Coche, Eugénie; Kolk, Ans; Dekker, Martijn

Article

Navigating the EU data governance labyrinth: A business perspective on data sharing in the financial sector

Internet Policy Review

Provided in Cooperation with:
Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin

Suggested Citation: Coche, Eugénie; Kolk, Ans; Dekker, Martijn (2024) : Navigating the EU data governance labyrinth: A business perspective on data sharing in the financial sector, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 13, Iss. 1, pp. 1-32,
https://doi.org/10.14763/2024.1.1738

This Version is available at:
https://hdl.handle.net/10419/285314

INTERNET POLICY REVIEW
Journal on internet regulation

Volume 13 **Issue** 1

RESEARCH ARTICLE

OPEN ACCESS

PEER REVIEWED

Navigating the EU data governance labyrinth: A business perspective on data sharing in the financial sector

Eugénie Coche *University of Amsterdam*
Ans Kolk *University of Amsterdam* akolk@uva.nl
Martijn Dekker *University of Amsterdam*

DOI: https://doi.org/10.14763/2024.1.1738

Published: 12 February 2024
Received: 19 October 2023 **Accepted:** 31 January 2024

Funding: The PhD trajectory of the first author is funded by ABN AMRO (but without any conditions as to contents and without any publication restrictions).
Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Citation: Coche, E. & Kolk, A. & Dekker, M. (2024). Navigating the EU data governance labyrinth: A business perspective on data sharing in the financial sector. *Internet Policy Review*, *13*(1). https://doi.org/10.14763/2024.1.1738

Keywords: Data governance, Innovation, Open banking, Data privacy, Security

Abstract: This paper offers a business perspective on the EU data governance framework, particularly related to data sharing in the financial sector. With policy-making ("on the books") centred on guaranteeing data privacy and data security whilst promoting innovation, firms face complexities when implementing this framework "on the ground". We build on existing work in internet policy, governance and law, multidisciplinary insights from business and management studies, and equally consider practitioner reports, legal/policy documents and industry consultations. Using the Revised Payment Services Directive as an illustrative case, our exploratory analysis reveals an implementation labyrinth, with a so-called "privacy-security-control" nexus at its core. Already problematic for firms operating across borders in the EU, this proves to be even more the case for global companies subject to various data sharing frameworks. Our analysis also reveals that the sectoral framework by the books neither reckons with the heterogeneity of firms (incumbent and new banks, fintechs and bigtechs) nor with their business models. We expose how these "on the ground" business realities might bring unintended effects that could be further aggravated by the (inherently slower) pace of regulation, and offer recommendations for policymakers, researchers and practitioners.

1. Introduction

When discussing the EU's data strategy in 2020, a striking statement was made by Margrethe Vestager, then the Commission's digital and competition chief: "I've had people coming to me saying: we in the financial sector will have to share the data that we have but Amazon will not have to share the data the other way around" (Espinoza et al., 2020). Pointing to this data sharing imbalance, which should be seen in light of data sharing obligations present in the financial sector, she stressed the need for ex-ante laws to complement the existing legal framework. Besides illustrating the power of large digital technology firms (e.g. Amazon and Google) in the data sphere, her statement exposes the discrepancies between regulation and industry needs in the context of financial data governance, possibly leading to unintended situations and requiring ex-post amendments (or even new laws) to remedy recently-implemented legal regimes. This issue has in the meantime, however, led to a legislative package to ensure that "the EU's financial sector is fit for purpose and capable of adapting to the ongoing digital transformation" (European Commission, 2023a), a move welcomed by industry experts (Ifrim, 2023).

Against this backdrop, this paper offers a business perspective on the EU data governance framework by exposing different elements playing a role in its implementation at the firm level. Using the financial sector as an illustrative case, it addresses the following question: "To what extent does the EU data governance framework allow for a translation at the firm level, considering the legal and (international) business realities faced by firms?". By doing so we respond to calls by multidisciplinary scholars who have started to pay attention to the dynamics that exist between macro- and meso-level data governance models, suggesting that the materialisation of the EU data governance framework (i.e. the macro-level) is not homogenous but depends on how industries and municipalities (i.e. the meso-level) respond (Bodó et al., 2021). Although limited to one particular sector (i.e. the financial sector), our work adds the micro-level to this equation in view of the crucial role of firms for implementing and realising the Union's ambitions. When looking at the EU's macro-level framework, where innovation is increasingly being pursued through data sharing initiatives, such as in finance, one may presume that firms develop data governance approaches that are in line with European values and fundamental human rights, as required by law. From that perspective, Bodó and colleagues (2021, p. 26) suggest that the EU has the ability to become "the largest exporter of value-sensitive meso-level governance logics", which means in line with EU values and human rights. However, considering the practical difficul-

ties encountered by (financial) firms in implementing the EU data governance framework, as noted by managers and in business outlets (which sometimes use the term "regulatory failure") (Radnejad et al., 2021), it seems that what is "on the books" cannot be easily applied "on the ground" and is, in certain sectors, not as straightforward as the legislator may have assumed.

To explore these issues and address our research question, we build on existing work in internet policy, governance and law, multidisciplinary insights from business and management studies and equally consider practitioner reports, legal/policy documents and industry consultations related to the financial sector, as explained in section 2. This is followed by a brief overview of EU data governance, and its policy goals of stimulating innovation through data sharing and human rights safeguards (section 3). Section 4 then zooms in on the sectoral framework, outlining financial data governance on the books and on the ground, using the Second Payment Services Directive (PSD2) as an illustrative example. Through an analysis of two targeted consultations concerned with "open finance" and the "review of PSD2", we focus on what gave rise to the ensuing payments regime (including PSD3) by shedding light on implementation hurdles, particularly relating to overlapping laws, which we label the "privacy-security-control" nexus. This nexus is further discussed in section 5, where its implications are placed within the broader international business context and in relation to two underlying aspects deserving further research and policy attention, i.e. the heterogeneity of firms and the pacing of regulation. Section 6 concludes, and discusses limitations and interesting avenues for further research.

2. The role of firms in shaping data governance

The importance of considering firms in the implementation of data governance has been recognised for quite some time already. The former European Data Protection Supervisor Peter Hustinx (2014), for example, stated in the context of the then-upcoming General Data Protection Regulation (GDPR): "The review of the EU legal framework for data protection is taking place in a context where both the need for more effective protection and the challenges to deliver that protection *in practice* have increased enormously" (our emphasis). He hereby referred to the 2013 Snowden revelations, which exposed the value of data as a monitoring tool for both firms and governments, and the shortcomings of the EU legal framework to safeguard users' data protection rights in the face of such business practices. Similarly, on the other side of the Atlantic, US-based legal scholars Kenneth Bamberger and Deirdre Mulligan (2011) emphasised the pivotal role of firms in shaping data gov-

ernance, with "on the ground" privacy protection differing significantly from "on the book" legal requirements. From interviews with chief privacy officers, they learned that "decisions at the corporate level might provide the best way to avoid privacy harms", taking into account that these have "far greater power to shape privacy's treatment" (p. 298). These authors therefore argue that there should be more attention to the implications of legal requirements on corporate practices. Hence, for policymakers to issue data governance laws that are effective on the ground requires a careful balancing between regulation, on the one hand, and firms' abilities for implementation, on the other.

As noted above, there is awareness of this complexity in the EU. Indeed, since the 2016 so-called "better regulation agenda" (European Commission, 2016), EU law is characterised by public and stakeholder consultations that can help shape legislative proposals. However, the extent to which these insights are fully leveraged and optimally translated into policy is uncertain. As noted by EU consultation expert Adriana Bunea, "the data is gathered, analysed across descriptive statistics, such as how many business groups say yes or no to one new rule or another, and then Commission officials write a consultation report, some of which ends up feeding into policy" (Naujokaitytė, 2023). Underutilisation of input might harm the approach to data governance legislation that puts firms at the forefront of data privacy management. For example, the EU's GDPR ((EU) 2016/679) imposes an obligation on firms to have "appropriate technical and organizational measures" in place and to ensure that their systems are "by design and by default" in line with data protection principles (Art 32 & 25 GDPR).

Although the delegation of data governance roles and functions to firms seems a powerful tool to reconcile "on the book" data governance laws with "on the ground" practicalities, we posit that this amplifies the need for comprehensive insights into how regulation affects industry practices and vice versa. As law professor Ari Ezra Waldman (2021) observed, regulatory compliance is intrinsically linked with firms' business models and corporate practices, such as the delegation of privacy responsibilities that are core to data protection to employees who may be unaware of privacy laws (e.g. "privacy by design" under Art 25 GDPR to IT engineers). This perspective adds to economists and business scholars pleading for more attention to the business models of large technology firms (e.g. Google, Apple, Facebook) in designing platform regulation (Jacobides et al., 2020; Morton et al., 2020; Morton & Caffarra, 2021) (see section 4.2. for more details). Therefore, for compliance to be effective, policymakers need a good understanding of the factors that shape firms' compliance and implementation strategies as these could, ultimately,

affect the materialisation of the EU data governance framework.

Bodó et al. (2021) paid attention to the existence of meso-level governance regimes within the EU macro framework. However, their work stays more generic when it comes to the specific business dynamics at stake within the meso-level and involving a range of different firms at the micro-level. This is where our paper aims to contribute, inspired by the distinction between data governance on the books and on the ground from the US context. We take the EU-macro framework as starting point and zoom in on a specific sector to shed light on the interplay of law and implementation choices by firms so as to increase our understanding of the challenges encountered, as well as assist the EU in its promulgation of data governance laws that are effective in practice.

