Universiteit Utrecht

LL.M Thesis

Law and Technology in Europe, 2023-2024

Student name: Adriana Riva Dobrovinsky

Student number: 1693328

Supervisor: Dr. Nikita Divissenko

Second reader: Prof. dr. N.N. Purtova

Word count: 17 487 (including footnotes)

Date of submission: 28 June 2024

Title: The FIDA Proposal: Striking a Balance between Data Protection and Financial Innovation

TABLE OF CONTENTS

INTRODUCTION

1. FIDA

The financial industry is currently experiencing a momentous shift due to technological advancements.[1] One key element of this shift is the rising significance of data in financial services.[2] Data can be utilised to create inventive solutions, tailor customer experiences, and enhance productivity. Nevertheless, this greater dependence on data has sparked concerns about safeguarding and respecting consumer privacy.

In 2023, the European Commission proposed the Financial Data Access (FIDA) regulation.[3] This regulation aims to improve and digitise the financial sector with its new way of sharing consumer financial data. FIDA will create a legislative framework that enables the sharing and access of financial data between customers and financial service providers.[4] For financial institutions and data holders, such as credit institutions, insurers, and other financial entities that collect, store, and process customer data, failing to comply with FIDA may result in significant fines and the prohibition of management roles in financial services firms. The FIDA regulation is part of the EU's broader strategy to digitise finance and create a 'Europe fit for the digital age.'[5] This strategy includes other legislative acts, such as the EU's Artificial Intelligence Act (AI Act) and cybersecurity regulations.[6]

1.1 THE FOCUS OF THE THESIS

This thesis aims to examine the delicate balance between innovation and data protection in the context of FIDA. It will provide an overview of FIDA, including its connection to the EU's legal framework for data protection, focusing on the General Data Protection Regulation

[1] Stefanini 2024 '5 Ways Banking & Financial Sectors Have Adapted to Technology' <https://stefanini.com/en/insights/articles/5-ways-banking-financial-sectors-have-adapted-to-technology> accessed 2 April 2024

[2] KPMG 2024 'Data-driven: The new value of financial services data' https://kpmg.com/xx/en/home/insights/2022/04/data-driven-the-new-value-of-financial-services-data.html accessed 2 April 2024

[3] EC, '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' (Text with EEA relevance) COM(2023) 360 final (Brussels, 28.6.2023)

[4] EC 2023 'Financial data access and payments package' https://finance.ec.europa.eu/publications/financial-data-access-and-payments-package_en accessed 2 February 2024

[5] EC, 'A Europe Fit for the Digital Age' (European Commission, 9 March 2021) accessed 2 February 2024

[6] Long, W., and others, 'New EU FIDA Proposal: How Does This Affect GDPR?'(Thomson Reuters, September 26, 2023), https://www.sidley.com/-/media/publications/fida-article-sidley.pdf?la=en&rev=c0463f46d7a54abeb130dd907514d3ea, accessed 2 February 2024

(GDPR).[7] The thesis will analyse the critical provisions of FIDA, emphasising how they strive to reconcile the need for data sharing with the need for data protection. This analysis will include a review of the new articles presented in the proposal, such as the obligations of data holders and users (art. 5, 6 FIDA), the implementation of permission dashboards for financial data-sharing (art. 8 FIDA), and the consent to sharing consumer data (art. 10 FIDA).

Furthermore, this thesis will assess the potential innovative impact of FIDA on data protection and vice versa. It will weigh the possible benefits, such as innovative ways to share the data and customer control, against the potential risks, such as data breaches, the misuse of customer data and possible compliance issues. Ultimately, this thesis will determine whether FIDA appropriately balances innovation and data protection. For instance, the study will examine if FIDA's ability to enhance transparency, consent mechanisms, and data security in the financial sector pushes innovation forward. It will also consider the potential challenges to implementing FIDA effectively and propose recommendations for ensuring that FIDA strengthens data protection in the financial sector. The primary goal of this thesis is to explore the current state of data protection and privacy in the financial industry. It aims to provide an overview of proposed regulation, highlight potential areas for improvement, and suggest practical measures to enhance data protection. By doing so, this study seeks to contribute to future consumer privacy and foster greater confidence in the financial sector.

1.2 THE CHALLENGE OF BALANCING INNOVATION AND DATA PROTECTION

The FIDA regulation is a promising avenue for advancing the financial industry and promoting digital progress. Its goal of enabling the exchange of financial information among customers, financial institutions, and third-party providers (TPPs) is poised to foster a more vibrant and competitive financial ecosystem.[8] Nevertheless, balancing innovation with data security and protection becomes increasingly critical as data sharing expands.

Despite its potential to revolutionise financial services, FIDA has raised concerns regarding its compatibility with existing data protection regulations, specifically the General Data Protection

[7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[8] KPMG 2024 'Embracing the future with open finance and FIDA' https://kpmg.com/lu/en/blogs/home/posts/2024/04/embracing-the-future-with-open-finance-and-fida.html#:~:text=This%20shift%20acknowledges%20the%20value,a%20diverse%20and%20competitive%20ecosystem, accessed 12 April 2024

Regulation.[9] The increased data flow between institutions and TPPs under the FIDA framework may increase the risks associated with data privacy. Unrestricted data sharing through FIDA poses potential risks to sensitive financial information, including credit scores, income data, and transaction history. Such unauthorised access, misuse, and privacy violations could have significant consequences, undermining GDPR's data protection principles of purpose limitation and data minimisation. Financial entities with extensive customer data may be tempted to engage in activities countering these principles. Data breaches or unauthorised access to financial data can damage the public's trust in financial institutions, negatively impacting their reputation and business operations.[10] Moreover, customers affected by data breaches may suffer financial losses and other consequences that can significantly harm their well-being.[11]

A dynamic interplay of technological innovation, regulatory requirements, and data privacy concerns shapes consumer perspectives and challenges in financial data access. Therefore, understanding initiatives like FIDA is crucial due to the intricate relationship between technological innovation and consumer concerns in the financial sector. Balancing innovation with privacy protection is essential for maintaining consumer trust and confidence in financial services. The conflict between fostering innovation and protecting individual rights necessitates thoroughly examining FIDA's legal and ethical implications. This research is crucial because it directly impacts individual rights and freedoms in the digital age. Privacy and data protection are fundamental human rights under European law and essential for building trust in the digital economy. Regulations like FIDA must strive for a balance between innovation and data protection in our data-driven financial world.

This thesis delves into how FIDA's emphasis on data sharing creates tension with data protection principles. It will explore potential solutions to safeguard data privacy while fostering innovation in the financial sector. Ultimately, the thesis aims to recommend ways to

[9] Loyens & Loeff 2024 'Data sharing in the financial sector: An introduction to FIDA' <https://www.loyensloeff.com/insights/news--events/news/data-sharing-in-the-financial-sector-an-introduction-to-fida/#:~:text=In%20addition%2C%20the%20EDPS%20raised,category%20data%20protected%20under%20GDPR> accessed 2 February 2024

[10] Imperva 2024 'Financial services cybersecurity' https://www.imperva.com/learn/data-security/financial-services-cybersecurity/#:~:text=Maintaining%20Consumer%20Trust&text=Any%20breach%20of%20this%20trust,services%20helps%20maintain%20consumer%20trust accessed 12 April 2024

[11] Long, W. and others (n6) 2

ensure data-sharing initiatives like FIDA prioritise transparency, accountability, and individual control over personal financial data.

2. LITERATURE REVIEW

The rapid digital transformation of the financial industry has ignited a continuous debate on data protection and privacy. As financial institutions utilise open financial data to drive innovation, ensuring consumer privacy and data security has become a top priority.[12] This literature review delves into the effectiveness of the FIDA in striking a balance between robust data protection and the promotion of innovation.

Europe has previously implemented the Payment Services Directive (PSD2) to regulate payment data.[13] One of the main provisions of PSD2 is that it requires banks to allow third-party firms to access payment services only with the account holder's consent, giving customers greater control over who can access their data. Encouraging innovation in the financial sector, this directive facilitates the consolidation of payment accounts and transactions from different banks into a single overview. However, it also amplifies existing risks, such as illegal access to data through phishing, making them more significant and potentially more dangerous.[14]

In 2023, the European Commission proposed a FIDA framework to meet the growing demand for data-driven financial services and ensure consumer data control. The FIDA framework will extend data sharing beyond payment data to include other financial products like insurance, loans, and investments.[15] This proposal is expected to significantly impact the financial sector by promoting the use of open financial data while ensuring that data protection and consumer privacy are not compromised.[16] FIDA aims to emphasise customer-centricity, trust, and transparency, aligning with GDPR's objectives of empowering individuals with control over their data.[17]

---

[12] Aldasoro, I. and others, 'Intelligent Financial System: How AI is Transforming Finance' (BIS Working Papers No 1194, Monetary and Economic Department, June 2024) 2

[13] EPC 2023 'Exploring FIDA: Revised rules for financial data sharing access' <https://www.europeanpaymentscouncil.eu/news-insights/insight/exploring-fida-revised-rules-financial-data-sharing-access> accessed 2 April 2024

[14] De Nederlandsche Bank 'Everything you should know about PSD2' https://www.dnb.nl/en/innovations-in-payments-and-banking/fintech-ai-and-innovation/everything-you-should-know-about-psd2/ accessed 2 April 2024

[15] EPC (n13) 4

[16] Eurofi, 'Open Finance and FIDA Proposal' (Eurofi, February 2024) 147 https://www.eurofi.net/wp-content/uploads/2024/03/eurofi_open-finance-fida-proposal_ghent_february-2024.pdf accessed 20 May 2024

[17] Long. W. and others (n6) 2

Introducing the FIDA is crucial to advancing Open Finance in the financial sector. Sigrid Hansen provides valuable insights into FIDA's transformative potential. FIDA expands data sharing beyond payment accounts and introduces new opportunities for stakeholders.[18] The implementation of FIDA has significant consequences for how data is shared and the responsibilities of stakeholders. This includes navigating complex regulatory frameworks, implementing data-sharing schemes, and addressing compensation for data holders.[19]

However, while FIDA seeks to facilitate data sharing for innovation, it imposes strict requirements on data processing, consent, and accountability.[20] Scholars have raised concerns about the extent of data sharing, particularly regarding sensitive financial information, such as the potential for data breaches and the misuse of said information.[21] For instance, EDPS emphasises the need for clear boundaries and safeguards to prevent misuse of economic data, which directly relates to FIDA's objective of ensuring robust data protection.[22] Hansen underscores the necessity for regulatory standardisation and enhancement to provide high-quality data security and consumer trust in Open Finance. This work investigates whether FIDA can balance innovation with robust data protection measures. Reyna and Merkou discuss the EC's proposal, emphasising its benefits for competition and consumer choice while highlighting the need for improved consumer protection measures.[23] Their work points to a knowledge gap on how FIDA can foster competition and ensure comprehensive consumer protection simultaneously. Other authors, Porter and Lubowicka, emphasise the importance of the proposal's compliance with GDPR principles to protect individuals' rights and privacy within the framework of open banking.[24][25]

[18] Hansen, S, 'How will Open Finance and the Financial Data Access Regulation impact the Financial Sector?' (2024) EY Belgium, Financial Services Risk, Compliance and Internal Audit Partner, https://www.ey.com/en_be/financial-services/how-will-open-finance-and-financial-data-access-regulation-impact-financial-sector, accessed on 7 February 2024

[19] ibid

[20] EDPS (23 Aug 2023) Financial and Payment Services: Use of Personal Data Should Remain Proportionate and Fair, https://www.edps.europa.eu/system/files/2023-08/2023-0730_d2425_opinion_en.pdf accessed on 7 February 2024

[21] Chatzigiannis, P. and others 'Privacy-Enhancing Technologies for Financial Data Sharing', https://arxiv.org/abs/2306.10200, accessed on 7 February 2024

[22] EDPS (n20)

[23] BEUC, 'The Consumer Voice in Europe: ACCESS TO CONSUMERS' FINANCIAL DATA: BEUC position paper on the proposed Financial Data Access Regulation'

[24] Porter, A., 'GDPR vs. PSD2: Safeguarding Sensitive Financial Data', BigID Blog, https://bigid.com/blog/gdpr-vs-psd2-compliance/, accessed on 7 February 2024

[25] Lubowicka, K., 'GDPR in Banking – How to be Sure Your Web Analytics Complies With the New Law', Piwik PRO Blog, November 30, 2017, updated October 14, 2020, https://piwik.pro/blog/gdpr-in-banking-web-analytics/, accessed on 7 February 2024

Nevertheless, small and medium-sized enterprises often need more resources to meet GDPR requirements.[26] This raises a pertinent issue for the research question of the effectiveness of FIDA in ensuring GDPR compliance and protecting consumer privacy. Financial institutions face challenges in balancing regulatory compliance with innovation, highlighting the need for regulatory support in technological advancement.[27] Vrabec indicates a gap in how FIDA might leverage technological advancements to strengthen data protection by examining the effectiveness of data subject rights under GDPR and suggests exploring technological solutions to enhance data.[28] Wilson discusses the trade-offs of increased data sharing in open banking for consumer privacy, emphasising the importance of consumer control and regulatory limitations on third-party data collection[29], which explores whether FIDA can balance open data benefits with stringent privacy controls. Boissay et al. discuss how efficiency gains and broader financial access are promising but raise data privacy and competition concerns, stressing the need for coordinated policies.[30]

This review highlights the delicate balance regulators must strike between promoting innovation and protecting traditional financial institutions' interests.[31] Implementing FIDA has significant consequences for data-sharing and stakeholder responsibilities, requiring navigation of complex regulatory frameworks, data-sharing schemes, and compensation for data holders.[32] Kurapati and Gilli highlight the communication gaps between legal and tech experts under GDPR concerning personal data protection and innovation.[33] This broader perspective

[26] Mladinić, A., Vukić, Z., Rončević, A., GDPR Compliance Challenges in Croatian Micro, Small and Medium Sized Enterprises, https://hrcak.srce.hr/ojs/index.php/pravni-vjesnik/article/view/23972, accessed on 7 February 2024

[27] Elliott, K. and others 'Know Your Customer: Balancing innovation and regulation for financial inclusion. Data & Policy.' 2022;4:e34. doi:10.1017/dap.2022.23

[28] Vrabec, H.U., Data Subject Rights under the GDPR (Oxford, 2021; online edn, Oxford Academic, 22 July 2021), https://doi.org/10.1093/oso/9780198868422.001.0001, accessed 7 Feb. 2024

[29] Wilson C. M. II, 'Data Sharing Is Caring: Consumer Privacy and International Approaches to Open Banking' (2022) 53 Geo Wash Int'l L Rev https://www.proquest.com/openview/557ee7b920a5b40de190e139d8862bd4/1?pq-origsite=gscholar&cbl=44595

[30] Boissay, F. and others 'Big techs in finance: on the new nexus between data privacy and competition' (2021) (BIS Working Papers No. 970). Monetary and Economic Department, https://www.bis.org/publ/work970.pdf, accessed on 7 February 2024

[31] ESBG, 'Response to the EC Call for Feedback on the Proposed Regulation on the Financial Data Access Framework' (October 2023) ESBG Transparency Register ID 8765978796-80, https://www.wsbi-esbg.org/esbg-response-to-the-ec-public-consultation-on-the-proposed-regulation-on-the-financial-data-access-framework-fida/, accessed on 7 February 2024

[32] Hansen (n18)

[33] Kurapati S., Gilli L., 'Synthetic Data: A Convergence between Innovation and GDPR' (2023) 11 J Open Access L 1, accessed on 7 February 2024

underscores the EU's commitment to promoting transparency, competition, and market integrity in the financial sector.[34]

2.1 THE GAP IN LITERATURE

Although there is existing literature on data protection and innovative approaches within open banking systems, further research is needed to understand the specific implications of the Digital Financial Package for consumer protection and future innovations in the European financial sector. Specifically, a gap exists in comprehensively evaluating how the proposed Financial Data Access framework can balance the dual objectives of promoting innovation and ensuring robust data protection. This thesis aims to address this gap by providing a scholarly analysis of the EC's proposed FIDA. It will examine the evolution of data protection within the European financial industry, focusing on the debate between proponents of stringent data protection compliance and data minimisation and those advocating for accessible data-sharing to facilitate innovation and collaboration among stakeholders. The thesis will critically evaluate the FIDA proposal, particularly its provisions regarding data access obligations on data holders and users (Articles 5 and 6 FIDA), implementation of permission dashboards (Article 8 FIDA), and financial data sharing consent (Article 10 FIDA).[35] It will assess FIDA's potential to enhance transparency, consent mechanisms, and data security in the financial sector, addressing the research question. Furthermore, the thesis will propose potential avenues for future studies on safeguarding consumer data under FIDA while maintaining its innovative approach to data sharing. It will pinpoint current trends, unresolved concerns, and ambiguous aspects within the literature to guide future research initiatives and legal discussions in this dynamic field.

