly and have to offer more choices to their users for them to choose the best fit services for their needs.[2] As a response to these developments, many users, particularly millennials, do not want to think about whether they have enough cash and credit or debit cards with them all the time; instead, they prefer to make their payments seamlessly via their mobile phones and wearables (e.g., the AppleWatch, Samsung's Gear smartwatches)[3] without spending too much time and effort.[4] As payment service providers should have their users' relevant personal data and information to provide a more user-friendly payment experience, the security of payment transactions and protection of users' data are crucial aspects for the payment sector.[5] Thus, the EU and some other countries (e.g., Singapore, USA) took certain steps to regulate such developments in the online/mobile payment sector.[6]

Following such trend in the payment sector, due to the emergence of the data-driven technologies[7], the Second Payment Service Directive (PSD2), an EU legislative instrument, was adopted on 8 October 2015 to catch up with digital and technological changes in online payment transactions.[8] In parallel to the developments in the online payment sector, the General

---

[1] Alja Poklar, 'Does the Same Word Mean the Same Thing? An Exploration of the Notion of Consent in PSD2 and GDPR' (*Tilburg University*, 2019) p.2 <https://arno.uvt.nl/show.cgi?fid=148995> accessed 26 May 2021

[2] Deutsche Bank Global Transaction Banking, 'Are You PSD2-Ready? A Guide to the latest information and sources of support' (*White Paper*, October 2017) p.2 <https://cib.db.com/docs_new/PSD2_White_Paper_October_2017.pdf> accessed 26 May 2021; Letitia Booty, 'The importance of a payments strategy' (*Real Business*, 3 January 2017) <https://realbusiness.co.uk/the-importance-of-a-payments-strategy/> accessed 26 May 2021

[3] Ben Regnard-Weinrabe and Jane Finlayson-Brown, Adapting to a Changing Payments Landscape. in Jelena Madir (ed), Fintech Law and Regulation (Edward Elgar Publishing 2019) p.23-24

[4] Leena Rao, 'How Visa Plans To Dominate Mobile Payments, Create The Digital Wallet And More' (*TechCrunch*, 7 August 2011) <https://techcrunch.com/2011/08/07/how-visa-plans-to-dominate-mobile-payments-create-the-digital-wallet-and-more/> accessed 26 May 2021; Melcom Copeland, 'Millennials choose digital payment methods over cash' (*LinkedIn*, 30 June 2020) <https://www.linkedin.com/pulse/millennials-choose-digital-payment-methods-over-cash-melcom-copeland-/> accessed 26 May 2021

[5] Ibid.

[6] Ben Regnard-Weinrabe and Jane Finlayson-Brown, Adapting to a Changing Payments Landscape. in Jelena Madir (ed), Fintech Law and Regulation (Edward Elgar Publishing 2019) p.23-24

[7] Seeunity, 'The main differences between DPD and the GDPR and how to address those moving forward' (*White Paper British Legal Technology Forum*, 2017) <https://britishlegalitforum.com/wp-content/uploads/2017/02/GDPR-Whitepaper-British-Legal-Technology-Forum-2017-Sponsor.pdf> accessed 26 May 2021

[8] 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*; Mckinsey&Company, 'PSD2: Taking advantage of open-banking disruption' (*Our Insights*, 24 January 2018) p.3 <https://www.mckinsey.com/industries/financial-services/our-insights/psd2-taking-advantage-of-open-banking-disruption> accessed 26 May 2021; Reinhard Steennot, 'Reduced payer's liability for unauthorized payment transactions under the second Payment Services Directive (PSD2)' [2018] 34(4) Computer Law & Security Review p.954

Data Protection Regulation (GDPR), an EU regulation containing general data protection rules that also complements data protection provision of PSD2, was drafted during the preparation of PSD2 and adopted right after the adoption of PSD2, on 14 April 2016.[9] Before PSD2, the (first) Payment Service Directive (PSD1) entered into force on 25 December 2007 to create an EU-wide internal market for payment services concerning all types of electronic and non-cash payments (e.g., card payments, mobile and online payments, direct debits, credit transfers).[10]

As for PSD2, it was created to cover the new technological developments and replace PSD1.[11] Then new and nonconventional players were included in the online payment services regulatory framework to provide their services.[12] PSD2 introduced two new types of services, namely account information services and payment initiation services.[13] As for payment initiation services, payment initiation service providers (PISPs)[14] (e.g., PayPal, Sofort, IDeal, Tikkie) initiate payment order from the user's bank account after the user's request; as for account information services, account information service providers (AISPs)[15] (e.g., Moneybox, Spiir, Trustly, Fintonic) shows consolidated information obtained from the users' one or more bank accounts.[16] Although PISPs[17] and AISPs[18] exist before PSD2, the main change that PSD2 brought is regulating PISPs and AISPs and establishing the legal ground for their operation in the online payment market.[19] To provide their innovative services, these third-party providers

[9] 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*; Mckinsey&Company, 'PSD2: Taking advantage of open-banking disruption' (*Our Insights*, 24 January 2018) <https://www.mckinsey.com/industries/financial-services/our-insights/psd2-taking-advantage-of-open-banking-disruption> accessed 26 May 2021; Covington & Burling, 'Overlap Between the GDPR and PSD2' (*Inside Privacy*, 16 March 2018) <https://www.insideprivacy.com/financial-institutions/overlap-between-the-gdpr-and-psd2/> accessed 26 May 2021

[10] 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;* Ducuing Charlotte, Dutkiewicz Lidia and Miadzvetskaya Yuliya, 'D62 Legal and Ethical Requirements' (*Trusts Trusted Secure Data Sharing Space*, August 2020) p.118 <https://www.trusts-data.eu/wp-content/uploads/2020/10/D6.2-Legal-and-Ethical-Requirements.pdf> accessed 26 May 2021

[11] Ibid.

[12] Mckinsey&Company, 'Data sharing and open banking' (*McKinsey on Payments*, July 2017) p.7 <https://www.mckinsey.it/sites/default/files/data-sharing-and-open-banking.pdf> accessed 26 May 2021

[13] P.T.J. Wolters, B.P.F. Jacobs, 'The security of access to accounts under the PSD2' [2019] 35(1) Computer Law & Security Review, p.30

[14] Article 4 (1)(18) PSD2

[15] Article 4 (1)(19) PSD2

[16] P.T.J. Wolters, B.P.F. Jacobs, 'The security of access to accounts under the PSD2' [2019] 35(1) Computer Law & Security Review, p.31; Morrison Foerster, 'FinTech Focus: New European Directive on Payment Services (PSD2) Comes into Force' (*Client Alert*, 1 February 2016) p.3 <https://media2.mofo.com/documents/160129fintechfocus.pdf> accessed 26 May 2021; Clearhaus, 'PSD2 - New business opportunities and how to exploit them' (*Clearhaus Blog*, 18 September 2018) <https://www.clearhaus.com/blog/psd2-new-business-opportunities/> accessed 26 May 2021

[17] Article 4 (1)(18) PSD2

[18] Article 4 (1)(19) PSD2

[19] Ducuing Charlotte, Dutkiewicz Lidia and Miadzvetskaya Yuliya, 'D62 Legal and Ethical Requirements' (*Trusts Trusted Secure Data Sharing Space*, August 2020) p.119 <https://www.trusts-data.eu/wp-content/uploads/2020/10/D6.2-Legal-and-Ethical-Requirements.pdf> accessed 26 May 2021

(TPPs)[20], an umbrella term referring to both PISPs and AISPs, have to reach the relevant payment account information and personal data of the users.[21]

PISPs are seen as an alternative to payment cards for online payment transactions, as they provide fast and accessible payment services, provided that the user has an online payment account. Compared to the payment cards' high costs, PISPs' services are considerably cheaper.[22] Thanks to PISPs' mobile payment intermediary role, users may make their online payments via smartphones and PISPs' mobile applications.[23] Practically speaking, PISPs create an online bridge between the user's bank account and merchant's bank account and allow users to make their payments fast and easy.[24] Once the user makes a payment request, PISP contacts the relevant "account servicing payment servicing provider" (ASPSP/bank) and then asks for authentication from the user.[25] When the user authenticates and verifies the payment transaction, payment is made to the merchant's bank account.[26] While agreeing on terms and conditions between the user and PISP is mandatory, having an agreement between PISP and bank or PISP and AISP is not necessary.[27] Thus, banks cannot reject AISPs' account information or PISPs' payment initiation requests.[28]

AISPs, with the approval of the user, may access the user's bank accounts,[29] help users classify and categorize their expenses under different groups (e.g., rent, food, transportation) and plan their financial situation more diligently and spend less time and effort, thanks to the consolidated and up-to-date information.[30] Through AISPs, users can analyze their spending patterns on different things and improve their control over their financial situation.[31]

Under this thesis, the data protection questions arising from the new open banking system introduced by PSD2 will be elaborated. Under PSD2, in addition to the banks, even TPPs may process the users' financial transaction data held in users' bank accounts.[32] However, as such data is necessary for PISPs and AISPs to provide their services, banks should allow TPPs access

---

[20] European Data Protection Board, 'Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR Version 2.0' (*Guidelines*, 15 December 2020) p.7 <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202006_psd2_afterpublicconsultation_en.pdf > accessed 26 May 2021 (EDPB, PSD2 Guidelines)

[21] Mckinsey&Company, 'Data sharing and open banking' (*McKinsey on Payments*, July 2017) p.5 <https://www.mckinsey.it/sites/default/files/data-sharing-and-open-banking.pdf> accessed 26 May 2021

[22] Dilja Helgadottir, 'The Interaction between Directive 2015/2366 (EU) on Payment Services and Regulation (EU) 2016/679 on General Data Protection concerning Third Party Players' (2020) 23 Trinity CL Rev p. 225

[23] Dilja Helgadottir, 'The Interaction between Directive 2015/2366 (EU) on Payment Services and Regulation (EU) 2016/679 on General Data Protection concerning Third Party Players' (2020) 23 Trinity CL Rev p. 206

[24] Ibid.

[25] Ibid.

[26] Ibid.

[27] Dilja Helgadottir, 'The Interaction between Directive 2015/2366 (EU) on Payment Services and Regulation (EU) 2016/679 on General Data Protection concerning Third Party Players' (2020) 23 Trinity CL Rev p. 206 and 207

[28] Ibid.; Article 66(4) PSD2; Article 67(3) PSD2

[29] Dilja Helgadottir, 'The Interaction between Directive 2015/2366 (EU) on Payment Services and Regulation (EU) 2016/679 on General Data Protection concerning Third Party Players' (2020) 23 Trinity CL Rev p. 207

[30] European Commission, 'Payment Services Directive: frequently asked questions' (*Press Corner* 12 January 2018) <https://ec.europa.eu/commission/presscorner/detail/fr/MEMO_15_5793> accessed 26 May 2021

[31] Dilja Helgadottir, 'The Interaction between Directive 2015/2366 (EU) on Payment Services and Regulation (EU) 2016/679 on General Data Protection concerning Third Party Players' (2020) 23 Trinity CL Rev p. 207

[32] P.T.J. Wolters, B.P.F. Jacobs, 'The security of access to accounts under the PSD2' [2019] 35(1) Computer Law & Security Review, p.30; FinTech Focus: New European Directive on Payment Services (PSD2) Comes into Force p. 3

to their users' relevant data if users give their permission.[33] Therefore, it is crucial to interpret the data protection provisions in GDPR and PSD2 coherently to prevent any inconsistencies and damages that users may incur (e.g., arising from payment refusals claiming (by banks) that TPPs failed to obtain users' data as required).[34]

2. Problem Statement and Literature Review

Since PSD2 is a directive, the national transposition of PSD2 in the EU member states, including in the Netherlands, was quite challenging and caused some delays.[35] Besides, as PSD2 brought a conflict of interest between banks and TPPs, sharing users' data with TPPs and clearing the crucial topics may take additional time.[36] For example, if some banks state that TPPs should obtain users' explicit consent under GDPR, rather than under PSD2, claiming that explicit consent under PSD2 has the same meaning as explicit consent under GDPR, some banks may reject granting access to TPPs due to lack of users' explicit consent under GDPR. In such a case, if TPPs, on top of the explicit consent under PSD2, do not have to obtain the explicit consent of users under GDPR, the relevant competition or banking authorities may impose fines against banks due to preventing TPPs' access to users' banking data unlawfully. But, if banks' legal interpretation is correct and if TPPs, on top of the explicit consent under PSD2, have to obtain the users' explicit consent under GDPR, but banks granted access to TPPs without the users' explicit consent under GDPR, the data protection authorities may impose fines against banks for giving access to TPPs unlawfully. Thus, due to lack of clarity and conflict of interest, while banks may claim that TPPs have to obtain explicit consent for some data processing operations under GDPR, TPPs may claim that they only need to obtain the users' explicit consent based on PSD2. [37] Thus, perfect compliance to PSD2 and GDPR may not be easy for all players in practice.[38]

GDPR contains a definition of and conditions[39] for consent as one of the legal grounds for the data processing operations.[40] Under GDPR, consent means *"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"*.[41] In addition to consent, GDPR also mentions that explicit consent is required

---

[33] Ducuing Charlotte, Dutkiewicz Lidia and Miadzvetskaya Yuliya, 'D62 Legal and Ethical Requirements' (*Trusts Trusted Secure Data Sharing Space*, August 2020) p.119 <https://www.trusts-data.eu/wp-content/uploads/2020/10/D6.2-Legal-and-Ethical-Requirements.pdf> accessed 26 May 2021; Pranay Gupta and T. Mandy Tham, Fintech: The New DNA of Financial Services (Walter de Gruyter 2019) p.159

[34] Covington & Burling, 'Overlap Between the GDPR and PSD2' (*Inside Privacy*, 16 March 2018) <https://www.insideprivacy.com/financial-institutions/overlap-between-the-gdpr-and-psd2/> accessed 26 May 2021

[35] Deutsche Bank Global Transaction Banking, 'Are You PSD2-Ready? A Guide to the latest information and sources of support' (*White Paper*, October 2017) p.16 <https://cib.db.com/docs_new/PSD2_White_Paper_October_2017.pdf> accessed 26 May 2021

[36] Tycho Van Ewijk and Josje Fiolet, 'PSD2 licensing: solving the puzzle of becoming a Third Party Provider' (*Innopay Blog Item*, 21 February 2019) <https://www.innopay.com/en/publications/psd2-becoming-a-third-party-provider> accessed 26 May 2021

[37] Covington & Burling, 'Overlap Between the GDPR and PSD2' (*Inside Privacy*, 16 March 2018) <https://www.insideprivacy.com/financial-institutions/overlap-between-the-gdpr-and-psd2/> accessed 26 May 2021

[38] 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 26 May 2021

[39] Article 7 GDPR

[40] Article 6 (1) (a) GDPR

[41] Article 4 (1) (11) GDPR

when a serious data protection risk arises and a high level of data subject control over his or her personal data is necessary.[42] Obtaining explicit consent is necessary when the data; (i) need to be processed is sensitive (special categories of) personal data[43] (ii) will be transferred to the third countries which do not have adequate safeguards[44] or (iii) will be used for automated decision-making, including profiling that may produce legal effects or similar significant effects on the users.[45]Despite the lack of explicit consent definition under GDPR, the meaning of explicit consent has been clarified afterwards.[46]

On the other hand, although there are references to consent and explicit consent in PSD2, no definition exists for both "consent" and "explicit consent" under PSD2.[47] Thus, it is highly crucial to determine whether the terms of "consent" and "explicit consent" in PSD2 have the same meaning as the terms of "consent" and "explicit consent" under GDPR.[48] Under GDPR, obtaining consent from the data subjects is one of the six legal grounds for data processing.[49] PSD2 establishes that obtaining explicit consent is required to process users' data while providing payment initiation and account information services to users.[50] Since there is no certainty on the hierarchy of rules for implementing some data protection provisions in PSD2 into national legislations, this uncertainty caused some ongoing discussions among certain administrative bodies and scholars.[51] To prevent any uncertainties, the European Data Protection Board (EDPB) adopted the Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR (Versions 1.0 and 2.0) (Guidelines) to clarify data protection issues.[52] In the Guidelines, EDPB interprets that since the legal grounds in the Article

---

[42] European Data Protection Board, 'Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1' (*Guidelines*, 4 May 2020) p.20 <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf> accessed 26 May 2021

[43] Article 9 (1) GDPR

[44] Article 49 (1) GDPR

[45] European Data Protection Board, 'Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1' (*Guidelines*, 4 May 2020) p.20 <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf> accessed 26 May 2021

[46] Ibid.

[47] Ducuing Charlotte, Dutkiewicz Lidia and Miadzvetskaya Yuliya, 'D62 Legal and Ethical Requirements' (*Trusts Trusted Secure Data Sharing Space*, August 2020) p.121 <https://www.trusts-data.eu/wp-content/uploads/2020/10/D6.2-Legal-and-Ethical-Requirements.pdf> accessed 26 May 2021

[48] Johan Peeters, 'Data protection in mobile wallets' (*KU Leuven*, 2019) p.34-35 <https://www.scriptiebank.be/sites/default/files/thesis/2019-10/PEETERS_s0107530_thesis.pdf> accessed 26 May 2021; Dilja Helgadottir, 'The Interaction between Directive 2015/2366 (EU) on Payment Services and Regulation (EU) 2016/679 on General Data Protection concerning Third Party Players' (2020) 23 Trinity CL Rev p. 220

[49] Johan Peeters, 'Data protection in mobile wallets' (*KU Leuven*, 2019) p.32 <https://www.scriptiebank.be/sites/default/files/thesis/2019-10/PEETERS_s0107530_thesis.pdf> accessed 26 May 2021

[50] Article 94 (2) PSD2

[51] Deloitte, 'PSD2 and GDPR: An awkward match?' (*Deloitte Legal*, 2018) <https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/legal/deloitte-nl-psd2-and-gdpr-an-awkward-match.pdf> accessed 26 May 2021; Beuc, 'Beuc's Recommendations to the EDPB on the interplay between the GDPR and PSD2' (*Recommendations*, 11 April 2019) p.3 <https://www.beuc.eu/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf> accessed 26 May 2021

[52] European Data Protection Board, 'Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR Version 1.0' (*Guidelines*, 17 July 2020) <https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202006_interplaypsd2andgdpr.pdf> accessed 26 May 2021; European Data Protection Board, 'Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR Version 2.0' (*Guidelines*, 15 December 2020)

6 GDPR are exhaustive and PSD2 does not provide an additional legal basis to process personal data, explicit consent under PSD2 should be accepted an additional contractual and transparency requirement regarding the performance of a contract.[53] Under PSD2, explicit consent sets forth that users should be fully aware of the types of data that will be processed by the controller for a particular payment service purpose and give their approval explicitly.[54] Thus, EDPB states that explicit consent under 94(2) PSD2 should be accepted as a contractual approval.[55] Although Guidelines are helpful to create legal certainty and consistency in data protection law application in the EU, as Guidelines are not legally binding,[56] some scholars and institutions criticized some points regarding the interpretation of explicit consent under PSD2.

To illustrate different opinions on explicit consent, the European Consumer Organisation (BEUC), an institution co-funded by the European Union, recommended that the explicit consent conditions in GDPR be the same for explicit consent under PSD2 before the Guidelines.[57] Following the Guidelines, BEUC still insists that an ordinary (opt-in) user consent should not be sufficient to process personal data under PSD2; instead, in addition to the opt-in ticking, users should insert a statement showing that users are granting access to their financial and personal data to TPPs.[58]

Dutch DPA (*Autoriteit Persoonsgegevens*) also interpreted explicit consent under Article 94(2) PSD2 in parallel with the explicit consent under GDPR.[59] Dutch DPA stated that explicit consent should be free, unambiguous, informed, specific, retractable, and obtained separately.[60] Dutch DPA also insisted that tacit consent and pre-ticked (opt-out) boxes cannot be accepted as explicit consent under Article 94(2) PSD2; instead, the data subjects should be asked clearly and explicitly give their explicit consent with an active behavior just like explicit consent under GDPR.[61]

Unlike BEUC's and Dutch DPA's opinion on consent, some stakeholders welcome EDPB's approach in Guidelines stating that Guidelines enables TPPs to provide more user-friendly services, as obtaining explicit consent is more burdensome than obtaining contractual consent.[62]

<https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202006_psd2_afterpublicconsultation_en.pdf> accessed 26 May 2021

[53] EDPB, PSD2 Guidelines, p. 14

[54] EDPB, PSD2 Guidelines, p. 14

[55] EDPB, PSD2 Guidelines, p. 14

[56] Christina Etteldorf, 'EDPB Publishes Guidelines on Data Processing through Video Devices' (2020) 6 Eur Data Prot L Rev 102, p. 105

[57] Beuc, 'Beuc's Recommendations to the EDPB on the interplay between the GDPR and PSD2' (*Recommendations*, 11 April 2019) p.3 <https://www.beuc.eu/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf> accessed 26 May 2021; Beuc, 'Guidelines 06/20 on the Interplay on the Second Payment Services Directive and the GDPR BEUC comments on the EDPB public consultation' (*Recommendations*, 15 September 2020) p.3-4 <https://edpb.europa.eu/sites/edpb/files/webform/public_consultation_reply/beuc-x-2020-086_position_paper_on_gdpr.pdf> accessed 26 May 2021

[58] Ibid.

[59] Bird & Bird, 'EN Translation FAQ PSD2 Dutch Data Protection Authority' (*Translation*, 18 October 2018) p.1 <https://www.twobirds.com/~/media/pdfs/psd2-dutch-data-protection-authority1.pdf?la=en&hash=55C83B022519F9EFC8C968C7D1EB892F83AD882B> accessed 26 May 2021

[60] Ibid.

[61] Ibid.