3. EU's data governance framework: data innovation vs. human rights safeguards

As outlined by Bodó and colleagues (2021, p. 6), the EU's data governance framework can (unlike the US and China) be characterised as a "mixed approach" in which fundamental human rights are balanced against the need for innovation. Whereas the Union promotes an internal market for the free flow of data across member states, such flows shall always be in accordance with fundamental human rights, including people's right to privacy and personal data protection as guaranteed under numerous legal instruments, including the EU Charter of Fundamental Rights (Art 8), the European Convention on Human Rights (Art 8) and the GDPR ((EU) 2016/679). This hybrid approach, whereby personal data shall both be protected and its societal and economic value maximised, has given rise to a swirl of regulatory incentives at the EU-level to encourage so-called "open data schemes" (i.e. based on data sharing).

Indeed, and as part of the EU's overall Data Strategy, data sharing initiatives are seeing the light of day, requiring data to be shared between firms, between firms and governments and vice versa, as well as between public authorities (European Commission, 2020b). The aim is to realise a single European data space, in which personal and non-personal data can freely flow. To attain this goal, the Commission identified a set of ten somewhat idiosyncratic economic "sectors" which would each have their own common data space, namely health, finance, agriculture, industrial and manufacturing, energy, mobility, green deal, public administration and skills. Others were subsequently added, such as the media and cultural heritage sectors (European Commission, 2022a). In certain areas, the creation of such data spaces builds further on already existing EU data sharing initiatives.

For example, in the energy sector, electricity suppliers are already required to share consumer data, including "metering and consumption data as well as data required for customer switching, demand response and other services" (Art 23; (EU) 2019/944). Data sharing obligations are also present in the automotive industry, where manufacturers are required to share vehicle-on-board diagnostic and vehicle repair and maintenance data with independent repairers (Art 61; (EU) 2018/858). Since 2015, the financial sector in the EU faces sector-specific data sharing obligations stemming from PSD2, which requires financial institutions to share their customers' payments accounts data with permitted third parties such as so-called fintechs (see section 4). In parallel to private sector firms facing data sharing obligations, some also apply to public bodies, such as the 2019 Open Data Directive concerning publicly-owned data ((EU) 2019/1024).

The reason for introducing data sharing requirements resides in the power of data which, as a non-rivalrous resource, has a value potential that is potentially unbounded and can be used simultaneously by numerous actors and for different purposes (Jones & Tonneti, 2020). For example, location data not only contains information about where a person is or goes but can also reveal what that person likes, such as hobbies (if the location is a tennis club) or food consumption habits (by regularly going to certain eateries). Such data could also reveal more sensitive information such as that person's gender (if that tennis club happens to be solely for women) or religion (through regular church or mosque visits). Hence, if shared between sectors and amongst firms, the value of one dataset multiplies and can benefit both businesses and users with, one the one hand, the creation of entirely new product offerings and, on the other hand, more personal, friction-free opportunities. Data and the sharing of it thus enables a digital transformation in which new business models, products and services emerge (e.g. the sharing economy, Ciulli & Kolk, 2019), as well as novel approaches and facilities (e.g. social media platforms, cloud computing, the internet of things).

On the presumption that fundamental rights are duly respected, such innovation might ultimately lead to a more sustainable, healthier and prosperous society, based on the fact that its processing and analysis can generate new insights and better choices for citizens, firms and public authorities. With these benefits in mind, two complementary EU regulations, the Data Act (DA) (EU 2023/2854) and the Data Governance Act (EU 2022/868) have seen the light of day. Whereas the former encourages the sharing of industrial data (both personal and non-personal data), the latter develops "the processes and structures to facilitate data sharing by companies, individuals and the public sector" (European Commission, 2022b) To

this end, the DGA encourages the use of "data intermediation" actors, which are neutral third parties facilitating data exchange, as well "data altruistic" actions by which consumers can voluntarily share their data for public interest goals (European Commission, 2022c).

Given the growing body of legislation requiring data sharing, paired with the growing responsibilities of businesses for ensuring its proper implementation, the next section takes a closer look at different elements playing a role in these laws' implementation at the firm level. The financial sector has been chosen as the object of study for several reasons. First, preparations for data sharing obligations in banking started a decade ago already, leaving enough time for implementation dynamics to be witnessed. Second, data sharing legislation in banking is gaining a foothold in a growing number of countries, such as Australia, Brazil, Canada, China, Hong Kong, India, Israel, Japan, Mexico, New Zealand, Singapore, South Africa, the United Arab Emirates, the UK and the US. Interestingly, there is a wide variety in approaches in terms of scope and obligations, whether through regulation (e.g. Australia, EU, UK), market forces (e.g. China and US) (Buckley et al., 2021) or a mix of both (e.g. Canada) (Ohab & Shariff, 2023). Finally, the EU is moving towards an "open finance" framework, which broadens the types of financial data to be shared. This goes beyond payment data to also include, for example, mortgage, savings, investments or insurance data, which makes the dynamics observed so far relevant for the EU's future policy agenda (European Commission, 2022d, 2023b).

4. The financial sector as illustrative case

4.1. PSD2 as the book

Building on its predecessor (PSD1), PSD2 was published in 2015, with the requirement to member states for implementation in their local laws by the end of 2018. PDS2 was established to promote innovation and competition in retail payments, whilst guaranteeing minimum security thresholds in line with citizens' personal data protection. It also aimed to improve the integration of the EU's payment market, competition, and financial inclusion (through lower prices of payment services). In terms of innovation and competition, the EU saw it as a necessary step given the emergence and growth of many (relatively new) commercial actors, commonly known as "fintechs", which undertake "financial innovation based on the use of digital technologies and big data" (Stulz, 2019, p.1). Examples include Paypal or Spendee, which were previously constrained in their expansion because of banks' monopoly on customer data. To realise a 'level playing field', PSD2 imposed an obligation on banks to share their customers' payments account data with such

third-party providers (TPPs).

However, such data sharing obligation only exists in relation to two types of TPPs, namely providers of "account information services" (Art 4, sub. 16) and providers of "payment initiation services" (Art 4, sub. 15). The former category offers services to give consumers a full overview of their different accounts to better understand their spending patterns and financial needs without having to access each banks' internet platform separately (e.g. Tink or Plaid). The latter enables users to pay merchants immediately without having to possess a credit card; it thus "creates a software 'bridge' between these accounts, fills in the information necessary for a transfer (amount of the transaction, account number, message) and informs the merchant once the transaction has been initiated" (European Commission, 2018). An example is the German company Sofort, which "allows for direct and secure payments using personal online banking credentials" or, more well-known, Apple Pay or Google Pay.

Importantly, bringing these two types of TPPs within the scope of PSD2 would not only serve innovation and competition but also security. Prior to PSD2, these fintechs were neither supervised by a competent authority nor required to comply with PSD1 obligations (e.g. the right to refund in case of unauthorised debit payment), which caused risks to their users in terms of "consumer protection, security and liability as well as competition and data protection" (rec. 29 PSD2). Indeed, fintechs commonly relied on "screen scraping" techniques to access customer data, which is a practice that relies on the use of customers' interface and security credentials and does not require any prior identification vis-à-vis banks (European Commission, 2017). In such cases, fintechs literally "scrape" customers' accounts information using their login credentials (i.e. account details and passwords) and connect to banks' apps or websites by means of software robots. With no security checks in place and the possibility for a limitless amount of data to be collected, this technique opens the door to both fraud and data misuse (Bailey, 2021).

To counter these security risks, PSD2 mandates banks to have in place secured interface mechanisms through which data sharing takes place. Although not required, the most appropriate and popular technology for this turns out to be Application Programming Interfaces (APIs): interfaces between programs that contain "a set of rules and specifications for software programs to communicate with each other" (Basel Committee on Banking Supervision, 2019, p. 19). Moreover, only licensed TPPs (as authorised by competent authorities) can benefit from such data access (Art 11 &12) and data sharing must be based on users' explicit consent and in respect of both the GDPR and the technical guidance developed by the Euro-

pean Banking Authority on "strong customer authentication" (SCA) ((EU) 2018/389). Unless exemptions apply, such SCA applies to all payment service providers (both traditional banks and fintechs), meaning that these providers must – once payment initiation is required - enable their users to confirm the transaction based on "the use of two or more elements categorised as knowledge (something only the user knows, e.g. a password or a PIN), possession (something only the user possesses, e.g. the card or an authentication code generating device) and inherence (something the user is, e.g. the use of a fingerprint or voice recognition)" (European Commission, 2018, pt. 16).

4.2. Implementation of PSD2 on the ground

Several (consultancy) reports and business outlets have considered implications of firms' compliance efforts with PDS2 in the context of "open banking"[1] regulation (Bric et al., 2018; Botta et al., 2018; Folcia & Fringes, 2017; Hafstad et al., 2017; Omarini, 2018; Petrović, 2020; Jones & Ozcan, 2021; Ozcan & Zachariadis, 2021). Challenges include incumbents' defensive mindsets, with banks expressing fears of losing their customers in the face of new innovative players, issues relating to (lack of) standards for data sharing interfaces between firms and so-called regulatory uncertainty resulting from this "imposed innovation" (cf. Verbeke et al., 2017; Radnejad & Osiyevskii, 2020). Indeed, given that PSD2 is a Directive and, unlike a Regulation, allows for some implementation discretion at member state level, uncertainties exist as to how every EU country and, in turn, credit institute interprets and translates PSD2 on the ground (Radnejad et al., 2021). Taking into account that PSD2's implementation directly intertwines with technology deployment by banks in terms of data access interfaces, a fragmented approach can lead to the situation that fintechs need to interface differently with each incumbent bank, i.e. using different technology standards. Also, liability management between fintechs and incumbent banks, in case of unauthorised payment transactions, is unclear (Ozcan & Zachariadis, 2021).