3. RESEARCH QUESTION

As one delves deeper into this topic, it becomes apparent that there is a pressing question about FIDA's transformative power in the financial industry. While open data access holds immense potential, concerns surrounding data protection and compliance with regulations such as GDPR introduce a crucial tension that must be addressed.

Given the potential conflict, a critical research question emerges:

[34] Moloney N, EU Securities and Financial Markets Regulation (4th edn, Oxford University Press 2023) https://global.oup.com/academic/product/eu-securities-and-financial-markets-regulation 9780198844877?cc=nl&lang=en&#, accessed on 7 February 2024
[35] FIDA

Does the Financial Data Access (FIDA) proposal effectively balance the potential benefits of open financial data for innovation within the financial sector with the need to ensure robust data protection, privacy, and consumer rights?

This central question will steer the analysis of FIDA's provisions, their potential impact on data protection, and possible solutions to implement the proposal without causing harm. By exploring these aspects, this thesis endeavours to uncover whether FIDA can unleash innovation while simultaneously upholding individual rights and consumer autonomy within financial data.

4. CHAPTERS AND METHODOLOGY

4.1 CHAPTERS

The research begins with exploring FIDA's background and context in the First Chapter. The focus will be on the evolution of financial data regulation, shedding light on the origins and progression of FIDA and its predecessor, the Payment Services Directive (PSD2). Subsequently, one will delve into the provisions of FIDA, with a particular emphasis on data protection, and how these provisions encourage innovation in the financial industry.

The Second Chapter will delve into FIDA's central challenge: the delicate balance between driving innovation and maintaining strong data protection measures. Through a comprehensive analysis, this thesis will explore how FIDA’s innovative ways jeopardise data protection by examining the effectiveness of its proposed safeguards in protecting consumer rights and privacy and how the other data protection measures hinder innovation by making it hard to comply with. Ultimately, the thesis will investigate the potential conflict between FIDA's focus on innovation and the established data protection principles.

Chapter Three explores potential solutions within this discussion while referencing FIDA's articles. In particular, it analyses the tension points from Chapter Two and considers how they could be resolved with the appropriate approach, balancing innovation and data protection.

The conclusion will present a comprehensive summary of the thesis's key findings. The analysis of FIDA's impact on data protection and innovation will be carefully synthesised, emphasising the potential benefits and risks associated with the regulation and answering the stated research question.

4.2 METHODOLOGY

The research will primarily utilise a doctrinal methodology, systematically examining the provisions of FIDA through legal text analysis.[36] This approach focuses on clauses and articles relating to data access and sharing, including conditions for sharing, the role of customer consent, and limitations on access. Additionally, the analysis will explore the safeguards proposed by FIDA to protect consumer data privacy, such as provisions on data security, minimisation, purpose limitation, and data subject rights. The methodology will also assess how FIDA promotes innovation in the financial sector, including provisions encouraging data-driven products and services and potential conflicts between innovation and data protection principles. The research will employ comparative analysis with GDPR as a secondary method to provide a comprehensive understanding.[37] Although the main emphasis is on FIDA, the study will incorporate a comparative perspective to underscore the degree of alignment or divergence between FIDA's data protection approach and the established framework of GDPR. By adopting this doctrinal approach, the research aims to provide a thorough legal analysis of FIDA's provisions and their implications for data protection and innovation within the financial sector.

[36] Hutchinson, T., Duncan, N., (2012). Defining and Describing What We Do: Doctrinal Legal Research. Deakin Law Review 17 85 10.21153/dlr2012vol17no1art70

[37] Zahidul I., Moin U., (2023). IMPORTANT ROLE OF COMPARATIVE LEGAL RESEARCH. *Journal of Asian and African Social Science and Humanities*. 9. 31 10.55327/jaash.v9i3.316.

CHAPTER I. A NEW ERA FOR FINANCIAL DATA REGULATION

1. FINANCIAL INNOVATION

The rise of Financial Technology, commonly known as FinTech, has significantly transformed the way individuals and businesses handle their finances.[38] This innovative approach uses cutting-edge technology solutions to provide more efficient, secure, and accessible financial services.[39] With the integration of FinTech, individuals can now enjoy a wide range of financial products and services, including mobile banking, peer-to-peer lending, cryptocurrency transactions, budgeting tools, and investment management platforms. FinTech has transformed the traditional financial landscape, making it more convenient and accessible.[40]

While the advent of fintech is undoubtedly groundbreaking, it has brought concerns regarding safeguarding data privacy and security.[41] The financial industry, in particular, is grappling with this issue, with fintech companies implementing various measures to tackle the challenge. These measures include adopting regulatory, technical, and compliance measures, such as access controls, encryption, and data governance policies, to ensure the safety and privacy of financial data stored in the cloud.[42]

Additionally, fintech companies embrace consumer and data protection laws as part of their compliance measures.[43] Regulators are grappling with balancing FinTech's benefits with consumer protection worldwide. Various approaches have been implemented to address the efficiency-privacy trade-off that arises from the widespread use of personal data.

---

[38] Jain R., Prajapati D., Dangi A., 'Transforming the Financial Sector: A Review of Recent Advancements in FinTech' (2023) *International Journal for Research Trends and Innovation*, 256 https://ijrti.org/papers/IJRTI2302043.pdf accessed on 10 April 2024

[39] Hazar A., Babuşcu S., *Financial Technologies: Digital Payment Systems and Digital Banking. Today's Dynamics* (2023) 162 https://ritha.eu/storage/320/4_jorit_HazarA_BabuscuS.pdf accessed on 10 April 2024

[40] Innovation & Tech Today. (n.d.). How Has Technology Impacted The Way We Manage Our Finances?, innotechtoday.com, accessed on 10 April 2024

[41] Oyewole A.T. and others, 'Data Privacy Laws and Their Impact on Financial Technology Companies: A Review' (2024) 5 *Computer Science & IT Research Journal* 629 https://ijrti.org/papers/IJRTI2302043.pdf accessed on 10 April 2024

[42] Aldboush H.H.H., Ferdous M. 'Building Trust in Fintech: An Analysis of Ethical and Privacy Considerations in the Intersection of Big Data, AI, and Customer Trust'. *International Journal of Financial Studies*. 2023; 11(3):90. 16 https://doi.org/10.3390/ijfs11030090

[43] Rehman, F.U. and others DataDefense: Examining Fintech's Security and Privacy Strategies. Eng. Proc. 2023, 32, 3., 6, https://doi.org/10.3390/engproc2023032003

One approach is to restrict the processing of user data, which recent data protection laws have clarified to protect personally identifiable information.[44] However, these laws need to balance differences in privacy concerns and the use of data, which can lead to cost inefficiencies and limit potential benefits.

Another approach is to give consumers greater control over their personal data, which can foster competition by allowing customers to grant firms access to relevant information.[45] Recent open banking initiatives are examples of concrete policy actions in this direction, requiring financial firms to make their customers' transactions data portable through open Application Programming Interfaces (APIs). These policies help resolve inefficiencies by allocating property rights and creating a competitive market for data.[46]

Still, due to asymmetrical access, they do not fully level the playing field between big tech firms and incumbent service providers.[47]

The EC proposed a FIDA framework to address the increasing need for data-driven financial services. The proposal aims to ensure that consumers retain control over their data while meeting this demand from both consumers and financial firms. This chapter explores the evolution of financial data regulations, focusing on introducing the FIDA regulation.

1.2 THE PREDECESSOR: PAYMENT SERVICES DIRECTIVE (PSD2)

Before FIDA emerged, the European financial sector depended on the Payment Services Directive (PSD2), implemented in 2018, to govern payment data. PSD2's objective was to establish a more transparent and equitable payment services market by mandating banks to disclose customer information to authorised TPPs.[48] Adopting an "open banking" approach has

[44] Hoepman, JH., "Making Privacy By Design Concrete." (2018) 28 https://www.semanticscholar.org/paper/Making-Privacy-By-Design-Concrete-Hoepman/ede8df242f6f58629e079ab21af80b4b63b81f1e accessed on 10 April 2024

[45] Bhattacharya A, 'Do privacy and competition concerns go hand in hand? Exploring the theoretical and practical hurdles for the incorporation of privacy concerns in a competition law regime that emphasizes economic efficiency and consumer welfare' (2021) SSRN 1 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3792169 accessed on 10 April 2024

[46] Billiam B., Abubakar L., Handayani T., 'The Urgency of Open Application Programming Interface Standardization in the Implementation of Open Banking to Customer Data Protection for the Advancement of Indonesian Banking' (2022) 9(1) *Padjadjaran Journal of Law* 71 https://doi.org/10.22304/pjih.v9n1.a4 accessed on 10 April 2024

[47] Boissay (n30) 5

[48] EC (2023, November 28). Revised rules on payment services - Questions and Answers, ec.europa.eu, accessed on 14 April 2024

led to innovation, empowering FinTech companies to offer exciting new financial products and services.[49]

This approach has enhanced security and data protection measures while driving competition, with established tech giants and nimble fintech startups providing innovative services. These players have seized the opportunity created by open banking to offer tailored applications, personalised financial advice, and efficient payment solutions that elevate the customer experience.[50] The growth of a vibrant third-party ecosystem has been a critical factor in driving the progress of open banking, with both established tech companies and emerging fintech startups contributing to this momentum.[51]

Standardisation and cross-border collaboration have enabled open banking in Europe, with the EU prioritising harmonising best practices. Despite the challenges posed by regulatory compliance, data security, and customer trust, the progress made by open banking in Europe has been substantial.[52]

However, PSD2 has limitations. This regulation primarily deals with payment services and access to payment data and does not adequately address broader financial data sharing.[53] Access to financial data upholds the rights of consumers and small businesses to share their payment data with regulated entities of their choice, preventing Account Servicing Payment Service Providers (ASPSPs) from hindering competition and third-party innovation.[54] The strategy for TPPs to link access to payment data to mandatory security standards with the goal of using payment data as a stepping stone towards a broader "Open Finance" policy[55] has led

[49] Dhuri M.P, 'Open Banking: Digital Innovation in Banking Service in India' (2022) 21(7) YMER 543 https://ymerdigital.com/uploads/YMER210752.pdf accessed on 14 April 2024

[50] Wilson (n29) 53

[51] Belén B.P. and others, '"Pick Someone Who Can Kick Your Ass" - Moneywork in Financial Third Party Access' (2021) 4 CSCW Proceedings of the ACM on Human-Computer Interaction 1 https://doi.org/10.1145/3432917 accessed on 14 April 2024

[52] Macro Global (2023, November 21). Regulators & its Role in Open Banking Innovation in Europe, Macroglobal.co.uk, accessed on 14 April 2024

[53] EBA, Final Report on the amendment of the RTS on SCA&CSC, https://www.eba.europa.eu/sites/default/files/document_library/Publications/Draft%20Technical%20Standards/2022/EBA-RTS-2022-03%20RTS%20on%20SCA%26CSC/1029858/Final%20Report%20on%20the%20amendment%20of%20the%20RTS%20on%20SCA%26CSC.pdf, 6, accessed on 15 of April 2024

[54] DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL Of 25 November 2015 On Payment Services In The Internal Market, Amending Directives 2002/65/EC, 2009/110/EC And 2013/36/EU And Regulation (EU) No 1093/2010, And Repealing Directive 2007/64/EC, Article 66

[55] FDATA (2019, June). The Unintended Consequences of PSD2 RTS., https://fdata.global/europe/wp-content/uploads/sites/2/2019/06/The-Unintended-Consequences-of-PSD2-RTS-FDATA-EUROPE-and-ETPPA.pdf, accessed on 15 of April 2024

to the creation of Regulatory Technical Standards (RTS), developed by the European Banking Authority (EBA) to ensure uniform application of the PSD2 across the European Economic Area (EEA).[56]

To further promote the innovative approach to developing open data sharing, the EC introduced the FIDA. FIDA's primary goal is not only to enhance open banking but also to facilitate innovation and business growth using financial data as a business tool.[57] FIDA seeks to empower consumers by giving them greater control over their financial data and stimulating innovation in the financial sector by enabling fintech firms and other industry participants to develop new services based on this data.[58] Unlike PSD2, FIDA encompasses a wider array of financial data beyond just payment information, thus taking a more comprehensive approach to open finance.[59] FIDA aims to build on PSD2's achievements by offering a more all-encompassing and unified approach to financial data management. Moreover, the proposal strives to strike a better balance between leveraging open financial data for innovation and safeguarding data protection, privacy, and consumer rights. It was necessary to examine the previous introduction of innovation to fully assess whether the FIDA effectively addresses the challenge of balancing the potential benefits of innovation with the need to ensure data protection and consumer rights.