[62] Bitkom, 'Bitkom views on EDPB Guidelines 6/2020 on the interplay of the Second Payment Services Directive and the GDPR' (*Position Paper*, 16 September 2020) p.3 <https://www.bitkom.org/sites/default/files/2020-09/03_20200916_bitkom-position-on-edpb-guidelines-interplay-psd2-and-gdpr.pdf> accessed 26 May 2021

Besides, TPPs may have to obtain the users' explicit consent under GDPR in many situations since payment data may reveal sensitive personal data of users.[63]

The personal data that banks and TPPs could process under PSD2 and GDPR with explicit consent is still unclear.[64] This thesis aims to analyze the meaning of explicit consent and explain the types of personal data that could be processed under GDPR and PSD2 in general.[65] Thus, this thesis aims to clarify data processing in online payment transactions for online payment service companies and users under data privacy and data protection principles to create a more coherent and seamless online payment environment. Therefore, this thesis targets academia, scholars, practitioners, policy/lawmakers, and other stakeholders related to the online banking payment sector. Because of the abovementioned uncertainties, how and when explicit consent will be required, how such explicit consent should be obtained, alternative legal grounds for data processing operations, and which additional measures should be taken matter a lot for banks and TPPs while providing their services, considering significant monetary fines and reputation loss due to GDPR and PSD2 noncompliance.[66]

3. Main Research Question and Sub-Questions

After entering into force PSD2, TPPs' access to the users' data triggered various data protection issues.[67] As bank account data contains various personal data types that could identify users, controllers and processors should also comply with GDPR provisions.[68] Controllers have to base their data processing on at least one of six legal bases under the Article 6(1)(a-f) GDPR.[69] However, TPPs can only process the personal data necessary to provide their services, provided that they obtain "explicit consent" of users under PSD2.[70] In line with this explanation, the research question of this thesis is as follows:

What kind of personal data, including silent party data, could be processed under the notion of explicit consent as per GDPR and PSD2 in online payment transactions?

---

[63] Dutch Data Protection Authority, 'Investigation into the combining of personal data by Google' (*Report*, November 2013) p.44 <https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/en_rap_2013-google-privacypolicy.pdf> accessed 26 May 2021

[64] Deloitte, 'PSD2 and GDPR: An awkward match?' (*Deloitte Legal*, 2018) <https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/legal/deloitte-nl-psd2-and-gdpr-an-awkward-match.pdf> accessed 26 May 2021; Bird & Bird, 'EU: The interplay of PSD2 and GDPR - some select issues' (*DataGuidance*, February 2019) <https://www.twobirds.com/~/media/pdfs/eu-the-interplay-of-psd2-and-gdpr--some-select-issues.pdf> accessed 26 May 2021

[65] EDPB, PSD2 Guidelines

[66] Deloitte, 'PSD2 and GDPR: An awkward match?' (*Deloitte Legal*, 2018) <https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/legal/deloitte-nl-psd2-and-gdpr-an-awkward-match.pdf> accessed 26 May 2021

[67] Deutsche Bank Global Transaction Banking, 'Are You PSD2-Ready? A Guide to the latest information and sources of support' (*White Paper*, October 2017) p.17 <https://cib.db.com/docs_new/PSD2_White_Paper_October_2017.pdf> accessed 26 May 2021

[68] Ducuing Charlotte, Dutkiewicz Lidia and Miadzvetskaya Yuliya, 'D62 Legal and Ethical Requirements' (*Trusts Trusted Secure Data Sharing Space*, August 2020) p.123 <https://www.trusts-data.eu/wp-content/uploads/2020/10/D6.2-Legal-and-Ethical-Requirements.pdf> accessed 26 May 2021

[69] Johan Peeters, 'Data protection in mobile wallets' (*KU Leuven*, 2019) p.32 <https://www.scriptiebank.be/sites/default/files/thesis/2019-10/PEETERS_s0107530_thesis.pdf> accessed 26 May 2021

[70] PSD2, Article 94

To provide a proper answer to the research question, the questions below should also be answered:

1. What kind of personal data requires explicit consent under GDPR, and what is the role of these data in online transactions?

2. What is the scope of explicit consent under PSD2 considering the Guidelines, and what is the overlap with the data requiring explicit consent in GDPR?

3. If the silent party data does not fall under explicit consent, how should silent party data be processed?

4. Limitations, methodology and methods

This thesis will be based on the doctrinal research method; it deals with legal doctrines and concepts considering laws, regulations, and cases.[71] With this method, this thesis will be mainly based on EU-level legal sources, including regulations, directives, case law, guidelines, particularly GDPR, PSD2, EDPB Guidelines, and secondary sources (e.g., books, articles). In this thesis, various scholars' and institutions' opinions will be elaborated and analyzed, and, then, considering the Guidelines and other official EU documents, the answer to the research question of the thesis will be provided. Furthermore, this thesis will contain some interdisciplinary insights and technical aspects, considering the new online payment systems' technological complexities.

All searches will be conducted via Tilburg University's online databases and other online databases, including Hein Online, Google Scholar.

5. Structure

This thesis will be composed of five chapters and a conclusion. Following the introduction chapter, the second chapter will explain how the online payment system works under PSD2 and give information about the relevant parties, such as TPPs and banks, to understand their interaction in the online payment sector and the potential data protection issues better.

The third chapter will explain the personal data that can be processed with and without the payment service users' consent and explicit consent under GDPR. This chapter will then analyze to what extent these personal data are used in online payment transactions.

The fourth chapter will elaborate on the meaning and scope of the consent and explicit consent in PSD2, considering the EDPB's interpretation in the Guidelines. This chapter will also explain similarities and differences of consent and explicit consent under GDPR and PSD2, considering the Guidelines and options and alternatives for GDPR and PSD2 compliance.

Silent party data is also processed in the online payment sector. But, since the users' consent or consent explicit consent do not legitimize data processing operations of silent parties, such data processing operation will be explained under a separate chapter. The fifth chapter will explain how silent party data could be processed in online payment transactions and which legal grounds could be used for the processing. Also, the steps taken while processing the personal data of silent parties will be explained.

[71] Terry Hutchinson and Nigel Duncan, 'Defining and Describing What We Do: Doctrinal Legal Research' [October 2012] 17(1) Deakin Law Review p.84-86

2. CHAPTER 2 – PSD2, Open Banking, TPPs and Data Processing

1. The Background of PSD2

This chapter will explain the background and reason behind the entering into force of PSD2 and particular concepts, such as; open banking and TPPs, and the change in the online payment sector's personal data processing operations. Firstly, this chapter will provide an overview regarding the recent developments in the online payment sector, particularly creating new players and increased competition between the PSD1 and PSD2 eras. Then, the online banking concept and TPPs' role in the online payment sector will be elaborated. Lastly, this chapter will explain personal data processing operations in the online payment sector after PSD2 and interaction between banks and TPPs regarding personal data access and processing.

Compared to PSD1, PSD2 covers significantly more payment services and obliges payment service providers to adopt the new payment structure and comply with the new provisions.[72] Before entering into force of PSD2, banks benefited from a monopoly on the online payment services market and had controlling power on access to user accounts.[73] Other online payment service providers did not have any legal access rights to the users' bank account information (e.g., IBAN no, bank, branch name) in such a situation.[74] With PSD2, it is arguable that the EU aimed to provide a level playing field to both traditional players (e.g., banks), considering the strict regulatory burden in the banking sector against the new and competitive entrants (e.g., Sofort, Trustly, Google, Apple).[75] These companies, TPPs in this context, focused on improving user experience, increasing online payment process efficiency, and making the traditional services more personalized, transparent, and accessible in the digital environment as an alternative to conventional financial service providers, such as banks.[76]

2. Open Banking and TPPs Effects on Online Payments

Open banking is a new model that allows sharing users' bank account data with TPPs in a secure environment via the application programming interface (API).[77] Under API, a standardized protocol enabling communication between computer programs, previously determined communication occurs between the computer programs.[78] As the different information and data silos may communicate and share data with each other, multiple products and services can be provided.[79]

Before PSD2, if users approved giving access to their bank accounts concerning an online payment transaction, PISPs and AISPs could have used the users' online banking channel, and they collected and used the same information available to users via a method called "screen

---

[72] Morrison Foerster, 'FinTech Focus: New European Directive on Payment Services (PSD2) Comes into Force' (*Client Alert*, 1 February 2016) p.3 <https://media2.mofo.com/documents/160129fintechfocus.pdf> accessed 26 May 2021

[73] Marijana Petrović, 'PSD2 influence on digital banking transformation: Banks' perspective' [2020] 8(4) Journal of Process Management New Technologies p.8

[74] Ibid.

[75] Dilja Helgadottir, 'The Interaction between Directive 2015/2366 (EU) on Payment Services and Regulation (EU) 2016/679 on General Data Protection concerning Third Party Players' (2020) 23 Trinity CL Rev p. 204

[76] Marijana Petrović, 'PSD2 influence on digital banking transformation: Banks' perspective' [2020] 8(4) Journal of Process Management New Technologies p.3

[77] Anshu Premchand and Anurag Choudhry, 'Open Banking & APIs for Transformation in Banking' (International Conference on Communication, Computing and Internet of Things (IC3IoT), 2018) p.1 <https://ieeexplore-ieee-org.tilburguniversity.idm.oclc.org/stamp/stamp.jsp?tp=&arnumber=8668107> accessed 26 May 2021

[78] Stian Abusdal & Ricardo Gjermundnes, p. 25

[79] Ayo Eso and Anna Masłoń-Oracz, 'The Impact of Payment Services Directive 2 (Psd2) on Financial Services in the European Union Single Market' [2018] 2(2) The Review of European Affairs p.37

scraping".[80] This was a kind of technology and the practical solution used by AISPs and PISPs before PSD2 to access the users' data, as the user, without identifying itself to the bank, to provide their online payment services, since they would not have a legal right to request access to their users' banking data from the users' banks.[81] When a user authorizes a PISP or AISP for an online payment transaction, the relevant TPP may also see the same page and access the same information that the user sees and accesses.[82] However, after the entering into force of PSD2, "account servicing payment servicing providers" (ASPSPs/banks) should grant access to PISPs and AISPs for them to reach their users' relevant data, provided that the users' explicit consent has been obtained as required, even though a commercial/contractual relationship between banks and TPPs does not exist.[83] A more detailed overview of how these services work can be found in Figure 1 below.

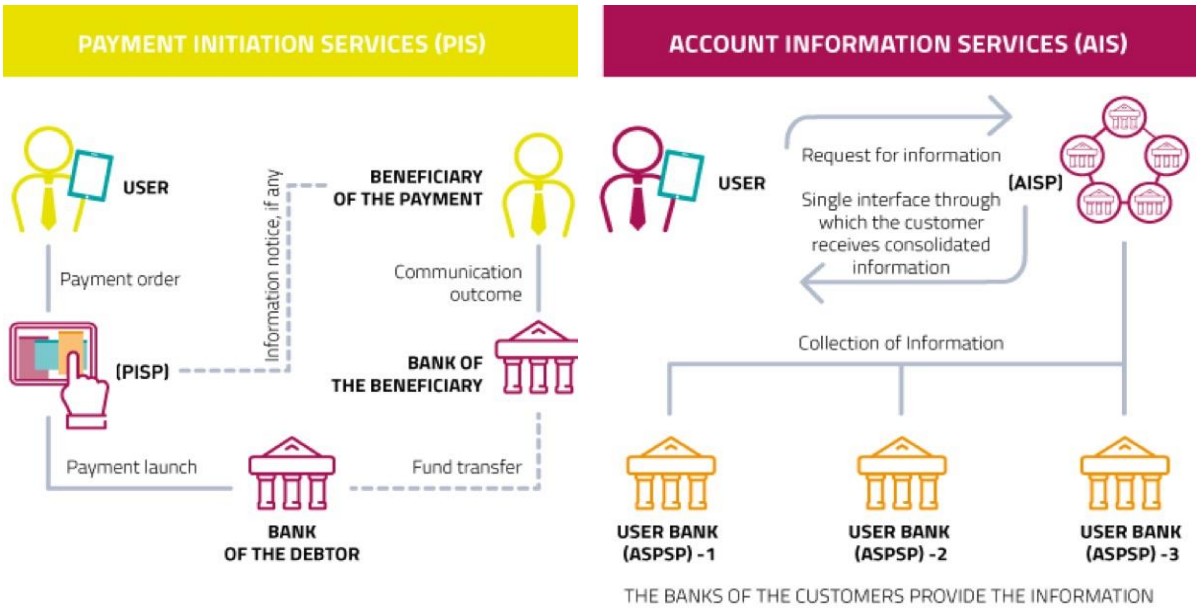

Figure 1: How TPPs work[84]

Provided that PISPs obtain users' consent, they can initiate the payment directly from their bank account without needing a debit card or credit card.[85] As for AISPs, with the user's consent,

[80] Beuc, 'Consumer-friendly Open Banking Access to Consumers' Financial Data by Third Parties' (*Publications*, 20 September 2018) p.3 <https://www.beuc.eu/publications/beuc-x-2018-082_consumer-friendly_open_banking.pdf> accessed 26 May 2021

[81] P.T.J. Wolters, B.P.F. Jacobs, 'The security of access to accounts under the PSD2' [2019] 35(1) Computer Law & Security Review, p.35

[82] P.T.J. Wolters, B.P.F. Jacobs, 'The security of access to accounts under the PSD2' [2019] 35(1) Computer Law & Security Review, p.35

[83] P.T.J. Wolters, B.P.F. Jacobs, 'The security of access to accounts under the PSD2' [2019] 35(1) Computer Law & Security Review, p.30; Covington & Burling, 'Overlap Between the GDPR and PSD2' (*Inside Privacy*, 16 March 2018) <https://www.insideprivacy.com/financial-institutions/overlap-between-the-gdpr-and-psd2/> accessed 26 May 2021; Dilja Helgadottir, 'The Interaction between Directive 2015/2366 (EU) on Payment Services and Regulation (EU) 2016/679 on General Data Protection concerning Third Party Players' (2020) 23 Trinity CL Rev p. 204

[84] CBI Globe, 'PSD2 Tech Specifications of the PSD2 services exposed to the Third Party Providers' (*Global Open Banking Ecosystem Wiki*, 2018) <https://www.cbiglobe.com/Wiki/index.php/2._Actors_and_definitions> accessed 26 May 2021

[85] Piotr Kuszewski, 'Impact of the PSD2 directive and strategic use of costly innovation' (*Warsaw School of Economics, Banking Institute*, October 2018) p.4 <https://www.researchgate.net/profile/Piotr-Kuszewski-2/publication/330347466_Impact_of_the_PSD2_directive_and_strategic_use_of_costly_innovation/links/5c3a5a

AISPs can access not only the basic bank account information of the user but also the user's status and bank account history.[86] Apart from the new players, banks can also provide payment initiation and account information services and still be better off as they may also access other banks' user data.[87] In line with the explanations above, PSD2 helps establish the new business model, namely "open banking".[88] Open banking will help accelerate innovation in the online payment services sector and create room for TPPs to grow in the EU.[89] After PSD2, the number of companies in 2018 and 2019 that obtained TPP licenses increased fourfold.[90]

Adopting PSD2 is beneficial for users as they can either prefer to receive services from new and innovative TPPs or easily access their bank accounts via the existing players (e.g., banks).[91] Following PSD2, the big tech companies (e.g., Google, Facebook, Apple) may have an advantage against banks, as they have the vast size of behavioral personal data of their users, capital and resources, technological expertise, and have already been integrated with billions of users' daily life.[92] In other words, they may create a more complete and accurate profile of their users, as the volume and variety of personal data will be significantly higher.[93] On the other hand, as start-up companies (i.e., TPPs) are known that they do not make too much investment in security and data protection, but user experience itself, the increased number of newly developed TPPs may cause specific personal data-related concerns in the online payment services sector.[94] Therefore, as high data protection risks may arise for hundreds of millions of people, it is a must to determine the level of data subject-control over their data, explain the meaning of explicit consent under PSD2, and eventually, clarify the types of data that could be processed with explicit consent under PSD2.

3. Conclusion

The first part of this chapter explains what PSD2 brings and shows some differences between PSD1 and PSD2. While making such an explanation, the technological and digital developments have been evaluated. As a result of such developments, TPPs gain more ground

---

cc92851c22a370cb43/Impact-of-the-PSD2-directive-and-strategic-use-of-costly-innovation.pdf> accessed 26 May 2021

[86] Ibid.

[87] P.T.J. Wolters, B.P.F. Jacobs, 'The security of access to accounts under the PSD2' [2019] 35(1) Computer Law & Security Review, p. 31

[88] Michał Polasika, Agnieszka Huterskaa, Rehan Iftikhar, Štepán Mikula, 'The impact of Payment Services Directive 2 on the PayTech sector development in Europe' [2020] 178 Journal of Economic Behavior & Organization p.387

[89] Ibid.

[90] Michał Polasika, Agnieszka Huterskaa, Rehan Iftikhar, Štepán Mikula, 'The impact of Payment Services Directive 2 on the PayTech sector development in Europe' [2020] 178 Journal of Economic Behavior & Organization p.397

[91] Piotr Kuszewski, 'Impact of the PSD2 directive and strategic use of costly innovation' (*Warsaw School of Economics, Banking Institute*, October 2018) p.5 <https://www.researchgate.net/profile/Piotr-Kuszewski-2/publication/330347466_Impact_of_the_PSD2_directive_and_strategic_use_of_costly_innovation/links/5c3a5acc92851c22a370cb43/Impact-of-the-PSD2-directive-and-strategic-use-of-costly-innovation.pdf> accessed 26 May 2021

[92] Mckinsey&Company, 'PSD2: Taking advantage of open-banking disruption' (*Our Insights*, 24 January 2018) p.2 <https://www.mckinsey.com/industries/financial-services/our-insights/psd2-taking-advantage-of-open-banking-disruption> accessed 26 May 2021; Ayo Eso and Anna Masłoń-Oracz, 'The Impact of Payment Services Directive 2 (Psd2) on Financial Services in the European Union Single Market' [2018] 2(2) The Review of European Affairs p.39

[93] Ayo Eso and Anna Masłoń-Oracz, 'The Impact of Payment Services Directive 2 (Psd2) on Financial Services in the European Union Single Market' [2018] 2(2) The Review of European Affairs p.39

[94] Ilkka Saarnilehto, Problems and possibilities of the payment services directive (PSD2) p. 78

in the online payment market. After TPPs' involvement, a new business model named "open banking" became popular in the online payment sector.

In open banking, banks have to allow third-party providers who obtained their licenses to access their accounts regarding payment initiation and account information services. However, this new business model caused some concerns in the data protection area, as many new players will be able to access users' financial data that may also reveal sensitive personal data regulated under Article 9 GDPR. Thus, this necessitates a critical legal evaluation of personal data that could be processed under the notion of explicit consent as per GDPR and PSD2 in online payment transactions.

3. CHAPTER 3 – Processing Grounds under the GDPR: Consent, Explicit Consent, and Necessary for the Performance of a Contract

1. Introduction

This chapter will explain the terms of "consent", "explicit consent", and "necessary for the performance of a contract" under GDPR. Explaining consent and explicit consent aims to analyze GDPR's approach first before comparing the approaches of GDPR with PSD2 in Chapter 4. Since EDPB considers "explicit consent" under PSD2 *"as an additional requirement of a contractual nature"*, different from "consent" and "explicit consent" under GDPR, we will evaluate EDPB's approach of *"additional requirement of a contractual nature"* in the first place.[95] While providing their payment initiation or account information services, TPPs provide their services to users based on a commercial contract. Therefore, the legal base of "necessary for the performance of a contract" under Article 6(1)(b) GDPR will be explained to analyze TPPs' data processing activities.[96]

In the first part, the definition and conditions of consent under GDPR will be discussed. Then, a detailed analysis of explicit consent under GDPR will be made. In the third part of this chapter, the legal base necessary for the performance of a contract will be briefly explained. The whole chapter will reflect GDPR's approach.

Under the "Explicit consent under GDPR" part, two important reasons for obtaining explicit consent under GDPR will be explained: processing special categories of personal data and automated decision-making, including profiling, since these two reasons are directly related to online payment transactions. Although the third reason for obtaining explicit consent is transferring personal data to third (non-EU) countries which do not have an adequacy decision taken by the EU Commission and appropriate safeguards, this third ground will not be elaborated any further as this third ground for obtaining explicit consent is not directly related to the personal data processing in online payment services.[97]

2. Consent under GDPR

GDPR introduced a more complete and detailed data protection system directly applicable in all the EU countries compared to the 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 (DPD) and PSD2.[98] Although consent was a legal base under the DPD and even mentioned under the Charter of Fundamental Rights of the EU (Charter), consent is one of the six legal bases to process personal data under this new data protection system.[99] If the controller obtains the data subject's consent under GDPR provisions, consent will be a vital tool empowering individuals and granting them control over

[95] EDPB, PSD2 Guidelines, p. 14

[96] Article 6 (1)(b) GDPR

[97] Article 45(3) GDPR; Article 46 GDPR; Article 49(1)(a) GDPR; Recital 101 GDPR; Article 44-50 GDPR

[98] 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*; Dilja Helgadottir, 'The Interaction between Directive 2015/2366 (EU) on Payment Services and Regulation (EU) 2016/679 on General Data Protection concerning Third Party Players' (2020) 23 Trinity CL Rev p. 217

[99] Charter of Fundamental Rights of the European Union [2000] *OJ C364/1*; Article 6 (1)(a) GDPR; Article 4 (1)(11) GDPR; Stephen Breen, Karim Ouazzane and Preeti Patel, 'GDPR: Is your consent valid?' [2020] 37(1) Business Information Review, p.22; Article 7(1)(a) DPD; Article 8 Charter

their data.[100] Even if consent is obtained as required, controllers still cannot collect the personal data that is not necessary regarding the purpose of processing and could be regarded as unfair.[101]

Consent should be requested for all data processing activities related to the same processing purpose or purposes.[102] If the processing has several and different purposes, consent should be given for each of them.[103] Due to the usage of "purposes", data subjects should be informed on both the primary and other secondary purposes, if any.[104] Consent cannot be presumed freely given when the option to give consent for different personal data processing operations is not submitted separately.[105] In other words, data subjects should have an option to give or not to give consent for each specific data processing activity.[106]

If consent is bundled/tied with non-negotiable parts of the agreement to be signed between the controller and data subject, the consent will not be freely given and legally valid.[107] Besides, consent will not be valid if the requested consent is a precondition for providing a service, in case the personal data requested with consent is not necessary for the performance of a contract.[108] For example, a photo editing application requests its users' consent to process their GPS location and use their collected data for behavioral advertising purposes.[109] GPS data and more personalized targeted advertising are not strictly necessary to provide photo editing services.[110] Therefore, if users cannot use the photo editing application without giving their consent for these two processing operations, such consent will not be freely given.[111]

In case of a clear imbalance between the controller and data subject, consent may not be given freely considering the particulars of each case.[112] Apart from public institutions' authority on individuals, such a clear imbalance could be seen between companies having monopoly status in their market and individuals who are obliged to use these companies' services.[113] For example, the German Competition Authority (*Bundeskartellamt*) determined that Facebook has

---

[100] Mark Foulsham, Brian Hitchen and Andrew Denley, GDPR How To Achieve and Maintain Compliance (Routledge 2019) p.76; European Data Protection Board, 'Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1' (*Guidelines*, 4 May 2020) p.5 <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf> accessed 26 May 2021

[101] Ibid.