Another element, captured by Vestager's quote at the beginning of this article, concerns data sharing imbalances between banks (and fintechs) on the one hand, and bigtechs on the other. Whereas bigtechs are active in a wide variety of sectors and are, from an EU antitrust perspective rather designated as "gatekeepers" ((EU 2022/1925); Directorate-General for Competition & Directorate-General for Com-

1. Although cross-national variations exist regarding the term "open banking", we use this term in line with the definition by the Basel Committee on Banking Supervision (2019, p. 4), namely "the sharing and leveraging of customer-permissioned data by banks with third party developers and firms to build applications and services".

munications Networks, Content and Technology, 2023)[2], the Financial Stability Board (FSB) (2019, p. 21) defines bigtechs as "large technology companies that expand into the direct provision of financial services or of products very similar to financial products".[3] Examples include Amazon, Microsoft and Alibaba. They are, in this context, sometimes also referred to as "techfins", as opposed to "fintechs". As the name suggests, with the "tech" preceding the "fin", these types of firms "start with technology, data, and access to customers. Then they move into the world of finance by leveraging their access to data and customers and seek to out-compete incumbent financial firms or fintech startups." (Zetzsche et al., 2017, p. 9). Active in a wide variety of sectors (which explains why the EU designates them as "gatekeepers") these firms derive their influence "from access to data rather than money" (Zetzsche et al., 2017, p. 14).

In the policy debate, challenges on the ground were exposed through the Commission's targeted consultation on open finance, which ended on 5 July 2022. In its wish to extend data sharing obligations to a broader range of actors and datasets in finance, whereby a shift from open banking – as triggered by PSD2 – and open finance would occur, the Commission explored experiences of data sharing practices of different parties, including customers, financial institutions and other firms falling under the PSD2 framework (European Commission, 2022e). Ultimately, they received 94 answers, covering 88 questions. One question is particularly relevant for the present paper as it directly concerns implementation challenges encountered by firms in relation to their data strategy and puts forward a somehow "ideal" data governance scenario, whereby firms would share more data than required, thereby increasing the EU's innovation potential. It reads as follows:

2. The term "gatekeeper" designates "a few large platforms [that] increasingly act as gateways or gatekeepers between business users and end users and enjoy an entrenched and durable position, often as a result of the creation of conglomerate ecosystems around their core platform services" (European Commission, 2020a); for the definition of gatekeeper, see Art 3 DMA.

3. When discussing "bigtechs" in finance, the Bank for International Settlements (BIS) refers to the FSB definition (Carstens, 2023, p. 1).

14. As a financial firm holding customer data, do you make any data available to third parties beyond the data that you are required to share under PSD2, GDPR or other laws?
    a) Yes
    b) No

If yes, please also specify the main obstacles to make such data available (multiple answers possible):

a) Legal
b) Technical
c) Operational
d) Business considerations
e) Other (please specify) _____

If not, is it due to (multiple answers possible):

a) lack of legal basis under GDPR and other legal prohibitions
b) the associated costs
c) lack of technical capabilities
a) limiting potential competition from third parties
b) uncertainty about how to price these data
c) potential liability claims due to the sharing of outdated or incomplete data sets, data misuse (e.g. under the applicable data protection and privacy laws) and/or uncertainty about data ownership rights
d) reputational risks
e) lack of requests from third parties

FIGURE 1: Section of the Commission's questionnaire for financial firms holding customer data (European Commission, 2022e).

Amongst all parties, 32 (34%) declared sharing more data than required, six (6%) said the opposite and 56 (60%) answered "not applicable". A specification of what the "yes" category indicated as being particularly challenging is found in Table 1. Technical challenges were mentioned most often (23 times, 26%), followed by business (22, 25%), legal (19, 21%) and operational considerations (13, 15%). Other reasons (12, 13%) were, for example, related to cybersecurity, reputational risks, liability, lack of incentives and data privacy issues. The open finance consultation explores some of these issues further,[4] pointing at a wide variety of challenges playing a role in the materialisation of EU's data governance framework from a range of actors. However, from the way the consultation document is formulated and structured we cannot figure out how far (the answers to) question 14 are fur-

4. See for example Q. 26 on particular risks relating to data sharing or Q. 62 about API implementation.

ther substantiated in follow-up questions. Moreover, at no stage does the document require respondents who answered 'no' to the first part of question 14 to provide further insights into their reluctance to share more data than required. A further analysis of Table 1 could be useful for follow-up research.

Table 1: Nature of the obstacles to data sharing mentioned in the targeted consultation on open finance (answers to question 14, per respondent)

PARTIES	LEGAL	TECHNICAL	OPERATIONAL	BUSINESS	OTHER
1. European Banking Federation					X
2. Deutsche Bank AG	X	X	X	X	
3. Société Générale	X	X		X	
4. BNP Paribas		X		X	
5. Confédération Nationale du Crédit Mutuel		X		X	
6. Klarna Bank AB	X	X		X	
7. Groupe AEMA		X	X	X	X
8. Italian Banking Association	X	X	X	X	
9. French Banking Federation		X		X	
10. Banca Sella Holding S.p.A.	X			X	
11. Insurance Europe	X	X	X	X	
12. Anonymous (in insurance sector)	X	X	X	X	X
13. France Assureurs (Fédération Français' de l'Assurance)		X	X	X	X
14. European Payment Institution Federation	X	X			
15. Mastercard Europe					X
16. Gesamtverband der Deutschen Versicherungswirtschaft e.V. (GDV)	X			X	
17. Schroders Investment Management (Europe) SA		X			
18. Swedish Bankers' Association	*NO INFORMATION*				
19. ING Group	X	X		X	X
20. The Association for Financial Markets in Europe (AFME)					X
21. Barclays	X	X	X	X	X
22. Anonymous (in banking sector)	X	X		X	
23. Anonymous	X	X	X		
24. Pensioenfederatie (Federation of the Dutch Pension Funds)					X
25. FRIDA e.V. (Free Insurance Data Initiative)	X	X		X	
26. Dutch Association of Insurers	X	X	X	X	

PARTIES	LEGAL	TECHNICAL	OPERATIONAL	BUSINESS	OTHER
27. Zurich Insurance			X		
28. Insurance and Pension Denmark	X	X	X	X	
29. Anonymous					X
30. Finans Danmark	X	X		X	X
31. Anonymous (in payments sector)	X	X	X	X	
32. Finance Finland	X	X	X	X	X

Given these limitations, we also looked at the targeted consultation on the review of PSD2, even though it is narrower in scope. It ran in parallel to the open finance consultation and provides some more details as to implementation hurdles on the ground. With 169 respondents sharing their views on 56 questions, it enabled the Commission to "assess the effectiveness, efficiency, coherence, relevance and EU-added value of the Directive" (European Commission, 2022f, p. 3). The answers shed light on significant issues, some of which echo an earlier open letter by the payments sector (Mijs et al., 2022) in response to guidelines from the European Data Protection Board (EDPB) (2020) vis-à-vis (mis)alignments between PSD2 and GDPR. Taking these three documents into account (both targeted consultations and the open letter by the payment sector), shared opinions seem to exist in relation to data privacy, data security and data control uncertainties in a PSD2 context. We contend this privacy-security-control nexus to be at the heart of the EU data governance labyrinth faced by firms in a data sharing context, as explained below.

4.3. Unravelling the privacy-security-control nexus

To shed light on this complexity on the ground, we zoom in on the different components highlighted in both consultations and in relevant documents (i.e. the open letter and explanatory literature), addressing the three relationships consecutively (i.e. data sharing vs. respectively data privacy, data security and data control) (see Table 2 for a summary of key points explained in the text).

Table 2: Examples of regulatory issues emerging in the data privacy-security-control nexus (per relationship)

DATA SHARING *VERSUS*	
DATA PRIVACY	• How to comply with GDPR's "data minimisation" principle – through banks' deployment of digital tools - if banks are unaware of the processing purpose between payment service users (PSUs) and TPPs? • Allocation of responsibilities and liability handling in case of misuse of data by TPPs or fraud: who can PSUs sue in case of data breach and who should

DATA SHARING *VERSUS*	
	be held liable for damage(s)? • Is financial data always considered as "special categories of personal data" under Art 9 GDPR, i.e. is "explicit consent" always required as a legal basis for the sharing of financial data or (and if so when) can exemptions apply? • "Further processing" prohibition by TPPs and how to guarantee GDPR's accountability principle: shouldn't TPPs decide whether "further processing" is allowed in a given situation?
DATA SECURITY	• Misalignment of sector-specific & general cybersecurity laws (e.g. PSD2 with AML, GDPR and DORA; for explanation of AML/DORA abbreviations, see the accompanying text) • PSD2's prescriptive security standards through SCA, precluding certain (more) secure technologies from being regarded as such because of non-compliance with the law.
DATA CONTROL	• Many firms seem unaware of the lack of data "ownership" rights but data "control" rights instead. • Processing of "silent party" data: to what extent shall non-users of a TPP service keep control over their data?

Data sharing vs. data privacy

When asked in the targeted consultation whether the PSD2 framework is aligned and consistent with GDPR's data privacy framework, the vast majority (66, 70%) disagrees (Q. 22(a)).[5] Although the data sharing requirements under PSD2 could be seen as a sector-specific use case of GDPR's data portability right for the financial industry (Zetzsche et al., 2020), the relationship between these two instruments is not as straightforward as the legislator makes it seem under Art 94 PSD2 (Helgadottir, 2020; Peeters, 2020). Elaborating on that question, one respondent (PSD2 stakeholders, 2022, party no. 3) explicitly refers to the lack of clarity in the EDPB (2020) guidelines on how these two instruments interplay "as parts of the Guidelines go against PSD2 provisions". These inconsistencies also formed the core object of the aforementioned industry letter by nine European payments associations (Mijs et al., 2022), on which we will reflect below considering the GDPR, PSD2 and the EDPB guidelines (EDPB, 2020).