1.3 THE RISE OF FIDA

The FIDA proposal marks a significant change in the EU's financial regulations.[60] This introduction of 'Open Finance' opens up opportunities for innovative services and business models in the financial industry.[61] FIDA takes a comprehensive approach to data sharing and innovation in the financial sector.[62] It builds on the concept of Open Banking by enabling the sharing, accessing, and reusing of personal and non-personal data to provide a broad range of

[56] EBA (n53)
[57] EY, 'Why FiDA Will Unleash Change Across European Financial Services' (EY, 12 June 2023) https://www.ey.com/en_gl/insights/financial-services/emeia/why-fida-will-unleash-change-across-european-financial-services accessed 21 June 2024
[58] Brite Payments, 'What Is Financial Data Access (FIDA)? And What Does It Mean for Your Business?' (Brite Payments, 11 June 2024) https://britepayments.com/resources/article/fida/ accessed 21 June 2024
[59] ibid
[60] Insurely. (2023, October 26). Ensuring Data Privacy and Security in Open Finance, https://www.insurely.com/blog/ensuring-data-privacy-and-security-in-open-finance-0#:~:text=Unleashing%20the%20Power%20of%20Data&text=In%20the%20world%20of%20finance,empowerment%2C%20and%20transparency%20are%20key, accessed 15 of April 2024
[61] Zeynalova A, 'From Closed Banking to Open Banking: Risks and Opportunities' (2024) 3(3) *Journal of Applied Business, Taxation and Economics Research* doi.org/10.54408/jabter.v3i3.278 accessed 15 of April 2024
[62] ibid

financial services.[63] That means the financial industry can create innovative products and services by sharing data to benefit consumers and businesses. As with open banking, open finance can lead to more personalised financial products and better services when compared to other financial products.[64] However, both concepts face common challenges, such as ensuring data security, protecting consumer rights, and maintaining customer trust. FIDA promises that customers remain in control as they must grant permission before sharing their data and can withdraw this permission at any time.[65] FIDA aims to bolster data protection measures, instilling consumer confidence within the open finance ecosystem. Its pivotal role lies in establishing rigorous standards for customer agency and oversight over their data. By prioritising transparency in data sharing and making control mechanisms easily comprehensible and accessible to consumers, FIDA aims to fortify trust in open finance. This regulation recognises that safety encompasses more than just data protection; it also encompasses how the customer shares and manages information. As a result, FIDA aims to ensure that a solid foundation of trust and security underlies open finance.[66] The question of whether this promise is justified will be examined further.

1.4 KEY PROVISIONS OF FIDA

The proposal has significantly reshaped the financial services landscape.[67] Focusing on open banking and fostering competition, FIDA has introduced several vital provisions directly impacting data protection.

FIDA aims to transform the financial services industry by promoting secure data sharing and empowering consumers.[68] Article 2 of FIDA's purview encompasses a wide range of data, including but not limited to information on investments, crypto-assets, insurance, pensions, loans, mortgages, and savings.[69] This also includes data on individual and business customers

[63] Sugarda P.P., Wicaksono M.R., 'Enhancing the Competitiveness of Indonesia's Financial Services Sector in the Digital Era through Open Banking: Lessons Learned from the UK's Experience' (2023) 2(1) *Journal of Central Banking Law and Institutions* 159 https://doi.org/10.21098/jcli.v1i2.15 accessed 15 of April 2024

[64] iGCB, Open Opportunities with Open Finance Whitepaper in collaboration with AWS (iGCB, 2024) 3 https://www.igcb.com/wp-content/uploads/Open_Opportunities_with_Open_Finance_iGCB_AWS_compressed.pdfaccessed 21 June 2024

[65] Loyens & Loeff (n9)

[66] KPMG (n8)

[67] Wessing T., PSD3 & PSR: Reshaping the EU payment services regulatory landscape, 4 July 2023, https://www.taylorwessing.com/en/insights-and-events/insights/2023/07/reshaping-the-eu-payment-services-regulatory-landscape#:~:text=Since%20adoption%20of%20the%20Second,role%20model%20for%20other%20jurisdictions, accessed 16 April 2024

[68] EC (n4)

[69] FIDA article 2

that financial institutions typically gather, store, and manage during regular customer interactions. Additionally, it covers data that customers transmit and transactional data that arise from customers' interactions with their financial service providers. It is important to note that this data includes personal data about identified or identifiable individuals and non-personal data about business entities or financial product features.[70]

The regulatory guidelines detail the crucial roles of financial institutions and TPPs in the context of data sharing. Articles 5 and 6 set forth specific obligations for data holders and users. Under Article 5, data holders are required to furnish requested data to data users in a standardised format and quality. This must be done while maintaining secure communication and upholding confidentiality, trade secrets, and intellectual property rights. Furthermore, data holders must provide customers with a permission dashboard. Compensation for the data holder is only possible under a financial data sharing scheme or the Commission delegated act if no such scheme exists (Article 5.2). [71][72]

Additionally, in its draft report in December 2023, the European Parliament stated that data holders should obtain 'explicit permission' from customers to share their data.[73] Article 6 of FIDA delineates the responsibilities of data users, which primarily focus on utilising customer data solely for the purpose for which permission has been granted, safeguarding customer data, and adhering to storage limitations by deleting unnecessary data.[74][75] Moreover, Financial Information Service Providers (FISPs) must comply with authorisation and organisational requirements. The EP proposed that to ensure fair competition, effective oversight of new participants, and safeguarding customer data, non-EU businesses should not be eligible for authorisation as FISP.[76] These articles pave the way for responsible data handling practices, protecting consumer information while enabling secure sharing.

[70] EC, 'Finance Events Presentation' (5 September 2023) 5 https://finance.ec.europa.eu/system/files/2023-09/finance-events-230905-presentation_en.pdf accessed 16 April 2024
[71] FIDA article 5
[72] Projective Group 2023 'Unveiling FIDA: Financial transparency and consumer empowerment' https://www.projectivegroup.com/unveiling-fida-financial-transparency-and-consumer-empowerment/ accessed 2 April 2024
[73] EP, 'Draft Report on the Proposal for a Regulation of the European Parliament and of the Council on a Framework for Financial Data Access' 52 https://www.europarl.europa.eu/doceo/document/ECON-PR-757355_EN.pdf accessed 16 April
[74] FIDA article 6
[75] EC (n70) 9
[76] EP (n73) 53

To ensure responsible and secure management of financial data, FIDA has implemented additional safeguards. Data holders are required to provide permission dashboards to customers, according to Article 8.[77] The implementation of the dashboards promises to grant customers unparalleled control over their data, allowing them to manage how it is used. Data users must also adhere to strict boundaries to protect consumers from high-risk activities. Only authorised financial institutions and FISPs are permitted to access customer data. The permission dashboard must be easily accessible, accurate, and understandable, meeting all requirements outlined in Article 8. Customers have the ability to withdraw and re-establish permissions, view ongoing permissions with real-time updates and their purpose, and utilise a user-friendly interface.[78] The permission dashboard fosters trust between customers and data users, paving the way for innovative financial products and services.

Article 10 ensures that consumers consent before their data is shared. This provision allows consumers to control how their information is used and creates a responsible data-sharing framework. It promotes innovation within a secure environment, providing fintech companies the confidence to develop cutting-edge solutions, knowing that consumer data is safeguarded.[79] Moreover, Article 9 states that within 18 months of FIDA coming into effect, all data holders and users must join a financial data-sharing program that complies with Article 10. They can become members of multiple sharing schemes, but all data sharing must adhere to the program's guidelines, which both parties are enrolled in.[80]

2. OUTCOME AND NEW CHALLENGES

A look at the evolution of financial data regulation in Europe shows the importance of innovation and adaptation of regulations to meet the modern needs of the financial sector. PSD2 played a key role in promoting the concept of "open banking", leading to significant innovation and improvements in the quality of financial services. However, FIDA seeks a more integrated and comprehensive approach to financial data management.

Despite FIDA's potential, important data protection issues and challenges exist, such as ensuring consumers' rights to control and manage their data, measures to prevent data misuse, and, of course, the balance between innovation and data security. These issues require further

[77] FIDA article 8
[78] ibid
[79] FIDA article 10
[80] FIDA article 9

analysis to ensure that the new framework proposal is effective and can balance innovation with the need for strong data protection and consumer rights.

CHAPTER II. INNOVATION VS. DATA PROTECTION

1. THE PARADOX OF FIDA

The financial industry relies on accessing, analysing, and utilising large amounts of data to drive innovation.[81] An extensive amount of businesses initiated the innovation process because they required specific types of data.[82] Technologies like artificial intelligence, machine learning, and big data analytics require extensive datasets to develop models offering personalised financial services, improving risk assessment, and streamlining operations.[83] However, it is crucial to have robust data protection regulations to protect consumer privacy, prevent misuse of personal information, and uphold ethical standards.[84] This creates a balancing act between promoting innovation and maintaining strict data protection. On one hand, relaxed data protection rules could lead to rapid technological advancements and new financial products.[85] On the other hand, stringent data protection can hinder innovation by creating regulatory obstacles[86], limiting data availability, and increasing compliance costs for financial institutions.

In this scenario, FIDA presents a complex dilemma. While it aims to unleash a new wave of innovation in the financial sector, promote competition, and generate novel data-driven services[87], it also raises concerns regarding the potential compromise of consumer financial data protection.[88] This chapter will delve into the fundamental tension between these two objectives, examining the main points of contention in this ongoing debate.

Advocates of FIDA assert that progress hinges on having access to comprehensive financial data sets. They contend this will pave the way for developing advanced algorithms for customised financial guidance, simplified loan applications, and effective risk management

[81] Zetsche D.A. and others 'From Fintech to Techfin: The Regulatory Challenges of Data-Driven Finance' (2018) 14 NYU JL & Bus 393 415

[82] Trabucchi, D., Buganza, T. (2019), "Data-driven innovation: switching the perspective on Big Data", *European Journal of Innovation Management*, Vol. 22 No. 1, 16. https://doi.org/10.1108/EJIM-01-2018-0017

[83] DNB and AFM, 'Data Mobility and the Financial Sector' (Discussion Paper, Dutch National Bank, 2021) 57 https://www.dnb.nl/media/qekh0qka/afm-dnb-discussion-paper-data-mobility-and-the-financial-sector.pdf accessed 10 May 2024

[84] Hutchinson E., 'Keeping Your Personal Information Personal: Trouble for the Modern Consumer' (2015) 43 Hofstra L Rev 1177

[85] Martin N. and others 'How Data Protection Regulation Affects Startup Innovation' *Information Systems Frontiers*. (2019). 21. 10.1007/s10796-019-09974-2. 1309

[86] Schroeder C., Winters B., Davisson J., 'We Can Work It out: The False Conflict between Data Protection and Innovation' (2022) 20 Colo Tech LJ 254

[87] EBF, 'EBF Recommendations on FIDA' (11 December 2023) 1 https://www.ebf.eu/wp-content/uploads/2023/12/EBF_046342-EBF-recommendations-on-FIDA_11.12.23.pdf accessed 10 May 2024

[88] Martin N. and others (n85) 1308

tools.[89] They argue that the end result will be enhanced financial products better designed to suit consumers' needs, potentially resulting in lower costs.[90] Furthermore, FIDA's endorsement of Open Finance bolsters consumers' autonomy by granting them the ability to manage and distribute their data, thereby cultivating a sense of control and potentially intensifying competition among financial institutions.[91]

Despite an optimistic outlook, concerns regarding data protection persist. Detractors contend that the heightened data sharing places consumers at increased risk of breaches and unauthorised access.[92] The financial data gathered through FIDA is substantial, making it potentially vulnerable to sophisticated cyberattacks, resulting in financial losses and identity theft. Additionally, there are apprehensions about algorithmic bias and discriminatory practices within the financial sector due to the potential for third-party vendors to aggregate and profile data. It's worth examining the situation from both perspectives to identify what's preventing this imbalance.[93]

2. INNOVATION JEOPARDISES DATA PROTECTION

2.1 INCREASED DATA COLLECTION AND SHARING

FIDA seeks to unleash a new wave of innovation in the financial industry by enabling the exchange of customer financial data with third-party providers.[94] Although this holds the potential for personalised financial products and services, it also presents a substantial challenge: the heightened risk of data breaches and unauthorised access to sensitive financial information. This underscores the inherent vulnerabilities of expanding data-sharing practices.[95] Breaches can result from human error or sophisticated cyberattacks, exposing consumers to financial losses and identity theft.[96] This issue aligns with the principles of the

[89] Truchet M., 'Open Finance: Objectives of the Financial Data Access (FIDA) Proposal' (Eurofi, September 2023) 53 https://www.eurofi.net/wp-content/uploads/2023/11/eurofi_open-finance_objectives-of-the-financial-data-access-fida-proposal_santiago_september-2023-1.pdf accessed 10 May 2024
[90] ibid 58
[91] ibid 53
[92] Xiong W., 'Privacy and Personal Data Protection' (Princeton University, 2024) 33 https://wxiong.mycpanel.princeton.edu/papers/Privacy.pdf accessed 10 May 2024
[93] CIPL, 'First Report on Artificial Intelligence: AI and Data Protection in Tension' (Centre for Information Policy Leadership, 2021) 11 https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_first_ai_report_-_ai_and_data_protection_in_tension__2_.pdf accessed 10 May 2024
[94] Eurofi, 'Open Finance: FIDA Proposal' (Eurofi, February 2024) 146 https://www.eurofi.net/wp-content/uploads/2024/03/eurofi_open-finance-fida-proposal_ghent_february-2024.pdf accessed 13 May 2024.
[95] Martin K.M., Borah A., Palmatier R.J. Data Privacy: Effects on Customer and Firm Performance. Journal of Marketing., (2016) 36, 81. 10.1509/jm.15.0497
[96] Acquisti A., Taylor C., Wagman L., 'The Economics of Privacy' (2016) 54(2) *Journal of Economic Literature*, 36, <https://doi.org/10.1257/jel.54.2.442> accessed 13 May 2024

GDPR, highlighting the significance of data minimisation. This means that organisations should only gather and retain the data essential for their lawful purposes.[97] FIDA's extensive data-sharing practices go against this principle, prompting worries about the appropriateness and requirement of sharing large volumes of financial data with external parties.