[102] Stephen Breen, Karim Ouazzane and Preeti Patel, 'GDPR: Is your consent valid?' [2020] 37(1) Business Information Review, p.22; Recital 32 GDPR

[103] Recital 32 GDPR

[104] Anton Lindberg, 'Alternatives for the Individual Consent in Data Protection Law' (*Tilburg University*, 2018) p.23 <https://arno.uvt.nl/show.cgi?fid=145717> accessed 26 May 2021

[105] Recital 43 GDPR

[106] Alan Calder, EU GDPR - A pocket guide (2nd edn, IT Governance Publishing 2018) p.34; Recital 43 GDPR

[107] European Data Protection Board, 'Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1' (*Guidelines*, 4 May 2020) p.7 <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf> accessed 26 May 2021

[108] Recital 43 GDPR

[109] European Data Protection Board, 'Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1' (*Guidelines*, 4 May 2020) p.8 <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf> accessed 26 May 2021

[110] Ibid.

[111] Ibid.

[112] Recital 43 GDPR

[113] Tobias Kugler and Daniel Rücker LL.M., New European General Data Protection Regulation A Practitioner's Guide (Bloomsbury Publishing 2018), p.93-94

a dominant position in the social platform market and does not ask for separate/additional consent from its users for each data processing operation.[114] Therefore, Bundeskartellamt decided that as users did not give separate/additional consent for each data processing operation and had to give their consent to benefit from Facebook's services, such consent is not freely given under GDPR.[115] Because of such an "imbalanced" situation, even though the data subjects give their consent for the processing operations, big companies having dominant positions in particular markets should pay more attention to not processing unnecessary data as the validity of consent could be at stake.[116] In addition, GDPR's high monetary fines could be another reason for big companies to limit their unnecessary data processing operations, in addition to the loss of trust and reputation.[117] Since the legality of consent could be questioned more in the future, finding different legal grounds could be an option for the dominant companies (e.g., Facebook, Google, Amazon).[118]

Not taking any action, being silent, not behaving in a certain way, pre-ticked boxes (opt-out), or a passive behavior cannot be regarded as consent.[119] Active behavior, oral and written statement, the statement by electronic means, or ticking an empty box in an online environment could be regarded as an active behavior for giving consent.[120] The controller should take necessary measures to ensure that the data subject is fully informed and aware of the consent that he or she is given.[121]

If consent is requested in an electronic/online environment, such request should be short, in plain language, without legal jargon, understandable for an ordinary person, easily accessible, and provided in a way that does not prevent users benefiting from the service.[122] The scope, limits, and consequences of consent should be clear, precise, and specific.[123]

Graphically highlighting the consent request in written and electronic forms, making it more distinguishable from other texts, and using the word "consent" rather than other non-legal terms are well-advised.[124] Besides, framing, bolding, underlining, and using other colors for the consent request will make it more distinguishable.[125] To provide precise and specific information for consent, layered (one short and one long privacy policies) and granular

---

[114] Bundeskartellamt, 6th Decision Division, B6-22/16 p.184-186
[115] Bundeskartellamt, 6th Decision Division, B6-22/16 p.184-186
[116] Paul Voigt and Axel von dem Bussche, The EU General Data Protection Regulation (GDPR) A Practical Guide (Springer 2017), p.96
[117] Ibid.; Article 83(5)-(6) GDPR; The EU General Data Protection Regulation (GDPR) A Practical Guide (Springer 2017), p.96e, p. 96; Article 83(5) GDPR
[118] Tobias Kugler and Daniel Rücker LL.M., New European General Data Protection Regulation A Practitioner's Guide (Bloomsbury Publishing 2018), p.94
[119] Tobias Kugler and Daniel Rücker LL.M., New European General Data Protection Regulation A Practitioner's Guide (Bloomsbury Publishing 2018), p.91-92; Recital 32 GDPR
[120] Recital 32 GDPR
[121] Recital 42 GDPR
[122] Recital 32 GDPR; Recital 42 GDPR; EDPB, European Data Protection Board, 'Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1' (*Guidelines*, 4 May 2020) p.16 <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf> accessed 26 May 2021
[123] Tobias Kugler and Daniel Rücker LL.M., New European General Data Protection Regulation A Practitioner's Guide (Bloomsbury Publishing 2018), p.95
[124] Paul Voigt and Axel von dem Bussche, The EU General Data Protection Regulation (GDPR) A Practical Guide (Springer 2017), p.94; Article 7 (2) GDPR
[125] Tobias Kugler and Daniel Rücker LL.M., New European General Data Protection Regulation A Practitioner's Guide (Bloomsbury Publishing 2018), p.96

information (for each processing operation) could be preferable to give a proper, complete, and understandable document.[126] Using standardized icons can simplify the long and complicated privacy policies convey and save users' time.[127]

Freely given consent necessitates having a real choice and not having any fear of detriment in refusal of consent.[128] However, the controllers are free to provide discounts and premiums to the data subjects for them to give their consent for the relevant data processing activities.[129] To ensure that consent is given freely, the design of the online environment matters. [130] Placing bottoms with the words of "agree" or "allow" over "reject" or "block" for giving consent will be non-compliant since such terms manipulate users to choose "agree" or "allow".[131] Some other "nudging" examples are highlighting "accept" buttons or using contrasting colors and techniques to manipulate the data subjects' decision-making process and steering them towards accepting privacy-unfriendly options.[132] An advocate general of the CJEU highlighted that both "giving consent" and "not giving consent" should be *"optically in particular, be presented on an equal footing"*.[133]

Without providing any reason, data subjects have the right to withdraw their consent easily and any time they want.[134] Consent cannot be regarded as freely given if data subjects do not have the free choice or cannot withdraw or reject to give consent without any detriment.[135] Data subjects may withdraw some processing activities and not withdraw other activities.[136] In case

---

[126] European Data Protection Board, 'Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1' (*Guidelines*, 4 May 2020) p.16 <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf> accessed 26 May 2021

[127] Article 13(7) GDPR; I. Van ooijen and Helena U. Vrabec, 'Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective' [2018] 42 Journal of Consumer Policy p. 7

[128] Anton Lindberg, 'Alternatives for the Individual Consent in Data Protection Law' (*Tilburg University*, 2018) p.22 <https://arno.uvt.nl/show.cgi?fid=145717> accessed 26 May 2021

[129] Eleni Kosta, 'Consent in European Data Protection Law' [2013] 3 Nijhoff Studies in European Union Law p.172-173

[130] Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger and Lalana Kagal, 'Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence' (*CHI '20 CHI Conference on Human Factors in Computing Systems*, 30 April 2020) p.2 <https://arxiv.org/pdf/2001.02479.pdf> accessed 26 May 2021

[131] Ibid.; Forbrukerradet, 'Deceived by Design How tech companies use dark patterns to discourage us from exercising our rights to privacy' (*Forbrukerradet*, 27 June 2018) p.27 <https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf> accessed 26 May 2021

[132] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub and Thorsten Holz, '(Un)informed Consent: Studying GDPR Consent Notices in the Field' (CCS '19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, 15 November 2019) p. 976-978 <https://arxiv.org/pdf/1909.02638.pdf> accessed 26 May 2021

[133] Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger and Lalana Kagal, 'Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence' (*CHI '20 CHI Conference on Human Factors in Computing Systems*, 30 April 2020) p.2 <https://arxiv.org/pdf/2001.02479.pdf> accessed 26 May 2021; Advocate General Szupunar. 2019. Case C-673/17 Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. ECLI:EU:C:2019:246, Opinion of the Advocate General. (2019), paragraph 66

[134] Article 7(4) GDPR; Tobias Kugler and Daniel Rücker LL.M., New European General Data Protection Regulation A Practitioner's Guide (Bloomsbury Publishing 2018), p.100; IT Governance Privacy Team, EU General Data Protection Regulation (GDPR) An Implementation and Compliance Guide (4th edn, IT Governance Publishing 2020), p.137

[135] Anton Lindberg, 'Alternatives for the Individual Consent in Data Protection Law' (*Tilburg University*, 2018) p.22 <https://arno.uvt.nl/show.cgi?fid=145717> accessed 26 May 2021; Recital 42 GDPR

[136] IT Governance Privacy Team, EU General Data Protection Regulation (GDPR) An Implementation and Compliance Guide (4th edn, IT Governance Publishing 2020) p.132-133;

of withdrawal, withdrawal should be simple and easy (e.g., mouse-click, swipe, keystroke), and website and technological infrastructure should be designed suitably, in compliance with data protection by design and by default.[137]

If a controller decides to collect personal data based on consent, this may empower data subjects as they will generally have more rights (e.g., right to erasure, right to data portability) and control over their data.[138] Moreover, 70% of people are concerned about how companies use their data, and 74% of people want to (or refuse to) give consent before the personal data processing operation in the online environment.[139] Furthermore, "consent" is the main condition for benefiting from one of the fundamental rights, the right to privacy and protection of personal data, which everyone can enjoy under Article 8 Charter.[140]

As the downside of consent, based on users' behaviors, it was found that users prefer the immediate benefit obtained by data sharing compared to its negative consequences that they may face in the future.[141] As such data technologies are pretty new, users do not have enough experience concerning the harmful effects of misused data, and they may assume that giving their data to these companies may not cause problems for them at the later stage.[142] Even if the controllers provide their consent requests in line with GDPR and other applicable legislation, most users do not know the consequences of data processing operations, what they have consented and the potential adverse effects on them.[143]

Because people are busy, distracted, and tired of reading privacy policies, terms and conditions, and other digital contractual texts all the time in the digital environment, trying to comprehend these texts and their potential effects on them could be pretty challenging in daily life.[144] Thus, receiving many consent requests diminishes these requests' warning effects.[145] For many digital users, clicking the "I agree" button is a better solution than spending too much time reading

---

[137] Article 25 GDPR; IT Governance Privacy Team, EU General Data Protection Regulation (GDPR) An Implementation and Compliance Guide (4th edn, IT Governance Publishing 2020) p.132-133; Tobias Kugler and Daniel Rücker LL.M., New European General Data Protection Regulation A Practitioner's Guide (Bloomsbury Publishing 2018), p.112; Michelle Goddard, 'The EU General Data Protection Regulation (GDPR): European regulation that has a global impact' [2017] 59(6) International Journal of Market Research p.703

[138] Mark Foulsham, Brian Hitchen and Andrew Denley, GDPR How To Achieve and Maintain Compliance (Routledge 2019) p.76

[139] Amaya Noain-sánchez, '"Privacy by default" and active "informed consent" by layers: Essential measures to protect ICT users' privacy' [2016] 14 Journal of Information, Communication and Ethics in Society p.128

[140] Article 8 Charter; Eleni Kosta, 'Consent in European Data Protection Law' [2013] 3 Nijhoff Studies in European Union Law p.140-141

[141] Barbara Engels and Mara Grunewald, 'Das Privacy Paradox, Digitalisierung versus Privatsphäre' (*Institut der deutschen Wirtschaft*, 14 August 2017) <https://www.iwkoeln.de/studien/iw-kurzberichte/beitrag/barbara-engels-mara-grunewald-das-privacy-paradox-digitalisierung-versus-privatsphaere-356747.html> accessed 26 May 2021

[142] Neil Richards and Woodrow Hartzog, 'The Pathologies of Digital Consent' [2019] 96(6) Washington University Law Review p.1484

[143] Neil Richards and Woodrow Hartzog, 'The Pathologies of Digital Consent' [2019] 96(6) Washington University Law Review p.1478

[144] Neil Richards and Woodrow Hartzog, 'The Pathologies of Digital Consent' [2019] 96(6) Washington University Law Review p.1478-1479; Stephen Breen, Karim Ouazzane and Preeti Patel, 'GDPR: Is your consent valid?' [2020] 37(1) Business Information Review, p.20

[145] European Data Protection Board, 'Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1' (*Guidelines*, 4 May 2020) p.19 <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf> accessed 26 May 2021

boilerplate documents that they cannot change.[146] Moreover, since users have to spend a certain time and effort to read and understand the consent requests of mobile applications, websites, or any other service providers, they may not read all of these consent requests carefully.[147] For example, according to research on privacy policies of mobile health apps, the average privacy policy has 3,783 words.[148] Considering that an ordinary person can read 200–250 words in a minute, only reading a privacy policy of a health app will take 15-20 minutes.[149] In addition, when the data controller is a dominant company in the relevant market, users tend to skip reading privacy policies more since they will consent to the dominant company anyway.[150]

Due to the complexity of user interface technologies, data subjects may not comprehend the potential negative consequences they may face when they read the privacy notices and hope that their data will be protected by the company they chose.[151] As recently seen in Facebook/Cambridge Analytica scandal, although users allegedly gave their consent for collection and sharing of their data with some third parties, when the details of the case are analyzed, it is seen that such consent was "manufactured" intentionally by Facebook via its user interface by using misleading, abstract and confusing words.[152]

Lastly, under the accountability principle,[153] the controller should prove that all consent requirements are collectively fulfilled.[154] After determining consent as the applicable legal base, if there is a problem with the validity of consent, the controller cannot rely on another legal ground under Article 6(1)(b-f) GDPR.[155]

3. Explicit consent under GDPR

Considering the high ordinary consent requirements under GDPR, it is essential to determine "explicit consent" requirements that the controllers must fulfill on top of the standard consent requirements.[156] As mentioned earlier, explicit consent is required when a serious data

---

[146] Neil Richards and Woodrow Hartzog, 'The Pathologies of Digital Consent' [2019] 96(6) Washington University Law Review, p.1478-1479

[147] Stefanie Hänold, Profiling and Automated Decision-Making: Legal Implications and Shortcomings. in Corrales and others (eds), Robotics, AI Marcelo Corralesand the Future of Law (Springer 2018) p.137; Stephen Breen, Karim Ouazzane and Preeti Patel, 'GDPR: Is your consent valid?' [2020] 37(1) Business Information Review, p.22-23

[148] Trix Mulder, 'Health Apps, their Privacy Policies and the GDPR' [2019] University of Groningen Faculty of Law Research Paper No15/2020 European Journal of Law and Technology, p.8

[149] Ibid.

[150] Bundeskartellamt, 6th Decision Division, B6-22/16 p.107-108

[151] Neil Richards and Woodrow Hartzog, 'The Pathologies of Digital Consent' [2019] 96(6) Washington University Law Review, p.1480

[152] Neil Richards and Woodrow Hartzog, 'The Pathologies of Digital Consent' [2019] 96(6) Washington University Law Review, p.1481

[153] Article 5(2) GDPR

[154] Alan Calder, EU GDPR - A pocket guide (2nd edn, IT Governance Publishing 2018) p.37; European Union Agency for Fundamental Rights and Council Of Europe, 'Handbook on European data protection law' (Handbook, April 2018) p.151 <https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition> accessed 26 May 2021; Recital 42 GDPR

[155] Article 6 1(b)-(f) GDPR

[156] Anton Lindberg, 'Alternatives for the Individual Consent in Data Protection Law' (*Tilburg University*, 2018) p.26 <https://arno.uvt.nl/show.cgi?fid=145717> accessed 26 May 2021; European Data Protection Board, 'Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1' (*Guidelines*, 4 May 2020) p.20 <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf> accessed 26 May 2021

protection risk arises, and a high level of data subject control over his/her data is necessary.[157] In cases where explicit consent is required under GDPR, data subjects must be aware that they are abandoning special protection and handing over their sensitive information to the relevant controller voluntarily. [158] When processing sensitive personal data with explicit consent, such explicit consent should be even better informed and more specific and unambiguous than the ordinary one.[159]

The term "explicit" refers to the data subject's active way of declaring their consent statement.[160] In a written declaration, obtaining the data subject's wet signature is a possible way for obtaining explicit consent.[161] However, in an electronic/online environment, the data subject may give his/her explicit consent, for example; (i) by filling out an online form, (ii) by sending an e-mail, (iii) by uploading a scanned document having his or her wet or electronic signature.[162] Although obtaining explicit verbal consent is allowed in theory, it would be difficult for controllers to prove all conditions of explicit consent have been fulfilled.[163] To be sure that the consent is an "explicit" one, in addition to an opt-in ticking, it is advised to request an additional explicit and active clarification from the data subjects.[164] Thus, a two-stage verification could be a suitable option. For example, after receiving a notification e-mail regarding the controller's intention to process sensitive personal data and ask the data subject's explicit consent, the data subject responds to this e-mail by clicking the "I agree" button as the first-stage verification. Then, the controller may send a verification link via another e-mail or an SMS to ask for the second-stage verification. Then data subject may click the verification link or insert the verification code provided by an SMS to confirm the agreement.[165]

---

[157] Michelle Goddard, 'The EU General Data Protection Regulation (GDPR): European regulation that has a global impact' [2017] 59(6) International Journal of Market Research, p.704; European Data Protection Board, 'Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1' (*Guidelines*, 4 May 2020) p.20 <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf> accessed 26 May 2021

[158] Anton Lindberg, 'Alternatives for the Individual Consent in Data Protection Law' (*Tilburg University*, 2018) p.26 <https://arno.uvt.nl/show.cgi?fid=145717> accessed 26 May 2021

[159] Bart Van der Sloot, The General Data Protection Regulation in Plain Language (Amsterdam University Press 2020) p.78

[160] Eleni Kosta, 'Consent in European Data Protection Law' [2013] 3 Nijhoff Studies in European Union Law p.150; European Data Protection Board, 'Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1' (*Guidelines*, 4 May 2020) p.20 <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf> accessed 26 May 2021

[161] European Data Protection Board, 'Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1' (*Guidelines*, 4 May 2020) p.21 <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf> accessed 26 May 2021

[162] Eleni Kosta, 'Consent in European Data Protection Law' [2013] 3 Nijhoff Studies in European Union Law p.150-151; European Data Protection Board, 'Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1' (*Guidelines*, 4 May 2020) p.21 <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf> accessed 26 May 2021

[163] Ibid.

[164] Eleni Kosta, 'Consent in European Data Protection Law' [2013] 3 Nijhoff Studies in European Union Law p.151

[165] European Data Protection Board, 'Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1' (*Guidelines*, 4 May 2020) p.21 <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf> accessed 26 May 2021

a. Special categories of personal data (sensitive personal data)

By their nature, special categories of personal data are highly sensitive since they are directly related to people's fundamental rights and freedoms.[166] Processing of these data may pose severe risks to data subjects' fundamental rights and freedoms.[167] In principle, processing of *"personal 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 orientation"* is prohibited.[168] It is necessary to note that these categories are interpreted broadly; for example, a data subject's skin color (racial or ethnic origin) and drug or alcohol misuse (health) may also consider sensitive personal data.[169]

Article 9(2) GDPR exhaustively lists the exceptional conditions where processing special categories of personal data are allowed.[170] Apart from obtaining explicit consent from the data subjects,[171] other conditions are related to statutory exceptions that will not be elaborated further since these exceptions are not directly relevant to payment initiation and account information services.[172] For example, users' bank account data are not publicly available data, or the collection of such data does not constitute substantial public interest since it is only about accessing users' bank account data by TPPs.[173]

b. Automated decision-making, including profiling

The mere automated decision-making is being able to take decisions by technological means without any human involvement.[174] As for profiling, it is *"any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular, to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements"*.[175] Data subjects have *"the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her"*.[176] In other words, automated decision-making, including profiling having no meaningful human involvement that leads to legal effects or similar significant effects on data subjects, cannot be implemented by the controllers unless Article 22(2) GDPR exceptions, including explicit consent, exist.

