Open Banking, Open Data and Open Finance: Lessons from the European Union

Douglas W. Arner, Ross P. Buckley and Dirk A. Zetzsche

[2021] *UNSWLRS* 69
Forthcoming in Linda Jeng (ed), *Open Banking* (Oxford University Press, 2021), Chapter 8.

UNSW Law
UNSW Sydney NSW 2052 Australia

Open Banking, Open Data and Open Finance: Lessons from the European Union

Douglas W. Arner,[1] Ross P. Buckley[2] and Dirk A. Zetzsche[3]

Europe's path to 'open banking', 'open data' and 'open finance' rests upon four apparently unrelated pillars: (1) the facilitation of open banking to enhance competition in banking and particularly payments; (2) strict data protection rules reflecting European cultural concerns about dominant actors in the data processing field; (3) extensive reporting requirements imposed after the Global Financial Crisis to control systemic risk and change financial sector behaviour; and (4) a legislative framework for digital identification imposed to further the European Single Market.

This chapter analyses these four pillars and suggests that together they will underpin the future of digital finance in Europe and that together they effectively establish the framework for not only 'open banking' and 'open data' but 'open finance'. These European experiences provide profound insights for other societies facing choices as to the role of data in their future. In some, data will be controlled by a small number of massive firms and governments which use it for profit and suppression. In others, data will be under the control of individuals – democratized data – which should

[1] Kerry Holdings Professor in Law and Co-Founder, Asian Institute of International Financial Law, Faculty of Law, University of Hong Kong.

[2] Australian Research Council Laureate Fellow; KPMG Law and King & Wood Mallesons Chair of Disruptive Innovation; Scientia Professor; and Member, Centre for Law, Markets and Regulation, UNSW Sydney.

[3] Professor of Law, ADA Chair in Financial Law (Inclusive Finance), Faculty of Law, Economics and Finance, University of Luxembourg, and Director, Centre for Business and Corporate Law, Heinrich-Heine-University, Düsseldorf, Germany.

We would like to thank the Australian Research Council Laureate Fellowship, the Hong Kong Research Grants Council Research Impact Fund and the Qatar National Research Fund for financial support. This work builds upon our analysis in DA Zetzsche, DW Arner, RP Buckley & RH Weber, *The Evolution and Future of Data-Driven Finance in the E.U.*, (2020) 57 Common Mkt L. Rev. 331; and DW Arner, DA Zetzche, RP Buckley & RH Weber, *The Future of Data-Driven Finance and RegTech: Lessons from EU Big Bang II*, (2020) 25(2) Stanford J. L. Bus. & Fin. 245.

support a more open and innovative economy and society. In the evolution of these futures, legal and regulatory systems will play a key role.

Contents

1. INTRODUCTION

The next decade appears to be focused on questions of data in its role in finance, the economy and society more generally. An increasing range of these discussions focus on the idea of 'open banking', an idea that is being expanded to ideas of 'open finance' and 'open data' more broadly, in support of ideas of 'open innovation'.[4] The idea is that opening access to data will increase competition and innovation, thus benefiting both individuals and society more broadly. These ideas are taking on increasing importance as we see an increasing concentration of power in data industries, with related questions about the implications for innovation, prosperity and inequality.

One can in some ways see a battle of visions of the future, from one where data are controlled by a small number of giant firms and governments which use their control for profit and suppression, to one where data are under the control of individuals – the 'democratization' of data – supporting a more open and innovative economy and society. In the evolution of these futures, legal and regulatory systems will play a key role in determining the paths taken by different societies. The 2020 pandemic is strongly reinforcing these pre-crisis trends: COVID-19 has dramatically increased digitization generally, accelerated digitization of finance in particular through electronic payments and other transactions, and increased concentration of power in major data firms around the world.

Emerging from the COVID-19 pandemic, societies are faced with major questions about how to balance positive and negative aspects of digitization

[4] Henry Chesbrough, *Open Innovation: The New Imperative for Creating and Profiting from Technology* (Harvard Business School 2003).

and datafication, in particular risks of concentration and dominance. 'Open banking', 'open finance' and 'open data' are being presented as possible responses, both reducing the risks of concentration and dominance while at the same time maximizing the benefits of data for innovation and sustainable development.

