European Review of Private Law 1-2022 [73–102] © 2022 Kluwer Law International BV, The Netherlands.

Open Banking: Gordian Legal Knots in the Uncomfortable Cohabitation between the PSD2 and the GDPR

Federico Ferretti*

Abstract: This work analyses problems in the legal framework of Open Banking enabled by the Payment Services Directive 2 (PSD2). It goes through the role of EU law in the regulation of payment services up to their transition towards digitalization and fintech, to show the scale of the changes brought by the PSD2 in a territory unfamiliar to traditional banking. The resulting conflation between banking and the data economy reveal a brand-new market. The normative intersection between the PSD2 and the General Data Protection Regulation (GDPR) expose not only poor coordination but also a growing entanglement of legal knots. The legal inconsistencies, loopholes, and interpretative difficulties are examined to expose operational risks beyond difficulties of legal technicism. A rethinking, or at least a correction, of the European regime of Open Banking is necessary to reconcile the needs of an emerging market and the protection of its users.

Résumé: Cet article analyse les problèmes du cadre juridique de l'Open Banking permis par la PSD2. Il passe par le rôle du droit communautaire dans la régulation des services de paiement jusqu'à leur transition vers la digitalisation et la fintech, pour montrer l'ampleur des changements apportés par la PSD2 dans un territoire peu familier à la banque traditionnelle. L'amalgame qui en résulte entre la banque et l'économie des données révèle un tout nouveau marché. L'intersection normative entre la PSD2 et le RGPD expose non seulement une mauvaise coordination, mais aussi un enchevêtrement croissant de nœuds juridiques. Les incohérences juridiques, les lacunes et les difficultés d'interprétation sont examinées pour exposer les risques opérationnels au-delà des difficultés de technicité juridique. Repenser, ou du moins corriger, le régime européen d'Open Banking est nécessaire pour concilier les besoins d'un marché émergent et la protection de ses utilisateurs.

Zusammenfassung: Diese Arbeit analysiert die Probleme im rechtlichen Rahmen des Open Banking, das durch die PSD 2 ermöglicht wurde. Sie erläutert die Rolle des EU-Rechts bei der Regulierung von Zahlungsdiensten bis hin zu ihrem Übergang in Richtung Digitalisierung und Fintech, und zeigt das Ausmaß der Veränderungen auf, welche die PSD2 in einem – dem traditionellen Bankwesen unbekannten – Gebiet mit sich gebracht hat. Die daraus resultierende Verschmelzung von Bankdienstleistungen und Datenökonomie eröffnet einen völlig neuen Markt. Die normative Überschneidung zwischen der PSD 2 und der DSGVO offenbart nicht nur die mangelnde Abstimmung zwischen diesen Materien, sondern auch eine wachsende Verstrickung rechtlicher

* University of Bologna (Italy). Director of the Jean Monnet Centre of Excellence 'Consumers and SMEs in the Digital Single Market (Digi-ConSME'). Co-funded by the Erasmus+ Programme of the European Union. The final version of this contribution was submitted on 28 September 2021.
E-mail: f.ferretti@unibo.it.

Knoten. Die normativen Inkonsistenzen, Rechtslücken und Auslegungsschwierigkeiten werden untersucht, um operative Risiken jenseits der rechtstechnischen Schwierigkeiten aufzudecken. Ein Umdenken oder zumindest eine Korrektur der europäischen Regelung des Open Banking ist notwendig, um die Bedürfnisse eines Schwellenmarktes mit dem Schutz seiner Nutzer in Einklang zu bringen.

1. Introduction

1. This article identifies and examines problems in the legal framework of EU Open Banking.

2. Under Open Banking, banks allow access and control of customers personal and financial data to third-party service providers. Customers are normally required to grant consent to let the bank allow such access. Third-party providers can then use the customer's shared data. For example, uses may include comparing the customer's accounts and transaction history to a range of financial service options, aggregating data to create marketing profiles, or making new transactions and account changes on the customer's behalf. It can facilitate the process of switching from using one bank's account to another bank's account. It can look at consumers' transaction data to identify the best financial products and services for them, such as a new accounts that would earn a higher interest rate than the current account or a different credit card with a lower interest rate. It could help lenders get a more accurate picture of a consumer's financial situation and risk level to offer more profitable loan terms. It could also help consumers get a more accurate picture of their own finances before taking on debt.

3. Until recently, the term 'open' associated with 'banking' may have sounded like an oxymoron, the rhetorical expedient that uses an ostensible self-contradiction to reveal a paradox. By contrast, the closure of banking relations has long been characterized by the expectation of secrecy and duty of confidentiality on people's financial affairs, colliding with the idea that their dealings and transactions may be open.[1] Likewise, the prospect that banking can be open may rise eyebrows if one

1 These expectations have a long tradition. E.g., see S Guex, 'The Origins of the Swiss Banking Secrecy Law and Its Repercussions for Swiss Federal Policy', 74 *Business History Review* 2000, p (237). Bank secrecy raises complex legal issues that are beyond the scope of this work. Moreover, the legal protection for confidentiality at the disposal of banking customers presents differences from jurisdiction to jurisdiction and legal tradition. To simplify, in common law countries the duty of confidentiality is an implied term in the contractual relationship between a bank and its customer. The obligation does not arise from statute but from precedents. The historic leading case is *Tournier* v. *National Provincial and Union Bank of England* [1924] 1 KB 461 (UK), where it was established that the bank owed its customers a legal, and not merely a moral, duty of confidentiality and could not lawfully disclose to third parties information concerning the customer

considers the growing emphasis of the EU over data protection that has culminated in the adoption of the General Data Protection Regulation ('GDPR').[2]

4. However, as the financial services industry embraces digitalization, traditional banks and other emerging firms use increasing data analysis and profiling to target customers and offer them customised products with personalized pricing. Technological innovation is becoming the key aspect for new models in the provision of finance. Technologically enabled financial innovation in financial services to consumers ('fintech'), capable of making use of large datasets from various unrelated sources ('big data') through artificial intelligence, are the most important facet of late accelerations in digitization that is generating significant interest in retail financial markets for its disruptive effects in the sector.[3]

5. As the data business permeates the global economy, banking and electronic payment services represent a frontier very exposed to competitive pressures from

---

unless disclosure is under compulsion by law, there is a duty to the public to disclose, the interests of the bank require disclosure, or disclosure is made by the express or implied consent of the customer. In civil law countries, by contrast, bank secrecy is not limited to a contractual obligation of the bank to its customers, but the obligation may also arise from legislation, generally in banking law or civil code, or from tradition. This, however, can be overridden by other legislation making an exception to the rule. In some cases, a breach of bank secrecy may constitute a criminal offence, unlike in common law jurisdiction where it gives rise to a civil claim for damages and/or a right to an injunction to prevent further disclosure. See generally D CAMPBELL, *International Bank Secrecy* (London: Sweet & Maxwell 1992). At EU level, see case C-594/16 *Enzo Bucioni* v. *Banca d'Italia* [2018] ECLI:EU:C:2018:717, where the CJEU confirmed that 'it is for the competent authorities and courts to weigh up the interest of the applicant in having the information in question and the interests connected with maintaining the confidentiality of the information covered by the obligation of professional secrecy, before disclosing each piece of confidential information requested'.

2 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, 1–88.

3 European Banking Authority, *Discussion Paper on innovative uses of consumer data by financial institutions* (London, 4 May 2016); The Financial Inclusion Centre, 'FinTech – Beware of the "Geeks" Bearing Gifts?', *A Financial Inclusion Centre Discussion Paper* (January 2018). New fintech services to consumers are developing and expanding significantly in the EU. according to B ZHANG ET AL, *Sustaining Momentum – the 2nd European Alternative Finance Industry Report* (Cambridge: Cambridge University 2016), the total European online alternative finance market grew by 92% to reach EUR 5,431m in 2015 alone. The growth trend is confirmed by subsequent reports for the year 2018. See T ZIEGLER ET AL, *The Global Alternative Finance Market Benchmarking Report* (Cambridge: Cambridge University Press 2020). Since the outbreak of COVID-19, the market has continued to grow globally reporting a year-on-year increase in transaction numbers and volumes of 13%. See CCAF, WORLD BANK and WORLD ECONOMIC FORUM, *The Global Covid-19 FinTech Market Rapid Assessment Report* (Cambridge: University of Cambridge, World Bank Group and the World Economic Forum 2020).

the infant fintech industry. For some time, payments have been characterized by electronic fund transfer systems having gone through the transition from paper payment services (e.g., cash, bank cheques, traveller's cheques, etc.) to electronic means. In the digital economy, payment accounts and data have become an essential source from which services can be provided, not only by banks but also by new market players capable of extracting value from them competitively.