In that letter, they argued that the GDPR's data minimisation principle (Art 5(1)(c)), which means that no more data shall be transferred than what is necessary in rela-

5. As opposed to 20 respondents who agreed (four "strongly agreed"; 16 "somewhat agreed"), 13 who answered "neutral" and 69 who provided no information.

tion to the processing's intended purpose, is at risk in a PSD2 context. Whereas PSD2 explicitly stipulates that TPPs accessing data should not "use, access or store" data for other purposes than what has initially been consented by the payer (Art 66(3)(g) jo. Art 67(2)(f)), they argue that the EDPB's (2020) recommendation for banks to support – through the deployment of digital tools – TPPs in their compliance efforts (para. 64), seems at odd with GDPR's delegation of responsibilities whereby each controller should comply with data minimisation vis-à-vis its own data processing operations. As the European payments sector (Mijs et al., 2022, p. 2) explains, even if banks would put in place such technical tools, "ASPSPs [banks] have no means to be aware of the contract between the PSU [the customer] and the TPP, meaning that banks cannot know the purpose for which the TPP asks to access the PSU payment account". In particular, the PSD2 AIS [account information service] function allows TPPs to receive transaction history with which multiple data-driven business models are conceivable, meaning that there is a panoply of purposes for which payment account data could be used. Whilst data regarding the "communication of payment transfers" would be essential for budget planning apps such as Mint or NerdWallet, it may not be for account overview apps such as Revolut.

Besides these recommendations causing uncertainties as to whether or not banks should amend their APIs with additional technical safeguards, it also casts doubt on each party's responsibilities in the data sharing process and, in turn, liability distribution in case of breach of the data minimisation principle. Hence, respondents (Open finance stakeholders, 2022, party no. 92 & 94 to Q. 14) specified that "incidents handling and liability" caused by ambiguous GDPR interpretations were perceived as particularly problematic. Other privacy concerns relate to the EDPB's presumption that financial transaction data can qualify as "special categories of personal data"[6] (SCPD) under Art 9 GDPR (EDPB, 2020, p. 17), which would have far-reaching implications for the lawful processing under PSD2. Examples include donations made to political parties (which could reveal a political opinion) or membership fees for dating sites, by which someone's sexual orientation could be revealed (e.g. Grindr targets the LGBTQ community). Indeed, in a data sharing context, this characterisation would require either "explicit consent" of the PSU as lawful basis for data sharing or the applicability of another exemption under Art 9(2) GDPR, without which no such sharing to TPPs would be permitted. Crucially,

6. Defined as data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation" (EDPB, 2020, p. 17).

although PSD2 already requires "explicit consent" of the PSU for data sharing (Art 94(2) jo. 67(2)(a)), which would make such SCPD qualification meaningless, the EDPB has clarified that these two types of consent are not the same (EDPB, 2020, p. 13).

Whilst explicit consent under PSD2 is an "additional requirement of a contractual nature", the GDPR consent serves as legal basis and must meet the threshold of being "freely given, specific, informed and unambiguous" (EDPB, 2020, p. 12). The European payments sector (Mijs et al., 2022, pp. 3-4), however, disputes the EDPB reasoning vis-à-vis payment data's qualification as SCPD because it supposedly conflicts with recital 51 of the GDPR which suggests that such qualification depends on whether the data in itself – and thus without deployment of technical means – reveals such unique characteristics. From that perspective, photographs for example do not automatically qualify as SCPD (rec. 51 GDPR) and, in turn, neither should payment account data if the processor has no intention to infer such type of information. As argued in the targeted consultation (PSD2 stakeholders, 2022, party no. 5 to Q. 22 (b)): "clarifications are needed with regard to certain definitions and the regime of customer consent relating to the sharing of data". Investigations by the Dutch data protection authorities into the types of data TPPs (can) access under PSD2, particularly in relation to SCPD, and whether this is in line with the GDPR, illustrates how data privacy considerations play out in real life (McNamee, 2020). Crucially, as one stakeholder explains, the complexity regarding data privacy resides in the fact that APIs – unlike screen scraping – may result in situations where TPPs have no other alternative than to obtain consent "for data they don't need to deliver their services to the user" (McNamee, 2020).

Finally, the European payments sector (Mijs et al., 2022, p. 4) expressed uncertainties towards the EDPB's (2020, para. 22) opinion that "further processing" of payment account data accessed by TPPs shall not be allowed based on the "compatibility test" of Art 6(4) GDPR. In their view, given that one same dataset can serve multiple purposes and business models (see section 3), TPPs may want to "further process" data for purposes not initially agreed upon by PSUs. Although PSD2 considerably restricts this possibility (Art 66(3)(g) jo. Art 67(2)(f)), the European payments sector argues that the EDPB's assessment in that regard undermines the GDPR's accountability principle: controllers shall be able to evaluate the risks of "further processing" and come to their own "compatibility" conclusions for which they shall take responsibilities (Art 24 GDPR jo. rec. 50 GDPR). Closely related uncertainties mentioned in the consultation concern the "definition of responsibilities and legal roles under GDPR"; data transfers to third countries and misuse of

data by TPPs (Open finance stakeholders, 2022, party no. 92 & 94 to Q. 14), which also relate to data security, to which we move next.

Data sharing vs. data security

For the purpose of this paper, it is important to understand what distinguishes data security from data privacy. As explained by information technology expert Thomas Lenhard (2022, p. 3), "data protection is inconceivable without data security. But data security encompasses much more than just measures to protect personal data". Data security ensures data is only accessed by authorised users and is protected against disruption or modification. Data privacy is about the right and ability to control who accesses or uses personal data. Therefore, data security should be seen as a necessary compound of data privacy but the opposite is not true. To illustrate, a prerequisite for data privacy is for data controllers to have certain security measures in place such as "appropriate technical and organizational measures" (Art 24 GDPR)[7], which as such does not guarantee data security. For data security to be effective in a data sharing context, both the GDPR (e.g. privacy by design and by default) and PSD2's security standards must be taken into account. They should be incorporated into a broader "cybersecurity agenda", in which "the people, processes, and technology all complement one another to create an effective defence from cyber attacks" (Michael et al., 2019, p. 9). Consequently, any uncertainty or misalignment regarding data security requirements under PSD2, GDPR or other data security laws applicable to the financial sector could affect the wider cybersecurity framework. In both targeted consultations, "risks related to cybersecurity" were often mentioned (Open finance stakeholders, 2022, party no. 63 & 94 to Q. 14; PSD2 stakeholders, 2022; party no. 17 & 55 to Q. 6(b)).

Regarding regulatory misalignments with data security implications, one must bear in mind that financial firms' security obligations are part of a multi-layered and complex European regulatory landscape, with two general pieces of legislation and eight sector-specific ones (Kruger & Brauchle, 2021, pp. 7-8). Besides the GDPR, seven EU laws, including the Anti-Money Laundering Directive (AML; EU (2015/849)) and the Digital Operational Resilience Act (DORA, Commission Proposal)), are perceived as potentially inconsistent with PSD2 (European Commission, 2022f, Q. 22(a)). In sharing their thoughts on that question in the targeted consultation, respondents primarily highlight severe misalignments between PSD2 on the one hand, and, on the other hand, both GDPR and AML, followed by the Markets in Crypto Assets Regulation (MiCA (Commission proposal)) and the revised eI-

7. As complemented by Art 35 GDPR jo. rec. 76 in terms of what amounts to an "appropriate" measure.

DAS (electronic Identification, Authentication and trust Services; EU (910/2014)) Regulation.[8] Regarding inconsistencies with DORA, whose interaction with the Network and Information security Directive NIS (EU (2016/1148) had already been disputed (Council of the EU, 2022), the Electronic Money Association (PSD2 stakeholders, 2022, party no. 2 to Q. 22(b)) clarifies that it is unclear "whether the operational risk monitoring and incident reporting requirements that the DORA regulation introduces are to be treated as part of the operational and security risk frameworks that regulated entities have already deployed to comply with the relevant requirements in PSD2". In line with this, the Luxembourg Bankers' Association (PSD2 stakeholders, 2022, party no. 5 to Q. 22(b)) argues that for DORA, "coordination with PSD2 is necessary". Notwithstanding these data security risks emanating from regulatory misalignment (as is the case with data privacy risks), PSD2's security standards are also seen to threaten the wider data security ecosystem.

Indeed, a significant number of actors (PSD2 stakeholders, 2022, party no. 6; 52; 54; 80; 97; 102; 111 to Q. 10(b)) labelled PSD2's security standards as being "too prescriptive" and not technology-neutral enough, and therefore "likely to give rise to greater systemic payment ecosystem security risks" (party no. 80 to Q. 10(b)). As one respondent (PSD2 stakeholders, 2022, party no. 97 to Q. 10(b)) explained: "The current provisions have led to situations where some of the most secure and frictionless security methods for online payments were discarded for being non-compliant". For example, behavioural analytics solutions – which firms regard as being highly secure authentication mechanisms– can only be used if they reveal a behaviour "created by the body", such as users' keystroke dynamics (i.e. stemming from the finger) or voice recognition (EBA, 2019, p. 4). This excludes a wide range of ever-expanding authentication mechanisms, enabled by artificial intelligence and machine learning (European Commission et al., 2023, p. 137) and relating to "non-body" related behaviours (e.g. users' spending habits based on purchase frequency), which firms consider more effective at preventing fraud (Snagg et al., 2023). Whereas PSD2 requires financial institutions to have appropriate technologies in place for secure data transfers, giving rise to a so-called "API economy" (Borgogno & Colangelo, 2019, p. 4), no API standardisation took place. Unlike under the UK's data sharing initiative in banking (open banking), where such standardisation exists, the only common denominator between all APIs flowing from PSD2 is that they must comply with the security standards as prescribed in the

8. For PSD2 // GDPR: 66 respondents disagree with their alignment as opposed to 20 respondents who agree; for PSD2 // AML: 49 respondents disagree with their alignment as opposed to 22 who agree; for PSD2 // Revised eIDAS: 28 respondents disagree with their alignment as opposed to 24 who agree; for PSD2 // Markets in Crypto Assets: 25 respondents disagree with their alignment as opposed to 7 who agree.

"Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Communication" ("RTS on SCA and CSC"). As feared by one respondent (PSD2 stakeholders, 2022, party no. 11 to Q. 10(b)): "whilst the principle of two-factor SCA remains valid, the requirements in the Directive are now inadequate due to advanced attack vectors (…) attackers have learned how to compromise authentication tools that are based on "shared secrets".

Data sharing vs. data control

Regarding the third relationship, it is important to point out that we use the term data 'control' instead of data 'ownership'. Indeed, while the European Commission (2022d, p. 9), in its targeted consultation on open finance, recognises uncertainties about "data ownership rights" as possibly refraining firms from sharing more data than required (Q. 14), the term is prone to misunderstandings about whether data can be "owned". Unlike objects, data is intangible and "can be replicated many times without concrete evidence that its value is lost", making it an ambiguous type of property (Karanasiou & Douilhet, 2016, p. 2). Although debates about data ownership have existed for a long time, with some in favour of the concept (Tarkowski & Vogelezang, 2021; Wiebe, 2017) – EU Commissioner Oettinger even declared in 2015 that the EU "need[s] a virtual and digital law of property that includes data" (Wiebe, 2017, p. 62) – no such ownership rights exist. Nevertheless, uncertainties on the ground seem to exist (Wiebe, 2017, p. 63), with many firms reluctant to share their data from the "mistaken assumption" that it is theirs (Vlieger, Kapitan & Van der Poel, 2023). Crucially and without overlooking the special regime applicable to databases[9], the EU merely grants "control" rights over both personal and industrial data (Geiregat, 2022).

Whereas PSD2 is meant to empower individuals with more control over their personal data (i.e. by allowing them to decide which firms can access data about them), data control rights are not absolute, which is especially the case when the data at stake concerns numerous people. In a data sharing context, the practical difficulties surrounding control rights were highlighted by the European payments sector (Mijs et al., 2022) with regard to "silent party data", which are personal data of non-users (of a payment service provider) processed in the context of a financial

9. Data that are part of a database could be owned based on the "sui generis database right" under the EU Database Directive (EU (96/9/EC)). For this to exist, the content of the database must be the result of a "substantial" investment in the obtaining, verification or presentation of the data. In this case, the owner of the database can prevent the extraction or re-use of a "substantial" part of the database (cf. Gogia, 2021 for a discussion on how the data portability right may clash with the sui generis database right; and Margoni, Gils & Kun, 2022 for a discussion on data ownership uncertainties in an Internet of Things context under the Data Act).

transaction undertaken by users. Concretely, whenever a fintech (e.g. Revolut) provides its users payment services (e.g. an overview of their different accounts), it inevitably needs to process data of non-users (given the bidirectional nature of payment transactions, whereby both "payer" and "payee" are involved). Information about that non-user then amounts to silent party data and could entail that person's bank account number, name, address or amount of money transferred. In such a scenario, silent parties have no control over their own personal data and may not even be aware that the payee/payer with whom they interact uses a particular payment service. The challenge then concerns the extent to which silent parties should expect/accept to lose control over their personal data and for firms to implement PSD2 in line with their expectations.

According to the EDBP (2020a), TPPs can process silent party data based on the GDPR's legitimate interest ground (Art 6(1)(f)) and non-users' reasonable expectations that such a situation could occur (p. 15). However, it also recognises that silent parties' lack of data control is not absolute: TPPs should under no circumstances, except to comply with an EU or member state law, "further process" data about them. Reasons include silent parties' inability to give their consent (which is one of the grounds allowing for further processing), financial data's sensitivity (see our discussion about SCPD under "data sharing vs. data privacy") and silent parties' (unreasonable) expectations given their lack of relationship with payment service providers (p. 16). Such conclusions caused uncertainties in the payments sector, in case silent parties are companies (e.g. a supermarket or phone provider) or public authorities (e.g. a tax authority) and thus in principle falling outside the scope of the GDPR (Mijs et al., 2022, p. 5). Moreover, confusion exists as to which legitimate interest ground, besides TPPs' need to "perform a contract" (the only example cited by the EDPB (2020, para. 48), would constitute a valid ground for initial processing (vs. further processing) (p. 16). Although these uncertainties seem rather abstract at first sight, incidents in other sectors (e.g. telecom), have shown how far-reaching their business and societal implications can be. WhatsApp's 225 million euro fine by the Irish Data Protection Commission for lack of transparency towards non-users of its services is a case in point. (Data Protection Commission, 2021). Hence, the public consultation on the EDPB's draft guidelines (06/2020) triggered concerns regarding this aspect of data sharing: "The more users consent to sharing their data, the less control silent parties have over their information, and these (or other) corporations gain a bigger and better picture about all silent parties that never wanted to share their data to begin with. Although this kind of further processing is limited according to the draft guidelines, companies of this scale have shown time and time again they cannot be blindly trusted" (Reply to the public

consultation on the EDPB guidelines, 2020).

5. Discussion

In order for the EU data governance framework to be effective in practice, our analysis points towards the need for greater insights into firms' implementation activities "on the ground", a finding that also came to the fore in an OECD policy workshop regarding data sharing initiatives in finance (2023). In a PSD2 context, we show that firms face a data governance labyrinth, with at its core a data "privacy-security-control" nexus that primarily encompasses uncertainties vis-à-vis regulatory overlaps (Salemans & Chen, 2020). These complexities are even greater for firms operating across borders (cf. Coche et al., 2023). Our analysis reveals that PSD2 fragmentation exists across EU member states, both in relation to the Directive's textual (e.g. what qualifies as "payment account"; cf. Salemans & Chen, 2020), and technical implementation (i.e. vis-à-vis APIs). For example, the PSD2 impact assessment study (European Commission et al., 2023) contains frequent assumptions that the EDPB guidelines 06/2020 have clarified alleged inconsistencies (e.g. pp. 172-173). This could have better been taken into account from the beginning in regulatory design and implementation, also to find a good balance between innovation and compliance, as well as encouraging (more) interoperability. Despite industry-led API standardisation initiatives (e.g. Berlin group; STET; Polish API), interoperability challenges remain (OECD, 2023, p. 8), which complicate firms' engagement in open banking activities (OECD, 2023, p. 25).

Interestingly, such fragmentation contrast with the UK open banking framework, where standardisation was mandated and initiated by the nine largest banks, giving rise to a "reliable" and "resilient" ecosystem (OECD, 2023, p. 13), described by some as an "early gold standard" for data sharing initiatives worldwide (Awrey & Macey, 2023, p. 17). Hence, whether PSD2 or parts of it should become a Regulation was a main focus in the targeted consultation (European Commission, 2022f, Q. 10), with the vast majority of respondents in favour (PSD2 stakeholders, 2022)[10]. On that note, policy experts emphasise the need for a broader international interoperability agenda (OECD, 2023, p. 25), which our work echoes (i.e. on top of EU interoperability). At the same time, considering the time and costs made by firms for APIs in the meantime already, rather than imposing new standards (cf. Payment Services Regulation proposal (COM(2023)367)), supporting and guiding organizations in the further development of existing standards, (e.g. Berlin Group;

10. 63 respondents agreed (29 "strongly agreed"; 34 "somewhat agreed"), 30 answered "neutral"; 33 disagreed (18 "strongly disagreed"; 15 "somewhat disagreed), 43 provided no information.

SEPA payment access scheme) is preferable. Encouraging more interoperability would not only facilitate international business activities but also help counter another risk related to API fragmentation: the rise and global expansion of "data aggregators" (Awrey & Macey, 2023). In a fragmented API landscape, data aggregators play a fundamental role and are therefore described by legal scholars as "the connective tissue of open finance" (Awrey & Macey, 2023, p. 5). Predominantly present in the US (e.g. Plaid) and the EU (e.g. Tink), they allow banks and fintech to reduce their API implementation costs whilst ensuring a high degree of interoperability (Awrey & Macey, 2023, pp. 35-39). Indeed, by integrating the aggregator's API, TPPs can simultaneously connect to different banks' APIs without having to connect to each individual API. Crucially, data aggregators are characterised by a platform-based business model that relies on economies of scale and scope[11], which entails business and societal risks somehow similar to those of bigtechs (Awrey & Macey, 2023). This points at two underlying "on the ground" aspects deserving further research and policy attention, i.e. the heterogeneity of firms and the pacing of regulation.

As to the first, we indicated above how different types of firms exist, with multinational ones facing increased complexities in implementing PSD2. It is therefore essential for policymakers to take due account of the heterogeneous landscape of business actors (small and large incumbent banks, fintechs and bigtechs), as well as their specific business models, which can show large variations even between similar types of firms (e.g. Ciulli & Kolk, 2019). A first step in this direction is the proposed exemption in the revised Payment Services Regulation (COM(2023)367), which makes it possible for very small banks to not have to implement 'open banking' APIs in case this would be "disproportionately burdensome" for them (Art. 39 jo. rec. 62). Regarding bigtechs, overlooking their firm characteristics could give rise to unintended risks, such as the creation of "data monopolies" in a data sharing context (European Commission, 2022e, Q. 13)[12]. To understand these dangers, policymakers should have a thorough understanding of these firms' data-driven business models, which allows for "envelopment" techniques based on "bundling" strategies and strong network effects (Cavallo, 2018; Eisenmann et al., 2011), a phenomenon also witnessed in finance (e.g. ApplePay, GooglePay; cf. Crisanto et al., 2021). In that regard, economists (Jacobides et al., 2020) have expressed com-

11. Economies of scale refer to the fact that the supply of data aggregation services decreases as the number of customer increases; economies of scope entail that data aggregators are able, based on the analysis of their ever-increasing large dataset, to expand into new financial markets (i.e. many data aggregators also offer advanced data analytics services to financial institutions).