The FIDA initiative to enable the sharing of customer financial data with third-party providers presents many opportunities and challenges.[98] It holds the potential to revolutionise the financial industry by offering more personalised products and services. Still, it introduces new risks and complexities that the industry has yet to navigate. One of the most pressing concerns surrounding third-party access is the potential for data breaches and unauthorised access to sensitive financial information.[99] The interconnected nature of modern financial systems means that any breach or lapse in security could have far-reaching consequences for individual consumers and the stability of the entire financial ecosystem.[100] From the proliferation of human error to the ever-evolving landscape of sophisticated cyberattacks, the vulnerabilities inherent in expanding data-sharing practices are manifold and looming.[101] Furthermore, the issue of data minimisation, as underscored by principles such as those laid out in the GDPR, takes on heightened significance in this context.[102]

However, FIDA's extensive data-sharing practices, which involve the transfer of significant amounts of financial information, often include more data than is necessary for a particular purpose, contrary to the principle of data minimisation. This raises valid concerns about the appropriateness and necessity of transferring significant financial data to outside organisations. Additionally, the consequences of third-party access go beyond just data security worries. More profound inquiries about privacy, consent, and safeguarding consumer interests need to be thoroughly examined and resolved.[103] How can consumers be confident that TTPs will ethically and responsibly use their data? What measures are in place to guarantee transparency and

[97] Null E., Oribhabor I., Escoto W., 'Data Minimization: Key to Protecting Privacy and Reducing Risks' (Access Now, May 2021) 8 https://www.accessnow.org/wp-content/uploads/2021/05/Data-Minimization-Report.pdf accessed 13 May 2024
[98] Eurofi (n94) 146
[99] Martin, Borah, Palmatier (n95) 36
[100] Adelmann F. and others *It's a Small World After All: Cyber Risk and Financial Stability* (IMF Staff Discussion Note, SDNEA2020007, 2020) 12
[101] Oluka, A., Analysing the implications of cybersecurity breaches on firm leadership. Technology audit and production reserves. 6. 22. 10.15587/2706-5448.2023.286985.
[102] Null, Oribhabor, Escoto, (n97) 8
[103] Eurofi, (n94) 148

accountability in the data-sharing procedure? These are just a few intricate issues requiring careful consideration and strong regulatory supervision.

2.2 LACK OF TRANSPARENCY AND USER'S CONSENT

The introduction of new tools, such as the permission dashboards[104], while seemingly valuable for addressing transparency and consent issues within the financial data access framework, has several problems and limitations that must be considered. The permission dashboard risks fostering a misleading sense of transparency despite its aim to empower customers with data control (Article 6).[105] Customers might perceive it as a comprehensive tool for managing their data use permissions. Still, it might not entirely reflect the breadth of data-sharing practices or the intricacy of consent mechanisms (Article 9). This can lead to financial institutions and data users continuing to employ opaque data practices that the dashboard doesn't fully reveal, thereby diminishing its effectiveness as a consent management and trust-building tool. In addition, implementing the dashboard does not guarantee meaningful customer consent (Article 7). While the dashboard may allow customers to revoke or reinstate consents, it does not address the underlying problems associated with informed consent.[106]

Firstly, in the context of shared databases, obtaining consent is made more difficult by data modification and retrieval, which requires overly extensive consent. [107] This means that customers are forced to consent to using their data in various contexts without knowing how and where it will be used. Thus, a dashboard can serve as a formal tick box rather than a fundamental mechanism for informed consent. [108]

Second, as financial data moves across interconnected systems, it can be difficult for consumers to understand when and how they consent to its use. Consent forms can be confusing, with lengthy terms and conditions often written in legal jargon, making the consent process opaque

[104] FIDA Article 8
[105] DIGITALEUROPE, 'FIDA Position Paper' (DIGITALEUROPE, November 2023) 10 https://cdn.digitaleurope.org/uploads/2023/11/DIGITALEUROPE-FIDA-position-paper.pdf accessed 13 May 2024
[106] Bless C., and others, 'Raising Awareness of Data Sharing Consent Through Knowledge Graph Visualisation' in M Alam and others (eds), *Further with Knowledge Graphs* (Studies on the Semantic Web, vol 53, IOS Press 2021) 47 https://doi.org/10.3233/SSW210034 accessed 13 May 2024
[107] Drien O., Amarilli A., Amsterdamer Y., 'Managing Consent for Data Access in Shared Databases' (Bar-Ilan University and LTCI, Télécom Paris, Institut Polytechnique de Paris, 2024) 3 https://u.cs.biu.ac.il/~amstery/files/managingconsent.pdf accessed 13 May 2024
[108] ibid 45

and difficult to understand.[109] Even if consumers overcome these obstacles and learn about FIDA's data-sharing mechanisms, they may feel powerless to exercise meaningful control over their information.

Finally, without robust governance and consent revocation mechanisms, consumers cannot effectively assert their preferences or protect their privacy rights. [110] This weakens consumers' control over their data and increases their vulnerability to potential misuse of their financial information, ultimately undermining trust in the financial ecosystem.

2.3 ALGORITHMIC BIAS

The rise of algorithmic bias presents a formidable challenge within the context of FIDA's implementation, particularly concerning the utilisation of AI algorithms for financial analysis and decision-making.[111] These algorithms, fueled by vast datasets made accessible through FIDA, hold immense potential to revolutionise financial services by enabling more accurate risk assessments, personalised product recommendations, and streamlined processes. However, they also carry inherent risks of perpetuating and exacerbating existing biases within the financial system.[112]

One of the primary concerns is the potential for unequal access to financial products and services.[113] If new data-sharing algorithms inadvertently incorporate or amplify biases present in historical data, they may discriminate against certain groups based on race, gender, or income.[114] Furthermore, the nature of many innovative algorithms exacerbates the challenge of identifying and addressing bias.[115] Unlike traditional decision-making processes where human judgment can be scrutinised and corrected, algorithms operate behind a veil of complexity that can obscure the mechanisms driving their decisions.[116] As a result, it can be

[109]Omri B.S., 'The Myth of Opportunity to Read' (2018) 13 https://home.uchicago.edu/omri/pdf/articles/The_Myth_Of_Opportunity_To_Read.pdf accessed 13 May 2024.
[110] Bruhner C.M., Hasselquist D., Carlsson N., 'Bridging the Privacy Gap: Enhanced User Consent Mechanisms on the Web' (MADWeb 2023) 2 https://dx.doi.org/10.14722/madweb.2023.23017 accessed 13 May 2024
[111] KPMG LLP, 'Algorithmic Bias and Financial Services: A Report Prepared for Finastra International' (March 2021) 3 https://www.kpmg.com/uk accessed 13 May 2024
[112] Zhuang L.J., Sockin M., Xiong W., 'Data Privacy and Algorithmic Inequality' (May 2023) 33 https://wxiong.mycpanel.princeton.edu/papers/Privacy.pdf accessed 13 May 2024
[113] Klein A., 'Reducing Bias in AI-based Financial Services' (Brookings, 2020) 4 https://www.brookings.edu/articles/reducing-bias-in-ai-based-financial-services/ accessed 13 May 2024
[114] Bajracharya A. and others Recent Advances in Algorithmic Biases and Fairness in Financial Services: A Survey. (2022). 2. 10.1007/978-3-031-18461-1_53
[115] ibid 7
[116] Herzog L., 'Old Facts, New Beginnings: Thinking with Arendt about Algorithmic Decision-Making' (2021) 83 The Review of Politics 555, 568 https://doi.org/10.1017/S0034670521000474 accessed 13 May 2024

challenging to ascertain whether algorithmic outputs are influenced by bias and, if so, how to rectify these issues effectively. When it comes to data protection, algorithmic bias raises significant concerns about privacy, fairness, and accountability.[117] As AI algorithms become more prevalent in financial institutions' decision-making processes, consumers must trust that these systems are not unfairly treating them or infringing on their privacy rights.[118] To achieve this level of trust and accountability, robust regulatory frameworks and oversight mechanisms are needed to ensure that algorithms are developed, implemented, and monitored in a way that upholds ethical standards and prevents discriminatory practices.[119]

Moreover, the rise of algorithmic bias highlights the significant impact of data protection regulations on the framework and operations of the financial sector. Rules and standards designed to safeguard privacy and data security affect companies' behaviour, competitive strategies and overall dynamics. Data protection laws influence the development of the financial sector, whether it is to account for economies of scale or to evaluate different business models.[120] The following guidelines are especially pertinent within the Markets in Cryptoassets Regulation (MiCA), establishing the legal foundation for utilising crypto assets.[121] For instance, using algorithms to evaluate risks and determine insurance premiums in the insurance industry necessitates substantial volumes of data.[122] Data protection assumes excellent significance as businesses must adhere to rigorous regulations concerning storing, processing, and safeguarding customer data. This could constrain their capacity to innovate and diminish the efficacy of business models reliant on big data and machine learning. Stringent data protection protocols might restrict access to this data or necessitate additional anonymisation and encryption measures, leading to heightened expenses and diminished accuracy of

[117] Nengfeng Z., 'Bias, Fairness, and Accountability with AI and ML Algorithms' (6 May 2021) 1 https://wxiong.mycpanel.princeton.edu/papers/Privacy.pdf accessed 13 May 2024

[118] EPRS, The ethics of artificial intelligence: Issues and initiatives (2020) 58 https://wxiong.mycpanel.princeton.edu/papers/Privacy.pdf accessed 13 May 2024

[119] Giurca A., 'AI Qualitative Report' (July 2020) 9 https://probability.nl/wp-content/uploads/2020/08/AI_qualitative_final.pdf accessed 13 May 2024

[120] Christodoulou P., Limniotis K., 'Data Protection Issues in Automated Decision-Making Systems Based on Machine Learning: Research Challenges' (2024) 4 *Network* 91, 94 https://doi.org/10.3390/network4010005 accessed 27 May 2024

[121] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937

[122] Salman A., Shastri S., Fernandez Vidal M., 'The Role of Data in Inclusive Insurance' (May 2024) 3 https://www.cgap.org/research/publication/role-of-data-in-inclusive-insurance accessed 23 June 2024

algorithms. Consequently, insurance companies may require assistance developing novel products and services, impeding their innovation potential.

Therefore, although data protection regulations are designed to safeguard consumers, they can also impact financial institutions' capacity to embrace and implement new technologies. This underscores the importance of a balanced regulatory approach considering data protection and fostering innovation.

3. DATA PROTECTION HINDERS INNOVATION

3.1 CONSUMER'S AWARENESS

FIDA proposal aims to enhance data sharing in the financial sector to promote innovation, competition, and consumer choice. However, the stringent data protection requirements embedded within the proposal present significant challenges to these objectives. Although data protection laws are designed to safeguard individuals' privacy, they can also create significant barriers to innovation, especially in the financial sector.[123]

One of the critical issues is consumer trust and reluctance to share personal data. Consumers are increasingly aware of the value and risks associated with their personal data.[124] High-profile data breaches and misuse of personal information have heightened these concerns.[125] As a result, individuals are often reluctant to share their data, fearing it might be misused or fall into the wrong hands.[126] This hesitancy poses a significant challenge for financial institutions and fintech companies that rely on data to offer personalised and innovative services.

The consent mechanisms in the FIDA Proposal play an essential role in building consumer trust. Article 5 of the FIDA proposal highlights the significance of securing explicit consumer permission for data sharing. This measure safeguards consumer privacy and empowers individuals to maintain control over their personal information.[127] However, the requirement

[123] Schroeder C., Winters B., Davisson J., (n86) 254
[124] Lee K., Attablayo P., 'Examining the Impacts of Privacy Awareness on User's Self-Disclosure on Social Media' (2023) 5 https://www.researchgate.net/publication/369233614_Examining_the_impacts_of_privacy_awareness_on_user's_self-disclosure_on_social_media accessed 14 May 2024
[125] EC, 'H2020 Programme: Ethics and Data Protection' (European Commission, 2018) 12 https://commission.europa.eu/system/files/2020-06/5._h2020_ethics_and_data_protection_0.pdf accessed 14 May 2024
[126] ibid
[127] FIDA Article 5

for explicit permission may result in consumer hesitance[128], making it more challenging to collect the necessary data for innovative financial services.

Thus, strict data protection requirements may make it more difficult to obtain consumer consent and reduce consumers' willingness to share data, undermining innovation opportunities. If consumers are unwilling to share their data, these services may not operate effectively, hampering the advancement and implementation of new financial products. [129] However, if the FIDA would prioritise strong encryption standards and transparent data storage rules to protect consumer data and drive significant progress in financial technology, the problem might be solved. Strong encryption standards and transparent data retention rules could create an environment where consumers can feel confident sharing their data. This would increase trust in financial institutions and fintech companies, encouraging greater use of their services. This idea will be covered in chapter three.

3.2 COMPLIANCE

Even when consumers are willing to share their data, the process is fraught with complexities. Companies must ensure data sharing complies with stringent data protection regulations like the GDPR.[130] This involves obtaining explicit consent[131], ensuring data is anonymised or pseudonymised where necessary[132], and maintaining robust security measures to protect the data[133]. These requirements can complicate data-sharing, making it cumbersome and less appealing for consumers. The ambiguity of data protection laws creates legal uncertainties, causing financial institutions to be cautious about data-sharing practices.[134]

Ensuring compliance with data protection laws incurs significant costs and operational delays.[135] Financial institutions must invest heavily in compliance infrastructure, which can be

[128] EC (n125) 12
[129] CIPL, 'Recommendations on Transparency, Consent and Legitimate Interest under the GDPR' (Centre for Information Policy Leadership, 19 May 2017) 9 https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf accessed 14 May 2024
[130] Long. W. and others (n6) 1
[131] GDPR Article 6
[132] GDPR Article 5
[133] GDPR article 32
[134] Eiss R., 'Confusion over data-privacy law stalls scientific progress' (2020) 584 *Nature* 498
[135] Fortra, 'The True Cost of Compliance with Data Protection Regulations' (Fortra, 2023) 21 https://static.fortra.com/globalscape/pdfs/guides/gs-true-cost-of-compliance-data-protection-regulations-gd.pdf accessed 14 May 2024

particularly burdensome for smaller fintech companies.[136] These additional costs and delays can prevent new and innovative services from reaching the market promptly, reducing the overall pace of innovation in the sector.

A particular feature of the FIDA proposal is that it requires more detailed consent and transparency in data sharing. Article 8 requires financial institutions to implement strong technical and organisational measures to safeguard consumer data. This may include stricter data storage and processing requirements, tracking, and reporting on each data use.[137] While these measures are crucial for ensuring data security, they also bring considerable complexity and expenses. As mentioned, financial institutions must invest in advanced technologies and processes to meet these requirements, which can be particularly challenging for smaller fintech startups with limited resources.[138]

The high cost and complexity of compliance can serve as a barrier to entry for new players in the market.[139] Smaller companies may struggle to fulfil these strict requirements, reducing the financial sector's diversity and competitiveness.[140] In the FIDA context, new and innovative companies may be forced out of the market, limiting innovation and reducing the sector's growth.

Thus, while FIDA's data protection rules are intended to protect consumers, they may also discourage innovation, especially for smaller companies with insufficient resources to fulfil all the requirements.