The regulation of payment services at EU level is not new. Over time, it has transformed to serve the developments of the single market and the single currency. Progressively, it has been adapted to the changing market to foster competition and create a level playing field in an environment where consumers are protected from abuses.

6. Lastly, digital innovation and competition have been the shove for the enactment of the late legislative intervention – the Payment Services Directive 2 ('PSD2').[4] On the one hand, the law has modernized the existing regulation of payment transactions and consumer protection to the changing needs brought by digitalization. On the other hand, the PSD2 has opened the market to new services and competitive forces brought by fintech. It has enabled Open Banking, a new banking model that provides third-party financial service providers ('TPP') open access to consumer banking, transactions, and other financial data through the use of interoperable interfaces. Open banking breaks the concentration of information in traditional banks, and allows the networking of accounts and data across a novel sector made of traditional and new service providers. Fresh competition is created for a more efficient provision of existing services, as well as the development of others. Examples are new methods of mobile payments or the delivery of complimentary personalized financial services such as financial advice, loans, insurance products, etc. In so doing, Open Banking reshapes the EU banking industry.

7. At the same time, Open Banking comes with open questions. This is an area where the sectoral PSD2 intersects with the omni-comprehensive GDPR, demanding congruous coordination between the two. However, the combined reading of the two pieces of legislation points to the opposite direction, casting doubts over its proper transposition in the Member States, application by market operators, and safeguards for service users.

It is the aim of this article to analyse problems and interpretative difficulties in the legal framework of Open Banking that lead to legal uncertainty and risks. To reach its goal, this work is construed as follows.

---

4 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, OJ L 337, 23 December 2015, 35–127.

8. Section 2 traces back EU law in the area of payment services to exhibit their transition towards digitalization and fintech, as well as the magnitude of the changes brought by the PSD2 in an unfamiliar territory for traditional banks.

Section 3 examines the provisions of the PSD2 that institute the new market model of Open Banking, introducing the reader to the mingling between banking and the data business.

The normative intersection between the PSD2 to the GDPR concludes the Section.

The inevitable applicability of the GDPR and the provisions relevant to Open Banking are presented in the subsequent section 4, with particular focus on the legitimate bases for accessing and processing account data. These expose a poor coordination with the PSD2.

The entangling of legal meanings in the PSD2 and in the GDPR for the legitimacy of open data access is examined in section 5 to serve as the basis for the analysis of the inconsistencies, loopholes, and interpretative difficulties (depicted as legal knots) evaluated in the following section 6.

Section 7 concludes, pointing to the practical consequences and risks of an unclear legal framework for Open Banking.

2. EU Payment Services Law and the PSD2

9. The PSD2 sets the legal framework of the EU single market in payments. Its objective is to lay down the normative terms for the achievement of integrated retail payments in the Union that are inclusive of existing and new payment services delivered by new market players. Its ambitious goal is to take advantage of innovative technology-enabled solutions (fintech) to generate efficiencies and reach a broader market with more choice and integrated services. At the same time, it pursues transparency and consumer protection.[5]

10. The thrust towards innovation and competition in a market traditionally dominated by the banking sector has motivated the substantial revision and reordering of the regime formerly established by the foregoing Payment Services Directive ('PSD1').[6]

The regulation of payment services finds its roots in the pre-euro currency era where the regulation of payments was addressed mainly in their cross-border element through soft law and negative integration.[7] Only the introduction of the

5 Recital 6, PSD2.

6 Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC, OJ L 319, 5.12.2007, 1-36.

7 A JANCZUK-GORYWODA, 'Evolution of EU Retail Payments Law', 40 *European Law Review* 2015, p 858; G GRIMIGLIANO, 'The Lights and Shadows of the EU law on Payment Transactions', in G Grimigliano (ed.), *Money, Payment Systems and the European Union* (Cambridge: Cambridge

single currency and the setting-up of the Single Euro Payments Area ('SEPA')[8] provided the framework for a hybrid public-private regulatory model of positive integration. This model was engineered by the banking industry – i.e., actors external from the EU institutions – to secure on a private ordering basis the interoperability, rights, and obligations in the inter-bank sphere. EU law was mainly elicited to support this system of self-regulation of the banking industry which interacted with sparse EU legislation relating to areas of payment of circumscribed applicability.[9] It is from the impetus of this industry initiative that the EU legislator adopted the PSD1, which responded to the needs of creating a uniform legal framework for payments across the EU and providing the legislative underpinning for SEPA in the Eurozone.[10]

11. As a first attempt to regulate comprehensively the sector and provide the necessary infrastructure for the perfection of the internal market, the PSD1 specified the allocation of risks among service providers and customers, it regulated a vast array of payment instruments, it enhanced market transparency, and it strengthened competition by harmonising market access requirements, licencing and access to technical infrastructures.[11]

Taking a pro-competition attitude, the PSD1 also enabled the operativity of new end-to-end providers, i.e., new firms in the form of closed platforms that interact digitally with the payer and the payee arranging for the payment transaction within their closed system, with no dependency on other providers such as the firm where the payment account is held.[12]

12. At the same time, the market witnessed the emergence of infant front-end providers, i.e., third-party providers (TPP) of digital services based on the customer's

---

Scholars Publishing 2016), p 25; N VARDI, 'Regulation of Payments after the PSD: Is there still a Role for Domestic Law', in G Grimigliano (ed.) *Money, Payment Systems and the European Union* (Cambridge: Cambridge Scholars Publishing 2016), p 39.

8 European Payments Council, *About SEPA*, https://www.europeanpaymentscouncil.eu/about-sepa (accessed 14 February 2022).

9 For example, see Directive 97/5/EC of the European Parliament and of the Council of 27 January 1997 on cross-border credit transfers, OJ L 43, 14 February 1997, pp 25-30; Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions, OJ L 275, 27 Oct. 2000, pp 39-43. A JANCZUK-GORYWODA, 40 *European Law Review*, p. 858.

10 Recital 1, PSD1.

11 For example, see Art. 10 and 28, PSD1, and Recitals 10, 16, 17, and 42, PSD1. In the literature, see D MAVROMATI, *The Law of Payment Services in the EU: The EC Directive on Payment Services in the Internal Market* (Alphen aan den Rijn: Kluwer Law International 2008).

12 A typical example of end-to-end are e-money schemes such as the one provided by PayPal, a well-known firm operating as a payment processor and online payments system that supports instant online money transfers and serves as an electronic alternative to traditional methods like checks or money orders. Other end-to-end examples are virtual currencies/crypto-assets, or electronic money providers.

payment account held by banks. These services could include payment initiation (Payment Initiation Services or 'PIS')[13] or account information (Account Information Services or 'AIS'),[14] either requiring direct and continuous access to the customer's account and the data therein contained. However, the banks holding the payment account (also known with the alternative terminology of 'Account-Servicing Payment Service Providers – ASPSP') could legitimately refuse access to their infrastructures on grounds of intellectual property protection, security risks, or the permanence of unclear rules over liabilities towards the customers.[15]

Thus, whilst applying in principle to online payment services, the PSD1 ignored both the particular issues and the new developments of the fast-growing digital market.

As a regulatory instrument conceived for payment services offered by traditional incumbents, the legal framework of the PSD1 displayed essentially two limits: i) the de facto low competition in the retail-banking sector characterized by low elasticity of demand, lock-in problems, and exclusivity of payment services linked to the holding of bank accounts[16]; ii) obsolescence towards the reality of fintech acceleration prompted by the great financial and economic crisis of 2008, with new unregulated market players and services operating outside the relationship between the banks and their account holder customers.[17]

---

13 PIS operate as a bridging software between a trader's website and a payer's bank account. Examples of PIS are internet payment gateway providers or mobile wallets that position themselves as interfaces between the payers or the payees and the bank of the payment account.

14 AIS provide a single source of information on the current state of the aggregated finances of payment service users. Examples of AIS are services consolidating in one all the accounts of a person, money management, credit-risk analysis and scoring, financial advice, comparisons, access to targeted offers of other financial services such as credit or insurance, etc. They all analyse a person's transactions on their accounts to provide services based on information.