12. To the question of risk for data monopolies, 59 respondents answered "yes', 13 "no" and 22 did not answer.

petition concerns: the more data bigtechs access, the more they can target their users with specific services and, in turn, lock them in (i.e. making it hard for consumers to leave the platform)[13]. Moreover, risks of discrimination exist, with less educated users being more prone to making "bad investments" because of unawareness of these firms' modus operandi: the ranking of financial offerings may be based on fees paid to the platform instead of on the quality and suitability of these offerings for the person concerned (De la Mano & Padilla, 2018, p. 17). Finally, these actors could put financial stability at risk because of conflicts of interests: the more loans bigtechs facilitate, the more they can offer complementary services to borrowers (i.e. a snowball effect), which is likely to make these tech giants less risk averse vis-à-vis consumers' potential credit defaults (De la Mano & Padilla, 2018, pp. 17-19). Similarly, EU retail banks may also become less risk averse in the face of such powerful tech players, and be more inclined to take "excessive risks in an effort to counterbalance the downward pressure on their profits" (Financier Worldwide et al., 2021).

To overcome these risks in a PSD2 context, some suggest the adoption of symmetric regulation (Cartens, 2021; Crisanto et al, 2021) and/or the introduction of "reciprocity" obligations[14] (De la Mano & Padilla, 2018; Di Porto & Ghidini, 2020). However, if TPPs were to share their data in the same way as banks, a core question that then occurs is the type and amount of data that should be shared (Borgogno & Colangelo, 2020, p. 506). As shown with PSD2, where data should be accessed within banks' ecosystems (such as by API technology; cf. Holland, 2022), the EU seems to move towards data sharing obligations "from within", whereby third parties can access user data within its original location (as opposed to the GDPR's data portability right, which only allowed access to data "from without", by means of external copies (Art 20)[15]. According to platform scholars (Van Alstyne et al., 2021), such "in situ" data access rights, whereby algorithms move to the data instead of the other way around, is valuable for TPPs in view of data's context-dependency (e.g. a Facebook post carries more valuable insights when seen in its contextual environment, such as the amounts of comments it triggered, the time

13. A lock-in effect occurs when "consumers are dependent on a single manufacturer or supplier for a specific service, and cannot move to another vendor without substantial costs or inconvenience" (Eurich & Burtscher, 2014, p. 2). For a discussion on how bigtechs achieve this through the deployment of multi-product ecosystems, see Jacobides et al., 2020.

14. Symmetric regulation entails that the same activities should be governed by the same rules; reciprocity obligations imply that TPPs share their data in the same way as banks do (i.e. it is more specific than symmetric regulation).

15. For a discussion on the limitations of the GDPR's data portability right, and more particularly in light of the Data Act, see Lalova-Spinks & Spajić, 2022.

of posting, by whom it got shared, etc.). By obliging gatekeepers to provide third parties with "continuous and real time access to data" when allowed to do so by users (Art 6 (9-10) DMA), the EU's 2022 Digital Markets Act (DMA), which is aimed at countering data-related competition issues, takes a step in the same direction.

Interestingly, the European Commission (2022g) observed that this DMA was approved in "record-time" (i.e. proposed in December 2020 and agreed in March 2022). This points at the second aspect deserving further policy attention, namely the inherent complexity of "pacing" regulation to the realities of business and society, a problem traditionally highlighted in the US setting (Downes, 2009; Marchant, 2011). Indeed, whereas technology is known to be fast and ever-evolving, regulation tends to go much slower, often leading to situations where the law catches up on (digital) innovation instead of the other way around (cf. Marchant, 2011).

As we noted regarding data security in a PSD2 context, the prescriptive nature of regulatory security standards proves to be problematic in view of technologies' dynamic nature. In addition to these market discrepancies, firms face uncertainties vis-à-vis these laws' longevity: not knowing whether the regulation is "there to stay", which is particularly the case for innovation-driven laws such as PSD2 (cf. Ferrari, 2022). The fact that full implementation of PSD2 took place in December 2020[16] and that, within three years, the EU proposed A PSD3 framework (European Commission, 2023a) is a case in point of this problem and the associated challenges for firms, with "uncertainties about the future" supposedly impacting their innovation activities (cf. Radnejad et al. (2021, p. 91). At the same time, it is inherently difficult to design future-oriented laws on issues that even corporate observers often find hard to predict; policy/regulatory uncertainty has been part and parcel of doing business and a long-standing scholarly concern (e.g. Marcus, 1981). Striking the right balance between regulatory-led initiatives and market-developments is therefore a delicate task that requires multidisciplinary efforts.

6. Conclusions

Whilst the EU is often cited as a leading example for the rest of the world in terms of data governance, an influence as standard-setter sometimes referred to as the "Brussels effect" (Bradford, 2019), little research so far has focused on the actual gap that may exist between the law – as promulgated at the EU-level – and the

16. The implementation date of the Regulatory Technical Standards was 31 December 2020, after postponement.

actual implementation within the firms targeted. To pave the way for a better understanding of these "by the book" versus "on the ground" issues, this exploratory paper sheds light on numerous implementation obstacles faced by firms when striving to realise the EU's ambitions to unlock the full potential of data. We used the financial sector, particularly PDS2, as an illustrative case. Leveraging insights from various (sub)disciplinary studies, as well as practitioner reports, legal/policy documents and consultations, our work reveals important implementation challenges entailed in the law itself. In this regard, we contend the "privacy-security-control nexus" to be at the heart of the EU data governance labyrinth, making it complex for firms to develop data sharing approaches that are in line with EU policies. Already problematic for firms operating across borders in the EU, this proves to be even more the case for global companies subject to various data sharing frameworks. We encourage both business and legal scholars to build further on our analysis by providing more granular insights (i.e. Table 1), such as whether certain firms (e.g. incumbent banks vs. fintechs) tend to struggle more with certain types of challenges (e.g. legal or technical).

PSD2 illustrates that policy assumptions may not always strike with reality and may require short-term amendments or even new laws to remedy recently-implemented legal frameworks. Our paper highlights the need for policymakers to take due account of firms' heterogenous nature, including the variety of business models at play, which could affect firms' compliance and innovation efforts. In a data sharing context, we particularly call for more policy attention regarding platforms' network effects, which present important business and societal risks as illustrated by big techs and data aggregators. Given the extraterritorial implications of many EU laws and the (often more implicit) Brussels effect, it would be helpful if policymakers can develop data sharing frameworks that are coherent with similar international initiatives, in line with what the OECD promulgates.

To facilitate decision-making, business scholars might be of help by exploring the implications of the privacy-security-control nexus on (different types of) firms' strategies, business models and implementation activities. In addition, studies comparing on the ground findings with other sectors faced with EU data sharing obligations (such as health, energy, automobiles) would be worthwhile for cross-learnings, be it from the policy, managerial and/or academic perspective. This also applies to other regions with similar or different data sharing frameworks in place or in the making. In view of the EU focus on innovation and human rights safeguards through its data strategy, there is a need for more insight into how this works out in and vis-à-vis countries with (partly) different "values" (cf. Irion et al.,

2021), considering the implications for citizens and organisations. Similarly, we emphasise the need for a more fine-grained understanding by firms and business researchers of the regulatory intricacies of cross-country data governance, given the growing importance of regulation on all dimensions, from the use to the transfer, storage and flow of data (Coche et al., 2023).

References

Awrey, D., & Macey, J. (2023). The promise & perils of open finance. *Yale Journal on Regulation*, *40*(1). https://doi.org/20.500.13051/18234

Bailey, S. (2021, November 16). What's holding open banking back? *Sifted*. https://sifted.eu/articles/open-banking-back-nordigen-api

Bamberger, K. A., & Mulligan, D. K. (2011). Privacy on the books and on the ground. *Stanford Law Review*, *63*(2), 247–315. http://www.jstor.org/stable/41105400

Basel Committee Banking Supervision. (2019). *Report on open banking and application programming interfaces* [Report]. Bank for International Settlements. https://www.bis.org/bcbs/publ/d486.pdf

Bodó, B., Irion, K., Janssen, H., & Giannopoulou, A. (2021). Personal data ordering in context: The interaction of meso-level data governance regimes with macro frameworks. *Internet Policy Review*, *10*(3). https://doi.org/10.14763/2021.3.1581

Borgogno, O., & Colangelo, G. (2019). Data sharing and interoperability: Fostering innovation and competition through APIs. *Computer Law & Security Review*, *35*(5), Article 105314. https://doi.org/10.1016/j.clsr.2019.03.008

Borgogno, O., & Colangelo, G. (2020). The data sharing paradox: BigTechs in finance. *European Competition Journal*, *16*(2–3), 492–511. https://doi.org/10.1080/17441056.2020.1812285

Botta, A., Digiacomo, N., Höll, R., & Oakes, L. (2018). *PSD2: Taking advantage of open banking disruption* [Report]. McKinsey and Company. https://www.mckinsey.com/industries/financial-services/our-insights/psd2-taking-advantage-of-open-banking-disruption

Bradford, A. (2019). *The Brussels effect: How the European Union rules the world*. Oxford University Press. https://doi.org/10.1093/oso/9780190088583.001.0001

Bric, P., Maewski, D., Scott, A., & Gallo, V. (2018). *European PSD2 survey. Voice of the banks* [Report]. Deloitte. https://www2.deloitte.com/content/dam/Deloitte/ce/Documents/financial-services/ce-deloitte-european-psd2-voice-of-banks-survey-2018.pdf

Buckley, R. P., Jevglevskaja, N., & Farrell., S. (2021). *Australia's data sharing regime: Six lessons for the world* (No. 21-67; UNSW Law Research Paper). UNSW Sydney. https://ssrn.com/abstract=3946668

Carstens, A. (2023). *Big Techs in finance: Forging a new regulatory path* [Speech]. Bank for International Settlements. https://www.bis.org/speeches/sp230208.pdf

Cartens, A. (2021). *Public policy for Big Techs in finance* [Speech]. Bank for International Settlements. https://www.bis.org/speeches/sp210121.htm