3.3 DATA MINIMISATION AND DATA PORTABILITY COMPLEXITIES

Nevertheless, Article 10 of the FIDA proposal enforces data minimisation and purpose limitation principles, which restrict the use of consumer data to specific, predefined purposes.[141] While these principles are crucial for protecting consumer privacy, they also limit the flexibility of financial institutions in using data for innovative purposes. Companies are

[136] Hamza M., 'Exploring Barriers and Pathways to Data Protection by Design within IT Companies' (Master's Programme in IT Management, Department of Informatics, Umeå University, 2017) 13 https://www.diva-portal.org/smash/get/diva2:1154866/FULLTEXT01.pdf accessed 14 May 2024.
[137] FIDA Article 8
[138] Hakizimana S., 'Fintech Startups: What does the Future hold for Financial Institutions in Kenya?' 1 https://www.ijssers.org accessed 15 May 2024
[139] Hieu C.V., Hai N.M., 'Financial Technology: Implementation Experience in Some Countries and Policy Implications' (2022) 42 https://doi.org/10.56097/binhduonguniversityjournalofscienceandtechnology.v5i4.76 accessed 15 May 2024
[140] ibid
[141] FIDA Article 10

unable to repurpose data for new, unforeseen applications that could drive innovation.[142] This restriction reduces the utility of the data available to financial institutions. For instance, data that could be valuable for developing new financial products or improving existing ones may be off-limits if it falls outside the initially defined purpose. Hence, the innovation potential is curtailed as financial institutions cannot fully leverage their collected data.[143]

For instance, an insurance company may gather data on its customers' health and lifestyle to determine premiums. However, based on the proposed guidelines by FIDA, this data can only be utilised for the specific purpose for which the customers have provided consent, i.e., to calculate premiums. If the company identifies that the data could be beneficial in creating a new product, such as personalised wellness programs, which could lower risks for customers and, in turn, lower premiums, using the data for this new purpose would be limited. Consequently, without obtaining customer consent, the insurance company cannot utilise the data collected to develop an innovative product. This results in added expenses and delays as the company will need to seek re-approval, which can be labour-intensive and impact the speed of launching the new product. Then, the capacity for innovation is constrained, as financial institutions cannot fully leverage the data they collect to develop and enhance their services.

Furthermore, Article 12 outlines the right to data portability, allowing consumers to transfer their data from one service provider to another.[144] While data portability is intended to enhance consumer control and market competition, it also presents challenges. Ensuring that data is transferred securely and efficiently between providers while maintaining compliance with data protection regulations requires substantial technical and administrative effort.[145] Once again, the potential for innovation resulting from competition among different entities may be hindered. The costs of meeting data portability requirements present a significant obstacle to innovation, especially for small and medium-sized businesses.[146] This could ultimately lead to

[142] Bitkom, 'GDPR Consultation Report' (Bitkom, February 2024) 22 https://www.bitkom.org/sites/main/files/2024-02/finalbitkomconsultationgdpr-report.pdf accessed 15 May 2024
[143] Custers B. and others, *Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases* (Springer 2013) 281 https://link.springer.com/chapter/10.1007/978-3-642-30487-3_15 accessed 15 May 2024
[144] FIDA Article 12
[145] Graef I., 'Data Portability at the Intersection of Data Protection and Competition Law' (Tilburg University, 2016) 5 https://pure.uvt.nl/ws/portalfiles/portal/45777953/CPI_Graef_data_portability.pdf accessed 15 May 2024
[146] Wohlfarth M., 'Data Portability on the Internet: An Economic Analysis' (2019) 61(5) *Business & Information Systems Engineering* 551, 560 https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1538&context=bise accessed 15 May 2024

market consolidation, with larger corporations dominating and smaller companies struggling to keep up, ultimately stifling overall market innovation.

Additionally, from an operational standpoint, ensuring data portability could delay introducing new products and services as companies prioritise compliance over innovation and adopt a more risk-averse approach.[147] While data portability may empower consumers to control their personal data, it could also reduce investment in user-centric innovations, leading to less innovative services. Finding a balance between data privacy and encouraging innovation is essential to avoid a conservative approach to utilising consumer data.[148]

The FIDA proposal is a crucial advancement towards a more transparent and competitive financial sector. Nonetheless, the strict data protection regulations outlined in the proposal pose notable obstacles to innovation. By comprehending the influence of consumer consent, the complexity of compliance, restrictions on data usage, and data portability, stakeholders can more effectively navigate the intricate equilibrium between safeguarding consumer privacy and promoting innovation. In the FIDA context, financial institutions will need to consider new requirements for explicit consent, data minimisation and purpose limitation, which may make it more difficult to use data for innovative products and services. Tackling these challenges through more precise regulatory direction and supportive actions can facilitate realising the complete potential of data-driven financial services.

4. IS BALANCE POSSIBLE?

Both factions of this discussion bring forth numerous controversies and inquiries. The key lies in delicately balancing the promotion of innovation with safeguarding consumer privacy. The efficacy of the FIDA proposal hinges on the capacity to achieve this equilibrium through the establishment of a robust data security framework encompassing stringent encryption protocols and well-defined data retention practices.[149] Moreover, it is imperative to prioritise transparency and user autonomy through unambiguous and easily accessible consent mechanisms.[150] Furthermore, stringent regulatory supervision and enforcement are essential

[147] ibid
[148] Lenard T.M., 'If Data Portability is the Answer, What is the Question?' (Tech Policy Institute, January 2020) 5 https://techpolicyinstitute.org/wp-content/uploads/2020/01/Lenard_If-Data-Portability.pdf accessed 15 May 2024.
[149] Apinity, 'FIDA Explained' https://apinity.io/fida-en/#:~:text=The%20Financial%20Data%20Access%20Framework,transparent%2C%20and%20interconnected%20financial%20ecosystem accessed 15 May 2024
[150] Long. W. and others (n6) 2

to uphold adherence to data protection principles and forestall potential misuse.[151] While the potential for innovation in the financial sector is undeniable, the question of effectively protecting consumers' financial data in this new ecosystem remains paramount. The adoption of new technologies and services depends heavily on consumer trust, which can only be achieved through stringent data protection measures.[152]

The proposal aims to facilitate access to financial data to foster competition and innovation, ensure a level playing field, and uphold stringent data protection standards to safeguard consumer privacy. FIDA's twofold emphasis is essential: it enables financial institutions and fintech companies to create enhanced services while maintaining consumer trust by protecting their personal data.[153]

Moreover, the expenses associated with compliance and the intricacy of these data protection measures may deter smaller fintech companies from entering the market, potentially hindering innovation. As a result, the regulatory framework needs to maintain a balance that safeguards consumers without excessively burdening innovators.[154]

In this innovative paradigm, the balance between innovation and privacy serves as a driving force for progress rather than just a challenge.[155] If done correctly, the proposal's focus on robust encryption standards and transparent data retention regulations establishes a new benchmark for data security. These measures must guarantee the protection of consumer data and its utilisation in a manner that fosters significant advancements in financial technology.

However, the ongoing discussion and the intricacy and ambition of the FIDA proposal mirror the complexity of the current financial environment. It acknowledges the importance of safeguarding consumer financial data in an increasingly interconnected and data-driven

[151] AmCham EU, 'FIDA Position Paper' (AmCham EU, 2024) 5 https://amchameu.eu/system/files/position_papers/amchameu_fida.pdf accessed 15 May 2024

[152] EPRS, 'Digital Sovereignty for Europe' (European Parliament, 2020) 32 https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf accessed 15 May 2024

[153] Payments Europe, 'Fintech and Digital Assets: Understanding the Regulatory Landscape' (Payments Europe, December 2023) 4 https://www.paymentseurope.eu/wp-content/uploads/2023/12/Payments-Europe_FIDA.pdf accessed 15 May 2024

[154] Hamza (n136) 13

[155] EP, 'The impact of the General Data Protection Regulation (GDPR) on artificial intelligence' 2(European Parliamentary Research Service, 2020) https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf accessed 15 May 2024

world.[156] Nonetheless, it also acknowledges that impeding innovation is not acceptable. The proposal aims to reconcile these conflicting dynamics, fostering a symbiotic relationship in which data security and innovation mutually strengthen each other. FIDA envisions a future in which financial institutions and fintech companies can use data to develop revolutionary products and services without compromising consumer privacy. This future is characterised by a thriving, competitive financial sector that offers consumers more choice, better services, and improved financial well-being.

The next chapter will reveal what solutions in FIDA can already be considered neutralisers of the pressing problem and what new solutions can be proposed for the future success of this regulation in the financial sector.

[156] Loyens & Loeff (n9)

CHAPTER III. POTENTIAL SOLUTIONS

1. INTRODUCTION OF THE SOLUTIONS

Despite extensive discussions, FIDA has introduced several measures to improve data sharing in the financial industry. The successful implementation of these measures depends on carefully planned strategies. This chapter will explore how FIDA regulation can effectively manage the balance between innovation and data protection when implemented correctly and what should be added. The existing FIDA provisions will be analysed to identify their potential to address critical issues. If current measures are found to be insufficient, additional solutions will be proposed to help balance the need for innovation with data protection requirements. Thus, this chapter will offer practical recommendations for creating a secure and innovative financial ecosystem that meets the interests of users and developers of new technologies and services.

1.1 SECURE DATA ACCESS SOLUTIONS

FIDA's framework aims to foster innovation by providing a secure and controlled environment for TPPs to access data. This system ensures that sensitive data remains protected while enabling TPPs to leverage it to develop innovative solutions and services. However, the question arises: how effective is this system in protecting consumer data without creating significant barriers to innovation?

On the one hand, FIDA offers a transparent and reliable set of regulations for TPPs, which should encourage investment and creativity in open banking solutions.[157] The framework sets unambiguous guidelines for managing the sharing of customer data in the financial industry beyond just payment accounts.[158] As a result, it promises to lead to the development of novel financial products and services for users. But how much do these rules encourage innovation if they also create additional complexity and costs for financial institutions?

At the core of FIDA's mission is enabling consumers to switch between financial service providers seamlessly. This should promote a healthy level of competition but requires strict adherence to data protection regulations. Yet, how realistic is it? Open banking APIs are central to FIDA, enabling standardised and efficient data exchange. However, standardised APIs can face security and regulatory compliance challenges. To what extent can APIs be secure and

[157] EC (n4)
[158] Eurofi, (n16) 147

functional, and will this not hinder innovation? Ideally, the switching process becomes more efficient by allowing for data portability. Customers can initiate the switch, and TPPs can then transfer crucial financial information, such as transaction history and account details, to the new provider. This simplifies the process and encourages competition by empowering customers with greater control over their financial data[159], reducing development time and costs.[160] But how viable is this scheme in an environment where legal and technical complexities can become serious barriers to implementation? How might these schemes affect smaller companies and start-ups that may not have sufficient resources to meet these requirements?

Consumers' interests must be prioritised when developing products and services for accessing and processing personal information.[161] Recital 5 of FIDA clearly states that ensuring customer control and trust is imperative to establish a well-functioning and effective data-sharing framework within the financial sector. [162] But how can putting control in customers' hands drive innovation and build trust in data sharing? What mechanisms are needed to ensure consumers feel confident sharing their data? Here are a few potential solutions that could help improve these challenges.

1.1.1 STRONG CUSTOMER AUTHENTICATION (SCA)

Establishing this trust is essential, and an excellent way to do so is to implement robust data protection protocols, such as strong customer authentication (SCA). SCA uses multi-factor authentication methods to access financial data, strengthening security and reducing the risk of unauthorised access.[163] It is important to analyse whether such measures can effectively balance security and support innovation.

As per Commission Delegated Regulation (EU) 2018/389, electronic payment services must be carried out securely, utilising technologies that ensure user authentication and minimise the

[159] Bracy J., 'Data Portability in the EU: An Obscure Data Subject Right?' (IAPP, 27 March 2023) https://iapp.org/news/a/data-portability-in-the-eu-an-obscure-data-subject-right/ accessed 20 May 2024
[160] Xueming S., and others, *Blockchain Technology and Application: Second CCF China Blockchain Conference, CBCC 2019, Chengdu, China, October 11-13, 2019, Revised Selected Papers* (Springer 2020) 4 https://link.springer.com/chapter/10.1007/978-981-15-3278-8_1 accessed 20 May 2024
[161] BEUC (n23)
[162] FIDA Recital 5
[163] Kukreti A. and others, *Access Control and Authentication for Secure Systems and Networks* (NeuroQuantology 2022) 14 DOI: 10.48047/nq.2022.20.5.nq22814 accessed 21 May 2024

risk of fraud.[164] An authentication code should be generated for electronic payment transactions or remote operations susceptible to abuse to achieve this.[165] The code must be resistant to forgery and disclosure of its elements.[166] For example, a code generated solely based on knowledge, such as a password, is vulnerable to compromise in case of a data breach. Therefore, the authentication shall be based on two or more elements, categorised as knowledge, possession and inherence and shall result in the generation of an authentication code.[167] A second factor, such as biometric identification, can be added to generate a code that authenticates the user during the transaction to mitigate the risk of unauthorised access.[168] Still, it is important to recognise that implementing such measures may increase complexity and cost for financial institutions.

FIDA recognises the heightened security risks associated with open access to financial data.[169] The regulation continues the principles of PSD2 by emphasising open banking and access to a broader range of financial data. Since SCA is crucial in securing access to payment accounts under PSD2[170], it could naturally extend to FIDA's wider scope of financial data access. SCA requires financial institutions to utilise multi-factor authentication (MFA) for specific payment transactions and account access attempts. This typically involves a combination of something the user knows (password), something the user has (mobile device), and something the user is (fingerprint).[171]

By analysing the effect of such measures, it can be concluded that enhancing security through SCA contributes to a sustainable and trusting environment for financial technology development. Implementing such measures can provide a high degree of protection; however, financial institutions will need to invest in the appropriate technology.

---

[164] Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication [2018] OJ L 69/23, recital 1 and art 1

[165] Commission Delegated Regulation (EU) 2018/389 recital 18

[166] Commission Delegated Regulation (EU) 2018/389 recital 1

[167] Commission Delegated Regulation (EU) 2018/389 article 1

[168] Commission Delegated Regulation (EU) 2018/389 recital 6

[169] FIDA p.1

[170] ACI Worldwide, *PSD2 and SCA: An Issuer Guide* (2021) 3 https://www.aciworldwide.com/wp-content/uploads/2021/04/PSD2-and-SCA-An-Issuer-Guide-thought-leadership-US.pdf accessed 21 May 2024

[171] EC, 'Stronger Protection and New Opportunities for Consumers and Businesses: Questions and Answers on the Payment Services Directive 2' (MEMO/17/4961, 13 January 2018) https://ec.europa.eu/commission/presscorner/detail/en/MEMO_17_4961 accessed 21 May 2024

1.1.2 DATA MINIMISATION PRINCIPLE

The principle of data minimisation is a critical component of data protection. It requires data controllers to gather only personal information that is directly relevant and necessary for a specific purpose and to retain that information only for the duration required to fulfil that purpose. Data controllers are responsible for collecting and keeping only the personal data they genuinely need. This principle is reflected in Article 5(1)(c) of the GDPR[172] and Article 4(1)(c) of Regulation (EU) 2018/1725[173], emphasising that personal data must be "adequate, relevant, and limited to what is necessary for relation to the purposes for which they are processed."[174]

FIDA prioritises collecting and utilising only the minimum financial data required for a TPP's service.[175] This helps protect consumer privacy and reduces the risk of data breaches. Open Banking APIs should be designed to enable access only to the specific data points needed for the TPP's services. In its statement 2/2024 on the financial data access and payments package adopted on 23 May 2024, the European Data Protection Board (EDPB) highlights the importance of the principle of data minimisation in the design of financial data exchange rules.[176]

However, there remains a concern that this principle hinders innovation.[177] If financial institutions and fintech companies are restricted in their access to data, they may find it difficult to develop new products and services that require extensive data analysis. The question is how to balance the need to minimise data with the need to innovate.