15 G Colangelo & O Borgogno, 'Data, Innovation and Transatlantic Competition in Finance: The Case of the Access to Account Rule', 31 *European Business Law Review* 2020, p (573).

16 European Commission, 'Commission staff working document Impact Assessment accompanying the Proposal for a directive on payment service in the internal market', SWD (2013) 288 final; European Central Bank, 'Financial Stability Review November 2016 – Special Feature' (2016), https://www.ecb.europa.eu/pub/pdf/fsr/financialstabilityreview201611.en.pdf (accessed 14 February 2022); UK Competition and Market Authority, 'The Retail Banking Market Investigation Ord. 2017' (2017), https://www.gov.uk/government/publications/retail-banking-market-investigation-order-2017 (accessed 14 February 2022); The Netherlands Authority for Consumers and Markets, 'Barriers to entry into the Dutch retail banking sector' (2014), https://www.acm.nl/sites/default/files/old_publication/publicaties/13257_barriers-to-entry-into-the-dutch-retail-banking-sector.pdf (accessed 14 February 2022).

17 European Banking Authority, 'Discussion Paper on the EBA's approach to financial technology (FinTech)', *EBA/DP/2017/02* (4 August 2017); European Banking Authority, 'Discussion Paper on innovative uses of consumer data by financial institutions', *EBA/DP/2016/01* (4 May 2016). In the literature see F Ferretti, 'Consumer Access to Capital in the Age of FinTech and Big Data: The Limits of EU Law', 25 *Maastricht Journal of European and Comparative Law* 2018, p (476); Da

13. The fundamental drawbacks of this market physiognomy were the high margins and profits of the traditional banking industry to the detriment of consumer welfare, and the weak protection of consumers exposed to the legal vacuum of an alternative market of emerging fintech in high demand[18] – all in a legal environment unfavourable to innovation, where the growth of the digital market played almost no role in the policy background.[19]

This historical primer of EU payments law proves functional to signal the shared and familiar context for the traditional banking industry at the level of procedures, technological structures and operational standards within which the PSD1 took shape and operated. Regardless of new competitive pressures, it shaped a market built on a comfort-zone for the banking industry.

At the same time, the historic journey turns out useful to appreciate the rationale and extent of the changes brought by the successor PSD2 in an uncharted territory for the banking industry, to the point that many have branded the resulting EU payment market as a 'revolution'.[20]

3. The PSD2 as the Game Changer: Open Banking and the Data Economy

14. With the PSD2 the EU legislature shifts its policy approach towards digitalization[21] and intervenes substantially in the single payments market.

Broadly, the law befalls on two interrelated levels.

On the one hand – like the PSD1 – it intervenes in the establishment, authorization, and supervision of payment firms and the regulation of payment transactions. Adjusting to the digital market, it enlarges the scope of coverage of the law, it clarifies the extent of consumer rights and service provider obligations, and it reinforces security and authentication requirements.[22]

On the other hand, it recognizes and regulates those TPP emerging from new fintech realties in payment services, bringing them under the same harmonized standards, requirements, and obligations on an equal footing with the traditional payment providers regardless of the business model they

---

Zetzsche, Rp Buckley, Dw Arner & Jn Barberis, 'From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance', *EBI Working Paper Series n. 6,* 2017.

18 For Example, consumer protection concerns related to data protection, money laundering and fraud risks, and the difficulties of proof in establishing authorization in cases of unauthorised payments. See European Commission, *Towards an integrated European market for card, Internet and mobile payments*, COM (2011) 941 final.

19 M Donelly, 'Payments in the digital market: evaluating the contribution of Payment Services Directive II', 32(6) *Computer Law & Security Review* 2016, p (827).

20 I Oliinyk & W Echikson, 'Europe's Payment Revolution', *CEPS Research Report No. 2018/06* (September 2018), recalling industry trade and consumer groups.

21 See in particular, Recital 95 PSD2.

22 See the various provisions of Titles II, III and IV of the PSD2.

apply.[23] In so doing, it opens the market to new services by granting TPP access to the customers' payment accounts held in the banks. The latter must allow TPP authorized by the competent authority in their home Member State[24] access to the data contained in payment accounts in real time on a non-discriminatory basis.[25]

15. Access by TPP is to payment accounts, defined as accounts 'held in the name of one or more payment service users *(...)* used for the execution of payment transactions'.[26] Savings accounts and other non-payment accounts seem therefore excluded from the application of the PSD2. This circumstance also finds support in *Bundeskammer für Arbeiter und Angestellte* where the Court confirmed that accounts which allow for sums deposited without notice and from which payment and withdrawal transactions may be made solely by means of a current account do not come within the concept of payment account.[27]

Access to payment accounts shall take place in a secure way under the guidelines laid down by the European Banking Authority ('EBA').[28]

Any access may occur only upon conclusion of a contractual relationship between the account holder and a TPP for the provision of PIS or AIS, unusually framed as 'explicit consent' by the PSD2, precisely for the purpose of providing those kinds of services that need the data contained in the account.[29]

16. These provisions have given rise to the novel concept of 'Open Banking', a market model that shifts from the money business to the data business and vice versa, where account data are shared with new market players of the fintech industry capable of capturing or creating value around existing un – or under-exploited

23 Recitals 27-33 PSD2.

24 Article 36 PSD2.

25 Articles 64 to 68 PSD2.

26 Article 4(12) PSD2.

27 Case C-191/17, *Bundeskammer für Arbeiter und Angestellte* v. *ING-DiBa Direktbank Austria Niederlassung der ING-DiBa AG* [2018] EU:C:2018:809.

28 Article 95 PSD2, followed by European Banking Authority, *Final draft RTS on SCA and CSC under PSD2 (EBA-RTS-2017-02)* (23 February 2017); Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication C/2017/7782, OJ L 69, 13 March 2018, pp 23-43; European Banking Authority, *Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC (EBA-Op-2018-04)* (13 June 2018).

29 For PIS, see Art. 66 PSD2, stating that 'when the payer gives its explicit consent for a payment to be executed and (*omissis*)'; for AIS, see Art. 67 PSD2 providing that 'the account information service provider shall: (a) provide services only where based on the payment service user's explicit consent; (*omissis*)'.

assets.[30] By law, banks have to share the data they control for the benefit of fintech firms for the creation of new products and provision of new services.

Payment accounts contain a vast amount of data for analysis, from financial data relating to incoming and outgoing transactions, balances, preferences, patterns, dependencies, behaviours, aspects of the social life, etc. They are an exceptional tool for consumer profiling and predictive purposes, at the same time revealing behavioural biases and vulnerabilities in all aspects of life, especially if integrated with data from other unrelated sources (here comes the concept of 'big data') and processed by algorithms powered by artificial intelligence technologies.

17. In the Open Banking model, therefore, the new paradigm reflects the unbundling of the provision of financial services in more market segments, and the disintermediation of the banking industry. The latter, however, becomes key in the fintech ecosystem, assuming a new form of necessary forced intermediation between the service user (the account holder) and the fintech TTP. Under the PSD2, TPP are subject to conduct of business restrictions and requirements that do not allow them to hold the payer's funds in connection with the service, store sensitive payment data of the service user, or process data beyond that necessary to provide the service.[31] The services can only exist via the traditional providers, creating a new market structure where the latter become digital platforms for the distribution of financial services. They facilitate and create a dependency for the contractual interactions of two or more market agents, but without having any contractual relationship with one of them (the TPP), at the same time allowing the other one (the customers) to continue the fruition of their own services. Schematising, Party A (the customer) can enter into a contract with Party B (TPP) only via the intermediation of Party C (bank), where Party A and Party C have a contract for the payment account (and still can have future contracts for other services), but where Party B and Party C have no contractual relationship (on the contrary, they may compete).

The Open Banking environment thus generates indirect network effects, making possible bilateral ventures otherwise not attainable with other means,[32] at the same time producing new dependencies.

---

30 H CHESBROUGH, 'Business Model Innovation: Opportunities and Barriers', 43 *Long Range Planning* 2010, p (354).

31 Article 66(3) PSD2.

32 M ZACHARIADIS & P OZCAN, 'The API economy and digital transformation in financial services: the case of Open Banking', *SWIFT Institute Working Paper No. 2016–001*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2975199 (accessed 14 February 2022); D MILANESI, 'A new banking paradigm: the state of Open Banking in Europe, the United Kingdom and the United States', *TTLF Working Papers No. 29, Stanford-Vienna Transatlantic Technology Law Forum* (2017), from, https://law.stanford.edu/publications/a-new-banking-paradigm-the-state-of-open-banking-in-europe-the-united-kingdom-and-the-united-states/ (accessed 14 February 2022).