---

[166] Recital 51 GDPR
[167] Recital 51 GDPR
[168] Article 9(1) GDPR; Paul Voigt and Axel von dem Bussche, The EU General Data Protection Regulation (GDPR) A Practical Guide (Springer 2017), p.111-112
[169] Eleni Kosta, 'Consent in European Data Protection Law' [2013] 3 Nijhoff Studies in European Union Law p.236
[170] Article 9(2) GDPR
[171] Article 9(2)(a) GDPR
[172] Tobias Kugler and Daniel Rücker LL.M., New European General Data Protection Regulation A Practitioner's Guide (Bloomsbury Publishing 2018), p.101;
[173] Article 9(2)(e) GDPR; Article 9(2)(g) GDPR; Beuc, 'Beuc's Recommendations to the EDPB on the interplay between the GDPR and PSD2' (*Recommendations*, 11 April 2019) p.5 <https://www.beuc.eu/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf> accessed 26 May 2021
[174] Article 29 Data Protection Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (*Guidelines*, 6 February 2018) p.8 <https://ec.europa.eu/newsroom/article29/items/612053> accessed 26 May 2021
[175] Article 4(1)(4) GDPR
[176] Article 22(1) GDPR

Automated decision-making occurs with or without profiling.[177] Likewise, profiling can also be made with or without automated decision-making.[178] For illustration, imposing standard fines on drivers based on recordings of speed cameras is straightforward automated decision-making without profiling.[179] But, if the imposed fines will be determined based on drivers' past driving habits (e.g., speeding fines, traffic accidents), this will be automated decision-making with profiling.[180] Although credit application evaluations may include profiling, the decision to grant or reject a credit application does not necessitate automated decision-making, a natural person may also analyze the constituted profile and render the final decision.[181] However, in practice, automated decision-making operations use profiling in the majority of cases.[182]

Apart from the EU and national law's authorization on automated decision-making, including profiling, controllers can only implement decisions based solely on automated decision-making, including profiling, having legal effects or similar significant effects on data subjects if it is necessary to perform a contract or the data subject gives their explicit consent.[183] "Legal effects" and "similarly significantly affects" should be interpreted that such processing should have the potential to (i) affect the data subjects' behaviors, choices, and the current circumstances, (ii) affect permanently or for a long time, and (iii) in extreme cases, lead to discrimination or exclusion of the data subjects.[184] For example, receiving a rejection from a bank for a loan request or from a potential employer for a job application, having rejection for immigration status, or any decision that may create difficulty for accessing education and health services will significantly affect the relevant individual.[185] Regarding applying different prices to data subjects based on their "profiles", such price discrimination can only be considered significant if the high price prevents someone from benefiting from certain goods or services.[186]

---

[177] Stefanie Hänold, Profiling and Automated Decision-Making: Legal Implications and Shortcomings. in Corrales and others (eds), Robotics, AI Marcelo Corralesand the Future of Law (Springer 2018), p.125-126; Article 29 Data Protection Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (*Guidelines*, 6 February 2018) p.8 <https://ec.europa.eu/newsroom/article29/items/612053> accessed 26 May 2021

[178] Ibid.

[179] Article 29 Data Protection Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (*Guidelines*, 6 February 2018) p.8 <https://ec.europa.eu/newsroom/article29/items/612053> accessed 26 May 2021

[180] Ibid.

[181] Stefanie Hänold, Profiling and Automated Decision-Making: Legal Implications and Shortcomings. in Corrales and others (eds), Robotics, AI Marcelo Corralesand the Future of Law (Springer 2018), p.126; Article 29 Data Protection Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (*Guidelines*, 6 February 2018) p.8 <https://ec.europa.eu/newsroom/article29/items/612053> accessed 26 May 2021

[182] Stefanie Hänold, Profiling and Automated Decision-Making: Legal Implications and Shortcomings. in Corrales and others (eds), Robotics, AI Marcelo Corralesand the Future of Law (Springer 2018), p.125

[183] Article 22(2) GDPR

[184] Frederike Kaltheuner and Elettra Bietti, 'Data is power: Towards additional guidance on profiling and automated decision-making in the GDPR' [2018] 2(2) Journal of Information Rights, Policy and Practice p.11; Article 29 Data Protection Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (*Guidelines*, 6 February 2018) p.21 <https://ec.europa.eu/newsroom/article29/items/612053> accessed 26 May 2021

[185] Stefanie Hänold, Profiling and Automated Decision-Making: Legal Implications and Shortcomings. in Corrales and others (eds), Robotics, AI Marcelo Corralesand the Future of Law (Springer 2018), p.135; Michael Veale & Lilian Edwards, Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling (computer law & security review 34, April 2018) p. 401

[186] Michael Veale & Lilian Edwards, p. 401

Since the definition of meaningful human involvement is subjective, meaningful human involvement and human oversight necessitate the ability to explain the reasoning behind automated decision-making, including profiling, and determining whether such a decision is non-discriminatory, fair, and accurate.[187] Under such a "right to explanation", TPPs must clearly explain how such complex systems and algorithms take their decisions properly to improve transparency and accountability in automated decision-making, including profiling operations.[188] Considering the vast volume and variety of input and output data and complex algorithmic and machine learning-based processes, it may not be easy to demonstrate meaningful human involvement/intervention in many big data-oriented operations.[189]

Using complex computational algorithms and machine learning technology, highly sensitive information could be inferred from even non-sensitive data.[190] With profiling, users can be identified, analyzed, and classified based on their current and expected traits and preferences.[191] To profile the data subjects, automated personal data processing takes place regarding the data subjects' personal aspects, such as; economic situation, sexual orientation, personal choices, interests, work performance, political opinions, reliability and behavior, health, location, and movements.[192] For example, a profiling model based on Facebook "likes" successfully reached; 88% accuracy on predicting male users' sexual orientation, 95% accuracy on users' ethnic origin, and 82% accuracy on deciding whether a user is Muslim or Christian.[193] Location data obtained from users' publicly accessible data points (e.g., foursquare) could be used to determine such users' average income, political opinions, housing costs, debts, and their demographic group.[194]

The value of a specific individual's consent for a particular personal data processing operation is decreasing.[195] Once a large group of people gives their consent for the specific personal data processing operation, data analysts may create certain profiles based on the data of the data subjects who gave their consent.[196] After a dataset reaches a certain level of data volume and

[187] Frederike Kaltheuner and Elettra Bietti, 'Data is power: Towards additional guidance on profiling and automated decision-making in the GDPR' [2018] 2(2) Journal of Information Rights, Policy and Practice p.13-14; Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' [2017] 7(2) International Data Privacy Law p.78-79

[188] Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' [2017] 7(2) International Data Privacy Law p.77-78

[189] Frederike Kaltheuner and Elettra Bietti, 'Data is power: Towards additional guidance on profiling and automated decision-making in the GDPR' [2018] 2(2) Journal of Information Rights, Policy and Practice p.92

[190] Frederike Kaltheuner and Elettra Bietti, 'Data is power: Towards additional guidance on profiling and automated decision-making in the GDPR' [2018] 2(2) Journal of Information Rights, Policy and Practice, p.3-4

[191] Mark Foulsham, Brian Hitchen and Andrew Denley, GDPR How To Achieve and Maintain Compliance (Routledge 2019) p.105

[192] Frederike Kaltheuner and Elettra Bietti, 'Data is power: Towards additional guidance on profiling and automated decision-making in the GDPR' [2018] 2(2) Journal of Information Rights, Policy and Practice, p.4; Recital 71 GDPR

[193] Michael Kosinski, David Stilwell, Thore Graepel, 'Private traits and attributes are predictable from digital records of human behavior' [2013] 110(15) Proceedings of the National Academy of Sciences of the United States of America p.5803

[194] Frederike Kaltheuner and Elettra Bietti, 'Data is power: Towards additional guidance on profiling and automated decision-making in the GDPR' [2018] 2(2) Journal of Information Rights, Policy and Practice, p.4

[195] Eugenia Politou, Efthimios Alepis and Constantinos Patsakis, 'Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions' [2018] 4(1) Journal of Cybersecurity p.7

[196] Ibid.

variety, based on the available data and created profiles, data analysts can incorporate a data subject who did not give his/her consent for the specific personal data processing operation into a profile based on his/her currently available data and make very accurate inferences.[197] As a result, based on some limited available data, the controllers may infer more and accurate personal data of the data subjects that have never given their consent to the controller due to the very precise profiling techniques.[198] In other words, the profiling itself may create new types of personal data which data subjects have never provided to the controllers.[199] As the data subjects may not be aware of such produced data, they cannot use their privacy and personal data-related rights against controllers.[200] Controllers use such vast volume and variety of data to predict, influence, and manipulate future behaviors and actions of the data subjects as they know their users' needs and preferences.[201]

4. Necessary for the performance of a contract under GDPR

If processing personal data is objectively and genuinely necessary to enter into or do preliminary works to enter into a contractual relationship, such processing will be lawful under Article 6(1)(b) GDPR.[202] This legal base also regulates pre-contractual relationships, collecting the necessary data to establish the contract or fulfill the contractual requirements.[203]

Under this legal base, controllers can only process as little data as possible that is essential and required for their services, considering the rationale of the contract and nature of the relevant service.[204] The controller should demonstrate that the main object of the contract cannot be performed without such data.[205] Useful but not objectively necessary data cannot be processed.[206] If there is an alternative service that necessitates processing fewer personal data, the controller should choose the less intrusive option, as the more intrusive option will not be objectively necessary for the performance of such a contract.[207] For example, when an online retailer company agrees with its user to provide a product and send it to its address, it needs the user's address for delivery. However, if a user chooses delivery of such product to a store (as a pick-up point) in its neighborhood, the user's address should not be processed as such data is not strictly necessary for the performance of such a contract. Only the address of such store is

---

[197] Ibid.
[198] Ibid.
[199] Stefanie Hänold, Profiling and Automated Decision-Making: Legal Implications and Shortcomings. in Corrales and others (eds), Robotics, AI Marcelo Corralesand the Future of Law (Springer 2018), p.131-132
[200] Ibid.
[201] Ibid.
[202] Article 6 (1)(b) GDPR; Recital 44 GDPR
[203] European Union Agency for Fundamental Rights and Council Of Europe, 'Handbook on European data protection law' (Handbook, April 2018) p.151 <https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition> accessed 26 May 2021; IT Governance Privacy Team, EU General Data Protection Regulation (GDPR) An Implementation and Compliance Guide (4th edn, IT Governance Publishing 2020) p.133
[204] IT Governance Privacy Team, EU General Data Protection Regulation (GDPR) An Implementation and Compliance Guide (4th edn, IT Governance Publishing 2020), p.133;
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 Version 2.0' (*Guidelines*, 8 October 2019) p.9 <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf> accessed 26 May 2021 (EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR)
[205] EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR, p.8
[206] Article 6(1)(b) GDPR; EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR p.7
[207] EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR p.7

required.[208] If the controller provides different services, such evaluation should be made for each service separately.[209] For example, a clothing company may provide both tailor-made clothing and sale of fabrics services. In the case of fabrics sale, the clothing company should only process the necessary personal data for the contract of sale and invoice. However, in the case of tailor-made suit order, in addition to the necessary personal data to be used for the contract of sale and the issuance of an invoice, the body size figures of the data subject should be processed by the clothing company to provide their services. If a data controller wants to process more data than necessary for the performance of a contract, exceeding data can only be processed if the controller relies on another suitable legal basis (i.e., consent) under Article 6(1) GDPR.[210] However, necessary for the performance of a contract cannot be a legal base while processing special categories of personal data under Article 9(2) GDPR.[211]

5. Conclusion

In the first part of the chapter, the definition, conditions, and withdrawal of consent were explained. How controllers can distinguish consent requests from other texts and create the technological infrastructure was elaborated. Then, empowering effects and weak sides of consent have been discussed, particularly in the online environment.

The second part elaborated on explicit consent and its difference with (ordinary) consent Following, other two situations that necessitate explicit consent have been explained briefly, namely, processing sensitive personal data and taking decisions solely based on automated decision-making, including profiling, having legal effects, or similar significant effects on the data subjects. In general, explicit consent increases the controller's duty to inform data subjects and ensure that the data subjects are fully aware of the consent they give.

In the last part, the legal base necessary for the performance of a contract was discussed, and conditions and essential aspects were highlighted. As we will discuss in Chapter 4, this legal base will have a vital role in data processing activities under PSD2.

[208] EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR p.10-11
[209] EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR p.10
[210] EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR p.6
[211] European Data Protection Board, 'Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1' (*Guidelines*, 4 May 2020) p.21 <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf> accessed 26 May 2021

4. CHAPTER 4 – Consent, Explicit Consent, and Data Processing under PSD2

1. Introduction

Chapter 3 explained three legal grounds for data processing that could be used in online payment transactions under GDPR. Chapter 4 will explain consent and explicit consent terms under PSD2 and analyze how TPPs and banks comply with both legislative instruments and overcome their GDPR and PSD2 compliance problems.

We will first explain the meaning of consent and explicit consent under PSD2. Then, we will focus on the relationship between consent and explicit consent under GDPR and analyze how to interpret explicit consent under PSD2 coherently with the legal ground necessary for the performance of a contract.[212] considering the relevant PSD2 provisions. The second part will discuss what personal data could be shared with TPPs according to PSD2 and GDPR. Then, we will focus on TPPs' further personal data processing operations, in addition to the initial processing purpose. Following, we will deal with conditions that necessitate obtaining explicit consent under GDPR, sensitive personal data processing, and automated decision-making, including profiling practices of TPPs. We will elaborate on some options and alternatives for banks and TPPs concerning GDPR and PSD2 compliance in the last part. Since Chapter 3 and Chapter 4 focus on users' own personal data that will be directly collected from them, the silent party data processing operations will be analyzed in Chapter 5. Considering the silent parties are not directly a party to the contractual relationship between TPPs and users and their data will be processed by TPPs in online payment transactions, Chapter 5 will analyze their exceptional situation under PSD2 in detail.

Under Article 33(2) PSD2, it is stated that AISPs are not bound with Article 94 PSD2 (Chapter IV). But, Article 67 PSD2 explains AISPs' obligation to obtain their users' explicit consent before providing their account information services.[213] However, even though it is accepted that Article 94 PSD2 will not be applied to AISPs, especially Article 94(2) PSD2, *"Payment service providers shall only access, process and retain personal data necessary for the provision of their payment services, with the explicit consent of the payment service user"*, AISPs (and also PISPs and banks) still have to comply with all data processing principles listed under GDPR.[214] PISPs, AISPs, and banks are also obliged to fully implement data protection by design and data protection by default and recent data protection-oriented technology to comply with data protection requirements under GDPR.[215] Thus, regardless of whether AISPs are bound with Article 94 PSD2 or excluded by PSD2 irrespective of the reason, AISPs are bound with GDPR, which is more detailed and strictly regulated than Article 94 PSD2.[216] In other words, even if there would be no data protection provision under PSD2, TPPs and banks would still had to access, process, and retain the personal data necessary for the provision of their payment services under GDPR principles and rules. Moreover, there is no meaningful explanation for and benefit to be gained when AISPs are exempted from Article 94 PSD2.[217] To clarify this

[212] Article 6(1)(b) GDPR
[213] Article 67 PSD2
[214] Article 5 GDPR
[215] European Data Protection Board, 'Letter regarding the PSD2 directive' (Letter, 5 July 2018) p.5 <https://edpb.europa.eu/sites/edpb/files/files/news/psd2_letter_en.pdf> accessed 26 May 2021 (EDPB, Letter PSD2); Recital 89 PSD2
[216] Article 2(1) GDPR; Article 3 GDPR
[217] Article 33(2) PSD2; Beuc, 'Beuc's Recommendations to the EDPB on the interplay between the GDPR and PSD2' (*Recommendations*, 11 April 2019) p.7 <https://www.beuc.eu/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf> accessed 26 May 2021

issue, EDPB itself accepted that obtaining explicit consent is necessary for AISPs to provide their account information services under PSD2, *"Pursuant to Article 33 (2) of the PSD2, this requirement of the explicit consent of the payment service user does not apply to AISPs. However, Article 67 (2)(a) of the PSD2 still provides for explicit consent for AISPs for the provision of the service"*.[218] Thus, similar to EDPB's and the Guidelines' approach, it is accepted that explicit consent is directly about providing a contractual service rather than processing users' personal data. Therefore, it is more suitable for TPPs to use the "necessary for the performance of a contract" legal base under GDPR for the data processing operations.

2. Consent under PSD2

Under PSD2, similar to GDPR, both terms of consent and explicit consent are used. Even though there is no "consent" definition in PSD2, consent is used 25 times in both recitals and articles. Under PSD1, without any reference to explicit consent, consent was used for direct debiting and execution of payment transactions.[219] Similarly, under PSD2, consent is used for; execution of a payment transaction, blocking funds of the payer's bank account, operation of PISPs' and AISPs' services, payment service for direct debiting, and blocking the funds.[220] Therefore, consent under PSD2 is not a data protection term; instead, it is, in most cases, an "authorization" for concerning online payment transactions within the scope of PSD2.[221] Without giving such authorization, users' online payment transactions cannot be carried out under Article 64(1) PSD2, *"Member States shall ensure that a payment transaction is considered to be authorized only if the payer has given consent to execute the payment transaction"*.[222]

As another indicator of the difference between "consent" in GDPR and PSD2, PSD2 grants contractual liberty to users and TPPs to determine the procedure for giving the consent, *"the procedure for giving consent shall be agreed between the payer and the relevant payment service provider(s)"*.[223] If both TPPs and users previously agree on it, users may authorize their payment transactions (by consent) even after the transaction.[224] In GDPR, it is clear that consent should be obtained before the processing operation.[225] Furthermore, GDPR regulates the definition, conditions, and consent obtaining procedure in detail, and the parties cannot change

---

[218] EDPB, PSD2 Guidelines, p.13-14

[219] Article 4(1)(28) PSD1; Article 42(1)(2)(c) PSD1; Article 53(1)(d) PSD1; Article 54 PSD1; Article 55(1) PSD1; Article 62(3) PSD1; Article 66(2) PSD1;
Beuc, 'Beuc's Recommendations to the EDPB on the interplay between the GDPR and PSD2' (*Recommendations*, 11 April 2019) p.3 <https://www.beuc.eu/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf> accessed 26 May 2021

[220] Recital 75 PSD2; Recital 76 PSD2; Recital 93 PSD2; Article 4(1)(23) PSD2; Article 52(2)(c) PSD2; Article 63(1)(d) PSD2; Article 64 PSD2; Article 65(1)(c) PSD2; Article 68(1) PSD2; Article 75(1) PSD2; Article 76(3)(a) PSD2; Article 80(2) PSD2

[221] Recital 75 PSD2; Recital 76 PSD2; Article 4(1)(23) PSD2; Article 52(2)(c) PSD2; Article 75(1) PSD2; Article 76(3) PSD2; Article 80(2) PSD2; Beuc, 'Beuc's Recommendations to the EDPB on the interplay between the GDPR and PSD2' (*Recommendations*, 11 April 2019) p.3 <https://www.beuc.eu/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf> accessed 26 May 2021

[222] Article 64(1) PSD2; Beuc, 'Consumer-friendly Open Banking Access to Consumers' Financial Data by Third Parties' (*Publications*, 20 September 2018) p.8 <https://www.beuc.eu/publications/beuc-x-2018-082_consumer-friendly_open_banking.pdf> accessed 26 May 2021

[223] Article 64(4) PSD2

[224] Article 64(1) PSD2

[225] Article 6(1)(a) GDPR; Bart Van der Sloot, The General Data Protection Regulation in Plain Language (Amsterdam University Press 2020) p.68

or undermine the consent conditions under GDPR by a mutual agreement.[226] Similarly, since obtaining consent is a prerequisite for providing a certain online payment service (e.g., authorization for a certain payment) and a security measure in online payment transactions, *"In the absence of consent, a payment transaction shall be considered to be unauthorized"*, such consent cannot be regarded as a data protection term under GDPR as it is not freely given and separate from the contractual approval on authorizing a payment transaction.[227]

Since the meaning of consent under PSD2 is different from GDPR, using the same term in PSD2 created unnecessary confusion. Therefore, although consent is used for consistency of the terms of PSD1 and PSD2, it would have been better to include the definitions of consent and explicit consent into PSD2 in the first place to prevent any confusion.

3. Explicit Consent under PSD2

a. Analysis based on PSD2 Articles

Under PSD2, there are three situations mentioned under three different PSD2 articles (Articles 65, 66, and 67 PSD2), where explicit consent is required. Under these three articles, explicit consent is mentioned five times; two times in Article 65 PSD2 (concerning ASPSPs'/banks' services), two times in Article 66 PSD2 (concerning PISPs' services), and one time in Article 67 PSD2 (concerning AISPs' services). In addition, explicit consent is also mentioned under Article 94 PSD2, an article with a *"Data Protection"* title. Each explicit consent usage is analyzed below:

1. *"the payer has given **explicit consent** to the account servicing payment service provider to respond to requests from a specific payment service provider to confirm that the amount corresponding to a certain card-based payment transaction is available on the payer's payment account"* (Article 65(1)(b) PSD2)

2. *"the payer has given **explicit consent** to the payment service provider to request the confirmation referred to in paragraph 1"* (Article 65(2)(a) PSD2)

The function of explicit consent above is an authorization to confirm the availability of a certain card-based payment transaction amount in users' payment account, not processing the personal data of users. Even the title of Article 65, *"Confirmation on the availability of funds"*, clearly shows that this provision is not related to personal data processing operations but is purely related to contractual approval. Users' bank will respond to this confirmation request as "Yes" or "No".

3. *"When the payer gives its **explicit consent** for a payment to be executed under Article 64, the account servicing payment service provider shall perform the actions specified in paragraph 4 of this Article to ensure the payer's right to use the payment initiation service."* (Article 66(2) PSD2)

The provision above is also related to a payment that can only be executed by users' explicit consent. Article 66(2) PSD2's reference to Article 64 PSD2 (entitled as *"Consent and withdrawal of consent"*) is also about the authorization for execution of payment transactions,

[226] Article 4(1)(11) GDPR; Article 7(1)(11) GDPR
[227] Article 64(2) PSD2; Bundeskartellamt, 6th Decision Division, B6-22/16 p.184-186

not processing of personal data.[228] As a payment transaction cannot be executed without users' explicit consent, explicit consent under PSD2 cannot be the same with explicit consent under GDPR, as explicit consent under GDPR should be freely and separately given from the contractual approval.[229] In other words, approval of a contract and giving explicit consent under GDPR should be two separate processes.