One possible solution is to adopt a tiered approach to data access. Basic data is provided initially, and additional data is requested based on the user's consent and specific needs.[178] This

[172] GDPR Article 5

[173] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC [2018] OJ L 295/39 art. 4

[174] EDPS, 'Glossary' (EDPS) https://www.edps.europa.eu/data-protection/data-protection/glossary/d_en accessed 21 May 2024.

[175] FIDA Recital 10

[176] EDPB, 'Statement 2/2024 on the Financial Data Access and Payments Package' (23 May 2024) 5 https://www.edpb.europa.eu/system/files/2024-05/edpb_statement_20230523_financialdatapaymentpackage_en.pdf accessed 26 May 2024

[177] Clemens A. and others, 'Extended Summary and Policy Recommendations' (Community Based Innovation Systems GmbH (cbased), SBA Research, Vienna University of Economics and Business Administration, December 2017) 4 https://cbased.com/wp-content/uploads/2019/03/extended-summary-and-policy-recommendations_final.pdf accessed 23 May 2024

[178] Budin-Ljøsne I., 'Dynamic Consent: A Potential Solution to Some of the Challenges of Modern Biomedical Research' (2017) 18 BMC Medical Ethics 4 https://doi.org/10.1186/s12910-016-0162-9 accessed 23 May 2024

will allow companies to access the necessary information as and when required without compromising the principle of data minimisation.[179]

Data anonymisation and pseudonymisation techniques can also facilitate innovation without compromising user privacy. Anonymised data can be used to analyse and develop new products while keeping personal information secure.[180] This is particularly important in the FIDA context, where large amounts of data are needed to develop innovative financial solutions.

Another approach is to issue specific authorisations under the scrutiny of regulators. This means that regulators will determine the types of data that TPPs can collect and the purposes for using that data. This approach can strike the right balance between data protection and innovation opportunities.

Creating detailed consent options that allow users to selectively authorise different levels of data sharing depending on their preferences and the services they want to access can also help to build trust and ensure the safe use of data. This approach allows users to feel more in control of their data, increasing their willingness to share information and leading to innovation.

In addition, the creation of regulatory 'data sandboxes' where fintech companies can experiment with new services and technologies using synthetic or anonymised full data can foster innovation. This allows companies to develop and test new products without compromising user privacy. Such sandboxes provide a safe environment for experimentation, ultimately fostering new financial technologies' development.[181]

Thus, the principle of data minimisation, while critical to protecting privacy, can be implemented to support and even stimulate innovation in the financial sector. Provided ideas can help to achieve this balance, demonstrating that data minimisation and innovation can effectively co-exist. This approach focuses specifically on compliance with data minimisation rather than general trust issues, although both aspects are closely related and work together to create a safe and innovative financial environment.

---

[179] ENISA, 'Data Pseudonymisation: Advanced Techniques & Use Cases - Technical Analysis of Cybersecurity Measures in Data Protection and Privacy' (January 2021) 43 https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases accessed 23 May 2024

[180] BMVD, 'Driving Progress with Data' (2024) 21 https://bmdv.bund.de/SharedDocs/DE/Anlage/K/driving-progress-with-data.pdf?__blob=publicationFile accessed 23 June 2024

[181] Truby, J. and others, 'A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications'. *European Journal of Risk Regulation*, (2022). *13*(2), 277. doi:10.1017/err.2021.52

2. NEW DASHBOARDS

The FIDA regulation aims to empower consumers by giving them more control over their financial data by enabling the future of permission dashboards.[182] A critical aspect of the regulation is to ensure that consumers can easily give and manage their consent to the use of data rather than just general data protection.

Moreover, the regulation encompasses important elements of the GDPR that give consumers specific rights regarding their data held by TPPs. According to Recital 10, the customer must be authorised to share customer data within the parameters of this Regulation. Data holders are legally required to share customer data only when prompted by the customer's permission to share it with a data user.[183]

It's important to note that the European Data Protection Board (EDPB) has emphasised that the ECON committee has put forward additional clarifications to the FIDA Proposal, particularly regarding the legal interpretation of the term "permission" instead of the concept of "explicit consent." This distinction is significant because "permission" in this context does not equate to the explicit consent required by GDPR for processing personal data. In this context, permission is granted to access financial data, but it does not serve as a legal basis for processing under GDPR. Therefore, while a user may grant permission for their data access, the entity accessing the data must still adhere to GDPR requirements for lawful processing, such as having a legitimate interest or contractual necessity. For instance, a user may grant permission to a third-party service to access their financial data to provide a service. Still, this permission alone does not obviate the need for the third party to have a legal basis under GDPR to process that data. This differentiation allows for a balance between access to data and users' rights to data protection.[184]

For consumers' trust, it's essential to envision implementing all granted rights through a user-friendly dashboard. This dashboard should clearly display granted permissions, specifying the recipients and purposes, and provide detailed information on data usage and access history. Real-time notifications should be in place to update users on any data access or usage, indicating whether it was done under permission or consent. Additionally, users should be able to easily manage and withdraw permissions and consents directly from the dashboard, ensuring

[182] Apinity (n149)
[183] FIDA Recital 10
[184] EDPB (n176) 7

complete control over their data. Transparent, easily accessible data policies written in clear, non-technical language are also crucial to help users understand their rights and how their data is handled. These measures will enhance consumer trust and ensure data security.

By integrating elements of the GDPR, the FIDA regulation aims to give consumers more control and the ability to consent to the use of their data. Creating easy-to-use tools to manage consent and transparent policies will help increase consumer confidence, which will balance data protection with the development of new technologies.

3. COMPLIANCE SOLUTIONS

Understanding and adhering to GDPR compliance and technical standards within the FIDA is crucial for fostering innovation in the financial sector while upholding strong data protection. Collaboration between regulators and industry stakeholders plays a pivotal role in finding this balance.[185] Analysing possible steps, several strategies can be identified to help achieve this goal.

Regulators should advocate for the integration of automated tools and software to enhance compliance with GDPR and other regulatory frameworks.[186] The deployment of these tools can significantly mitigate the manual workload and elevate the precision of compliance activities by providing real-time alerts and automated reporting mechanisms. This approach not only streamlines processes but also diminishes the likelihood of human error, a common source of regulatory infractions. By offering guidance on the appropriate selection and implementation of these tools, regulators can enable financial institutions to efficiently identify and rectify compliance issues.[187] This strategic support allows these institutions to allocate more resources towards innovation and the development of new products and services, thus fostering a more dynamic and compliant financial environment.

[185] Igbinenikaro, E., Adewusi, A.O., 'Policy Frameworks for Regulating Fintech Innovations: Ensuring Consumer Protection While Fostering Innovation' (2024) 6(4) *Finance & Accounting Research Journal* https://fepbl.com/index.php/farj/article/view/991 accessed 23 June 2024
[186] Chhetri, T.R. and others 'Data Protection by Design Tool for Automated GDPR Compliance Verification Based on Semantically Modeled Informed Consent'. Sensors 2022, 22, 2763. 13 https://doi.org/10.3390/s22072763
[187] ibid

Second, regular Data Protection Impact Assessments (DPIAs) serve as a critical mechanism for proactively identifying and mitigating risks associated with data processing.[188] The value of DPIAs lies in their ability to quantify and prioritise risks, enabling organisations to allocate resources more efficiently towards mitigating the most significant threats.[189] Integrating DPIAs into the regulatory framework underscores a proactive compliance culture, ensuring adherence to regulations and prioritising data protection and ethical innovation. Regular and well-guided DPIAs are essential for maintaining regulatory compliance and supporting the secure adoption of new technologies, contributing to a resilient data protection strategy that facilitates innovation while safeguarding privacy and security.

Regulators should also disseminate clear, specialised guidelines under FIDA to address the specific needs of the financial sector. These guidelines should cover all aspects of data protection, including data collection, processing, storage and sharing. The creation of such guidelines standardises compliance efforts across the sector, allowing organisations to benchmark their practices against industry norms.[190] This consistency is critical to creating a level playing field and ensuring all agencies are held to the same high data protection standards. Also, clear guidance facilitates effective navigation of the complex regulatory landscape, allowing institutions to focus resources on both compliance and innovation and a proactive measure to continually improve adherence. Therefore, regulators should focus on developing detailed industry guidance under FIDA to simplify compliance, ensure consistency, and support innovation in the financial sector.

Integrating GDPR requirements and technical standards, such as aligning ISO 27001 for information security management with GDPR compliance efforts, would also streamline processes and reduce redundancies.[191] The ISO 27001 standard serves as the international framework for information security management[192] and offers a structured approach to ensuring that all regulatory aspects are systematically considered and addressed, simplifying

[188] ICO, 'Data Protection Impact Assessments (DPIAs)' (Guide to the General Data Protection Regulation (GDPR), Version 1.0, January 2020) 2 https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias-1-0.pdf accessed 24 May 2024

[189] ibid 35

[190] Igbinenikaro (n185) 516

[191] Diamantopoulou V., and others Trust, Privacy and Security in Digital Business 'GDPR and ISO 27001: Synergies of Activities Towards Compliance' (Springer 2013) 107 https://link.springer.com/book/10.1007/978-3-030-58986-8 accessed 24 May 2024

[192] Lopes, I., Guarda T., Oliveira P., 'How ISO 27001 Can Help Achieve GDPR Compliance' (2019) 2 10.23919/CISTI.2019.8760937

compliance and enhancing the overall security posture of the institution.[193] Taking a holistic approach to compliance would enable financial institutions to ensure that their operations are resilient and adaptable to regulatory changes and emerging risks.

The FIDA proposal should include requirements for technical safeguards such as encryption and access controls and for adopting a privacy-by-design approach to enhance data protection within the financial sector. These measures should be integrated into the development process of financial products and services from the beginning to ensure seamless incorporation of data protection and compliance with regulations. Mandating encryption and access controls will protect sensitive data from unauthorised access and breaches, while privacy-by-design principles will ensure privacy considerations are embedded into every aspect of product development. The FIDA's mandate will help build consumer trust by demonstrating a strong commitment to data security and privacy in a market where data breaches are increasingly common. This regulatory requirement is essential for gaining a competitive edge and ensuring the successful adoption of new technologies and services. Additionally, embedding data protection measures aligns with a broader strategic focus on risk management and regulatory compliance. By including these requirements in the FIDA proposal, regulators can help financial institutions navigate the complex regulatory landscape, avoid potential fines and sanctions, and maintain their reputation for reliability and integrity.

4. WILL IT BE ENOUGH?

This chapter has delved into a wide array of strategies for effectively balancing innovation and data protection within the scope of FIDA. Addressing concerns such as compliance with personal data protection laws and technical standards can be achieved through automated tools, regular data protection impact assessments, and the establishment of clear guidelines. Enhancing consumer confidence and control is more intricate, contingent upon various factors, including the general implementation of the proposal and how individual financial institutions will execute it. It's important to recognise that consumers vary, and their level of trust may differ. Nonetheless, it's worth considering which measures could help alleviate concerns, particularly during the planning stages of implementing FIDA. For instance, employing transparent consent mechanisms to ensure secure and user-centred data sharing could offer consumers a more solid assurance that their data is being protected. Additionally, implementing

[193] Tomashchuk O. and others Trust, Privacy and Security in Digital Business 'A Data Utility-Driven Benchmark for De-identification Methods' (Springer 2013) 67 https://link.springer.com/book/10.1007/978-3-030-58986-8 accessed 24 May 2024

robust data management policies, continuous monitoring, and regular security assessments will fortify the overall security framework. Technical safeguards such as encryption and privacy by design principles will establish a sustainable environment for data-driven innovation. Collectively, these solutions can contribute to the creation of a secure and innovative financial ecosystem, allowing the financial sector to progress technologically while upholding high data protection standards. In doing so, FIDA will be able to cultivate a forward-thinking and secure financial landscape, striking a balance between regulatory adherence and the imperative for innovation.

CONCLUSION

The FIDA proposal represents a significant advancement in the development of financial services, expanding on the groundwork established by PSD2 and open banking. This shift towards a more comprehensive open finance framework is designed to leverage the opportunities presented by data-driven innovation, all while upholding strong data protection standards. Nevertheless, achieving a harmonious integration of these goals is riddled with challenges and intricacies.

Firstly, supporting innovation and balancing the goal of innovation with data protection are some of the key aspects that this proposal addresses. The emergence of FIDA signifies a natural progression from the concept of open banking, with the focus shifted from primarily sharing banking data to creating a more inclusive open finance framework that covers a wider range of financial services. This expanded scope is intended to encourage innovation by facilitating smooth data sharing across different financial sectors, potentially leading to new services and business models. However, this increased data-sharing capability also brings significant concerns related to data protection. Balancing data protection and innovation is a complex challenge within FIDA. The proposal's emphasis on facilitating easier data sharing has the potential to significantly drive innovation. By providing access to a wider range of financial data, businesses can develop more personalised and efficient services, enhancing customer experiences and new market opportunities.

Still, a major concern revolves around the potential erosion of user privacy. Simplified data sharing can lead to sharing user data more widely than intended, often without adequate transparency or explicit user permissions. This could lead to users losing control over their personal information, sparking concerns of potential misuse or unauthorised access. For

example, users may be unaware who has access to their data and for what specific purposes it is being utilised. This lack of clarity undermines trust and can increase vulnerabilities, such as data breaches and identity theft. Data minimisation, a key aspect of data protection laws such as GDPR, is at odds with the goals of widespread data sharing. Data minimisation dictates that only a minimal amount of necessary data should be gathered and processed for a specific purpose. Data minimisation involves collecting and processing only the minimum amount of data necessary for a specific purpose. Whilst important for user privacy, this principle can hinder innovation by limiting the data available to create and improve new financial services.

Second, consumer and end-user trust is critical to the success of the proposed initiative. A significant barrier is the lack of trust on the part of users. Users worried about their data's security and privacy are less likely to agree to data sharing, even if it means forgoing innovative financial services. This hesitance is compounded by compliance issues with GDPR and other regulations, which mandate stringent safeguards and transparent consent procedures. Suppose financial institutions fail to demonstrate robust data protection measures and clear data usage policies. In that case, they face not only regulatory penalties but also the potential erosion of consumer trust, which is crucial for the widespread adoption of open finance initiatives.