18. In this way, the Open Banking market structure moves towards a confluence between traditional financial service providers becoming technological firms (but still on the money business) and technological firms entering the financial services market, where the latter may be infant fintech businesses or established technological giants already dominating the data service market (the so-called 'Tech-Fin' or 'Big-Tech').[33]

From this angle, the PSD2 is the law that encourages an expanding use of personal data and enables a vast array of newcomers to access increasingly more data sources for novel purposes.

19. However, more data means more data protection concerns, especially given the nature of the account data and the conclusions that can be drawn from their processing. Misuses or abuses can have severe consequences for individuals. In this respect, the PSD2 contains no direct controls to protect consumers. All it does is to grant payment providers the permission to process personal data when necessary to safeguard the prevention, investigation, and detection of payment fraud. Otherwise, it refers to the application of data protection legislation,[34] with the caveat that TPP can only access and process data necessary for the provision of their services with the 'explicit consent' of the payment service user.[35]

4. Open Banking and the GDPR Under the Same Legal Roof

20. Account data processing triggers the application of the GDPR, thus overlapping with the PSD2.

As a EU Regulation, the GDPR has direct effect designed to eliminate risks of national particularities and diversity of practices, which would frustrate the goal of achieving uniformity.

---

33 Zetzsche et al, *EBI Working Paper Series n. 6,* 2017; F di porto & G Ghidini, 'I access your data, you access mine. Requiring data reciprocity in payment services', 51 *IIC - International Review of Intellectual Property and Competition Law* 2020, p (307); RM Stulz, 'FinTech, BigTech, and the future of banks', *NBER Working Paper No. 26312* (2019), https://www.nber.org/papers/w26312 (accessed 14 February 2022). For example, note that Google has secured an e-money license after Lithuania granted authorization. The license enables the company to process payments, issue e-money, and handle electronic money wallets. It gives permission to operate across the EU via the passporting rights system. Likewise, Facebook and Amazon obtained licenses in Ireland and Luxembourg. See M Seputyte & J Kahn, 'Google Payment Expands With E-Money License From Lithuania', *Bloomberg* (21 December 2018), https://www.bloomberg.com/news/articles/2018-12-21/google-payment-expands-with-e-money-license-from-lithuania (accessed 14 February 2022).

34 Article 94(1) PSD2.

35 Article 94(2) PSD2.

Prima facie the principle purposes of the PSD2 and the GDPR are in contrast to one another, with the former endorsing the stimulus for expansive data sharing, whilst the latter protecting and restricting the freedom to share them.

In the absence of derogations, it is in light of the significance of data protection legislation that one should read the processing of big data in financial services, including account data in Open Banking.[36]

21. The legal foundation of data protection lies in Article 16 TFEU elevating it to a provision of general application under Title II alongside other fundamental principles of the EU. Equally, Article 8 of the Charter of Fundamental Rights of the EU recognizes the protection of personal data as an autonomous fundamental right distinguished from that of 'privacy' of Article 7 of the Charter.

Data protection is a complex and multifaceted concept both from a societal and a legal point of view. Traditionally, its primary objective has been identified with the protection of personal privacy within the context of processing operations involving personal data. The considerable body of literature and many debates on privacy exemplify the difficulty in delineating what remains a broad and at times ambiguous concept,[37] but they also help to set the basis for distinguishing 'data protection' from 'privacy'. At least under EU law, the two have become distinct, yet complementary, fundamental legal rights which derive their normative force from values that – although at times coincidental and interacting in many ways – may be conceptualized independently. While privacy law stem from the need to protect the legitimate opacity of the individual through prohibitive measures, data protection law formulates the conditions under which information processing is legitimate by forcing the transparency of the processing of the data, thus enabling their full control by the data subjects where the processing is not authorized by the law itself as necessary for societal reasons. In short, data protection law focuses on the

---

36 See also Recital 90 PSD2.

37 For example, S Warren & L Brandeis, 'The Right to Privacy', 4 *Harvard Law Review* 1890, p (193); EJ BLOUSTEIN, 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser', 39 *New York University Law Review* 1964, p (962); S Stromholm, *Right of Privacy and Rights of the Personality* (Stockholm: Norstedt 1967); A Westin, *Privacy and Freedom* (New York: Atheneum 1967); C Fried, *An Anatomy of Values* (Cambridge: Harvard University Press 1970); J Rachels, 'Why Privacy is Important', 4 *Philosophy and Public Affairs* 1975, p (323); J Thomson, 'The Right to Privacy', 4 *Philosophy and Public Affairs* 1975, p (295); T Scanlon, 'Thomson on Privacy', 4 *Philosophy and Public Affairs* 1975, p (323); R GERSTEIN, 'Intimacy and Privacy', 89 *Ethics* 1978, p (76); R Gavison, 'Privacy and the Limits of the Law', 89 *Yale Law Journal* 1980,p (421); R Posner, *The Economics of Justice* (Cambridge: Harvard University Press, 1981); W Parent, 'Privacy, Morality and the Law', 12 *Philosophy and Public Affairs* 1983, 269-288; J Inness, *Privacy, Intimacy, and Isolation* (Oxford: Oxford University Press 1992); J Johnson, 'Constitutional Privacy', 13 *Law and Philosophy* 1994,161-193; J Decew, *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology* (New York: Cornell University Press, 1997); A Moore, 'Intangible Property: Privacy, Power, and Information Control', 35 *American Philosophical Quarterly* 1998, p (365).

activities of the processors and their accountability, thus regulating an accepted exercise of power.[38] Both privacy and data protection regimes (i.e., seclusion and legitimate opacity, and inclusion and participation) represent a bundle of legal protections to pursue the common goal of a free and democratic society where its members develop their personality freely and autonomously through individual reflexive self-determination. Granting to individuals control over their data is not only a tool to allow them control over the *persona* they project in society free from unreasonable or unjustified associations, manipulations, distortions, misrepresentations, simplifications, stereotypisations, discriminations, classifications, alterations, or constraints. It is also a fundamental value pertaining to humans to keep and develop their personality in a manner that allows them to fully participate in society without having to conform thoughts, beliefs, behaviours, or preferences to those of the majority or those set from above by the industry for commercial interests.[39]

Against this background, the rights conferred by data protection law become participatory rights of self-determination. The GDPR formulates the conditions under which information processing is legitimate.[40]

22. Among the many aspects regulated by the GDPR, some require attention for their overlap with the PSD2.

Within the respect of the key principles of purpose limitation and data minimization,[41] the GDPR sets the legal requirements for a valid basis for legitimate data processing. A data controller must be able to provide a basis for the processing activity only if it can claim that the processing relies on one of the criteria established by the law. The set of criteria is exhaustive, so that if a data controller is unable to rely on one of them the processing is unlawful. For this purpose, the law distinguishes between data of sensitive or non-sensitive nature. The special categories of sensitive data are those revealing racial or ethnic origin,

38 SG Davis, 'Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity', in PE Agre and M Rotenberg (eds), *Technology and Privacy: The New Landscape* (Cambridge: MIT Press 1997), p (143); P De Hert & S Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalization in Action', in S Gutwirth et al (eds), *Reinventing Data Protection?* (Amsterdam: Springer 2009), p (3); A Rouvroy & Y Poullet, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy', in S Gutwirth et al (eds), *Reinventing Data Protection?* (Amsterdam: Springer 2009), p (45).

39 A Rouvroy & Y Poullet, in *Reinventing Data Protection?* p (45).

40 P. De Hert & S. Gutwirth, in *Reinventing Data Protection?* p (3).

41 See Art. 5 GDPR, in particular where it states 'personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes' (purpose limitation) and 'personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed' (data minimization).

political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.[42]

23. For data of non-sensitive nature, the legal bases for a legitimate processing are expressed in Article 6(1) GDPR:

(a) the data subject has (unambiguously) given consent;
(b) the data processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering into a contract;
(c) the data processing is necessary for compliance with a legal obligation of the data controller;
(d) the data processing is necessary in order to protect the vital interests of the data subject;
(e) the data processing is necessary for the performance of a task in the public interest or in the exercise of official authority;
(f) the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party.