4. *"[PISP] shall ensure 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****."* (Article 66(3)(c) PSD2)

This provision stipulates that users' any other information (including both ordinary data and personal data under GDPR) that PISPs access to provide their payment initiation services to users can only be shared with payees if users give their explicit consent. Indeed, this provision is not clear whether this provision is related to personal data processing operation (sharing users' some personal data with payees) only or approval of a payment initiation transaction and data processing operation. However, as the provision of service necessitates obtaining users' explicit consent, such explicit consent will not be freely given and separate from the contractual approval. As the "user" definition under PSD2 also covers legal entities, explicit consent cannot be accepted as equivalent to the data protection term.

5. *"[AISP] shall provide services only where based on the payment service user's* ***explicit consent****."* (Article 67(2)(a) PSD2)

The provision is formulated as explicit consent should be obtained for providing account information services, rather than processing personal data of the data subjects.[230] As the formulation of these provisions necessitates explicit consent as a prerequisite for providing services, such "explicit consent" would be invalid under GDPR as it is not given freely and separate from the contractual approval.[231]

6. *"[payment service provider shall] only access, process and retain personal data necessary for the provision of their payment services, with the* ***explicit consent*** *of the payment service user."* (Article 94(2) PSD2)

Under this provision, explicit consent is a prerequisite to process the necessary for the performance of a contract data. Since the relevant payment service cannot be provided without such data, eventually, explicit consent is a prerequisite to provide payment services. From the data protection perspective, such "explicit consent" should be invalid as it is not given freely

[228] Article 66(2) PSD2; Article 64 PSD2; Beuc, 'Consumer-friendly Open Banking Access to Consumers' Financial Data by Third Parties' (*Publications*, 20 September 2018) p.8 <https://www.beuc.eu/publications/beuc-x-2018-082_consumer-friendly_open_banking.pdf> accessed 26 May 2021

[229] Bundeskartellamt, 6th Decision Division, B6-22/16 p.184-186

[230] Beuc, 'Consumer-friendly Open Banking Access to Consumers' Financial Data by Third Parties' (*Publications*, 20 September 2018) p.8 <https://www.beuc.eu/publications/beuc-x-2018-082_consumer-friendly_open_banking.pdf> accessed 26 May 2021; Alja Poklar, 'Does the Same Word Mean the Same Thing? An Exploration of the Notion of Consent in PSD2 and GDPR' (*Tilburg University*, 2019) p.19 <https://arno.uvt.nl/show.cgi?fid=148995> accessed 26 May 2021

[231] Information Commissioner's Office, 'What are the conditions for processing?' (*Information Commissioner's Office*) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-conditions-for-processing/#conditions1> accessed 26 May 2021

and obtained separately.[232] Therefore, explicit consent under PSD2 should be accepted as an ordinary contractual approval.

b. The legal ground for personal data processing to be used in case of services requiring explicit consent under PSD2

Since online payment transactions occur between users and TPPs based on their contractual relations, users' and TPPs' rights and obligations are regulated by the agreement between them and relevant legislation.[233] Furthermore, Recital 87 PSD2, *"This Directive should concern only **contractual** obligations and responsibilities between the payment service user and the payment service provider"*, also confirms that PSD2 is related to regulating contractual relations between users and TPPs only.[234] EDPB also clarified that explicit consent is *"an additional requirement of a contractual nature"*.[235] According to EDPB, explicit consent under PSD2 should be interpreted as a contractual approval and transparency requirement, not an additional *sui generis* legal base for personal data processing.[236] Therefore, the legal base for processing personal data under GDPR and PSD2 should be "necessary for the performance of a contract".[237] When applying this legal base, the processed personal data should be objectively necessary for the performance of a contract; otherwise, the objective service in the agreement should not be provided by the TPPs and also banks that provide account information and payment initiation services.[238] Determining the necessity for the performance of a contract should be made by considering the service's nature, users' and TPPs' mutual perspectives and expectations, and rationale and essential elements of the contract.[239]

Obtaining explicit consent under PSD2 rules and principles impose a transparency requirement on TPPs to inform data subjects explicitly (e.g., on what data and why and how such data will be processed) while obtaining their explicit approval, regardless of the legal base that is used (e.g., necessary for the performance of a contract, legitimate interest) for the personal data processing operation in online payment transactions.[240] Explicit consent under PSD2 increases transparency and data subjects' control over their data.[241] Although PSD2 does not list any definition and conditions for consent and explicit consent, these terms should be interpreted and applied in coherence with GDPR to prevent any contradiction and protect its useful effect.[242]

---

[232] Information Commissioner's Office, 'What are the conditions for processing?' (*Information Commissioner's Office*) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-conditions-for-processing/#conditions1> accessed 26 May 2021

[233] EDPB, PSD2 Guidelines, p. 9

[234] Recital 87 PSD2

[235] EDPB, PSD2 Guidelines, p. 9

[236] EDPB, PSD2 Guidelines, p.14; EDPB, Letter PSD2 p.4; Article 6(1)(b) GDPR; Bird & Bird, 'EU: The interplay of PSD2 and GDPR - some select issues' (*DataGuidance*, February 2019) p.3 <https://www.twobirds.com/~/media/pdfs/eu-the-interplay-of-psd2-and-gdpr--some-select-issues.pdf> accessed 26 May 2021

[237] Article 6(1)(b); Dilja Helgadottir, 'The Interaction between Directive 2015/2366 (EU) on Payment Services and Regulation (EU) 2016/679 on General Data Protection concerning Third Party Players' (2020) 23 Trinity CL Rev p.218; Recital 44 GDPR; EDPB, PSD2 Guidelines, p.14

[238] European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR p.4

[239] EDPB, PSD2 Guidelines, p. 9 and 10; European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR p.10

[240] Niels Vandezande, 'Reconciling Consent in PSD2 and GDPR' (*The Paypers*, 22 March 2019) <https://thepaypers.com/expert-opinion/reconciling-consent-in-psd2-and-gdpr--777976> accessed 26 May 2021

[241] EDPB, PSD2 Guidelines, p.14-15

[242] EDPB, PSD2 Guidelines, p.15; EDPB, Letter PSD2 p.4

Therefore, as explicit consent is not a *sui generis* legal ground for personal data processing, explicit consent under PSD2 compels TPPs to fully inform users concerning the specific personal data categories that will be processed and specific online payment service purposes.[243] In other words, even if TPPs apply, for example, necessary for the performance of a contract legal ground under GDPR when providing their services, explicit consent under PSD2 creates a higher-level duty for TPPs while informing their users. However, EDPB did not explain how such transparency requirement is different from the currently applied lawfulness, fairness and transparency principle under Article 5(1)(1) PSD2.[244] EDPB only referred to Article 29 Working Party Guidelines on Transparency for the transparency explanation.[245] If there is no difference between the transparency requirement under PSD2 and the transparency principle under GDPR, it is unclear what PSD2's transparency requirement brings to the data protection regime of GDPR.

Since the legal base for data processing in PSD2 is "necessary for the performance of a contract",[246] data subjects do not have a right to withdraw their "explicit consent" under PSD2, as the consent they gave to TPPs is not the same consent under GDPR.[247] Therefore, the right to withdraw their consent within the meaning of Article 7(3) GDPR cannot be used by users if TPPs process objectively necessary data to be used for their online payment services as the legal base is not consent under GDPR.[248]

c. Usage of Consent and Explicit Consent Terms under PSD2

Under PSD2, there are provisions where the terms of consent and explicit consent are used interchangeably:

i. Although Article 64 PSD2 regulates consent and withdrawal of consent under PSD2, the clause of *"When the payer gives its **explicit consent** for a payment to be executed under Article 64"* (Article 66(2) PSD2) refers to Article 64 for giving and withdrawal of consent procedures.[249] Given that there is no reference to explicit consent, but only consent, in Article 64 PSD2, this implies that PSD2 does not make a significant difference between these two terms.

ii. Article 65(1)(c) PSD2, *"the **consent** referred to in point (b) has been given before the first request for confirmation is made"*, also refers to Article 65(1)(b) PSD2 where the term of explicit consent is used, not consent.

iii. The first sentence of Recital 93 PSD2, *"It is necessary to set up a clear legal framework which sets out the conditions under which payment initiation service providers and account information service providers can provide their services with the consent of the account holder without being required by the account servicing payment service*

[243] EDPB, PSD2 Guidelines, p.14
[244] Article 5(1)(1) PSD2; EDPB, PSD2 Guidelines, p.14-15
[245] EDPB, PSD2 Guidelines, p.15
[246] Article 6(1)(b) GDPR
[247] Article 7(3) GDPR
[248] Dilja Helgadottir, 'The Interaction between Directive 2015/2366 (EU) on Payment Services and Regulation (EU) 2016/679 on General Data Protection concerning Third Party Players' (2020) 23 Trinity CL Rev p.218-219
[249] Article 66(2) PSD2

provider…", shows that PSD2 prefers to use "consent" in place of "explicit consent", either intentionally or mistakenly.[250]

Considering the name of Chapter 2, *"Authorisation of payment transactions"*, where five out of six explicit consent references are made, and the usages in PSD provisions,[251] consent and explicit consent have almost the same meaning under some PSD2 provisions, which is the authorization for payment transactions in general. Therefore, PSD2, either intentionally or unintentionally, uses consent and explicit consent interchangeably, except the usage of explicit consent under Article 94 PSD2.

4. The Personal Data that could be Shared with TPPs

PSD2 does not make any difference in the types of data that will be shared with TPPs.[252] As some data types are more privacy-sensitive compared to others and may cause more risks for data subjects, data subjects should have the option to choose the detail of the shared data while giving their explicit consent under PSD2.[253] The following information could be obtained via bank account access: *"names, addresses, social security numbers, credit card numbers, license plate numbers, income/wage, spending categories (preferences and dedicated worth), medical, religious, location, behavioral (events) and social (contacts)"*.[254]

TPPs are only allowed to access personal data for the specific purpose(s) explicitly requested by users.[255]. In other words, there is no need for TPPs to access the bank's users' full bank account data.[256] As each payment institution should have access to different types and volumes of data, depending on the services they provide, they should strictly comply with all GDPR principles and rules, including data minimization and purpose limitation principles while providing their services.[257] If TPPs can reach all the bank account data, without any limitation, this practice will circumvent GDPR's principles and rules, in particular, sensitive personal data processing and obtaining explicit consent in case of automated decision-making, including profiling, that may produce legal effects on users and significantly affect them.[258] Furthermore, no provision under PSD2 provides legal ground or exceptions to banks and TPPs for sensitive personal data sharing and automated decision-making, including profiling.[259] Thus, banks

---

[250] Recital 93 PSD2

[251] Article 66(2) PSD2; Article 65(1)(c) PSD; Recital 93 PSD2; Article 80(2) PSD2

[252] Jaimy van der Heijden, 'Privacy in Financial Innovation: a Value Sensitive Design for PSD2' (*TUDelft*, 2017) p.37 <https://repository.tudelft.nl/islandora/object/uuid%3Ac558efd2-692e-4b2e-9933-4cc248ccd4b1> accessed 26 May 2021

[253] Ibid.

[254] Ibid.

[255] Simonetta Vezzoso, Fintech, Access to Data, and the Role of Competition Policy. in V. Bagnoli (ed), Competition and Innovation (São Paulo: Scortecci 2018) p.32

[256] Ibid.

[257] Ducuing Charlotte, Dutkiewicz Lidia and Miadzvetskaya Yuliya, 'D62 Legal and Ethical Requirements' (*Trusts Trusted Secure Data Sharing Space*, August 2020) p.123 <https://www.trusts-data.eu/wp-content/uploads/2020/10/D6.2-Legal-and-Ethical-Requirements.pdf> accessed 26 May 2021

[258] Article 9 GDPR; Article 22 GDPR; Beuc, 'Beuc's Recommendations to the EDPB on the interplay between the GDPR and PSD2' (*Recommendations*, 11 April 2019) p.3-4 <https://www.beuc.eu/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf> accessed 26 May 2021

[259] Beuc, 'Beuc's Recommendations to the EDPB on the interplay between the GDPR and PSD2' (*Recommendations*, 11 April 2019) p.3-4 <https://www.beuc.eu/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf> accessed 26 May 2021

should take technical measures to separate the accounts that may include sensitive personal data or the data used to create more accurate profiles of users from ordinary accounts.[260]

Banks and TPPs should also take necessary steps to prevent any access that may reveal users' sensitive personal data, which is not necessary for the performance of the contract.[261] Thus, technical measures that may help separate the data necessary for the performance of a contract and the unnecessary and sensitive personal data should be put in place.[262] Currently, TPPs may access either all or no bank accounts of users.[263] Thus, banks should also take necessary technical measures and provide interfaces for their users to give them an option to choose the level of data and detail they want to be shared with TPPs.[264]

Currently, users cannot limit the level of data they want to be shared with TPPs. Even if a user wants to grant access to only a limited data of himself/herself, TPPs do not have any legal obligation to share such user's request with the bank. Thus, banks should limit the personal data shared with TPPs based on users' requests.[265] Therefore, users should be able to instruct their banks not to share certain types of data or to limit (with filtering out certain data, in particular, sensitive personal data) the data that will be shared with TPPs.[266] No provision forbids such instruction under PSD2.[267] EDPB also recommends using "digital filters" to support AISPs while collecting the strictly necessary personal data concerning the specific processing purpose and not to collect unnecessary personal data, since AISPs access more personal data (e.g., transaction histories of the bank accounts) than PISPs.[268] However, although filtering out users' data is technologically feasible, users should have the option and control to choose the level of data they would like to share with TPPs and the level of abstraction regarding the data they share.[269] For example, since AISPs do not need to know a supermarket's name (e.g., Albert

---

[260] Ibid.

[261] Beuc, 'Beuc's Recommendations to the EDPB on the interplay between the GDPR and PSD2' (*Recommendations*, 11 April 2019) p.6-7 <https://www.beuc.eu/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf> accessed 26 May 2021

[262] Ibid.

[263] Ibid.

[264] Jaimy van der Heijden, 'Privacy in Financial Innovation: a Value Sensitive Design for PSD2' (*TUDelft*, 2017) p.37 <https://repository.tudelft.nl/islandora/object/uuid%3Ac558efd2-692e-4b2e-9933-4cc248ccd4b1> accessed 26 May 2021; Beuc, 'Beuc's Recommendations to the EDPB on the interplay between the GDPR and PSD2' (*Recommendations*, 11 April 2019) p.6 <https://www.beuc.eu/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf> accessed 26 May 2021

[265] Beuc, 'Beuc's Recommendations to the EDPB on the interplay between the GDPR and PSD2' (*Recommendations*, 11 April 2019) p.6-7 <https://www.beuc.eu/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf> accessed 26 May 2021

[266] Beuc, 'Beuc's Recommendations to the EDPB on the interplay between the GDPR and PSD2' (*Recommendations*, 11 April 2019) p.6 <https://www.beuc.eu/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf> accessed 26 May 2021

[267] Beuc, 'Consumer-friendly Open Banking Access to Consumers' Financial Data by Third Parties' (*Publications*, 20 September 2018) p.7 <https://www.beuc.eu/publications/beuc-x-2018-082_consumer-friendly_open_banking.pdf> accessed 26 May 2021

[268] Ducuing Charlotte, Dutkiewicz Lidia and Miadzvetskaya Yuliya, 'D62 Legal and Ethical Requirements' (*Trusts Trusted Secure Data Sharing Space*, August 2020) p.123 <https://www.trusts-data.eu/wp-content/uploads/2020/10/D6.2-Legal-and-Ethical-Requirements.pdf> accessed 26 May 2021; Beuc, 'Beuc's Recommendations to the EDPB on the interplay between the GDPR and PSD2' (*Recommendations*, 11 April 2019) p.2-4 <https://www.beuc.eu/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf> accessed 26 May 2021

[269] Jaimy van der Heijden, 'Privacy in Financial Innovation: a Value Sensitive Design for PSD2' (*TUDelft*, 2017) p.37 <https://repository.tudelft.nl/islandora/object/uuid%3Ac558efd2-692e-4b2e-9933-4cc248ccd4b1> accessed 26 May 2021

Heijn), users should be able to choose to leave this just as "supermarket", rather than the exact name of the supermarket.[270] Furthermore, users may have an option to choose variables of data to share and different abstraction levels (e.g., all or non-sensitive data) before they give their explicit consent under PSD2.[271] For instance, in case of cash withdrawal from an ATM, without providing the ATM location and the amount of money, users should have an option to provide only information of "withdrawal of an undefined amount of money in an ATM within a certain timeslot" to TPPs.[272] The data subjects should receive payment initiation and account information services without giving up their right to privacy and protection of personal data protected under Article 8 Charter.[273]

5. Further Processing of Personal Data

Controllers can only process personal data obtained for a specific, explicit, and legitimate data processing purpose.[274] Any further processing not compatible with the initial processing purpose will be unlawful.[275] If TPPs want to process the personal data obtained due to the legal base necessary for the performance of a contract for additional purposes that are not compatible with the initial purposes, then the controllers have to rely on another legal ground (e.g., consent) under Article 6(1) GDPR for such further processing.[276] Under PSD2, there is no explanation regarding which further data processing purposes will be in line with the initial data processing purpose(s) and which processing purposes will not.[277] Concerning such further data processing, GDPR principles and rules will be fully applicable.[278]

As stated under Article 66(3)(g) PSD2, PISPs cannot *"use, access or store any data for purposes other than for the provision of the payment initiation service as explicitly requested by the payer"*.[279] Likewise, under Article 67(2)(f) PSD2, AISPs should *"not use, access or store any data for purposes other than for performing the account information service explicitly requested by the payment service user, in accordance with data protection rules"*.[280] Thus, TPPs cannot process data subjects' personal data which are obtained for the performance of the payment initiation or account information services for additional/different processing purpose, unless data subjects give their consent under GDPR or the processing is mandatory according to the EU or member state law that TPPs are subject to (e.g., prevention of money laundering).[281] While obtaining consent for such further data processing, since such further

---

[270] Ibid.

[271] Ibid.; Beuc, 'Beuc's Recommendations to the EDPB on the interplay between the GDPR and PSD2' (*Recommendations*, 11 April 2019) p.6 <https://www.beuc.eu/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf> accessed 26 May 2021

[272] Article 5(1)(b) GDPR; Jaimy van der Heijden, 'Privacy in Financial Innovation: a Value Sensitive Design for PSD2' (*TUDelft*, 2017) p.37 <https://repository.tudelft.nl/islandora/object/uuid%3Ac558efd2-692e-4b2e-9933-4cc248ccd4b1> accessed 26 May 2021

[273] Eleni Kosta, 'Consent in European Data Protection Law' [2013] 3 Nijhoff Studies in European Union Law p.140-141

[274] Article 5(1)(b) GDPR

[275] Article 5(1)(b) GDPR

[276] Article 6(1) GDPR; EDPB, Letter PSD2 p.4

[277] Beuc, 'Beuc's Recommendations to the EDPB on the interplay between the GDPR and PSD2' (*Recommendations*, 11 April 2019) p.2 <https://www.beuc.eu/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf> accessed 26 May 2021

[278] EDPB, Letter PSD2 p.2

[279] Article 66(3)(g) PSD2

[280] Article 67(2)(f) PSD2

[281] Article 6(4) GDPR; Article 6(1)(a) GDPR; Dilja Helgadottir, 'The Interaction between Directive 2015/2366 (EU) on Payment Services and Regulation (EU) 2016/679 on General Data Protection concerning Third Party

processing operation falls outside of PSD2, consent conditions under GDPR should be fulfilled.[282]

To illustrate further processing, if TPPs would like to use targeted advertising to promote their businesses by using the personal data obtained in online payment services, such processing will be unlawful since the initial purpose to process the data subjects' data, i.e., execution of a payment, is not in line with the latter advertisement purpose.[283] Also, using such data will be beyond the data subjects' reasonable expectations, as they gave their explicit consent under PSD2 to benefit from online payment services.[284] Thus, if the controller would like to process personal data for the targeted advertisement, in addition to the initial purpose of providing an online payment service, the controllers should ask for the data subjects' consent under GDPR as Article 66(3)(g) PSD2 and Article 67(2)(f) PSD2 explicitly prevent such further processing.[285] As another example, only by obtaining the valid consent of the data subjects under GDPR, PISPs and AISPs may share their users' data with price comparison websites for their users to receive additional offers and benefits for them.[286]

Concerning the further processed personal data only, the data subjects may always withdraw their consent under GDPR easily and without facing any detriment.[287] While the data subjects do not have a right to withdraw their "explicit consent" under PSD2 for the personal data that is processed for the performance of a contract, as for the further (and therefore, additional) processing operations, the data subjects have the right to withdraw their consent concerning the further data processing activity only.[288]

It is also claimed that PISPs should not process personal data for any additional processing purposes other than the original payment initiation purpose under Article 66(3)(g) PSD2, *"[PISP] shall: … not use, access or store any data for purposes other than for the provision of the payment initiation service as explicitly requested by the payer"*, even if a user gives his/her consent for further processing.[289] PSD2 also has a similar provision for AISP, Article 67(2)(f) PSD2, *"[AISP] shall … not use, access or store any data for purposes other than for performing the account information service explicitly requested by the payment service user, in accordance with data protection rules"*. Compared to the article on PISP, this includes an additional condition, *"in accordance with data protection rules"*.[290] During the PSD2 transposition into the national law, although some states (e.g., Germany, Sweden) did not include the condition

---

Players' (2020) 23 Trinity CL Rev p.220; EDPB, PSD2 Guidelines, p.10; Latham & Watkins, 'Privacy and Payments: New Draft EU Advice for Financial Institutions' (*JDSupra*, 4 November 2020) <https://www.jdsupra.com/legalnews/privacy-and-payments-new-draft-eu-89021/> accessed 26 May 2021; EDPB, PSD2 Guidelines, p.12; Article 6(1)(a) GDPR

[282] EDPB, Letter PSD2 p.4; Article 7 GDPR; Article 4(11) GDPR

[283] Johan Peeters, 'Data protection in mobile wallets' (*KU Leuven*, 2019) p.34 <https://www.scriptiebank.be/sites/default/files/thesis/2019-10/PEETERS_s0107530_thesis.pdf> accessed 26 May 2021

[284] Ibid.