To address these challenges, various solutions have been proposed to strike a balance between innovation and data protection and to build consumer trust. Secure data access solutions, such as strong customer authentication, can bolster security and increase user confidence. Moreover, reevaluating data minimisation strategies to allow specific, regulated permissions could foster innovation without compromising data protection. By offering users detailed consent options and a user-friendly dashboard for managing data access, trust can be established, and transparency can be ensured. This dashboard would provide clear visibility into who has access to what data and for what purpose, along with real-time notifications about any data access or usage, thereby keeping users informed about their data handling. Additionally, clear and user-friendly data policies help users understand their rights and how their data is managed.

In examining whether a harmony exists between innovation and data protection in the FIDA proposal, it is apparent that such equilibrium has not yet been fully attained. Nonetheless, the proposal lays a solid groundwork for establishing such an equilibrium. Through the implementation of suggested remedies and the continuous improvement of the data sharing and protection approach, it is feasible to cultivate an environment where innovation can thrive without compromising the privacy and security of user data. Striking this balance is essential

for the successful execution of FIDA and the broader goals of open finance, ensuring that innovation advantages are realised in a manner that honours and safeguards user data. As the financial services sector develops, ongoing communication and cooperation among regulators, industry participants, and consumers will be crucial in upholding this equilibrium and nurturing a sustainable, innovative, and secure financial environment.

BIBLIOGRAPHY

PRIMARY SOURCES

1. Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication [2018] OJ L 69/23

2. European Commission, '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' (Text with EEA relevance) COM(2023) 360 final (Brussels, 28.6.2023)

3. Directive (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL Of 25 November 2015 On Payment Services In The Internal Market, Amending Directives 2002/65/EC, 2009/110/EC And 2013/36/EU And Regulation (EU) No 1093/2010, And Repealing Directive 2007/64/EC

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

5. Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937

6. Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC [2018] OJ L 295/39

SECONDARY SOURCES

1. Aci Worldwide, PSD2 and SCA: An Issuer Guide (2021) https://www.aciworldwide.com/wp-content/uploads/2021/04/PSD2-and-SCA-An-Issuer-Guide-thought-leadership-US.pdf accessed 21 May 2024
2. Acquisti A., Taylor C., and Wagman L., 'The Economics of Privacy' 2016 54 *Journal of Economic Literature* pp. 442-92 https://doi.org/10.1257/jel.54.2.442 accessed 13 May 2024
3. Adelmann F. and others 'It's a Small World After All: Cyber Risk and Financial Stability', IMF Staff Discussion Note, SDNEA2020007, 2020
4. Aldasoro, I. and others, 'Intelligent Financial System: How AI is Transforming Finance' (BIS Working Papers No 1194, Monetary and Economic Department, June 2024)
5. Aldboush H.H.H., Ferdous M, 'Building Trust in Fintech: An Analysis of Ethical and Privacy Considerations in the Intersection of Big Data, AI, and Customer Trust' 2023 11, 90 International Journal of Financial Studies https://doi.org/10.3390/ijfs11030090

6. AmCham EU, 'FIDA Position Paper' (AmCham EU, 2024) https://amchameu.eu/system/files/position_papers/amchameu_fida.pdf accessed 15 May 2024
7. Bajracharya A. and others, 'Recent Advances in Algorithmic Biases and Fairness in Financial Services: A Survey' 2022 https://doi.org/10.1007/978-3-031-18461-1_53
8. Belén B.P. and others, ''Pick Someone Who Can Kick Your Ass' - Moneywork in Financial Third Party Access' 2021 4 CSCW Proceedings of the ACM on Human-Computer Interaction https://doi.org/10.1145/3432917
9. BEUC, 'The Consumer Voice in Europe: ACCESS TO CONSUMERS' FINANCIAL DATA: BEUC position paper on the proposed Financial Data Access Regulation'
10. Billiam AL, Handayani T, 'The Urgency of Open Application Programming Interface Standardization in the Implementation of Open Banking to Customer Data Protection for the Advancement of Indonesian Banking' 2022 *Padjadjaran Journal of Law* https://doi.org/10.22304/pjih.v9n1.a4
11. Bitkom, 'GDPR Consultation Report' (Bitkom, February 2024) https://www.bitkom.org/sites/main/files/2024-02/finalbitkomconsultationgdpr-report.pdf accessed 15 May 2024
12. Boissay F. and others 'Big techs in finance: on the new nexus between data privacy and competition' (*BIS Working Papers* No. 970). Monetary and Economic Department, https://www.bis.org/publ/work970.pdf, accessed on 7 February 2024
13. Bhattacharya A, 'Do privacy and competition concerns go hand in hand? Exploring the theoretical and practical hurdles for the incorporation of privacy concerns in a competition law regime that emphasises economic efficiency and consumer welfare' 2021 SSRN https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3792169 accessed on 10 April 2024
14. Bless C. and others, 'Raising Awareness of Data Sharing Consent Through Knowledge Graph Visualisation' in Alam M and others (eds), Further with Knowledge Graphs (Studies on the Semantic Web, vol 53, IOS Press 2021) https://doi.org/10.3233/SSW210034
15. BMVD, 'Driving Progress with Data' (2024) 21 https://bmdv.bund.de/SharedDocs/DE/Anlage/K/driving-progress-with-data.pdf?__blob=publicationFile accessed 23 June 2024
16. Bracy J., 'Data Portability in the EU: An Obscure Data Subject Right?' (IAPP, 27 March 2023) https://iapp.org/news/a/data-portability-in-the-eu-an-obscure-data-subject-right/ accessed 20 May 2024
17. Brite Payments, 'What Is Financial Data Access (FIDA)? And What Does It Mean for Your Business?' (Brite Payments, 11 June 2024) https://britepayments.com/resources/article/fida/ accessed 21 June 2024
18. Bruhner C.M, Hasselquist D., Carlsson N., 'Bridging the Privacy Gap: Enhanced User Consent Mechanisms on the Web' 2023 MADWeb https://dx.doi.org/10.14722/madweb.2023.23017 accessed 13 May 2024
19. Budin-Ljøsne I. and others 'Dynamic Consent: A Potential Solution to Some of the Challenges of Modern Biomedical Research' 2017 18 BMC Medical Ethics https://doi.org/10.1186/s12910-016-0162-9 accessed 23 May 2024
20. Centre for Information Policy Leadership (CIPL), 'First Report on Artificial Intelligence: AI and Data Protection in Tension', Centre for Information Policy Leadership, 2021 https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_first_ai_report_-_ai_and_data_protection_in_tension__2_.pdf accessed 10 May 2024
21. Centre for Information Policy Leadership (CIPL), 'Recommendations on Transparency, Consent and Legitimate Interest under the GDPR' (Centre for Information Policy Leadership, 19 May 2017) https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_recommendati

ons_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf accessed 14 May 2024
22. Chatzigiannis P, Gu WC, Raghuraman S, Rindal P, and Zamani M, 'Privacy-Enhancing Technologies for Financial Data Sharing' https://arxiv.org/abs/2306.10200, accessed on 7 February 2024
23. Chhetri T.R. and others 'Data Protection by Design Tool for Automated GDPR Compliance Verification Based on Semantically Modeled Informed Consent' 2022 Sensors https://doi.org/10.3390/s22072763
24. Christodoulou P., Limniotis K., 'Data Protection Issues in Automated Decision-Making Systems Based on Machine Learning: Research Challenges' (2024) 4 *Network* 91, https://doi.org/10.3390/network4010005 accessed 27 May 2024
25. Clemens A. and others, 'Extended Summary and Policy Recommendations', Community Based Innovation Systems GmbH (cbased), SBA Research, Vienna University of Economics and Business Administration, December 2017 https://cbased.com/wp-content/uploads/2019/03/extended-summary-and-policy-recommendations_final.pdf accessed 23 May 2024
26. Custers B. and others, Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases (*Springer* 2013) https://link.springer.com/chapter/10.1007/978-3-642-30487-3_15 accessed 15 May 2024
27. Dhuri M.P, 'Open Banking: Digital Innovation in Banking Service in India' (2022) 21(7) YMER https://ymerdigital.com/uploads/YMER210752.pdf accessed on 14 April 2024
28. Diamantopoulou V. and others, Trust, Privacy and Security in Digital Business 'GDPR and ISO 27001: Synergies of Activities Towards Compliance' (Springer 2013) https://link.springer.com/book/10.1007/978-3-030-58986-8 accessed 24 May 2024
29. Digitaleurope, 'FIDA Position Paper' (DIGITALEUROPE, November 2023) https://cdn.digitaleurope.org/uploads/2023/11/DIGITALEUROPE-FIDA-position-paper.pdf accessed 13 May 2024
30. Drien O, Amarilli A, Amsterdamer Y, 'Managing Consent for Data Access in Shared Databases' (Bar-Ilan University and LTCI, Télécom Paris, Institut Polytechnique de Paris, 2024) https://u.cs.biu.ac.il/~amstery/files/managingconsent.pdf accessed 13 May 2024
31. Dutch National Bank and AFM, 'Data Mobility and the Financial Sector' (Discussion Paper, Dutch National Bank, 2021) https://www.dnb.nl/media/qekh0qka/afm-dnb-discussion-paper-data-mobility-and-the-financial-sector.pdf accessed 10 May 2024
32. Eiss R., 'Confusion over data-privacy law stalls scientific progress' (2020) https://www-nature-com.proxy.library.uu.nl/articles/d41586-020-02454-7
33. Elliott K., and others, 'Know Your Customer: Balancing innovation and regulation for financial inclusion' 2022 4 Data & Policy e34 https://doi.org/10.1017/dap.2022.23
34. Eurofi, 'Open Finance and FIDA Proposal' (Eurofi, February 2024) https://www.eurofi.net/wp-content/uploads/2024/03/eurofi_open-finance-fida-proposal_ghent_february-2024.pdf accessed 20 May 2024
35. Eurofi, 'Open Finance: FIDA Proposal' (Eurofi, February 2024) https://www.eurofi.net/wp-content/uploads/2024/03/eurofi_open-finance-fida-proposal_ghent_february-2024.pdf accessed 13 May 2024.
36. European Banking Authority, Final Report on the amendment of the RTS on SCA&CSC, https://www.eba.europa.eu/sites/default/files/document_library/Publications/Draft%20Technical%20Standards/2022/EBA-RTS-2022-03%20RTS%20on%20SCA%26CSC/1029858/Final%20Report%20on%20the%20amendment%20of%20the%20RTS%20on%20SCA%26CSC.pdf accessed on 15 April 2024

37. European Banking Federation, 'EBF Recommendations on FIDA' (11 December 2023) https://www.ebf.eu/wp-content/uploads/2023/12/EBF_046342-EBF-recommendations-on-FIDA_11.12.23.pdf accessed 10 May 2024
38. European Commission, 'A Europe Fit for the Digital Age' (European Commission, 9 March 2021) https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en accessed 2 February 2024
39. European Commission, 'Financial data access and payments package' (2023) https://finance.ec.europa.eu/publications/financial-data-access-and-payments-package_en accessed 2 February 2024
40. European Commission, 'Finance Events Presentation' (5 September 2023) https://finance.ec.europa.eu/system/files/2023-09/finance-events-230905-presentation_en.pdf accessed 16 April 2024
41. European Commission, 'H2020 Programme: Ethics and Data Protection' (European Commission, 2018) https://commission.europa.eu/system/files/2020-06/5._h2020_ethics_and_data_protection_0.pdf accessed 14 May 2024
42. European Commission (2023, November 28). Revised rules on payment services - Questions and Answers, ec.europa.eu, accessed on 14 April 2024
43. European Commission, 'Stronger Protection and New Opportunities for Consumers and Businesses: Questions and Answers on the Payment Services Directive 2' (MEMO/17/4961, 13 January 2018) https://ec.europa.eu/commission/presscorner/detail/en/MEMO_17_4961 accessed 21 May 2024
44. European Data Protection Board, 'Statement 2/2024 on the Financial Data Access and Payments Package' (23 May 2024) https://www.edpb.europa.eu/system/files/2024-05/edpb_statement_20230523_financialdatapaymentpackage_en.pdf accessed 26 May 2024
45. European Data Protection Supervisor, 'Financial and Payment Services: Use of Personal Data Should Remain Proportionate and Fair' (23 Aug 2023) https://www.edps.europa.eu/system/files/2023-08/2023-0730_d2425_opinion_en.pdf accessed on 7 February 2024
46. European Data Protection Supervisor, 'Glossary' (EDPS) https://www.edps.europa.eu/data-protection/data-protection/glossary/d_en accessed 21 May 2024
47. European Parliament, 'Draft Report on the Proposal for a Regulation of the European Parliament and of the Council on a Framework for Financial Data Access' https://www.europarl.europa.eu/doceo/document/ECON-PR-757355_EN.pdf accessed 16 April
48. European Parliamentary Research Service, 'Digital Sovereignty for Europe' (European Parliament, 2020) https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf accessed 15 May 2024
49. European Parliamentary Research Service, The ethics of artificial intelligence: Issues and initiatives (2020) https://wxiong.mycpanel.princeton.edu/papers/Privacy.pdf accessed 13 May 2024
50. European Parliament, 'The impact of the General Data Protection Regulation (GDPR) on artificial intelligence' 2 (European Parliamentary Research Service, 2020) https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf accessed 15 May 2024