24. By contrast, where the processing of personal data is of sensitive nature, the legal bases change. Under Article 9(2) GDPR, the processing of these data is permitted only:

(a) if the data subjects have given their 'explicit consent';
(b) the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law;
(c) the processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent;
(d) the processing is carried out in the course of legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim;
(e) the processing relates to personal data which are manifestly made public by the data subject;
(f) the processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
(g) the processing is necessary for reasons of substantial public interest;
(h) the processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee,

42 Article 9(1) GDPR.

medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services;

(i) the processing is necessary for reasons of public interest in the area of public health;

(j) the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

25. In the case at study – especially for the provision of AIS – fintech solutions make an extensive use of profiling techniques which constitute their business model. Where profiling occurs, the GDPR requires for an additional layer of control. It postulates that individuals have the right not to be subject to a decision based solely on automated processing to evaluate certain personal aspects of a person.[43] Profiling can be used if it is necessary for contractual necessity, it is authorized by EU or national law, or it is based on the data subject's 'explicit consent'.

In the case of automated decisions based on 'explicit consent' or contractual fulfilment, controllers must respect a right for data subjects to obtain human intervention, express their point of view, and contest decisions. In any event, automated decisions cannot be based on the sensitive data of Article 9(1) GDPR.[44]

Last but not least, an innovation of the GDPR to empower data subjects is the right to data portability, i.e., their right to transmit or have the data transmitted to another controller where the processing is based on 'consent' or on a contract.[45]

From these norms of the GDPR related to the PSD2, it can be argued that in principle the two laws are not necessarily in conflict – as it may have prima facie appeared – since they both aim to grant transparency and user control.

26. However, inconsistencies arise from their necessary cohabitation and coordination, starting from the legal basis legitimising the use of account data and the ensuing rights and obligations of the parties.

The leitmotiv of 'consent' in the two laws, either in the form of being unqualified or explicit, has triggered discussions within Member States and stakeholders regarding the correct implementation of the PSD2, especially in relation to measures concerning the protection of personal data.[46] In turn, it prompts a cascade of burning issues of practical relevance for businesses and legal interpreters.

---

43 Article 4(4) GDPR.

44 Article 22 GDPR.

45 Article 20 GDPR.

46 See e.g., European Data Protection Board, *Letter to Sophie in 't Veld, Member of the European Parliament* (Brussels, 5 July 2018); BEUC, *Consumer-Friendly Open Banking* (Brussels, 20 September 2018); European Banking Federation, *European Banking Federation's comments on the Art. 29 Working Party guidelines on consent* (wp259) (Brussels, 23 January 2018).

5. Entangling Legal Meanings: The Knot of 'Consent'

5.1. 'Consent' in the PSD2

27. The PSD2 titles Chapter 4 'data protection', albeit composed of only one article subdivided in two limbs (Article 94 PSD2). The first limb makes an express referral to the application of the GDPR predecessor, Directive 95/46/EC.[47] This reference is certainly not a problem, since Article 94 GDPR makes it clear that any references to the repealed Directive 95/46/EC shall be construed as references to the GDPR.

28. At the same time, Article 94(2) PSD2 stipulates that 'payment service providers shall only *access, process and retain* personal data necessary for the provision of their payment services, with the *explicit consent* of the payment service user' (emphasis added).

In so doing, the PSD2 seems to qualify the basis for processing account data.

The requirement of the PSD2 of 'explicit consent' overlaps with the terms 'consent' and 'explicit consent' of the provisions of the GDPR,[48] casting the doubt whether they have the same meanings in the two laws. It also rises uncertainties over the need of the PSD2 to reproduce the term with the extra qualification of 'explicit'.

29. Moreover, other provisions of the PSD2 make reference to 'consent' as regards authorization of a payment transaction. Under Article 64 PSD2 'a payment transaction is considered to be authorized only if the payer has given *consent to execute the payment transaction*' (emphasis added). This simple 'consent' to authorize a payment is later referred as 'explicit consent' in Articles 65 and 66 PSD2 when specifying the actions that banks need to perform to ensure the payer's right to use a PIS.[49] Equally, AIS 'shall provide services only where based on the payment service user's *explicit consent*'.[50] (emphasis added).

30. Arguably, the 'consent' and 'explicit consent' referred in these provisions do not relate to access or processing of data but to the authorization of a PIS or AIS service. It signifies contractual agreement albeit equivocally normed in the 'simple' versus 'explicit' dichotomy in the realm of contract law. Here, too, the PSD2 casts shadows over the contractual form and implementation in the legal systems of the Member States, and its compatibility with national contract law. As interesting this is, this legal deviation is beyond the scope of this analysis.

---

47 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, 23 November 1995, 31-50.

48 Respectively, Art. 6(1)(a) GDPR and Art. 9(1) GDPR.

49 Article 66 PSD2.

50 Article 67 PSD2.

For what matters in this work, the use of the same terms within the PSD2 does not signify the same meaning, and the norms are not operating on the same ground: Articles 64–67 PSD2 refer to contractual agreement, and Article 94(2) PSD2 to data processing.

It remains to be seen if data processing 'explicit consent' under the PSD2 has the same meaning and should be interpreted as in the GDPR.

5.2. 'Consent' in the GDPR

31. Consent under the GDPR is probably one of the most complicated lawful bases to implement,[51] and the addition of the PSD2 does not help.

As conceived by data protection law, it is a key element that permits the processing of personal data by data controllers that would otherwise be forbidden. When a data subject gives valid consent, data controllers are released from the restrictions provided by law. The processing becomes lawful from the moment consent is unambiguously expressed.

By law, consent shall be granular and distinguished from declarations concerning other matters (Article 7[2] GDPR). It must be 'freely given, specific, informed and unambiguous' (Article 4[11] GDPR). Correspondingly, the law mandates 'affirmative consent' requiring the data subject to signal agreement by 'a statement or a clear affirmative action' (Article 4[11] GDPR). At the same time, as seen it continues to distinguish between 'explicit consent' if the data in question is sensitive personal data, and 'unambiguous' consent for all the other personal data (Article 6 GDPR combined with Article 4 GDPR).

32. The issue of what standard of consent should apply under the GDPR was the subject-matter of intense debates and negotiations at the lengthy proposal stage of the GDPR. The legislative history of the GDPR demonstrates that the final drafting was intentional in maintaining different qualifiers of consent and making the express distinction between 'unambiguous' and 'explicit' consent depending on the ordinary or sensitive nature of the data. To the extent that the GDPR makes clear that 'explicit' and 'unambiguous' consent is not the same, the boundaries of what is 'unambiguous' remain unclear, with the additional complication that the law states that it must be given by an 'affirmative action'. For example, it is unclear

51 Exemplified by the many interpretative interventions of the supervisory authority for data protection, the European Data Protection Board – 'EDPB' (formerly, Art. 29 Working Party): Art. 29 Working Party, *Opinion 15/2011 on the Definition of Consent*, 01197/11/ENWP187 (13 July 2011); Art. 29 Working Party, *Art. 29 Working Party Guidelines on consent under Regulation 2016/679* (Adopted on 28 November 2017, and last Revised and adopted on 10 April 2018); European Data Protection Board, *Guidelines 05/2020 on consent under Regulation 2016/679* (Brussels, 4 May 2020).

to what extent implied consent remains possible.[52] While the GDPR provides that 'silence, pre-ticked boxes or inactivity should not *(omissis)* constitute consent' (Recital 32 GDPR), it also states that consent can be given through 'another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data' (Recital 32 GDPR). In any event, controllers must be able to demonstrate that data subjects have consented (Article 7 GDPR).

33. The distinction between 'explicit' and 'unambiguous' consent matters in practice as long as different models of consent translate into very different engineered solutions within products and services, especially online. In the 'explicit' consent model an opt-in tick box or declaratory consent statement will be necessary. However, in the 'unambiguous' consent model that dominates commercial services a prominent notice together with an 'affirmative action' may suffice to obtain an implied consent without the need for an opt-in box or declaratory consent.

In the consumer protection realm, this can make a substantial difference in terms of the way consent is collected from consumers or the interface presented to them, and the way in which they interact with the product or service provider. Ultimately, this also makes a difference as to the real knowledge and control that consumers may have on the processing of their personal data, and the uses that can be made with the data. Consent must rely on transparency and an 'affirmative action' (whether explicitly given or inferred through conduct) but how this translates in practice remains vague, especially within the complexities of financial transactions.

34. For completeness, it has to be added that the GDPR establishes explicitly that data subjects have a subsequent right of withdrawal of consent. The data subject may withdraw consent at any time and this must be as practical as granting consent. Clearly, however, the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal (Article 7(3) GDPR).