Cavallo, A. (2018). *More Amazon effects: Online competition and pricing ehaviors* (Working Paper 25138; NBER Working Paper Series, p. w25138). National Bureau of Economic Research. https://doi.org/10.3386/w25138

Ciulli, F., & Kolk, A. (2019). Incumbents and business model innovation for the sharing economy: Implications for sustainability. *Journal of Cleaner Production*, *214*, 995–1010. https://doi.org/10.1016/j.jclepro.2018.12.295

Coche, E., Kolk, A., & Ocelík, V. (2023). Unravelling cross-country regulatory intricacies of data governance: The relevance of legal insights for digitalization and international business. *Journal of International Business Policy*. https://doi.org/10.1057/s42214-023-00172-1

Council of the European Union. (2022). *Digital finance: Provisional agreement reached on DORA* [Press release]. European Council - Council of the European Union. https://www.consilium.europa.eu/en/press/press-releases/2022/05/11/digital-finance-provisional-agreement-reached-on-dora/

Crisanto, J. C., Ehrentraud, J., & Fabian, M. (2021). *Big Techs in finance: Regulatory approaches and policy options* (Brief No. 12; FSI Briefs). Financial Stability Institute. https://www.bis.org/fsi/fsibriefs12.pdf

Data Protection Commission. (2021). *Data Protection Commission announces decision in WhatsApp inquiry* [Press release]. Data Protection Commission. https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-whatsapp-inquiry

de la Mano, M., & Padilla, J. (2018). Big Tech banking. *Journal of Competition Law & Economics*, *14*(4), 494–526. https://doi.org/10.1093/joclec/nhz003

Di Porto, F., & Ghidini, G. (2020). "I access your data, you access mine": Requiring data reciprocity in payment services. *IIC - International Review of Intellectual Property and Competition Law*, *51*(3), 307–329. https://doi.org/10.1007/s40319-020-00914-1

Directorate-General for Competition & Directorate-General for Communications Networks, Content and Technology. (September 6, 2023c). *Commission designates six gatekeepers under the Digital Markets Act* [News announcement]. European Commission. https://digital-markets-act.ec.europa.eu/commission-designates-six-gatekeepers-under-digital-markets-act-2023-09-06_en

Downes, L. (2009). *The laws of disruption: Harnessing the new forces that govern life and business in the digital age*. Basic Books.

Eisenmann, T., Parker, G., & Van Alstyne, M. (2011). Platform envelopment. *Strategic Management Journal*, *32*(12), 1270–1285. https://doi.org/10.1002/smj.935

Espinoza, J., Murgia, M., & Waters, R. (2020, February 19). Big Tech will have to share data under EU proposals. *Financial Times*. https://www.ft.com/content/a5c7b640-526c-11ea-8841-482eed0038b1

Eurich, M., & Burtscher, M. (2014). *The business-to-consumer lock-in effect* [Working paper]. Cambridge Service Alliance. https://cambridgeservicealliance.eng.cam.ac.uk/system/files/documents/2014AugustPaperBusinesstoConsumerLockinEffect.pdf

European Bank Authority. (2019). *Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2* [Opinion]. European Banking Authority. https://www.eba.europa.eu/sites/default/files/documents/10180/2622242/4bf4e536-69a5-44a5-a685-de42e292ef78/EBA%20Opinion%20on%20SCA%20elements%20under%20PSD2%20.pdf

European Commission. (2016). *Communication from the Commission.Better regulation: Delivering better results for a stronger Union* (Communication COM/2016/0615 final). European Commission. htt

ps://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016DC0615

European Commission. (2017). *Payment Services Directive (PSD2): Regulatory Technical Standards (RTS) enabling consumers to benefit from safer and more innovative electronic payments* [Memo]. European Commission. https://ec.europa.eu/commission/presscorner/detail/en/MEMO_17_4961

European Commission. (2018). *Payment Services Directive: Frequently asked questions* [Memo]. European Commission. https://ec.europa.eu/commission/presscorner/detail/en/MEMO_15_5793

European Commission. (2020a). *Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)* (Proposal COM(2020) 842 final). European Commission. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0842

European Commission. (2020b). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European strategy for data* (Communication COM/2020/66 final). European Commission. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066&qid=1663850880667

European Commission. (2022a). *Staff working document on data spaces* (Working Document SWD(2022) 45 final). European Commission. https://digital-strategy.ec.europa.eu/en/library/staff-working-document-data-spaces

European Commission. (February 23, 2022b). *Data Act: Commission proposes measures for a fair and innovative data economy* [Press release]. European Commission. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113

European Commission. (2022c). *Data Governance Act explained* [Report]. European Commission. https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained

European Commission. (2022d). *Targeted consultation on open finance framework and data sharing in the financial sector* [Consultation document]. European Commission. https://finance.ec.europa.eu/regulation-and-supervision/consultations/finance-2022-open-finance_en

European Commission. (2022e). *Consultation document: Targeted consultation on open finance framework and data sharing in the financial sector* [Questionnaire]. European Commission. https://finance.ec.europa.eu/system/files/2022-05/2022-open-finance-consultation-document_en.pdf

European Commission. (2022f). *Consultation document: Targeted consultation on the review of the revised Payment Services Directive 2 (PSD2)* [Questionnaire]. European Commission. https://finance.ec.europa.eu/system/files/2022-05/2022-psd2-review-consultation-document_en.pdf

European Commission. (October 31, 2022g). *Digital Markets Act: Rules for digital gatekeepers to ensure open markets enter into force* [Press release]. European Commission. https://ec.europa.eu/commission/presscorner/detail/en/IP_22_6423

European Commission. (June 28, 2023a). *Modernising payment services and opening financial services data: New opportunities for consumers and businesses* [Press release]. European Commission. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3543

European Commission. (2023b). *Proposal for a Regulation of the European Parliament and of the Council on a framework for Financial Data Access and amending regulations (EU) No 1093/2010, (EU) No 1094/2010, (EU) No 1095/2010 and (EU) 2022/2554* (Proposal COM/2023/360 final). European Commission. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0360

European Commission, Directorate-General for Financial Stability, Financial Services and Capital

Markets Union, Bosch Chen, I., Fina, D., & Hausemer, P. (2023). *A study on the application and impact of Directive (EU) 2015/2366 on Payment Services (PSD2)*. (Study FISMA/2021/OP/0002). Publications Office of the European Union. https://data.europa.eu/doi/10.2874/996945

European Data Protection Board. (2020). *Guidelines on the interplay of the Second Payment Services Directive 2 and the GDPR* (Guidelines 06/2020). European Data Protection Board. https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/guidelines-062020-interplay-second-payment_en

Ferrari, M. V. (2022). The platformisation of digital payments: The fabrication of consumer interest in the EU FinTech agenda. *Computer Law & Security Review*, *45*, Article 105687. https://doi.org/10.1016/j.clsr.2022.105687

Financial Stability Board. (2019). *FinTech and market structure in financial services: Market developments and potential financial stability implications* [Report]. Financial Stability Board. https://www.fsb.org/wp-content/uploads/P140219.pdf

Folcia, M., & Fringes, A. (2017). *Waiting until the eleventh hour: European banks' reaction to PSD2* [Report]. PwC. https://www.pwc.com/gx/en/industries/financial-services/publications/waiting-until-the-eleventh-hour.html

Geiregat, S. (2022). *The Data Act: Start of a new era for data ownership?* SSRN. https://doi.org/10.2139/ssrn.4214704

Gogia, J. (2021, July 2). *Intersection between the sui generis database right and the right to data portability*. LexGo. https://www.lexgo.se/post/clash-of-new-tech-and-data-portability-under-the-gdpr-part-2

Hafstad, T., Hjort, G. Z., Johansson, F., Crompton, D., Ullgren, J., Johnston, M. P., & Øyna, M. (2017). *PSD2—Strategic opportunities beyond compliance* [White paper]. Tietoevry. https://ctmfile.com/assets/ugc/documents/PMK_Evry_psd2.pdf

Helgadottir, D. (2020). The interaction between Directive 2015/2366 (EU) on Payment Services (PSD2) and Regulation (EU) 2016/679 on General Data Protection (GDPR) concerning third party players. *Trinity College Law Review*, *23*, 199–224. https://doi.org/10.2139/ssrn.3455428

Holland, M. (2022, January 13). EU closes in on regulating Big Tech with Digital Markets Act. *TechTarget*. https://www.techtarget.com/searchcio/news/252512011/EU-closes-in-on-regulating-big-tech-with-Digital-Markets-Act

Hustinx, P. (2014). *EU Data protection law: The review of Directive 95/46/EC and the proposed General Data Protection Regulation*. European Data Protection Supervisor. https://edps.europa.eu/data-protection/our-work/publications/speeches-articles/eu-data-protection-law-review-directive_en

Ifrim, O. (2023, June 30). Industry reactions to the European Commission's PSR, PSD3, and open finance proposals. *The Paypers*. https://thepaypers.com/expert-opinion/industry-reactions-to-the-european-commissions-psr-psd3-and-open-finance-proposals--1263234

Irion, K., Burri, M., Kolk, A., & Milan, S. (2021). Governing "European values" inside data flows: Interdisciplinary perspectives. *Internet Policy Review*, *10*(3). https://doi.org/10.14763/2021.3.1582

Jacobides, M. G., Bruncko, M., & Langen, R. (2020). *Regulating Big Tech in Europe: Why, so what, and how understanding their business models and ecosystems can make a difference* [White paper]. Evolution Ltd. https://www.evolutionltd.net/post/regulating-big-tech-in-europe

Jones, C. I., & Tonetti, C. (2020). Nonrivalry and the economics of data. *American Economic Review*,