[285] Ibid.; Article 6(1)(a) GDPR; Article 66(3)(g) PSD2; Article 67(2)(f) PSD2

[286] Simonetta Vezzoso, Fintech, Access to Data, and the Role of Competition Policy. in V. Bagnoli (ed), Competition and Innovation (São Paulo: Scortecci 2018) p.32

[287] EDPB, PSD2 Guidelines, p.12; Article 7(3) GDPR

[288] EDPB, PSD2 Guidelines, p.12; Article 7(3) GDPR

[289] Dilja Helgadottir, 'The Interaction between Directive 2015/2366 (EU) on Payment Services and Regulation (EU) 2016/679 on General Data Protection concerning Third Party Players' (2020) 23 Trinity CL Rev p.221; Article 6(1)(a) GDPR

[290] Article 67(2)(f) PSD2

of *"in accordance with data protection rules"*, some states (e.g., Romania, Hungary) kept the condition as it is.[291] Some claim that although PISPs cannot re-use such data for further processing, as for the countries that adopted PSD2 without deleting *"in accordance with data protection rules"*, AISPs may re-use such data for further processing if they obtain users' consent.[292] However, this interpretation is also not certain since Hungarian Central Bank declared that further processing is not allowed for AISPs even if they obtain users' consent, although Hungary kept the condition as it is.[293] On the contrary to these interpretations, EDPB stated in the Guidelines that further processing is allowed for both PISPs and AISPs as long as they have appropriate legal grounds (e.g., consent) under GDPR.[294] In line with the Guidelines, PSD2 is an EU directive regulating online payment services only, not regulating the data protection regime in the EU.[295] Therefore, based on the analysis in this chapter, I do not consider that Articles 66(3)(g) and 67(2)(f) PSD2 can prohibit further processing of personal data even if PISPs and AISPs obtain users' consent under GDPR.[296] However, further personal data processing conditions are difficult to fulfill in the online payment service market under PSD2.

6. Sensitive Personal Data Processing and Automated Decision-Making, including Profiling

As explained in Chapter 3, processing sensitive personal data is prohibited unless the controller proves that at least one of the derogations under Article 9(2)(a - j) is met.[297] However, apart from giving explicit consent under Article 9(2)(a) GDPR, the only other option that could be used in online payment transactions within the scope of PSD2 is Article 9(2)(g) GDPR, where *"processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law …"*.[298] The other derogations,[299] due to their own nature, may not be applicable in online payment transactions within the scope of PSD2.[300] Under Article 9(2) GDPR, sensitive personal data cannot be processed based on the necessity for the performance of a contract legal ground.[301]

---

[291] Dilja Helgadottir, 'The Interaction between Directive 2015/2366 (EU) on Payment Services and Regulation (EU) 2016/679 on General Data Protection concerning Third Party Players' (2020) 23 Trinity CL Rev p.221; CMS, 'The interplay between PSD2 and GDPR' (*CMS Law-Now*, 30 April 2020) <https://www.cms-lawnow.com/ealerts/2020/04/the-interplay-between-psd2-and-gdpr> accessed 26 May 2021

[292] Dilja Helgadottir, 'The Interaction between Directive 2015/2366 (EU) on Payment Services and Regulation (EU) 2016/679 on General Data Protection concerning Third Party Players' (2020) 23 Trinity CL Rev p.221; CMS, 'The interplay between PSD2 and GDPR' (*CMS Law-Now*, 30 April 2020) <https://www.cms-lawnow.com/ealerts/2020/04/the-interplay-between-psd2-and-gdpr> accessed 26 May 2021

[293] CMS, 'The interplay between PSD2 and GDPR' (*CMS Law-Now*, 30 April 2020) <https://www.cms-lawnow.com/ealerts/2020/04/the-interplay-between-psd2-and-gdpr> accessed 26 May 2021

[294] EDPB, PSD2 Guidelines, p.10

[295] Recital 87 PSD2

[296] Article 6(1)(a) GDPR

[297] Article 9(1) GDPR; EDPB, PSD2 Guidelines, p.19

[298] EDPB, PSD2 Guidelines, p.19

[299] Article 9(2) GDPR

[300] EDPB, PSD2 Guidelines, p.19

[301] Article 9(2) GDPR; European Data Protection Board, 'Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1' (*Guidelines*, 4 May 2020) p.21 <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf> accessed 26 May 2021

According to EDPB, online payment transactions may reveal users' sensitive personal data.[302] Expenses regarding health issues, treatments or medicines, or certain products revealing users' sexual orientation may also be used to identify users and be accepted as sensitive personal data.[303] If the controller realizes that it may process sensitive personal data, regardless of the chosen legal basis[304] (e.g., necessary for the performance of a contract, consent), the controller should either obtain the user's explicit consent under GDPR or prove that such processing is necessary for reasons of substantial public interest under the EU or member state law.[305] Nevertheless, as substantial public interest ground can only be used in limited circumstances provided that all conditions under Article 9(2)(g) GDPR are met, TPPs will be obliged to obtain users' explicit consent in order to process their sensitive personal data in most cases.[306]

Many TPPs benefit from automated decision-making, including profiling while providing their services.[307] Many profiling techniques may also create sensitive personal data and behavioral patterns of users by combining some other (ordinary) personal data (e.g., age, sex, salary, birthplace) and interpreting them in a meaningful way.[308] Then, profiling may create sensitive personal data by inference from data that is not sensitive on its own but becomes so when combined with other data.[309] For example, based on food expenses and preferences of a person, his/her health status and eating habits could be analyzed, which may lead to health data (and, therefore, sensitive personal data) concerning the relevant user.[310] Since AISPs may access not only the basic information about users' bank accounts but also the status and history of the bank account, AISPs may access a high volume and variety of personal data.[311]

Due to profiling, if sensitive personal data is inferred based on analysis of various ordinary data of the data subject, the controller should ensure that: (i) the processing activity is not incompatible with the initial purpose, (ii) it has a legal base for the sensitive personal data processing, and (iii) it informs the relevant data subject concerning such processing activity.[312] TPPs may only be exempted from obtaining users' explicit consent if TPPs demonstrate that automated individual decision-making, including profiling, does not produce legal effects on users and significantly affect them and a meaningful human intervention exists.[313]

---

[302] EDPB, PSD2 Guidelines, p.18; Beuc, 'Beuc's Recommendations to the EDPB on the interplay between the GDPR and PSD2' (*Recommendations*, 11 April 2019) p.7 <https://www.beuc.eu/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf> accessed 26 May 2021

[303] EDPB, PSD2 Guidelines, p.18

[304] Article 6(1) GDPR

[305] Article 9(2)(a) & (g) GDPR

[306] EDPB, PSD2 Guidelines, p.19

[307] Article 4(4) GDPR; Article 22 GDPR

[308] Article 29 Data Protection Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (*Guidelines*, 6 February 2018) p.15 <https://ec.europa.eu/newsroom/article29/items/612053> accessed 26 May 2021

[309] Ibid.

[310] Ibid.

[311] Piotr Kuszewski, 'Impact of the PSD2 directive and strategic use of costly innovation' (*Warsaw School of Economics, Banking Institute*, October 2018) p.4 <https://www.researchgate.net/profile/Piotr-Kuszewski-2/publication/330347466_Impact_of_the_PSD2_directive_and_strategic_use_of_costly_innovation/links/5c3a5acc92851c22a370cb43/Impact-of-the-PSD2-directive-and-strategic-use-of-costly-innovation.pdf> accessed 26 May 2021

[312] Article 29 Data Protection Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (*Guidelines*, 6 February 2018) p.15 <https://ec.europa.eu/newsroom/article29/items/612053> accessed 26 May 2021

[313] Article 22(1) GDPR

As AISPs' services constitute profiling in most situations, AISPs may be obliged to obtain users' explicit consent before the data processing activity.[314] Even in situations where AISPs do not use profiling, due to the volume and variety of personal data of users, such collected personal data could likely be regarded as sensitive personal data in most situations. Therefore, if TPPs do not want to obtain users' explicit consent under GDPR, they should not process sensitive personal data and use automated decision-making, including profiling, that may produce legal effects or similar significant effects on users.

7. Options and Alternatives for GDPR and PSD2 Compliance for Banks and TPPs

Banks should verify whether TPPs obtained consent or explicit consent of users in line with GDPR and PSD2.[315] If banks cannot check which data users have given their consent for, transferring the users' data from banks to TPPs will be a clear contradiction with GDPR principles and rules regarding data security, data transfer, and principles of data minimization and purpose limitation.[316] On the other hand, if banks verify consent, verification of consent or explicit consent will improve the data security and ensure that TPPs do not access more data that is strictly necessary for the performance of a contract.[317]

If a bank believes that the transferred information to the relevant TPP reveals sensitive personal data, banks should check whether users' explicit consent under GDPR has been obtained by the TPP as required.[318] Due to high GDPR fines for unlawful data transferring, banks may prefer to take a precautionary approach and be reluctant to transfer the requested data if it is sensitive personal data and users' explicit consent under GDPR has not been obtained by TPPs.[319]

If a TPP solely applies automated decision-making, including profiling that may produce legal effects or similar significant effects on users, such TPP should obtain the explicit consent of users. However, in case such TPP does not obtain users' explicit consent, under PSD2, there is no mechanism to be used by banks to check whether such TPP obtained the explicit consent of their users as required. However, under GDPR, banks, as the controllers, may only share the data subjects' personal data with TPPs only if data subjects give their explicit consent to TPPs under PSD2. In addition, under PSD2, no provision prevents banks from checking whether TPPs obtained users' explicit consent in case of sensitive personal data processing and solely

---

[314] Beuc, 'Beuc's Recommendations to the EDPB on the interplay between the GDPR and PSD2' (*Recommendations*, 11 April 2019) p.2 <https://www.beuc.eu/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf> accessed 26 May 2021

[315] Dilja Helgadottir, 'The Interaction between Directive 2015/2366 (EU) on Payment Services and Regulation (EU) 2016/679 on General Data Protection concerning Third Party Players' (2020) 23 Trinity CL Rev p.216

[316] Beuc, 'Beuc's Recommendations to the EDPB on the interplay between the GDPR and PSD2' (*Recommendations*, 11 April 2019) p.6 <https://www.beuc.eu/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf> accessed 26 May 2021

[317] Ibid.

[318] Beuc, 'Beuc's Recommendations to the EDPB on the interplay between the GDPR and PSD2' (*Recommendations*, 11 April 2019) p.6-7 <https://www.beuc.eu/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf> accessed 26 May 2021

[319] Alja Poklar, 'Does the Same Word Mean the Same Thing? An Exploration of the Notion of Consent in PSD2 and GDPR' (*Tilburg University*, 2019) p.21 <https://arno.uvt.nl/show.cgi?fid=148995> accessed 26 May 2021; Beuc, 'Beuc's Recommendations to the EDPB on the interplay between the GDPR and PSD2' (*Recommendations*, 11 April 2019) p.2 <https://www.beuc.eu/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf> accessed 26 May 2021; Paul Voigt and Axel von dem Bussche, The EU General Data Protection Regulation (GDPR) A Practical Guide (Springer 2017), p.96; Article 83(5) GDPR; Krzysztof Trojan, 'PSD2 & GDPR regulations on collision course?' (*LinkedIn*, 15 January 2017) <https://www.linkedin.com/pulse/psd2-gdpr-regulations-collission-course-krzysztof-trojan/> accessed 26 May 2021

applied automated decision-making, including profiling that may produce legal effects or similar significant effect on users.

Banks' refusal of TPPs' payment data requests due to lack of explicit consent under GDPR may cause operational problems in online payment services practice.[320] Banks may use alternative technological solutions to prevent conflicts between banks and TPPs, including the abstraction of some data requested by TPPs.[321] Thanks to such abstraction, if some TPPs do not obtain their users' explicit consent under GDPR, banks may still share the less detailed (abstract) versions of these data without providing any sensitive personal data or the unnecessary data that could be useful for automated decision-making, including profiling that may produce legal effects or similar significant effect on users. In this way, banks and TPPs may comply with both GDPR and PSD2 provisions. Moreover, as obtaining explicit consent under GDPR could be difficult for the controllers in some cases, as an alternative to explicit consent, TPPs may also focus on alternative technological solutions (e.g., digital filters) to prevent any potential sensitive personal data processing and automated individual decision-making, including profiling that may produce legal effects or similar significant effect on users.[322] While taking these steps, both banks and TPPs should take into account Article 32(1) GDPR, *"…the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk".*[323]

If TPPs would like to receive unfiltered versions of those sensitive personal data, they should obtain users' explicit consent under GDPR and submit them to banks. However, even though users give their explicit consent to TPPs, as such data are not necessary for receiving online payment service, such processing will be against data minimization and purpose limitation principles and will be unlawful under GDPR.[324] If TPPs do not want to obtain users' explicit consent, they have to use the digital filters (in cases, banks have not applied abstraction) when they receive the original data. Although explicit consent under PSD2 envisages processing personal data based on the legal base necessary for the performance of a contract,[325] this legal base cannot be used for processing sensitive personal data or solely applied automated decision-making, including profiling.[326]

All the points above are also in line with Article 36(1) PSD2, *"Member States shall ensure that payment institutions have access to credit institutions' payment accounts services on an objective, non-discriminatory and proportionate basis. Such access shall be sufficiently*

[320] Alja Poklar, 'Does the Same Word Mean the Same Thing? An Exploration of the Notion of Consent in PSD2 and GDPR' (*Tilburg University*, 2019) p.21 <https://arno.uvt.nl/show.cgi?fid=148995> accessed 26 May 2021
[321] Article 32(1) GDPR; Jaimy van der Heijden, 'Privacy in Financial Innovation: a Value Sensitive Design for PSD2' (*TUDelft*, 2017) p.37 <https://repository.tudelft.nl/islandora/object/uuid%3Ac558efd2-692e-4b2e-9933-4cc248ccd4b1> accessed 26 May 2021
[322] Article 25 GDPR
[323] Article 32(1) GDPR
[324] IT Governance Privacy Team, EU General Data Protection Regulation (GDPR) An Implementation and Compliance Guide (4th edn, IT Governance Publishing 2020), p.50-53; Article 5(1) GDPR
[325] Article 6(1)(b) GDPR
[326] Article 9(2) GDPR; European Data Protection Board, 'Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1' (*Guidelines*, 4 May 2020) p.21 <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf> accessed 26 May 2021

extensive as to allow payment institutions to provide payment services in an unhindered and efficient manner". As long as the data provided by banks to TPPs allow TPPs to provide their services in an unhindered and efficient way and banks limit the transferred personal data based on objective, non-discriminatory and proportionate reasons, banks are obliged to limit and abstract the personal data that will be shared with TPPs under GDPR.[327] Lastly, to have a seamless relationship between TPPs, banks, national data protection, and PSD2 compliance authorities, more meaningful cooperation is needed between all stakeholders.[328]

Considering the volume, variety, and sensitivity of the personal data of hundreds of millions of people who will be benefiting from payment initiation and account information services, utmost attention should be paid to mitigate the personal data risks. As explained in Chapter 3, controllers have various methods and tools to manipulate or steer the data subjects towards giving their consent. Therefore, obtaining consent under GDPR may not be the best option for processing the personal data of the data subjects in online payment services. To prevent TPPs from processing excessive personal data (e.g., ATM locations, full supermarket names, full product names) other than the objectively necessary personal data for the performance of a contract, it will be better to block TPPs' chance to process more data than the objectively necessary ones. Thus, without creating any possibility for TPPs to process more data based on consent and explicit consent under GDPR with steering the data subjects for "I agree" buttons, examining whether the personal data that they process are objectively necessary for the performance of the contract would be better and more privacy-friendly option.[329] Moreover, such transparency requirement arising from explicit consent under PSD2 empowers data subjects and helps them to be better-informed in online payment transactions.

8. Conclusion

In conclusion, this chapter focused on consent and explicit consent under PSD2 and the difference concerning definition and conditions of consent and explicit consent compared under GDPR and PSD2. It is crucial to evaluate GDPR and PSD2 provisions' interplay and interaction and mitigate any potential risks between banks and TPPs.[330] Although I agree with the majority of the literature on the topic that the terms of consent and explicit consent have different meanings under PSD2 and GDPR and that explicit consent in PSD2 should be accepted as an "additional contractual and transparency requirement", not an additional legal base for data processing, a coherent and noncontradictory interpretation, and implementation could be established between them. Cooperation of various law and fintech areas and taking technical measures for effective implementation is necessary for PSD2 and GDPR compliance.[331] This will eventually lead to more secure payments and better user protection, and online payment services.[332]

---

[327] Dilja Helgadottir, 'The Interaction between Directive 2015/2366 (EU) on Payment Services and Regulation (EU) 2016/679 on General Data Protection concerning Third Party Players' (2020) 23 Trinity CL Rev p.216; Article 5 GDPR; Article 9 GDPR; Article 22 GDPR

[328] Beuc, 'Beuc's Recommendations to the EDPB on the interplay between the GDPR and PSD2' (*Recommendations*, 11 April 2019) p.8 <https://www.beuc.eu/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf> accessed 26 May 2021

[329] Paul de Hert and Juraj Sajfert, 'Regulating Big Data in and out of the data protection policy field' [2019] 5(3) European Data Protection Law Review, p.11-12

[330] Dilja Helgadottir, 'The Interaction between Directive 2015/2366 (EU) on Payment Services and Regulation (EU) 2016/679 on General Data Protection concerning Third Party Players' (2020) 23 Trinity CL Rev p.224

[331] Ibid.

[332] Ibid.

In the second part of the chapter, further personal data processing, and its conditions have been evaluated. As such further processing is not directly regulated under PSD2, such processing can be carried out under GDPR provisions. In the third part, two situations that necessitate obtaining explicit consent under GDPR, sensitive personal data processing and automated decision-making, including profiling, have been evaluated. Then, alternative measures that could be taken by TPPs and banks have been elaborated if they refrain from obtaining explicit consent under GDPR.

In Chapters 3 and 4, this thesis focused on data processing based on consent and explicit consent under GDPR and PSD2. However, obtaining consent or explicit consent does not legitimize TPPs' silent party data processing operations since the silent party data only belongs to the silent parties, not to users. Therefore, in Chapter 5, such an exceptional situation will be analyzed.

5. CHAPTER 5 – Silent Party Data

1. Introduction

In the previous chapters, we discussed that the legal base for processing personal data between users and TPPs would be "necessary for the performance of a contract".[333] However, in online payment services, there is another situation where consent and explicit consent cannot be a legal base for data processing operations which is the data processing of the silent parties. Thus, this chapter will discuss how payment service providers may process the personal data of silent parties under GDPR and PSD2.

Silent party data are the personal data that belong to a natural person who is not a user of a TPP, for example, personal data of the recipient of a payment.[334] To provide a better explanation, If A (as the data subject) buys a product from B's website, A may benefit from a PISP's, such as iDEAL, payment initiation service. The PISP will access A's bank account information to initiate the payment as there is a contractual relationship between A and the PISP. However, while initiating such a payment, the PISP should also access B's bank account information to complete the payment, despite the lack of contractual relationship between the PISP and B. In this situation, B, the person who is getting paid, is the silent party.[335] Regarding account information service, Z buys medicines from a pharmacy, and such a pharmacy receives account information services from an AISP.[336] In this relationship, Z is the silent party, and his/her data will be silent party data as the account information service agreement is made between the pharmacy and the relevant AISP.

In daily life, people send money to each other via different PISPs. As for each money a payee receives, if a payer receives payment initiation service from a PISP, for example, Tikkie, the payee's bank account data necessary for the initiation of payment (as silent party data) will be collected by Tikkie for initiation of such payment. The data protection risks for AISPs are even higher. People purchase goods and receive services from different companies. To track their revenue and purchases and have more information about their financial situation, these companies may receive account information services from different AISPs. As each person enters into a contractual relationship with hundreds of companies, it is highly likely that various AISPs will access people's silent party data that provide their services to the companies they have entered into a contractual relationship. Therefore, the processing of silent party data is directly related to hundreds of millions of people.