35. The complexities of the fintech business models, data-collection practices, vendor-customer relationships, or technological applications may make it impossible for consumers to understand what they are consenting. Equally, these complexities may in practice render consumers unable to freely and actively decide to accept the consequences of consenting to data processing, particularly when faced with a perceived immediate economic benefit.

---

52 In this regard, the latest 2020 opinion of the EDPB does not help much, limiting their interpretation to 'all presumed consents that were based on a more implied form of action by the data subject (e.g., a pre-ticked opt-in box) will also not be apt to the GDPR standard of consent'. See European Data Protection Board, *Guidelines 05/2020 on consent under Regulation 2016/679*, at 20.

Despite the apparently robust legal protection afforded to data subjects, consent may be obtained by a number of methods and has proved problematic as a basis for data processing because it can be easily abused, confused, or conflated.[53]

36. Treating consent as a transactional moment using standard form agreements may constitute a mechanical or perfunctory means of obtaining overarching consent for data processing.[54]

For instance, the condition of consent in the provision of financial services is a common yet elusive method of obtaining consumer consent. Consent becomes associated with the legal paradigm of contract. At the same time, the contractual relationship is a situation with a typical imbalance between the consumer and the business counterpart. Consumers are presented with no much choice but to abide by the lenders' terms if they wish to receive a service. In practice, the consumer's consent becomes either mandatory or assumed. The fintech business models rely on data exploitation. As seen above, the PSD2 names contractual consent and data processing consent in the same way ('explicit consent'), albeit in two different Articles and contexts.[55]

37. The legal mechanism of consent becomes more confused where the GDPR further intends to protect data subjects stating that 'consent' should not be regarded as freely given if they are 'unable to refuse or withdraw consent without detriment' (Recital 42 GDPR) or 'where there is a clear imbalance between the data subject and the controller' (Recital 43 GDPR). Recent studies show that in order to gain specific transactional and personal advantages most consumers willingly consent or disclose information about themselves and their social activities without thinking about the effects of their disclosures, thus making consent de facto ineffective. Yet very few consumers understand the significant consequences of this trade-off, including how data controllers use their personal data. Not only data processing can be very complex and non-transparent, but most consumers lack both the information and the skills to properly evaluate their own decision to consent.[56]

---

53 In theory, consent that does not meet the requirements of the law or is vitiated should be regarded as void, and should invalidate all data processing *ex tunc*—from the outset. See Art. 29 Working Party, *Art. 29 Working Party Guidelines on consent under Regulation 2016/679.* For specific literature see e.g., A Mantelero, 'The future of consumer data protection in the EU. Re-thinking the "notice and consent" paradigm in the new era of predictive analytics' 30 *Computer Law and Security Review* 2014, p (643); E Kosta, *Consent in European Data Protection Law* (Leiden: Martinus Nijhoff 2013).

54 R Brownsword, 'Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality', in S Gutwirth et al. (eds) *Reinventing Data Protection?* (Amsterdam: Springer 2009), p (83).

55 Articles 64–67 PSD2 and Art. 94 PSD2.

56 F Pasquale, *The Black Box Society* (Cambridge: Harvard University Press 2015); Sr Peppet, 'Unraveling Privacy: The Personal Prospectus and the Threat of a Full Disclosure Future', 105

In the end, it remains unclear how the aspirations of the law are to be effectively reconciled with the reality of fintech.

6. Growing Intricate Legal Knots

6.1. The Legal Basis for Account Data Processing

38. The picture portrayed so far starts to become knotty when establishing the appropriate legal basis for data processing.

Prima facie, the processing of account data seems to find its legal basis in the contractual necessity under Article 6(1)(b) GDPR. Under the GDPR, TPP would not even need the consent of the customer.

Financial data are not considered sensitive data *per se.* The financial status of a person is not contemplated as a special category ex Article 9(1) GDPR. In principle, PIS or AIS are not services that make use of sensitive data or provide a service of sensitive nature:

39. This is the view endorsed by the European Data Protection Board ('EDPB') - the European Authority in charge of the supervision and consistent application of the GDPR – in a letter addressed to a European Member of Parliament (i.e., not laid down in the form of official guidelines). At the same time, the EDPB considers the 'explicit consent' of Article 94(2) PSD2 as contractual consent, thus not interfering with contractual necessity. According to the Authority:

> article 94(2) of PSD2 should be interpreted in the sense that when entering a contract with a payment service provider under PSD2, data subjects must be made fully aware of the purposes for which their personal data will be processed and have to explicitly agree to these clauses. *Such clauses should be clearly distinguishable from the other matters dealt with in the contract* and would need to be *explicitly accepted by the data subject.* The concept of explicit consent under Article 94(2) of PSD2 is therefore *an additional requirement of a contractual nature and is therefore not the same as (explicit) consent under the GDPR*[57] (emphasis added).

40. Arguably, the above interpretation is not convincing and needs rejection.

Northwestern University Law Review 2011, p (1153); M Borghi, F Ferretti & S Karapapa, 'Online Data Processing Consent Under EU Law: A Theoretical Framework and Empirical Evidence from the UK', 21 *International Journal of Law and Information Technology* 2013, p (109); A Edgar, A Whitley A and R Pujadas, 'Report on a study of how consumers currently consent to share their financial data with a third party', *Report provided for the Financial Services Consumer Panel* (London, 19 April 2018), https://www.fs-cp.org.uk/sites/default/files/fscp_report_on_how_consumers_currently_consent_to_share_their_data.pdf (accessed 14 February 2022).

57 European Data Protection Board, *Letter to Sophie in 't Veld.*

Holding the 'explicit consent' as contractual would not explain why it has been expressed in the norm addressing data protection under a separate dedicated heading of the PSD2. In addition, this interpretation not only would dispute the letter of the norm where it affirms that 'explicit consent' is required for the access, processing and retention only to the extent necessary for the provision of the services, but it would also contradict the contractual meaning of 'consent' used in Articles 64-67 PSD2. As seen, these are norms that do not operate on the same ground as Article 94 PSD2 (see section 5.1. above).

41. Worse, however, in so interpreting the EDPB seems to operate outside its mandate. The reading of the EDPB provides an original interpretation over contract law, not data protection. The influence of EU law in the area of contract law theory is already a complex area.[58] Introducing an additional layer of reinforced, separate, and 'explicit' consent (i.e., agreement) into the legal systems of several Member States would not come without added controversy. It would question the legality of the outreach of EU law in a sphere of national competence. Moreover, it is far from clear what is meant by 'an additional requirement of a contractual nature'. Surely, it is not the ambition of the EDPB to harmonize a contractual concept alien to a large number of private law systems of the Member States. A contractual concept, moreover, that would not bring a uniform implementation, interpretation, and application of the law in the Member States contrary to the EDPB's own remit.

In any case, it is worth insisting that it would not be a matter for the competence of the EDPB to determine. If anything, this begs an additional issue of supervisory competences over the PSD2 and the coordination between the EBA and the EDPB, especially since the EDPB does not qualify the matter as a data protection notion falling under the GDPR. Supervision is another overlapping area demanding attention but beyond the scope of this investigation.

Altogether, the EDPB attempt to close a leak would have the undesirable effect of opening a flood.

6.2. Sensitive versus Non-sensitive Data

42. In the attempt to establish the legal basis of account data processing, it must be noted that in certain situations payment data may reveal aspects of racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life, or sexual orientation of a person. Examples are payments to trade union, political, or religious associations. Payments may disclose

58 For example, see J Rutgers & P Sirena (eds), *Rules and Principles in European Contract Law* (Oxford: Intersentia 2015); L Miller, *The Emergence of EU Contract Law – Exploring Europeanization* (Oxford: Oxford University Press 2011).

sexual preferences or orientations. Medical expenses disclose many sensitive personal spheres. Illustrations of the like could be several.

43. Therefore, account data may well qualify as sensitive.

In the processing of sensitive data, however, Article 9(2) GDPR does not recognize the contractual necessity as an exception to the general prohibition to process special categories of data ex Article 9(1) GDPR. Instead, 'explicit consent' applies.

This observation challenges the legal basis that should be really used to process payment account data. Depending upon the circumstances, such a processing may be considered as either non-sensitive or sensitive. In certain situations, data can be processed on contractual grounds with no consent, in others on the 'explicit consent' by the data subject.