51. European Payments Council, 'Exploring FIDA: Revised rules for financial data sharing access' (2023) https://www.europeanpaymentscouncil.eu/news-insights/insight/exploring-fida-revised-rules-financial-data-sharing-access accessed 2 April 2024
52. European Savings and Retail Banking Group (ESBG), 'Response to the EC Call for Feedback on the Proposed Regulation on the Financial Data Access Framework' (October 2023) ESBG Transparency Register ID 8765978796-80, https://www.wsbi-esbg.org/esbg-response-to-the-ec-public-consultation-on-the-proposed-regulation-on-the-financial-data-access-framework-fida/, accessed on 7 February 2024
53. European Union Agency for Cybersecurity (ENISA), 'Data Pseudonymisation: Advanced Techniques & Use Cases - Technical Analysis of Cybersecurity Measures in Data Protection and Privacy' (January 2021) https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases accessed 23 May 2024
54. EY, 'Why FiDA Will Unleash Change Across European Financial Services' (EY, 12 June 2023) https://www.ey.com/en_gl/insights/financial-services/emeia/why-fida-will-unleash-change-across-european-financial-services accessed 21 June 2024
55. Financial Data and Technology Association (FDATA), 'The Unintended Consequences of PSD2 RTS' (June 2019) https://fdata.global/europe/wp-content/uploads/sites/2/2019/06/The-Unintended-Consequences-of-PSD2-RTS-FDATA-EUROPE-and-ETPPA.pdf accessed on 15 April 2024
56. Fortra, 'The True Cost of Compliance with Data Protection Regulations' https://static.fortra.com/globalscape/pdfs/guides/gs-true-cost-of-compliance-data-protection-regulations-gd.pdf accessed 14 May 2024
57. Giurca A., 'AI Qualitative Report' (July 2020) https://probability.nl/wp-content/uploads/2020/08/AI_qualitative_final.pdf accessed 13 May 2024
58. Graef I, 'Data Portability at the Intersection of Data Protection and Competition Law' (Tilburg University, 2016) https://pure.uvt.nl/ws/portalfiles/portal/45777953/CPI_Graef_data_portability.pdf accessed 15 May 2024
59. Hakizimana S., 'Fintech Startups: What does the Future hold for Financial Institutions in Kenya?' https://www.ijssers.org accessed 15 May 2024
60. Hamza M, 'Exploring Barriers and Pathways to Data Protection by Design within IT Companies' (Master's Programme in IT Management, Department of Informatics, Umeå University, 2017) https://www.diva-portal.org/smash/get/diva2:1154866/FULLTEXT01.pdf accessed 14 May 2024
61. Hansen S, 'How will Open Finance and the Financial Data Access Regulation impact the Financial Sector?' (2024) EY Belgium, Financial Services Risk, Compliance and Internal Audit Partner, https://www.ey.com/en_be/financial-services/how-will-open-finance-and-financial-data-access-regulation-impact-financial-sector accessed on 7 February 2024
62. Hazar A, and Babuşcu S, Financial Technologies: Digital Payment Systems and Digital Banking. Today's Dynamics (2023) https://ritha.eu/storage/320/4_jorit_HazarA_BabuscuS.pdf accessed on 10 April 2024
63. Herzog L. Old Facts, New Beginnings: Thinking with Arendt about Algorithmic Decision-Making. The Review of Politics. 2021;83(4):555-577. doi:10.1017/S0034670521000474
64. Hieu C.V., Hai N.M., 'Financial Technology: Implementation Experience in Some Countries and Policy Implications' (2022) https://doi.org/10.56097/binhduonguniversityjournalofscienceandtechnology.v5i4.76 accessed 15 May 2024
65. Hoepman JH., 'Making Privacy By Design Concrete' 2018 https://www.semanticscholar.org/paper/Making-Privacy-By-Design-Concrete-Hoepman/ede8df242f6f58629e079ab21af80b4b63b81f1e accessed on 10 April 2024

66. Hutchinson, E. (2015) "Keeping Your Personal Information Personal: Trouble for the Modern Consumer," Hofstra Law Review: Vol. 43: Iss. 4, Article 7 https://scholarlycommons.law.hofstra.edu/hlr/vol43/iss4/
67. Hutchinson, T., Duncan, N., (2012). Defining and Describing What We Do: Doctrinal Legal Research. Deakin Law Review 17 85 10.21153/dlr2012vol17no1art70
68. Igbinenikaro, E., Adewusi, A.O., 'Policy Frameworks for Regulating Fintech Innovations: Ensuring Consumer Protection While Fostering Innovation' (2024) 6(4) *Finance & Accounting Research Journal* https://fepbl.com/index.php/farj/article/view/991 accessed 23 June 2024
69. iGCB, Open Opportunities with Open Finance Whitepaper in collaboration with AWS (iGCB, 2024) https://www.igcb.com/wp-content/uploads/Open_Opportunities_with_Open_Finance_iGCB_AWS_compressed.pdf accessed 21 June 2024
70. Imperva, 'Financial services cybersecurity' (2024) https://www.imperva.com/learn/data-security/financial-services-cybersecurity/#:~:text=Maintaining%20Consumer%20Trust&text=Any%20breach%20of%20this%20trust,services%20helps%20maintain%20consumer%20trust accessed 12 April 2024
71. Information Commissioner's Office (ICO), 'Data Protection Impact Assessments (DPIAs)' Guide to the General Data Protection Regulation (GDPR), Version 1.0, January 2020) https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias-1-0.pdf accessed 24 May 2024
72. Innovation & Tech Today, 'How Has Technology Impacted The Way We Manage Our Finances?' innotechtoday.com accessed on 10 April 2024
73. Insurely, 'Ensuring Data Privacy and Security in Open Finance' (26 October 2023) https://www.insurely.com/blog/ensuring-data-privacy-and-security-in-open-finance-0#:~:text=Unleashing%20the%20Power%20of%20Data&text=In%20the%20world%20of%20finance,empowerment%2C%20and%20transparency%20are%20key accessed 15 April 2024
74. Jain R., Prajapati D., Dangi A., 'Transforming the Financial Sector: A Review of Recent Advancements in FinTech' (2023) *International Journal for Research Trends and Innovation*, https://ijrti.org/papers/IJRTI2302043.pdf accessed on 10 April 2024
75. Klein A, 'Reducing Bias in AI-based Financial Services' (Brookings, 2020) https://www.brookings.edu/articles/reducing-bias-in-ai-based-financial-services/ accessed 13 May 2024
76. KPMG LLP, 'Algorithmic Bias and Financial Services: A Report Prepared for Finastra International' (March 2021) https://www.kpmg.com/uk accessed 13 May 2024
77. KPMG, 'Data-driven: The new value of financial services data' (2024) https://kpmg.com/xx/en/home/insights/2022/04/data-driven-the-new-value-of-financial-services-data.html accessed 2 April 2024
78. KPMG, 'Embracing the future with open finance and FIDA' (2024) https://kpmg.com/lu/en/blogs/home/posts/2024/04/embracing-the-future-with-open-finance-andfida.html#:~:text=This%20shift%20acknowledges%20the%20value,a%20diverse%20and%20competitive%20ecosystem accessed 12 April 2024
79. Kukreti A. and others, 'Access Control and Authentication for Secure Systems and Networks' 2022 NeuroQuantology DOI: 10.48047/nq.2022.20.5.nq22814
80. Kurapati S., Gilli L., 'Synthetic Data: A Convergence between Innovation and GDPR' (2023) 11 J Open Access L, accessed on 7 February 2024

81. Lee K., Attablayo P., 'Examining the Impacts of Privacy Awareness on User's Self-Disclosure on Social Media' (2023) https://www.researchgate.net/publication/369233614_Examining_the_impacts_of_privacy_awareness_on_user's_self-disclosure_on_social_media accessed 14 May 2024
82. Lenard T.M., 'If Data Portability is the Answer, What is the Question?' (Tech Policy Institute, January 2020) https://techpolicyinstitute.org/wp-content/uploads/2020/01/Lenard_If-Data-Portability.pdf accessed 15 May 2024
83. Long, W., Blythe, F., Cuyvers, L., & Alquati-Bonisoli, N., 'New EU FIDA Proposal: How Does This Affect GDPR?'(Thomson Reuters, September 26, 2023), https://www.sidley.com/-/media/publications/fida-article-sidley.pdf?la=en&rev=c0463f46d7a54abeb130dd907514d3ea, accessed 2 February 2024
84. Lopes, I., Guarda T., Oliveira P., 'How ISO 27001 Can Help Achieve GDPR Compliance' (2019) 10.23919/CISTI.2019.8760937
85. Loyens & Loeff, 'Data sharing in the financial sector: An introduction to FIDA' (2024) https://www.loyensloeff.com/insights/news--events/news/data-sharing-in-the-financial-sector-an-introduction-to-fida/#:~:text=In%20addition%2C%20the%20EDPS%20raised,category%20data%20protected%20under%20GDPR accessed 2 February 2024
86. Lubowicka K, 'GDPR in Banking – How to be Sure Your Web Analytics Complies With the New Law' Piwik PRO Blog, November 30, 2017, updated October 14, 2020 https://piwik.pro/blog/gdpr-in-banking-web-analytics/ accessed on 7 February 2024
87. Macro Global, 'Regulators & its Role in Open Banking Innovation in Europe' (21 November 2023) Macroglobal.co.uk accessed on 14 April 2024
88. Martin K.M., Borah A., Palmatier R.J., 'Data Privacy: Effects on Customer and Firm Performance' 2016 36 Journal of Marketing https://doi.org/10.1509/jm.15.0497
89. Martin N. and others 'How Data Protection Regulation Affects Startup Innovation' 2019 21 Information Systems Frontiers https://doi.org/10.1007/s10796-019-09974-2
90. Mladinić A, Vukić Z, Rončević A, 'GDPR Compliance Challenges in Croatian Micro, Small and Medium Sized Enterprises' https://hrcak.srce.hr/ojs/index.php/pravni-vjesnik/article/view/23972, accessed on 7 February 2024
91. Moloney N, EU Securities and Financial Markets Regulation (4th edn, Oxford University Press 2023) https://global.oup.com/academic/product/eu-securities-and-financial-markets-regulation 9780198844877?cc=nl&lang=en&#, accessed on 7 February 2024
92. Nengfeng Z, 'Bias, Fairness, and Accountability with AI and ML Algorithms' (6 May 2021) https://wxiong.mycpanel.princeton.edu/papers/Privacy.pdf accessed 13 May 2024
93. Null E., Oribhabor I., and Escoto W., 'Data Minimization: Key to Protecting Privacy and Reducing Risks' (Access Now, May 2021) https://www.accessnow.org/wp-content/uploads/2021/05/Data-Minimization-Report.pdf accessed 13 May 2024
94. Oluka A, 'Analysing the implications of cybersecurity breaches on firm leadership' 2023 6 *Technology audit and production reserves* https://doi.org/10.15587/2706-5448.2023.286985
95. Omri BS., 'The Myth of Opportunity to Read' (2018) https://home.uchicago.edu/omri/pdf/articles/The_Myth_Of_Opportunity_To_Read.pdf accessed 13 May 2024
96. Oyewole A.T. and others, 'Data Privacy Laws and Their Impact on Financial Technology Companies: A Review' 2024 5 *Computer Science & IT Research Journal* https://ijrti.org/papers/IJRTI2302043.pdf accessed on 10 April 2024

97. Tomashchuk O. and others, 'Trust, Privacy and Security in Digital Business 'A Data Utility-Driven Benchmark for De-identification Methods' (Springer 2013) https://link.springer.com/book/10.1007/978-3-030-58986-8 accessed 24 May 2024
98. Payments Europe, 'Fintech and Digital Assets: Understanding the Regulatory Landscape' (Payments Europe, December 2023) https://www.paymentseurope.eu/wp-content/uploads/2023/12/Payments-Europe_FIDA.pdf accessed 15 May 2024
99. Porter A, 'GDPR vs. PSD2: Safeguarding Sensitive Financial Data' (BigID Blog) https://bigid.com/blog/gdpr-vs-psd2-compliance/, accessed on 7 February 2024
100. Projective Group, 'Unveiling FIDA: Financial transparency and consumer empowerment' (2023) https://www.projectivegroup.com/unveiling-fida-financial-transparency-and-consumer-empowerment/ accessed 2 April 2024
101. Salman A., Shastri S., Fernandez Vidal M., 'The Role of Data in Inclusive Insurance' (May 2024) https://www.cgap.org/research/publication/role-of-data-in-inclusive-insurance accessed 23 June 2024
102. Schroeder C., Winters B., Davisson J., 'We Can Work It out: The False Conflict between Data Protection and Innovation' (2022) 20 Colo Tech LJ
103. Stefanini, '5 Ways Banking & Financial Sectors Have Adapted to Technology' (2024) https://stefanini.com/en/insights/articles/5-ways-banking-financial-sectors-have-adapted-to-technology accessed 2 April 2024
104. Sugarda P.P., Wicaksono M.R., 'Enhancing the Competitiveness of Indonesia's Financial Services Sector in the Digital Era through Open Banking: Lessons Learned from the UK's Experience' (2023) 2(1) *Journal of Central Banking Law and Institutions* https://doi.org/10.21098/jcli.v1i2.15 accessed 15 of April 2024
105. Trabucchi D., Buganza T., 'Data-driven innovation: switching the perspective on Big Data' 2019 22 *European Journal of Innovation Management* https://doi.org/10.1108/EJIM-01-2018-0017
106. Truby J., and others, 'A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications' 2022 13 *European Journal of Risk Regulation* https://doi.org/10.1017/err.2021.52
107. Truchet M., 'Open Finance: Objectives of the Financial Data Access (FIDA) Proposal' (Eurofi, September 2023) https://www.eurofi.net/wp-content/uploads/2023/11/eurofi_open-finance_objectives-of-the-financial-data-access-fida-proposal_santiago_september-2023-1.pdf accessed 10 May 2024
108. Vrabec H.U, Data Subject Rights under the GDPR (Oxford, 2021; online edn, Oxford Academic, 22 July 2021) https://doi.org/10.1093/oso/9780198868422.001.0001 accessed 7 February 2024
109. Wessing T., PSD3 & PSR: Reshaping the EU payment services regulatory landscape, 4 July 2023, https://www.taylorwessing.com/en/insights-and-events/insights/2023/07/reshaping-the-eu-payment-services-regulatory-landscape#:~:text=Since%20adoption%20of%20the%20Second,role%20model%20for%20other%20jurisdictions, accessed 16 April 2024
110. Wilson C.M. II, 'Data Sharing Is Caring: Consumer Privacy and International Approaches to Open Banking' 2022 *Geo Wash International Law Review* https://www.proquest.com/openview/557ee7b920a5b40de190e139d8862bd4/1?pq-origsite=gscholar&cbl=44595
111. Wohlfarth M., 'Data Portability on the Internet: An Economic Analysis' 2019 *Business & Information Systems Engineering* https://www.econstor.eu/bitstream/10419/169506/1/Wohlfarth.pdf accessed 15 May 2024
112. Xiong W., 'Privacy and Personal Data Protection' (Princeton University, 2024) https://wxiong.mycpanel.princeton.edu/papers/Privacy.pdf accessed 10 May 2024

113. Xueming S. and others, Blockchain Technology and Application: Second CCF China Blockchain Conference, CBCC 2019, Chengdu, China, October 11-13, 2019, *Revised Selected Papers* (Springer 2020) https://link.springer.com/chapter/10.1007/978-981-15-3278-8_1 accessed 20 May 2024
114. Zahidul I., Moin U., (2023). IMPORTANT ROLE OF COMPARATIVE LEGAL RESEARCH. *Journal of Asian and African Social Science and Humanities*. 9. 31-43. 10.55327/jaash.v9i3.316.
115. Zetzsche, D.A. and others 'From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance' (April 28, 2017). *New York University Journal of Law and Business, Forthcoming, European Banking Institute Working Paper Series* 2017 - No. 6, University of Hong Kong Faculty of Law Research Paper No. 2017/007, University of Luxembourg Law Working Paper No. 2017-001, http://dx.doi.org/10.2139/ssrn.295992
116. Zeynalova A, 'From Closed Banking to Open Banking: Risks and Opportunities' (2024) 3(3) *Journal of Applied Business, Taxation and Economics Research* doi.org/10.54408/jabter.v3i3.278 accessed 15 of April 2024
117. Zhuang L.J., Sockin M., Xiong W., 'Data Privacy and Algorithmic Inequality' (May 2023) https://wxiong.mycpanel.princeton.edu/papers/Privacy.pdf accessed 13 May 2024