110(9), 2819–2858. https://doi.org/10.1257/aer.20191330

Jones, R., & Ozcan, P. (2021). *Rise of Bigtech platforms in banking* (White Paper 1; Industry Paper). Oxford University - Said Business School. https://www.sbs.ox.ac.uk/sites/default/files/2021-02/Rise%20of%20BigTech%20Platforms%20in%20Banking%20-%20Oxford%20White%20Paper%20Final%20%28002%29.pdf

Karanasiou, A. P., & Douilhet, E. (2016). *Never mind the data: The legal quest over control of information & the networked self*. 100–105. https://doi.org/10.1109/IC2EW.2016.39

Kruger, P. S., & Brauchle, J.-P. (2021). *The European Union, cybersecurity and the financial sector: A primer* [Working paper]. Carnegie Endowment for International Peace. https://carnegieendowment.org/2021/03/16/european-union-cybersecurity-and-financial-sector-primer-pub-84055

Lalova-Spinks, T., & Spajić, D. (2022, June 16). The broadening of the right to data portability for Internet-of-Things products in the Data Act: Who does the act actually empower? (Part I). *The CiTiP Blog*. https://www.law.kuleuven.be/citip/blog/the-broadening-of-the-right-to-data-portability-for-internet-of-things

Lenhard, T. H. (2022). Data protection and data security. In T. H. Lenhard, *Data security: Technical and organizational protection measures against data loss and computer crime* (pp. 3–4). Springer. https://doi.org/10.1007/978-3-658-35494-7_2

Marchant, G. E. (2011). Addressing the pacing problem. In G. E. Marchant, B. R. Allenby, & J. R. Herkert (Eds.), *The growing gap between emerging technologies and legal-ethical oversight: The Pacing Problem* (Vol. 7, pp. 199–205). Springer. https://doi.org/10.1007/978-94-007-1356-7

Marcus, A. A. (1981). Policy uncertainty and technological innovation. *The Academy of Management Review*, *6*(3), 443–448. https://doi.org/10.2307/257379

Margoni, T., Gils, T., & Kun, E. (2022, June 4). Chapter X of the Data Act and the sui generis database right. *The CiTiP Blog*. https://www.law.kuleuven.be/citip/blog/chapter-10-of-the-data-act-and-the-sui-generis-database-right/

McNamee, P. (2020, April 20). Why 'Dutch panic' surrounding PSD2 & GDPR interplay may be an overreaction. *Pont Data & Privacy*. https://privacy-web.nl/artikelen/why-dutch-panic-surrounding-psd2-gdpr-interplay-may-be-an-overreaction-engels/

Michael, K., Kobran, S., Abbas, R., & Hamdoun, S. (2019). *Privacy, data rights and cybersecurity: Technology for good in the achievement of sustainable development goals*. 1–13. https://doi.org/10.1109/ISTAS48451.2019.8937956

Mijs, W., Simon, P., Schindler, N., Ohlhausen, R., Roy, M., Beyrouthy, E., Sabri, T., Roberts, M., & Vandormael, R. (2022). *Final EDPB guidelines on the interplay of the Second Payment Services Directive and the GDPR* [Open letter]. European Banking Federation. https://www.ebf.eu/wp-content/uploads/2022/02/Joint-Payments-Industry-Letter-on-Final-EDPB-Guidelines-PSD2-GDPR-Interplay.pdf

Morton, F. S., & Caffarra, C. (2021, January 5). The European Commission Digital Markets Act: A translation. *VoxEU*. https://cepr.org/voxeu/columns/european-commission-digital-markets-act-translation

Morton, F. S., Etro, F., Latham, O., & Caffarra, C. (2020, June 4). Designing regulation for digital platforms: Why economists need to work on business models. *VoxEU*. https://cepr.org/voxeu/columns/designing-regulation-digital-platforms-why-economists-need-work-business-models

Naujokaitytė, G. (2023, March 7). Do big public EU policy consultations work? For the most part.

Science|Business. https://sciencebusiness.net/news/Horizon-Europe/do-big-public-eu-policy-consultations-work-most-part

Ohab, D., & Shariff, S. (2023). *Open banking in Canada—The path forward* [White paper]. EY Canada. https://www.ey.com/en_ca/banking-capital-markets/open-banking-in-canada-the-path-forward

Omarini, A. E. (2018). Banks and fintechs: How to develop a digital open banking approach for the bank's future. *International Business Research*, *11*(9), 23–26. https://doi.org/10.5539/ibr.v11n9p23

Open finance stakeholders. (2022). *Received contributions: Open finance framework and data sharing in the financial sector* [Consultation Outcome]. European Commission. https://finance.ec.europa.eu/regulation-and-supervision/consultations/finance-2022-open-finance_en

Organisation for Economic Co-operation and Development. (2023). *Data portability in open banking: Privacy and other cross-cutting issues* (Report No. 348; OECD Digital Economy Papers). OECD Publishing. https://www.oecd.org/digital/data-portability-in-open-banking-6c872949-en.htm

Ozcan, P., & Zachariadis, M. (2021). *Open banking as a catalyst for industry transformation: Lessons learned from implementing PSD2 in Europe* (Working Paper No. 2017-006). SWIFT Institute. http://dx.doi.org/10.2139/ssrn.3984857

Peeters, J. (2020). Data protection in mobile wallets. *European Data Protection Law Review*, *6*(1), 56–65. https://doi.org/10.21552/edpl/2020/1/8

Petrović, M. (2020). PSD2 influence on digital banking transformation: Banks' perspective. *Journal of Process Management. New Technologies*, *8*(4), 1–14. https://doi.org/10.5937/jouproman8-28153

PSD2 stakeholders. (2022). *Received contributions: Targeted consultation – Review of the revised payment services directive* [Consultation Outcome]. European Commission. https://finance.ec.europa.eu/regulation-and-supervision/consultations/finance-2022-psd2-review_en

Q&A: Competition and antitrust issues in digital markets. (2021, August). *Financier Worldwide Magazine*. https://www.financierworldwide.com/qa-competition-and-antitrust-issues-in-digital-markets#.Yx89AdNBw2w

Radnejad, A. B., Osiyevskii, O., & Scheibel, O. (2021). Learning from the failure of the EU Payments Services Directive (PSD2): When imposed innovation does not change the status quo. *Rutgers Business Review*, *6*(1), 79–94.

Radnejad, A. B., & Osiyevskyy, O. (2020). Navigating imposed innovation: A decision-making framework. *Business Horizons*, *63*(1), 97–107. https://doi.org/10.1016/j.bushor.2019.09.010

[Reply to the public consultation on the EDPB guidelines regarding the interplay between the GDPR and PSD2]. (2020). European Data Protection Board. https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/gdpr_psd2_guidelines_feedback.pdf

Salemans, C., & Chen, J. (2020). Navigating a trilemma: How the introduction of PSD2, AMLD5 and GDPR shaped a new paradigm for payment service providers. *Deloitte Blog*. https://web.archive.org/web/20230310161545/https://www2.deloitte.com/nl/nl/pages/financial-services/articles/navigating-a-trilemma.html

Snagg, F., Bumpus, G., & Wildner, A. (2023, May). Recent insights from the UK government on the future of UK payment services – Signs of regulatory divergence? *Financier Worldwide Magazine*. https://www.financierworldwide.com/recent-insights-from-the-uk-government-on-the-future-of-uk-payment-services-signs-of-regulatory-divergence

Stulz, R. M. (2019). *Fintech, Bigtech and the future of banks* (Working Paper 26312; NBER Working Paper Series). National Bureau of Economic Research. https://www.nber.org/system/files/working_papers/w26312/w26312.pdf

Tarkowski, A., & Vogelezang, F. (2021). *The argument against property rights in data* (Policy Brief 1). Open Future. https://openfuture.eu/wp-content/uploads/2021/12/Property-rights-in-Data_Open-Future-Brief.pdf

Van Alstyne, M. W., Petropoulos, G., Parker, G., & Martens, B. (2021, December). 'In situ' data rights. *Communications of the ACM*, *64*(12), 34–35.

Verbeke, A., Osiyevskyy, O., & Backman, C. A. (2017). Strategic responses to imposed innovation projects: The case of carbon capture and storage in the Alberta oil sands industry. *Long Range Planning*, *50*(5), 684–698. https://doi.org/10.1016/j.lrp.2017.03.002

Vlieger, A., Kapitan, D., & Poel, E. (2023, September 20). Eindelijk is data delen geen gunst, maar een recht [Finally, data sharing is not a favour, but a right]. *Het Financieele Dagblad*. https://fd.nl/opinie/1490368/eindelijk-is-data-delen-geen-gunst-maar-een-recht

Waldman, A. E. (2021). *Industry unbound: The inside story of privacy, data, and corporate power*. Cambridge University Press. https://doi.org/10.1017/9781108591386

Wiebe, A. (2017). Protection of industrial data – A new property right for the digital economy? *Journal of Intellectual Property Law & Practice*, *12*(1), 62–71. https://doi.org/10.1093/jiplp/jpw175

Zetzsche, D. A., Arner, D. W., Buckley, R. P., & Weber, R. H. (2019). The future of data-driven finance and RegTech: Lessons from EU big bang II. *Stanford Journal of Law, Business & Finance*, *25*(2), 245–288. https://doi.org/10.2139/ssrn.3359399

Zetzsche, D. A., Buckley, R. P., Arner, D. W., & Barberis, J. N. (2017). *From FinTech to TechFin: The regulatory challenges of data-driven finance* (Working Paper No. 6). European Banking Institute. https://dx.doi.org/10.2139/ssrn.2959925

ACKNOWLEDGMENTS

We received excellent feedback on the original and revised version of our paper, for which we would like to thank the three reviewers, academic editors Julia Pohle and Francesca Musiani, as well as managing editor Frédéric Dubois.

Published by

Alexander von Humboldt Institute for Internet and Society

in cooperation with

CREATe

cnrs centre internet et société

R&I IN3 Internet interdisciplinary Institute Universitat Oberta de Catalunya

University of Tartu Johan Skytte Institute of Political Studies