44. The PSD2 points to 'explicit consent' regardless of the distinction, begging the question of whether Article 94(2) of the PSD2 is *lex specialis* vis-à-vis the GDPR, meaning in the positive that 'explicit consent' should always be the legal basis for account data processing regardless of the nature of the data. By contrast, in the negative it would mean that TPP would have to comply with the requirements of both the PSD2 and the GDPR, or decide to use the PSD2 as prevailing over the GDPR *ad abundantiam.* In the absence of official interpretation, the referral of Recital 90 PSD2 to the necessary implementation of the articles of the PSD2 in accordance with – inter alia – data protection law[59] seems to exclude the *lex specialis* versus *lex generalis* relationship.[60]

45. Accepting that the PSD2 is not *lex specialis* and in the impossibility to practically separate the processing of sensitive and non-sensitive data, arguably 'explicit consent' should be the safe legal ground for account data processing under

59 According to Recital 90 PSD2, the Directive 'respects the fundamental rights and observes the principles recognized by the Charter of Fundamental Rights of the European Union, including the right to respect for private and family life, the right to protection of personal data, the freedom to conduct a business, the right to an effective remedy and the right not to be tried or punished twice in criminal proceedings for the same offence. This Directive must be implemented in accordance with those rights and principles'.

60 This question has puzzled also the Dutch Data Protection Authority. Initially, the Dutch authority took the view in a letter addressed to the Dutch Minister of Finance that the PSD2 is *lex specialis* vis-a-vis the GDPR. See letter of the Data Protection Authority addressed to the Ministry of Finance dated 20 December 2017, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/20171220_advies_aan_min_fin_implementatiebesluit_psd2.pdf (accessed 14 February 2022). Later, the same Authority took the opposite view that the PSD2 is not *lex specialis* versus the GDPR. See the Dutch Data Protection Authority on the interplay of the PSD2 and the GDPR of 18 October 2018, https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-geeft-betaaldienstverleners-uit leg-over-uitdrukkelijke-toestemming-psd2#subtopic-6852 (accessed 14 February 2022).

the GDPR. Thus, the *ad abundantiam* requirement of 'explicit consent' of the PSD2 should be held up to the same standard as in the GDPR.

This construal would also conform with the 'explicit consent' requirement for profiling under Article 22 GDPR.

However, this interpretation would contravene the Commission's Regulatory Technical Standards on Strong Consumer Authentication and Common and Secure Communication ('RTS'),[61] according to which banks shall provide AIS with information provided that sensitive payment data are not included,[62] thus indicating that they cannot be processed even with the 'explicit consent' of the account holder. That said, it remains unclear how technical standards may ever be in discontinuity with the GDPR.

Legal certainty via the official intervention of the Court of Justice of the EU (CJEU) or the EU legislator is essential.

6.3. Data Portability and Non-payment Accounts

46. All the snags identified so far need to be contextualized with the right of data portability of the GDPR, according to which an account holder should have the right to have her data transmitted to another controller as long as the processing is based on 'consent' or on a 'contract' as in the case at hand. A data subject may well continue to use the bank's services after a data portability operation, since this would not trigger the erasure of the data.[63] Under Article 20(1) GDPR data portability is limited to data which the data subject has provided herself to the data controller. The portability of data includes the observation of the activities of users but excludes their analysis.

47. Even in this case, whether the relationship between the PSD2 and the GDPR is that of *lex specialis* versus *lex generalis*, or the nature of payment account data, would make a practical difference. It would make the difference between having the chance of applying Article 20 GDPR or not.

Consistently with the view above expressed, coupled with the impracticability of determining the sensitive nature of account data or else, such data should not be treated as falling under the data portability right of the GDPR.

This deduction may seem trivial since it would carry no practical consequence for account data processing. TPP do not need Article 20 GDPR but Articles 64–67 PSD2 to access the data.

---

61 Commission Delegated Regulation (EU) 2018/389 of 27 November 2017.

62 See Art. 36(1)(a) RTS, according to which banks 'shall provide account information service providers with the same information from designated payment accounts and associated payment transactions made available to the payment service user when directly requesting access to the account information, *provided that this information does not include sensitive payment data*' (emphasis added).

63 Article 29 Working Party, Guidelines on the right to data portability (Adopted on 13 December 2016, last Revised and adopted on 5 April 2017).

However, it could become relevant for the supplementary processing of non-payment accounts, since the PSD2 grants no legal right of access to these accounts.[64] Making use of Article 20 GDPR and the 'consent' or 'contractual necessity' it requires, arguably a request to access non-payment accounts could in principle be treated as a data portability right as long as the account holder requests this formally. This view seems endorsed by the predecessor of the EDPB where in its Guidelines on Data Portability it includes the following example:

> if the data subject's request aims specifically at providing access to his banking account history to an account information service provider, for the purposes stated in the Payment Services Directive 2 (PSD2) such access should be granted according to the provisions of this directive[65]

48. Yet, as seen above, the above reasoning about the possible sensitive nature of payment account data may create an obstacle. At the same time, it has to be considered that savings or other non-payments accounts contain no payment data, thus shedding light over the possibility of allowing TPP access to these accounts, not under the PSD2 but under the GDPR.

In any event, legal certainty would be desirable even in this overlapping area of the two laws.

6.4. Account Data, Big Data, and Reuse

49. The processing of account data by TPP becomes increasingly complicated by the use of big data for the provision of services. This is especially the case for AIS that make of profiling their business model.

Here, the data subject should provide 'consent' for the use of data from other sources, e.g., social media or other browsing data. Since 'consent' must be granular,[66] this begs the practical issue of how many layers and forms of consent TPP need to ask for the provision of services. First, there is the contractual 'explicit consent' of Articles 64–67 PSD2, then the 'explicit consent' (or no consent at all if the view of the EDPB is taken) for processing account data, and finally 'unambiguous consent' for processing and aggregating data from other sources. The practical implementation of the legal requirements may be overly burdensome. At the same time, consumer protection cannot be lowered.

50. The problem is that, even in case of non-sensitive account data processing, their combination with big data may disclose sensitive areas of personal lives. The

64 See s. 3 above.

65 Article 29 WORKING PARTY, Guidelines on the right to data portability, at 8 (fn 15).

66 Article 7(2) GDPR.

borderline between data processing revealing sensitive or non-sensitive information becomes blurred.

In principle, moreover, under the GDPR TPP could reuse or recycle personal data for other services beyond the original one as long as the data subjects give their 'consent', be it unambiguously or explicitly.

However, Article 66(3)(g) PSD2 categorically forbids any additional use of PIS. In turn, Article 67(2)(f) PSD2 provides a similar prohibition for AIS, but adding that this should be 'in accordance with data protection rules'. The meaning of these added words for AIS is unclear. Does this mean that upon 'consent' AIS (but not PIS) can reuse or recycle account data in order to provide other services to account holders?

51. Yet again, the collision between the PSD2 and the GDPR brings problems of practical implementation, application, and consumer protection. In the absence of an official position, the business environment remains in the shadow of legal uncertainty.

6.5. Silent-parties

52. Payment account data inevitably contain personal data of other third-party individuals – i.e., the so-called silent-parties whose data are in a payment account for being the payee, the beneficiary of a payment, or a joint account holder.

Hence the reservation whether the processing of silent-party data is legitimate when 'explicit consent' for the processing of such data has been given by another data subject (the payment service user), or other grounds for processing are accepted.

53. This element probes once more the consistency of the PSD2 with the GDPR.

The difficulty here is twofold. On the one hand, there is the TPP access granted by banks of silent-party data. Granting access to personal data by a data controller is a data processing operation under Article 4(2) GDPR.[67] On the other hand, there is the subsequent processing of personal data by TPP which does not rely on the consent of (in any of its expressions), or a contractual obligation with, the silent data subject.

54. Either way, to establish the legal basis one may endeavour that the data processing is necessary for compliance with a legal obligation of the data controller under Article 6(1)(c) GDPR. Here, the legal obligation would be either that of the PSD2, or the contractual obligation between other parties.

---

67 Under Art. 4(2) GDPR, 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as [*omissis*] disclosure by transmission, dissemination or otherwise making available [*omissis*].

55. The counter-argument would confute this stance on the ground that such a processing is not done in pursue of a legal obligation. The PSD2 does not impose a legal obligation for the data processing of persons who are not party to a contract. On the contrary, the PSD2 imposes access to account data in the context of a contractual relationship only in the interest of the parties of the contract. From the side of banks, they are obliged by law to grant the access to the data of the service user, which can be considered a legal obligation under Article 6(1)(c) GDPR, but only vis-à-vis the contracting party. For third silent-parties the legal obligation does not stand.