2. Silent Party Data Processing

To perform payment initiation or account information services, TPPs have to process silent parties' data.[337] Without such data, payment initiation and account information services cannot

---

[333] Article 6(1)(b) GDPR

[334] Ducuing Charlotte, Dutkiewicz Lidia and Miadzvetskaya Yuliya, 'D62 Legal and Ethical Requirements' (*Trusts Trusted Secure Data Sharing Space*, August 2020) p.122 <https://www.trusts-data.eu/wp-content/uploads/2020/10/D6.2-Legal-and-Ethical-Requirements.pdf> accessed 26 May 2021; Dilja Helgadottir, 'The Interaction between Directive 2015/2366 (EU) on Payment Services and Regulation (EU) 2016/679 on General Data Protection concerning Third Party Players' (2020) 23 Trinity CL Rev p.218

[335] Dilja Helgadottir, 'The Interaction between Directive 2015/2366 (EU) on Payment Services and Regulation (EU) 2016/679 on General Data Protection concerning Third Party Players' (2020) 23 Trinity CL Rev p.218

[336] Krzysztof Trojan, '(Not so) legitimate interest in auxiliary data under PSD2 and GDPR' (*LinkedIn*, 15 May 2017) <https://www.linkedin.com/pulse/so-legitimate-interest-auxiliary-data-under-psd2-gdpr-trojan/> accessed 26 May 2021

[337] European Savings and Retail Banking Group, 'ESBG Response to the EDPB consultation on the Guidelines 06/2020 on the interplay between PSD2 and GDPR' (*Public Consultation Reply*, September 2020) p.11

be provided. Concerning the legal base of silent party data processing activities, if the controller or the third party has a legitimate interest in processing personal data, the controller may use this legal base to process only the objectively necessary personal data concerning such legitimate interest.[338] Under this legal base, the controller may only process the silent party data, which are strictly limited and directly related to the claimed legitimate interest.[339] Some silent party data could be listed as; name and surname, address, the IBAN, and bank account number of natural persons to whom the users transferred money or from whom they received the money.[340] However, since only the strictly limited data should be processed in each specific processing operation, for example, the silent party's identity, his/her IBAN, and the transaction characteristics may not be strictly necessary for many situations.[341]

Although using the silent party data is necessary for providing payment initiation and account information services, the protection of silent party data has utmost importance to consider. While using the legitimate interest legal base, GDPR sets forth that controllers, TPPs in our case, have to carry out a balancing test before the processing operations to determine whether the data subjects' rights and freedoms will be overridden.[342] Thus, TPPs should prove and demonstrate that they carried out a suitable balancing test, had a legitimate interest in processing, and did not override data subjects' rights in line with the accountability and transparency principles of GDPR.[343] Such interests could be economical, legal, or any other suitable one under the law.[344] To carry out such a balancing test, TPPs have to consider specific issues, including the scope of the processing operation, the kinds of data processing, and risks for data subjects.[345] While carrying out such a balancing test, specifics of the processing operation and its consequences on the silent parties' rights and freedoms and possible

<https://www.wsbi-esbg.org/SiteCollectionDocuments/ESBG-response-EDPB-interplay-psd2-gdpr.pdf> accessed 26 May 2021

[338] Dilja Helgadottir, 'The Interaction between Directive 2015/2366 (EU) on Payment Services and Regulation (EU) 2016/679 on General Data Protection concerning Third Party Players' (2020) 23 Trinity CL Rev p.218; Article 6(1)(f) GDPR

[339] P.T.J. Wolters, B.P.F. Jacobs, 'The security of access to accounts under the PSD2' [2019] 35(1) Computer Law & Security Review, p.33; Dilja Helgadottir, 'The Interaction between Directive 2015/2366 (EU) on Payment Services and Regulation (EU) 2016/679 on General Data Protection concerning Third Party Players' (2020) 23 Trinity CL Rev p.218

[340] Bird & Bird, 'EU: The interplay of PSD2 and GDPR - some select issues' (*DataGuidance*, February 2019) p.4 <https://www.twobirds.com/~/media/pdfs/eu-the-interplay-of-psd2-and-gdpr--some-select-issues.pdf> accessed 26 May 2021

[341] Sue Mclean, Michaela Nebel and Benjamin Slinn, 'European Union: How does PSD2 interplay with the GDPR?' (*Baker Mckenzie Global Compliance News*, 23 October 2020) p.4 <https://globalcompliancenews.com/european-union-how-does-psd2-interplay-with-the-gdpr/> accessed 26 May 2021

[342] Article 29 Data Protection Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' (*Opinion*, 9 April 2014) p.5 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf> accessed 26 May 2021

[343] Ibid.; Bird & Bird, 'EU: The interplay of PSD2 and GDPR - some select issues' (*DataGuidance*, February 2019) p.5 <https://www.twobirds.com/~/media/pdfs/eu-the-interplay-of-psd2-and-gdpr--some-select-issues.pdf> accessed 26 May 2021

[344] Paul Voigt and Axel von dem Bussche, The EU General Data Protection Regulation (GDPR) A Practical Guide (Springer 2017), p.96

Article 29 Data Protection Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' (*Opinion*, 9 April 2014) p.25 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf> accessed 26 May 2021

[345] Bird & Bird, 'EU: The interplay of PSD2 and GDPR - some select issues' (*DataGuidance*, February 2019) p.5 <https://www.twobirds.com/~/media/pdfs/eu-the-interplay-of-psd2-and-gdpr--some-select-issues.pdf> accessed 26 May 2021; Paul Voigt and Axel von dem Bussche, The EU General Data Protection Regulation (GDPR) A Practical Guide (Springer 2017), p.96

impairments should be analyzed carefully.[346] For example, if the silent parties' fundamental rights are at stake, they may outweigh the commercial interests of TPPs, such as sending targeted advertisements to the silent parties.[347] Furthermore, it should be analyzed whether such processing is necessary and proportionate and there are any less intrusive means that the controller may apply.[348] Thus, TPPs must take effective and appropriate measures to safeguard all parties' rights and freedoms, particularly the data subjects and silent parties, when they provide their online payment services.[349]

If the relevant bank account is a joint account used by both the user and the other account holder, TPPs will also access the personal data of the other account holder (i.e., silent party).[350] Although TPPs may process the other account holder's personal data based on legitimate interest, the second account holder should have a right to be informed of the personal data that will be processed, and he/she has an opportunity to object.[351] However, in many cases, as silent parties may not even know whether their banking information-related personal data are processed by TPPs or not, they may not use their rights to object effectively.[352]

EDPB did not provide its opinion on how TPPs should inform the silent parties to use their right to object since the legal ground for data processing is the legitimate interest.[353] The data subjects whose data have been processed under legitimate interest as the silent party data should be informed separately and explicitly by TPPs that the data subjects have no relationship before.[354]

As the number of payment service providers and the volume of online payment services increased markedly, this increases the risk of silent party data misuse significantly.[355] Therefore, TPPs and banks should find effective ways to prevent unnecessary personal data

---

[346] Paul Voigt and Axel von dem Bussche, The EU General Data Protection Regulation (GDPR) A Practical Guide (Springer 2017), p.105-106

[347] Irene Kamara and Paul De Hert, 'Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach' [2018] 4(12) Brussels Privacy Hub p.14

[348] Paul Voigt and Axel von dem Bussche, The EU General Data Protection Regulation (GDPR) A Practical Guide (Springer 2017), p.106; Johan Peeters, 'Data protection in mobile wallets' (*KU Leuven*, 2019) p.64 <https://www.scriptiebank.be/sites/default/files/thesis/2019-10/PEETERS_s0107530_thesis.pdf> accessed 26 May 2021

[349] EDPB, PSD2 Guidelines, p.15; Article 29 Data Protection Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' (*Opinion*, 9 April 2014) p.42-43 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf> accessed 26 May 2021

[350] Beuc, 'Beuc's Recommendations to the EDPB on the interplay between the GDPR and PSD2' (*Recommendations*, 11 April 2019) p.4 <https://www.beuc.eu/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf> accessed 26 May 2021

[351] Article 21(1) GDPR; Article 29 Data Protection Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' (*Opinion*, 9 April 2014) p.44-45 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf> accessed 26 May 2021; Beuc, 'Beuc's Recommendations to the EDPB on the interplay between the GDPR and PSD2' (*Recommendations*, 11 April 2019) p.4 <https://www.beuc.eu/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf> accessed 26 May 2021

[352] Alja Poklar, 'Does the Same Word Mean the Same Thing? An Exploration of the Notion of Consent in PSD2 and GDPR' (*Tilburg University*, 2019) p.37 <https://arno.uvt.nl/show.cgi?fid=148995> accessed 26 May 2021

[353] Article 21 GDPR; Latham & Watkins, 'Privacy and Payments: New Draft EU Advice for Financial Institutions' (*JDSupra*, 4 November 2020) <https://www.jdsupra.com/legalnews/privacy-and-payments-new-draft-eu-89021/> accessed 26 May 2021

[354] Ibid.; Article 21 GDPR

[355] Michał Polasika, Agnieszka Huterskaa, Rehan Iftikhar, Štepán Mikula, 'The impact of Payment Services Directive 2 on the PayTech sector development in Europe' [2020] 178 Journal of Economic Behavior & Organization p.397

sharing and processing operations by themselves, without any need for silent parties' involvement concerning their rights to object.[356]

From the banks' perspective, they are not breaching GDPR when they share the silent parties' necessary personal data with TPPs, when *"…processing is necessary for compliance with a legal obligation to which the controller is subject"*.[357] Banks should provide the necessary data allowing TPPs to provide their payment initiation and account information services.[358] Banks should only share the necessary personal data of silent parties with TPPs, using state-of-the-art technology, such as using digital filters.[359] Likewise, TPPs should also use state-of-the-art technologies to filter out the necessary personal data of silent parties only, as explained in Chapter 4.[360]

Taking Google or Apple as an example, the more users use these companies as PISP or AISP, the more personal data, including silent party data, they will have.[361] Moreover, the more users give their consent for online payment services, the number of silent parties and the volume and variety of silent party data will increase tremendously.[362] In such a case, even if the silent parties have never given their consent to these companies and thought that these companies might have their data, with more silent party data, big companies will have a better and more complete profile of the silent parties.[363] Although EDPB stated that further processing of silent party data is not allowed, TPPs may still tend to use such silent party data for further processing operations due to its substantial economic benefit.[364]

3. Further Processing of Silent Party Data

Processing silent parties' data for any other purposes (in addition to the initial purpose) is regarded as further processing. In line with GDPR principles, including data minimization and purpose limitations,[365] further processing will be unlawful unless the controller obtains the consent of the silent parties under GDPR.[366] This is also in line with PSD2 articles, namely Article 66(3)(g), *"[PISP] shall … not use, access or store any data for purposes other than for the provision of the payment initiation service as explicitly requested by the payer"*, and Article 67(2)(f), *"[AISP] shall … not use, access or store any data for purposes other than for*

[356] Alja Poklar, 'Does the Same Word Mean the Same Thing? An Exploration of the Notion of Consent in PSD2 and GDPR' (*Tilburg University*, 2019) p.37 <https://arno.uvt.nl/show.cgi?fid=148995> accessed 26 May 2021
[357] Article 6(1)(c) GDPR; Bird & Bird, 'EU: The interplay of PSD2 and GDPR - some select issues' (*DataGuidance*, February 2019) p.5 <https://www.twobirds.com/~/media/pdfs/eu-the-interplay-of-psd2-and-gdpr--some-select-issues.pdf> accessed 26 May 2021
[358] Article 66(4) PSD2; Article 67(3) GDPR
[359] PSD2 Guidelines, p.15; Article 24(2) GDPR; Article 5(1) GDPR; Article 66(3)(g) PSD2; Article 67(2)(f) PSD2
[360] Article 66(3)(g) PSD2; Article 67(2)(f) PSD2
[361] EDPB, 'GDPR PSD2 Guidelines Feedback' (*Public Consultation Reply*, 2020) <https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/gdpr_psd2_guidelines_feedback.pdf> accessed 26 May 2021
[362] Ibid.
[363] Ibid.
[364] Ibid.
[365] Ducuing Charlotte, Dutkiewicz Lidia and Miadzvetskaya Yuliya, 'D62 Legal and Ethical Requirements' (*Trusts Trusted Secure Data Sharing Space*, August 2020) p.123 <https://www.trusts-data.eu/wp-content/uploads/2020/10/D6.2-Legal-and-Ethical-Requirements.pdf> accessed 26 May 2021
[366] Dilja Helgadottir, 'The Interaction between Directive 2015/2366 (EU) on Payment Services and Regulation (EU) 2016/679 on General Data Protection concerning Third Party Players' (2020) 23 Trinity CL Rev p.218; Article 6(1)(a) GDPR

performing the account information service explicitly requested by the payment service user, in accordance with data protection rules".[367]

In line with the Guidelines, the controller's legitimate interest should be strictly determined by the data subjects' reasonable expectations that are assessed based on the type of relationship between the controller and the data subject.[368] TPPs have to assess whether the silent parties may reasonably expect the processing of their payment initiation or account information services-related data at the time and context of the data processing operation.[369] As there is no contractual or any other type of direct relationship between TPPs and silent parties, considering the reasonable expectations test, data processing operation of silent parties should be strictly limited as they do not expect a further data processing operation, other than the strictly necessary personal data for payment initiation or account information services, based on the legitimate interest legal ground.[370] Thus, TPPs should not use this legal base easily and automatically to process silent parties' data regarding the application of the legitimate interest.[371] Moreover, EDPB believes that silent party data cannot be used for any other purposes other than the initial purpose unless EU or the member state law declares otherwise.[372] But, some other stakeholders believe that EDPB cannot prevent further silent party data processing absolutely, as GDPR and PSD2 do not prohibit this further processing explicitly.[373] As long as the controllers fulfill the conditions listed under Article 6(4) GDPR, they claim that controllers may process silent party data.[374] However, in my opinion, similar to EDPB's opinion on the conditions of Article 6(4) GDPR[375], since there is no relation between the silent parties

[367] Article 66(3)(g) PSD2; 67(2)(f) PSD2

[368] EDPB, PSD2 Guidelines, p.15; Article 29 Data Protection Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' (*Opinion*, 9 April 2014) p.30 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf> accessed 26 May 2021; Paul Voigt and Axel von dem Bussche, The EU General Data Protection Regulation (GDPR) A Practical Guide (Springer 2017), p.106

[369] Irene Kamara and Paul De Hert, 'Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach' [2018] 4(12) Brussels Privacy Hub p.17

[370] Article 29 Data Protection Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' (*Opinion*, 9 April 2014) p.30 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf> accessed 26 May 2021; Paul Voigt and Axel von dem Bussche, The EU General Data Protection Regulation (GDPR) A Practical Guide (Springer 2017), p.106; EDPB, PSD2 Guidelines, p.15

[371] Bird & Bird, 'EU: The interplay of PSD2 and GDPR - some select issues' (*DataGuidance*, February 2019) p.5 <https://www.twobirds.com/~/media/pdfs/eu-the-interplay-of-psd2-and-gdpr--some-select-issues.pdf> accessed 26 May 2021

[372] EDPB, PSD2 Guidelines, p.15-16

[373] European Banking Federation, 'EBF response to the European Data Protection Board's consultation on the Guidelines 6/2020 on the interplay of the Second Payment Services Directive and the GDPR' (*Public Consultation Reply*, 16 September 2020) p.9 <https://edpb.europa.eu/sites/edpb/files/webform/public_consultation_reply/ebf_042474_-_european_banking_federation_response_edpb_guidelines_psd2-gdpr_.pdf> accessed 26 May 2021; European Savings and Retail Banking Group, 'ESBG Response to the EDPB consultation on the Guidelines 06/2020 on the interplay between PSD2 and GDPR' (*Public Consultation Reply*, September 2020) p.12-13 <https://www.wsbi-esbg.org/SiteCollectionDocuments/ESBG-response-EDPB-interplay-psd2-gdpr.pdf> accessed 26 May 2021

[374] European Banking Federation, 'EBF response to the European Data Protection Board's consultation on the Guidelines 6/2020 on the interplay of the Second Payment Services Directive and the GDPR' (*Public Consultation Reply*, 16 September 2020) p.9 <https://edpb.europa.eu/sites/edpb/files/webform/public_consultation_reply/ebf_042474_-_european_banking_federation_response_edpb_guidelines_psd2-gdpr_.pdf> accessed 26 May 2021; Article 6(4) GDPR

[375] EDPB, PSD2 Guidelines, p.15-16

and TPPs, considering the sensitivity of the personal data (e.g., the monetary amounts, personal or business relationships)[376] that could be processed based on the legitimate interest in online payment transactions and the number of people affected with this processing as the silent parties, in practice, conditions of Article 6(4) GDPR cannot be fulfilled. I also believe that it would be better for EDPB to provide an in-debt analysis in the Guidelines and explain why TPPs cannot fulfill the conditions listed under Article 6(4) GDPR regarding the silent party data to prevent any confusions and questions in the first place.

TPPs should also take necessary technical measures to ensure that silent parties' data cannot be processed for any other purposes apart from the initial purpose.[377] The personal data of silent parties cannot be used for marketing or profiling.[378] For example, if a go-go bar receives account information services from an AISP, such AISP may process the visitors' data under legitimate interest.[379] As a data subject, you will never know which AISP will have your data (e.g., how frequently you go to that go-go bar, how much money you pay) and whether such AISP is trustworthy and prudent.[380] To analyze the first example that we gave at the beginning of this chapter further, assuming that Z has serious mental health issues and buys medicines from a pharmacy and such pharmacy receives account information services from an AISP.[381] When the AISP have the transaction history of the pharmacy, an ordinary data analyst may find out that Z has serious mental health issues by cross-referencing various data, such as; Z's bank account number, a price tag of the mental health medicine (even if the drug name and Z's name are not mentioned in the pharmacy's transaction history) and some other transaction histories, for example, transaction history of a car insurance company (that may reveal Z's car plate) receiving account information services from the same AISP.[382] Therefore, in line with Article 6(4) GDPR, TPPs should strictly apply encryption, pseudonymization, and other techniques to improve data security and process the minimum amount of silent party data to fulfill the data minimization and purpose limitation principles.[383]

---

[376] Krzysztof Trojan, 'Data of silent parties under the legal mess called PSD2 & GDPR' (*LinkedIn*, 6 May 2019) <https://www.linkedin.com/pulse/data-silent-parties-under-legal-mess-called-psd2-gdpr-trojan/> accessed 26 May 2021

[377] EuroCommerce, 'EuroCommerce comments in response to the public consultation regarding the Guidelines 06/2020 published by the European Data Protection Board on the interplay of the Second Payment Services Directive and the GDPR version 10' (*Public Consultation Reply*, 13 August 2020) p.1-2 <https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/eurocommerce_response_to_edpb_guidelines_062020_on_the_interplay_of_the_second_payment_services_directive_and_the_gdpr.pdf> accessed 26 May 2021

[378] Ibid.

[379] Krzysztof Trojan, 'Data of silent parties under the legal mess called PSD2 & GDPR' (*LinkedIn*, 6 May 2019) <https://www.linkedin.com/pulse/data-silent-parties-under-legal-mess-called-psd2-gdpr-trojan/> accessed 26 May 2021

[380] Ibid.

[381] Krzysztof Trojan, '(Not so) legitimate interest in auxiliary data under PSD2 and GDPR' (*LinkedIn*, 15 May 2017) <https://www.linkedin.com/pulse/so-legitimate-interest-auxiliary-data-under-psd2-gdpr-trojan/> accessed 26 May 2021

[382] Ibid.

[383] EuroCommerce, 'EuroCommerce comments in response to the public consultation regarding the Guidelines 06/2020 published by the European Data Protection Board on the interplay of the Second Payment Services Directive and the GDPR version 10' (*Public Consultation Reply*, 13 August 2020) p.1-2 <https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/eurocommerce_response_to_edpb_guidelines_062020_on_the_interplay_of_the_second_payment_services_directive_and_the_gdpr.pdf> accessed 26 May 2021; Niels Vandezande, 'EDPB Clarifies the Interplay between GDPR and PSD2' (*Timelex*, 15 February 2021) <https://www.timelex.eu/en/blog/edpb-clarifies-interplay-between-gdpr-and-psd2> accessed 26 May 2021

According to some stakeholders, by invoking Article 18 GDPR, data subjects should be able to request their banks to limit the shared data with TPPs and inform TPPs that they reject any further processing when users are "silent parties" under PSD2.[384] Otherwise, considering the vast volume of data in the online payment market, silent parties' data could be used for very accurate profiling and credit rating operations, even though they do not have any information about such processing operations.[385]

Concerning payment initiation services, using legitimate interest legal ground makes sense since the silent party data is strictly necessary to execute the payment. The silent party has also benefited from such transactions, and the data processing activity and the amount and variety of personal data are low.[386] On the other hand, as for account information services, silent parties do not have any benefit from such data processing operations, and the amount and variety of personal data that could be processed are way more than the payment initiation services.[387] Therefore, GDPR principles and rules should be more strictly applied to AISPs. Also, regarding the further processing of the silent parties, AISPs' further processing operations should not be allowed as the conditions listed under Article 6(4) GDPR cannot be fulfilled in practice in line with the explanations above.

4. Conclusion

This chapter explained that TPPs could process the silent party personal data in online payment transactions based on Article 6(1)(f) GDPR. However, the burden of proof is on TPPs' side when claiming that TPPs have a legitimate interest in processing silent party data under the accountability principle. Based on the legitimate interest legal base, TPPs may only process the personal data strictly necessary to provide their payment initiation or account information services. Furthermore, TPPs can only process such data if their legitimate interests outweigh the data subjects' rights and freedoms. Although it is not practically possible on every occasion, in principle, silent parties should be able to use their right to object under GDPR. Moreover, banks and TPPs should take the necessary steps to filter out the "unnecessary silent party data" and prevent any excessing transfer (as for banks) and access (as for TPPs).

As the second point, this chapter elaborated that further processing of such silent party personal data should be subject to strict conditions. Considering hundreds of millions of people that will be affected by such processing and the nature of personal data (as various financial data may reveal personal characteristics of data subjects), it will be highly probable for data controllers to process such silent party data for other purposes, in addition to the initial processing purpose. Moreover, it was also highlighted that EDPB believes that, despite some opposing opinions, further processing of silent party data will not be lawful in any case.

---

[384] The Privacy First Foundation, 'Feedback on Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR' (*Public Consultation Reply*, 16 September 2020) p.13 <https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/20200915_privacy_first_foundation_feedback_on_guidelines_06_2020_v1.pdf> accessed 26 May 2021

[385] Ibid.

[386] Krzysztof Trojan, 'Data of silent parties under the legal mess called PSD2 & GDPR' (*LinkedIn*, 6 May 2019) <https://www.linkedin.com/pulse/data-silent-parties-under-legal-mess-called-psd2-gdpr-trojan/> accessed 26 May 2021

[387] Ibid.

6. CHAPTER 6 – Conclusion

The new technologies and, in particular, open banking changed the financial markets significantly. With PSD2, two new players, PISP and AISP, officially joined the online payment market and the ongoing competition. As users' data are vital for TPPs to provide payment initiation and account information services, arguably, access to users' personal data constituted the most critical aspect of PSD2. However, after entering into force of PSD2, some data protection questions, especially related to definitions and conditions of consent and explicit consent, were discussed. Despite the Guidelines, it was not certain when consent and explicit consent will be required under GDPR and PSD2, how such consent and explicit consent will be obtained under GDPR and PSD2, which additional measures should be applied by TPPs and banks, and whether alternative data processing grounds can be used in certain situations. In line with this, how to obtain consent and explicit consent under PSD2 and its similarities and differences with consent and explicit consent under GDPR matter for all the stakeholders in the online payment market, especially for users. Despite EDPB's efforts, there are still unclear points that need to be evaluated in detail. In particular:

1. Which personal data and silent party data can banks share with TPPs?
2. Whether banks and TPPs have to limit the personal data they share and receive, respectively, to comply with PSD2 and GDPR principles and rules using state-of-the-art technologies?
3. Should banks check whether TPPs obtained users' consent and explicit consent under PSD2 and GDPR before giving access to TPPs?
4. Should banks check whether TPPs will process sensitive personal data and use automated decision-making, including profiling, that may produce legal effects or similar significant effects on users?
5. To what extent and under what conditions further personal data and silent party data processing operations are allowed under PSD2 and GDPR?
6. Whether and how can individuals limit the personal data and silent party data that will be shared with TPPs?

In this thesis, we focused on the question of *"What kind of personal data, including silent party data, could be processed under the notion of explicit consent as per GDPR and PSD2 in online payment transactions?"*. We concluded that the meaning of explicit consent is different than its meaning under GDPR. Explicit consent under PSD2 is a contractual approval that brings an additional transparency requirement before processing personal data in accordance with PSD2 and GDPR provisions, not an additional *sui generis* legal ground. Due to the existence of a contractual relationship between users and TPPs, the necessary for the performance of the contract will be the most suitable legal base for data processing operations. However, if TPPs access sensitive personal data or they infer special categories of personal data thanks to advanced profiling techniques, TPPs have to obtain users' explicit consent under GDPR. If TPPs do not want to access sensitive personal data or banks do not want to grant access to TPPs on their users' sensitive personal data, different technological techniques could be used to prevent sensitive personal data processing. Even though TPPs do not process sensitive personal data or their automated decision-making, including profiling, techniques do not necessitate obtaining users' explicit consent under GDPR, if TPPs conduct further data processing operations, they may have to obtain users' consent under GDPR, since such further processing operations may not compatible with the initial processing operation. Although silent parties are not a part of the

payment services agreements between TPPs and users, legitimate interest legal ground can be used by TPPs, provided that Article 6(4) GDPR conditions are met.

Although specifics of each case matter to reach more accurate answers in response to the questions above, this thesis aims to create a general framework for them. Considering that online payment transactions should be fast and smooth in daily life, all stakeholders (e.g., banks, TPPs, data protection, and PSD2 compliance authorities) should discuss these issues and particulars of alternative scenarios to reach perfect compliance with GDPR and PSD2. In any case, all parties should consider one thing: hundreds of millions of people should be able to receive online payment services without giving up their right to privacy and protection of personal data that is protected under Article 8 Charter.

BIBLIOGRAPHY

TABLE OF CASES

Bundeskartellamt, 6th Decision Division, B6-22/16

TABLE OF LEGISLATION

Charter of Fundamental Rights of the European Union [2000] *OJ C364/1*

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 *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

Alan Calder, EU GDPR - A pocket guide (2nd edn, IT Governance Publishing 2018)

Alja Poklar, 'Does the Same Word Mean the Same Thing? An Exploration of the Notion of Consent in PSD2 and GDPR' (*Tilburg University*, 2019) <https://arno.uvt.nl/show.cgi?fid=148995> accessed 26 May 2021

Amaya Noain-sánchez, '"Privacy by default" and active "informed consent" by layers: Essential measures to protect ICT users' privacy' [2016] 14 Journal of Information, Communication and Ethics in Society

Anshu Premchand and Anurag Choudhry, 'Open Banking & APIs for Transformation in Banking' (International Conference on Communication, Computing and Internet of Things (IC3IoT), 2018) <https://ieeexplore-ieee-org.tilburguniversity.idm.oclc.org/stamp/stamp.jsp?tp=&arnumber=8668107> accessed 26 May 2021

Anton Lindberg, 'Alternatives for the Individual Consent in Data Protection Law' (*Tilburg University*, 2018) <https://arno.uvt.nl/show.cgi?fid=145717> accessed 26 May 2021

Article 29 Data Protection Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (*Guidelines*, 6 February 2018) <https://ec.europa.eu/newsroom/article29/items/612053> accessed 26 May 2021

Article 29 Data Protection Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' (*Opinion*, 9 April 2014) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf> accessed 26 May 2021

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 26 May 2021

Ayo Eso and Anna Masłoń-Oracz, 'The Impact of Payment Services Directive 2 (Psd2) on Financial Services in the European Union Single Market' [2018] 2(2) The Review of European Affairs

Barbara Engels and Mara Grunewald, 'Das Privacy Paradox, Digitalisierung versus Privatsphäre' (*Institut der deutschen Wirtschaft*, 14 August 2017) <https://www.iwkoeln.de/studien/iw-kurzberichte/beitrag/barbara-engels-mara-grunewald-das-privacy-paradox-digitalisierung-versus-privatsphaere-356747.html> accessed 26 May 2021

Bart Van der Sloot, The General Data Protection Regulation in Plain Language (Amsterdam University Press 2020)

Ben Regnard-Weinrabe and Jane Finlayson-Brown, Adapting to a Changing Payments Landscape. in Jelena Madir (ed), Fintech Law and Regulation (Edward Elgar Publishing 2019)

Beuc, 'Beuc's Recommendations to the EDPB on the interplay between the GDPR and PSD2' (*Recommendations*, 11 April 2019) <https://www.beuc.eu/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf> accessed 26 May 2021

Beuc, 'Consumer-friendly Open Banking Access to Consumers' Financial Data by Third Parties' (*Publications*, 20 September 2018) <https://www.beuc.eu/publications/beuc-x-2018-082_consumer-friendly_open_banking.pdf> accessed 26 May 2021

Beuc, 'Guidelines 06/20 on the Interplay on the Second Payment Services Directive and the GDPR BEUC comments on the EDPB public consultation' (*Recommendations*, 15 September 2020) <https://edpb.europa.eu/sites/edpb/files/webform/public_consultation_reply/beuc-x-2020-086_position_paper_on_gdpr.pdf> accessed 26 May 2021

Bird & Bird, 'EN Translation FAQ PSD2 Dutch Data Protection Authority' (*Translation*, 18 October 2018) <https://www.twobirds.com/~/media/pdfs/psd2-dutch-data-protection-authority1.pdf?la=en&hash=55C83B022519F9EFC8C968C7D1EB892F83AD882B> accessed 26 May 2021

Bird & Bird, 'EU: The interplay of PSD2 and GDPR - some select issues' (*DataGuidance*, February 2019) <https://www.twobirds.com/~/media/pdfs/eu-the-interplay-of-psd2-and-gdpr--some-select-issues.pdf> accessed 26 May 2021

Bitkom, 'Bitkom views on EDPB Guidelines 6/2020 on the interplay of the Second Payment Services Directive and the GDPR' (*Position Paper*, 16 September 2020) <https://www.bitkom.org/sites/default/files/2020-09/03_20200916_bitkom-position-on-edpb-guidelines-interplay-psd2-and-gdpr.pdf> accessed 26 May 2021

CBI Globe, 'PSD2 Tech Specifications of the PSD2 services exposed to the Third Party Providers' (*Global Open Banking Ecosystem Wiki*, 2018) <https://www.cbiglobe.com/Wiki/index.php/2._Actors_and_definitions> accessed 26 May 2021

Christina Etteldorf, 'EDPB Publishes Guidelines on Data Processing through Video Devices' (2020) 6 Eur Data Prot L Rev 102

Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub and Thorsten Holz, '(Un)informed Consent: Studying GDPR Consent Notices in the Field' (CCS '19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, 15 November 2019) <https://arxiv.org/pdf/1909.02638.pdf> accessed 26 May 2021

Clearhaus, 'PSD2 - New business opportunities and how to exploit them' (*Clearhaus Blog*, 18 September 2018) <https://www.clearhaus.com/blog/psd2-new-business-opportunities/> accessed 26 May 2021

CMS, 'The interplay between PSD2 and GDPR' (*CMS Law-Now*, 30 April 2020) <https://www.cms-lawnow.com/ealerts/2020/04/the-interplay-between-psd2-and-gdpr> accessed 26 May 2021

Covington & Burling, 'Overlap Between the GDPR and PSD2' (*Inside Privacy*, 16 March 2018) <https://www.insideprivacy.com/financial-institutions/overlap-between-the-gdpr-and-psd2/> accessed 26 May 2021

Deloitte, 'PSD2 and GDPR: An awkward match?' (*Deloitte Legal*, 2018) <https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/legal/deloitte-nl-psd2-and-gdpr-an-awkward-match.pdf> accessed 26 May 2021

Deutsche Bank Global Transaction Banking, 'Are You PSD2-Ready? A Guide to the latest information and sources of support' (*White Paper*, October 2017) <https://cib.db.com/docs_new/PSD2_White_Paper_October_2017.pdf> accessed 26 May 2021

Dilja Helgadottir, 'The Interaction between Directive 2015/2366 (EU) on Payment Services and Regulation (EU) 2016/679 on General Data Protection concerning Third Party Players' (2020) 23 Trinity CL Rev

Ducuing Charlotte, Dutkiewicz Lidia and Miadzvetskaya Yuliya, 'D62 Legal and Ethical Requirements' (*Trusts Trusted Secure Data Sharing Space*, August 2020) <https://www.trusts-data.eu/wp-content/uploads/2020/10/D6.2-Legal-and-Ethical-Requirements.pdf> accessed 26 May 2021

Dutch Data Protection Authority, 'Investigation into the combining of personal data by Google' (*Report*, November 2013) <https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/en_rap_2013-google-privacypolicy.pdf> accessed 26 May 2021

EDPB, 'GDPR PSD2 Guidelines Feedback' (*Public Consultation Reply*, 2020) <https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/gdpr_psd2_guidelines_feedback.pdf> accessed 26 May 2021

Eleni Kosta, 'Consent in European Data Protection Law' [2013] 3 Nijhoff Studies in European Union Law

Eugenia Politou, Efthimios Alepis and Constantinos Patsakis, 'Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions' [2018] 4(1) Journal of Cybersecurity

EuroCommerce, 'EuroCommerce comments in response to the public consultation regarding the Guidelines 06/2020 published by the European Data Protection Board on the interplay of the Second Payment Services Directive and the GDPR version 10' (*Public Consultation Reply*, 13 August 2020) <https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/eurocommerce_response_to_edpb_guidelines_062020_on_the_interplay_of_the_second_payment_services_directive_and_the_gdpr.pdf> accessed 26 May 2021

European Banking Federation, 'EBF response to the European Data Protection Board's consultation on the Guidelines 6/2020 on the interplay of the Second Payment Services Directive and the GDPR' (*Public Consultation Reply*, 16 September 2020) <https://edpb.europa.eu/sites/edpb/files/webform/public_consultation_reply/ebf_042474_-_european_banking_federation_response_edpb_guidelines_psd2-gdpr_.pdf> accessed 26 May 2021

European Commission, 'Payment Services Directive: frequently asked questions' (*Press Corner* 12 January 2018) <https://ec.europa.eu/commission/presscorner/detail/fr/MEMO_15_5793> accessed 26 May 2021

European Data Protection Board, 'Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1' (*Guidelines*, 4 May 2020) <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf> accessed 26 May 2021

European Data Protection Board, 'Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR Version 1.0' (*Guidelines*, 17 July 2020) <https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202006_interplaypsd2andgdpr.pdf> accessed 26 May 2021

European Data Protection Board, 'Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR Version 2.0' (*Guidelines*, 15 December 2020) <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202006_psd2_afterpublicconsultation_en.pdf> accessed 26 May 2021

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 Version 2.0' (*Guidelines*, 8 October 2019) <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf> accessed 26 May 2021

European Data Protection Board, 'Letter regarding the PSD2 directive' (Letter, 5 July 2018) <https://edpb.europa.eu/sites/edpb/files/files/news/psd2_letter_en.pdf> accessed 26 May 2021

European Savings and Retail Banking Group, 'ESBG Response to the EDPB consultation on the Guidelines 06/2020 on the interplay between PSD2 and GDPR' (*Public Consultation Reply*, September 2020) <https://www.wsbi-esbg.org/SiteCollectionDocuments/ESBG-response-EDPB-interplay-psd2-gdpr.pdf> accessed 26 May 2021

European Union Agency for Fundamental Rights and Council Of Europe, 'Handbook on European data protection law' (Handbook, April 2018) <https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition> accessed 26 May 2021

Forbrukerradet, 'Deceived by Design How tech companies use dark patterns to discourage us from exercising our rights to privacy' (*Forbrukerradet*, 27 June 2018) <https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf> accessed 26 May 2021

Frederike Kaltheuner and Elettra Bietti, 'Data is power: Towards additional guidance on profiling and automated decision-making in the GDPR' [2018] 2(2) Journal of Information Rights, Policy and Practice

I. Van ooijen and Helena U. Vrabec, 'Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective' [2018] 42 Journal of Consumer Policy

Information Commissioner's Office, 'What are the conditions for processing?' (*Information Commissioner's Office*) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-conditions-for-processing/#conditions1> accessed 26 May 2021

Irene Kamara and Paul De Hert, 'Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach' [2018] 4(12) Brussels Privacy Hub

IT Governance Privacy Team, EU General Data Protection Regulation (GDPR) An Implementation and Compliance Guide (4th edn, IT Governance Publishing 2020)

Jaimy van der Heijden, 'Privacy in Financial Innovation: a Value Sensitive Design for PSD2' (*TUDelft*, 2017) <https://repository.tudelft.nl/islandora/object/uuid%3Ac558efd2-692e-4b2e-9933-4cc248ccd4b1> accessed 26 May 2021

Johan Peeters, 'Data protection in mobile wallets' (*KU Leuven*, 2019) <https://www.scriptiebank.be/sites/default/files/thesis/2019-10/PEETERS_s0107530_thesis.pdf> accessed 26 May 2021

Krzysztof Trojan, '(Not so) legitimate interest in auxiliary data under PSD2 and GDPR' (*LinkedIn*, 15 May 2017) <https://www.linkedin.com/pulse/so-legitimate-interest-auxiliary-data-under-psd2-gdpr-trojan/> accessed 26 May 2021

Krzysztof Trojan, 'Data of silent parties under the legal mess called PSD2 & GDPR' (*LinkedIn*, 6 May 2019) <https://www.linkedin.com/pulse/data-silent-parties-under-legal-mess-called-psd2-gdpr-trojan/> accessed 26 May 2021

Krzysztof Trojan, 'PSD2 & GDPR regulations on collision course?' (*LinkedIn*, 15 January 2017) <https://www.linkedin.com/pulse/psd2-gdpr-regulations-collission-course-krzysztof-trojan/> accessed 26 May 2021

Latham & Watkins, 'Privacy and Payments: New Draft EU Advice for Financial Institutions' (*JDSupra*, 4 November 2020) <https://www.jdsupra.com/legalnews/privacy-and-payments-new-draft-eu-89021/> accessed 26 May 2021

Leena Rao, 'How Visa Plans To Dominate Mobile Payments, Create The Digital Wallet And More' (*TechCrunch*, 7 August 2011) <https://techcrunch.com/2011/08/07/how-visa-plans-to-dominate-mobile-payments-create-the-digital-wallet-and-more/> accessed 26 May 2021

Letitia Booty, 'The importance of a payments strategy' (*Real Business*, 3 January 2017) <https://realbusiness.co.uk/the-importance-of-a-payments-strategy/> accessed 26 May 2021

Marijana Petrović, 'PSD2 influence on digital banking transformation: Banks' perspective' [2020] 8(4) Journal of Process Management New Technologies

Mark Foulsham, Brian Hitchen and Andrew Denley, GDPR How To Achieve and Maintain Compliance (Routledge 2019)

Mckinsey&Company, 'Data sharing and open banking' (*McKinsey on Payments*, July 2017) <https://www.mckinsey.it/sites/default/files/data-sharing-and-open-banking.pdf> accessed 26 May 2021

Mckinsey&Company, 'PSD2: Taking advantage of open-banking disruption' (*Our Insights*, 24 January 2018) <https://www.mckinsey.com/industries/financial-services/our-insights/psd2-taking-advantage-of-open-banking-disruption> accessed 26 May 2021

Melcom Copeland, 'Millennials choose digital payment methods over cash' (*LinkedIn*, 30 June 2020) <https://www.linkedin.com/pulse/millennials-choose-digital-payment-methods-over-cash-melcom-copeland-/> accessed 26 May 2021

Michael Kosinski, David Stilwell, Thore Graepel, 'Private traits and attributes are predictable from digital records of human behavior' [2013] 110(15) Proceedings of the National Academy of Sciences of the United States of America

Michał Polasika, Agnieszka Huterskaa, Rehan Iftikhar, Štepán Mikula, 'The impact of Payment Services Directive 2 on the PayTech sector development in Europe' [2020] 178 Journal of Economic Behavior & Organization

Michelle Goddard, 'The EU General Data Protection Regulation (GDPR): European regulation that has a global impact' [2017] 59(6) International Journal of Market Research

Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger and Lalana Kagal, 'Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence' (*CHI '20 CHI Conference on Human Factors in Computing Systems*, 30 April 2020) <https://arxiv.org/pdf/2001.02479.pdf> accessed 26 May 2021

Morrison Foerster, 'FinTech Focus: New European Directive on Payment Services (PSD2) Comes into Force' (*Client Alert*, 1 February 2016) <https://media2.mofo.com/documents/160129fintechfocus.pdf> accessed 26 May 2021

Neil Richards and Woodrow Hartzog, 'The Pathologies of Digital Consent' [2019] 96(6) Washington University Law Review

Niels Vandezande, 'EDPB Clarifies the Interplay between GDPR and PSD2' (*Timelex*, 15 February 2021) <https://www.timelex.eu/en/blog/edpb-clarifies-interplay-between-gdpr-and-psd2> accessed 26 May 2021

Niels Vandezande, 'Reconciling Consent in PSD2 and GDPR' (*The Paypers*, 22 March 2019) <https://thepaypers.com/expert-opinion/reconciling-consent-in-psd2-and-gdpr--777976> accessed 26 May 2021

P.T.J. Wolters, B.P.F. Jacobs, 'The security of access to accounts under the PSD2' [2019] 35(1) Computer Law & Security Review

Paul de Hert and Juraj Sajfert, 'Regulating Big Data in and out of the data protection policy field' [2019] 5(3) European Data Protection Law Review

Paul Voigt and Axel von dem Bussche, The EU General Data Protection Regulation (GDPR) A Practical Guide (Springer 2017)

Piotr Kuszewski, 'Impact of the PSD2 directive and strategic use of costly innovation' (*Warsaw School of Economics, Banking Institute*, October 2018) <https://www.researchgate.net/profile/Piotr-Kuszewski-2/publication/330347466_Impact_of_the_PSD2_directive_and_strategic_use_of_costly_innovation/links/5c3a5acc92851c22a370cb43/Impact-of-the-PSD2-directive-and-strategic-use-of-costly-innovation.pdf> accessed 26 May 2021

Pranay Gupta and T. Mandy Tham, Fintech: The New DNA of Financial Services (Walter de Gruyter 2019)

Reinhard Steennot, 'Reduced payer's liability for unauthorized payment transactions under the second Payment Services Directive (PSD2)' [2018] 34(4) Computer Law & Security Review

Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' [2017] 7(2) International Data Privacy Law

Seeunity, 'The main differences between DPD and the GDPR and how to address those moving forward' (*White Paper British Legal Technology Forum*, 2017) <https://britishlegalitforum.com/wp-content/uploads/2017/02/GDPR-Whitepaper-British-Legal-Technology-Forum-2017-Sponsor.pdf> accessed 26 May 2021

Simonetta Vezzoso, Fintech, Access to Data, and the Role of Competition Policy. in V. Bagnoli (ed), Competition and Innovation (São Paulo: Scortecci 2018)

Stefanie Hänold, Profiling and Automated Decision-Making: Legal Implications and Shortcomings. in Corrales and others (eds), Robotics, AI Marcelo Corralesand the Future of Law (Springer 2018) 123-153

Stephen Breen, Karim Ouazzane and Preeti Patel, 'GDPR: Is your consent valid?' [2020] 37(1) Business Information Review

Sue Mclean, Michaela Nebel and Benjamin Slinn, 'European Union: How does PSD2 interplay with the GDPR?' (*Baker Mckenzie Global Compliance News*, 23 October 2020) <https://globalcompliancenews.com/european-union-how-does-psd2-interplay-with-the-gdpr/> accessed 26 May 2021

Terry Hutchinson and Nigel Duncan, 'Defining and Describing What We Do: Doctrinal Legal Research' [October 2012] 17(1) Deakin Law Review

The Privacy First Foundation, 'Feedback on Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR' (*Public Consultation Reply*, 16 September 2020) <https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/20200915_privacy_first_foundation_feedback_on_guidelines_06_2020_v1.pdf> accessed 26 May 2021

Tobias Kugler and Daniel Rücker LL.M., New European General Data Protection Regulation A Practitioner's Guide (Bloomsbury Publishing 2018)

Trix Mulder, 'Health Apps, their Privacy Policies and the GDPR' [2019] University of Groningen Faculty of Law Research Paper No15/2020 European Journal of Law and Technology

Tycho Van Ewijk and Josje Fiolet, 'PSD2 licensing: solving the puzzle of becoming a Third Party Provider' (*Innopay Blog Item*, 21 February 2019) <https://www.innopay.com/en/publications/psd2-becoming-a-third-party-provider> accessed 26 May 2021