56. Similarly, it is objectionable that alien contractual relationships could constitute a legal obligation serving as legal basis for the data processing of third-parties. If this were the case, data protection law would be generally frustrated altogether allowing for an indiscriminate processing of an undetermined number of data subjects only to satisfy private interests of contracts alien to data subjects.

57. Hypothetically, the 'legitimate interest' pursued by the controller or a third-party under Article 6(1)(f) GDPR may cover more appropriately the situation at hand, and provide the legal basis for the processing. At least, this is the view expressed by the EDPB in the mentioned letter addressed to a European Member of Parliament, where it states that:

> A lawful basis for the processing of these silent party data by PIP and AIS – in the context of payment and account services under PSD2 – could be the legitimate interest of a controller or a third-party ex Article 6(1)(f) to perform the contract with the service user.[68]

58. If 'consent' is one of the most complicated lawful bases to implement under data protection law, the 'legitimate interest' is arguably the most controversial.[69] It affirms that those data controllers who determine the purposes and means of the processing of personal data may do so lawfully, without meeting the other tight conditions of the law, if this is necessary for the purposes of their legitimate interest or that of a third party, except where such interests are overridden by the interests for fundamental rights and freedoms of data subjects. It is a processing criterion that expands the scope of permitted processing based on the other legal bases for data processing, in particular consent-based processing. The provision is formulated broadly enough also to address situations of conflicting legitimate private interests of data controllers or third parties vis-à-vis the legal right of data subjects, such conflicts requiring the exercise of a balancing test. This test

68 European Data Protection Board, *Letter to Sophie in 't Veld.*

69 F Ferretti, 'Data protection and the legitimate interest of data controllers: Much ado about nothing or the winter of rights?', 51 *Common Market Law Review* 2014, p (843).

provides flexibility to the legal system. It leaves the legitimacy of processing to a case-by-case determination. However, if on the one hand flexibility is welcomed by business-oriented supporters, on the other hand it removes a degree of legal certainty. The test requires interpretation by legally unqualified subjects who are meant to apply its results. Data controllers are left with the determination of whether they have a legitimate interest to justify the processing, and whether their interest overrides the rights and freedoms of data subjects. It is not free from controversy that the persons who are deemed to make the balancing and who determine which interests or rights prevail for processing the data are the data controllers themselves, albeit with possible judicial controls of difficult practical enforcement only *ex post.*[70]

59. Taking the above quibble into account, this means that banks and TTP cannot apply the legitimate interest basis automatically but need to carry the balancing test, having to take into consideration inter alia the type of data collected, the context, the circumstances, and the risks for individuals.

Yet, the legitimate interest of the controller is limited and determined by the reasonable expectations of data subjects,[71] in this case the silent-parties.

Therefore – against the view of the EDPB – it appears doubtful the extent to which the reasonable expectations of silent-parties can be met. This may be the case in the provision of PIS but debatable for the provision of AIS.

60. All the same, it remains uncontentious that under Articles 13 and 14 GDPR data controllers must give notice to data subjects of the processing, and need to find an appropriate technical way to do so for silent-parties.

As noted in the Sections above, however, the problem is that account data may easily contain sensitive information, or big data processing may easily reveal information of this nature. *Mutatis mutandis*, this circumstance applies for silent-parties too.

The legal issue is that under Article 9(1) GDPR the 'legitimate interest' cannot be used as a legal basis for the processing of sensitive data. Therefore, given the impracticable implementation by banks of technical measures to separate account data that might reveal information falling under Article 9(1) GDPR from other account data, it is questionable the extent to which silent-party data may be processed under the 'legitimate interest' legal basis of the GDPR.

The predicament is that such a denial could jeopardize the operativity of Open Banking and frustrate the norms of the PSD2. By contrast, turning the blind eye on the problem would weaken the protections afforded to data subjects by the GDPR.

Needless to insist, even here coherence and legal certainty are needed over this other ramming aspect between the PSD2 and the GDPR.

---

70 Ibid.

71 Recital 47 GDPR.

7. Conclusions: A Gordian Legal Knot

61. In regrouping the number of legal issues resulting from the intricacies between the PSD2 and the GDPR analysed in this work, the key takeaway is that all together they form a Gordian legal knot.

This work has examined Open Banking, the novel market model in the area of payments driven by the passing of the PSD2 in which traditional banking meets and is transformed by the data economy and the competition of innovative fintech firms. With the PSD2, the EU has shifted its single market approach towards digitalization and competition. At the same time, digitalization and competition are synonym of personal data and additional processing by an increasing number of new market actors. Inevitably, therefore, Open Banking is not only regulated by the PSD2 but it also falls under the scope of the GDPR.

However, the interplay of these two laws has created a number of juridical difficulties and questions over their relationship.

62. This work has identified a number of problems of legal coordination, starting with the different legal meanings of 'consent' used in both the PSD2 and the GDPR and the ambiguity over their degree of applicability for account data processing. In turn, the poor coordination of the two laws makes the application of the appropriate legal basis for account access and data processing unsure. Likewise, the scope and extent to which the right of data portability granted by the GDPR find effect are dubious. As a result, it is unclear how service providers should conduct their business and account holders are safeguarded, that is whether legitimate data access and processing occur by way of contract, a simple yet unambiguous consent, or explicit consent.

63. The sensitive nature of information contained in payment accounts and the impracticability of keeping it separate from other payment data is a particular source of concern, especially if the higher standards of protection of the GDPR do not find application. The possible aggregation of big data and the extent of possible reuse of the data are also obscure, especially in the digital domain where fintech have the potential to extract value for the provision of new competitive services.

Last but not least, the processing of account data implies the necessary access to third silent-party data, but once again the legitimacy of such processing is uncertain.

64. Arguably, all the identified legal issues culminate in dissatisfactory attempts of juridical constructions, stretches, or interpretations.

The impression is that the legal knots are numerous, thus making a single intractable bulge inapt to be solved by untying them one-by-one.

The Gordian knot is often used as a metaphor for a bold solution to solve a complicated problem – the untying of an impossibly tangled knot. As in the legendary version of Alexander the Great who drew his sword and sliced the

Gordian knot in half with a single stroke,[72] it is maintained that either the authentic interpretation of the CJEU or a legal review by the competent legislature are urgently needed to fix the uneasy cohabitation of the two laws. Lacking that, the operativity of Open Banking is jeopardized.

65. Possibly, an initial step in an orderly direction would be the inclusion of financial data altogether in the sensitive data category of the GDPR, when reviewed. However, this would not be resolutory to make the coordination of the PSD2 and the GDPR smooth.

Broader legal certainty is necessary for many reasons.

There is the EU market dimension, where different answers to the identified problems may be provided in the Member States, which have already started to transpose differently the PSD2.[73]

Not less importantly, businesses and consumers need legal certainty and an Open Banking environment with strong consumer protection to prevent freeriding. The development of a new market is at stake. This is in their common interest and in the general interest of an innovation that works for the real economy and society.

66. Already, taken individually the frameworks of the PSD2 and the GDPR may not be perfect. This was not for this article to determine. However, the legal uncertainties resulting from the poor coordination of the two pieces of legislation may carry risks beyond the difficulties of legal technicism.

67. In a financial services market that is mainly supply-driven and governed by the supply-side, there are conduct of business risks. Aggressive business models may expand via the digital development. Innovation and competition are welcome, but fintech are complex and business models take new unconventional forms where data feed new scenarios and create new markets. This can result in an environment favourable for targeted individual marketing, exploitation of consumers' behavioural biases, misselling of financial services, or financial discrimination. Freeriding wallows in legal uncertainty and may flourish.

68. The timely understanding by the legislator of the different business models is crucial to recognize how the market develops and the loopholes of the current legal framework. A rethinking of the regime for Open Banking would be necessary to reconcile the needs of a new market and the protection of its users.

---

72 However, in alternative versions it is reported that he found the ends of the rope by pulling the knot out of its pole pin, exposing the two ends of the cord and allowing him to untie the knot without having to cut through it.

73 For example, see the national laws of France, Germany, Denmark, and Sweden that did not include the words 'in accordance with data protection rules' of Art. 67(2)(f) PSD2. See European Commission, National transpositions by Member States, Document 32015L2366, https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32015L2366 (accessed 14 February 2022).