If we look at approaches to 'open banking', these are generally being characterized as mandatory (required by law, regulation etc.), collaborative (involving industry and regulators working together), or voluntary (led by industry). The European Union ('EU') has taken the leading role in the former by being the first to implement mandatory open banking,[5] with its implementation in 2015 of the Second Payment Services Directive ('PSD2').[6] It was thus the first jurisdiction to make data sharing by banks mandatory, from 2018. As such, the EU is central in all discussions of 'open banking', as jurisdictions around the world are watching closely to see whether or not it is a success, something which is still too early to call.

However, any discussion of EU 'open banking' cannot avoid looking at the broader context. In particular, the EU is also the first jurisdiction to pursue a comprehensive approach to individual data sovereignty, also on a mandatory basis, with the General Data Protection Regulation of 2016, also effective in 2018. While not quite 'open data', GDPR provides for individual control over personal data, thereby relating to 'open banking' provisions under PSD2.

[5] The EU was the first to implement 'open banking' and the first to make it mandatory.

[6] 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, 2015 O.J. (L 337) 35 (hereinafter 'PSD2').

Financial regulatory reforms, in parallel with and increasingly coupled to extensive reforms of data protection, the advent of open banking, and the development of digital identification regimes are forming a regulatory ecosystem in the EU underpinning ‘open banking’ and ‘open data’ as well as ‘open finance’. This chapter explores how these four areas of regulatory reforms, each introduced for their own discrete reasons, are interacting today in Europe.

One of the greatest challenges facing the financial industry globally today is the at times conflicting requirements of data regulation and financial regulation. Major questions abound for societies around finance and the digital economy, including the role of data, technology and regulation. This chapter demonstrates there is much to learn from a detailed analysis of the EU’s experience and its systems that govern finance and data in the EU itself and extend extraterritorially to all those interacting with EU markets and citizens from around the world.

This chapter explores the relationship between financial regulation, data protection, regulatory technology (‘RegTech’) and the evolution of ‘open banking’, ‘open data’ and ‘open finance’ in the EU.

In Part I, we consider briefly ‘open banking’ and ‘open finance’. In Parts II-V, we analyse the four EU regulatory frameworks which are empowering ‘open finance’ in the EU.

While ‘open banking’ is imposed on banks by PSD 2 requiring incumbent intermediaries to share client data with new competitors (Part II), it is PSD2’s synergistic interaction with other policy measures which is proving transformative.

This is paralleled in a framework applying to data protection, privacy and control more generally which together form the basis of 'open data': the rigorous data protection demanded by the General Data Protection Regulation ('GDPR'[7]) (Part III), which has fundamentally altered how all firms – including financial services firms – deal with personal data.

However, much of the actual impetus for digital finance in Europe did not come from PSD2 or GDPR but rather developed rapidly with the introduction of extensive, purely digital, reporting from intermediaries to regulators, pursuant to new financial legislation imposed after the Global Financial Crisis including, inter alia, the Alternative Investment Fund Managers Directive ('AIFMD 2011'[8]) and the European Markets Infrastructure Regulation ('EMIR 2012'[9]), the fourth Capital Requirements Directive and the Capital Requirements Regulation ('CRD IV'[10]/ 'CRR'[11]) in 2013, and the reformed Markets in Financial Instruments Directives ('MiFID II'[12]) in 2014 (Part IV).

---

[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), 2016 O.J. (L 119) 1.

[8] Directive 2011/61/EU of the European Parliament and of the Council of 8 June 2011 on Alternative Investment Fund Managers and Amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) No 1060/2009 and (EU) No 1095/2010, 2011 O.J. (L 174) 1.

[9] Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC Derivatives, Central Counterparties and Trade Repositories, 2012 O.J. (L 201) 1.

[10] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on Access to the Activity of Credit Institutions and the Prudential Supervision of Credit Institutions and Investment Firms, Amending Directive 2002/87/EC and Repealing Directives 2006/48/EC and 2006/49/EC, 2013 O.J. (L 176) 338.

[11] Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on Prudential Requirements for Credit Institutions and Investment Firms and Amending Regulation (EU) No 648/2012, 2013 O.J. (L 176) 1.

[12] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on

But more was required to tie the pieces together: The fourth facilitative measure was cross-border digital identity pursuant to the eIDAS (electronic IDentification, Authentication and trust Services) framework[13] that establishes a network of national identity providers which can be either public or private (Part V).

We discuss the implications in Part VI, comparing these EU developments with other major jurisdictions, in particular the United States ('US'), China and India. Part VII concludes.

I. OPEN BANKING AND OPEN FINANCE

A. Open Banking and Open Finance and Their Role in Antitrust

Open banking is the regulatory response to the anti-competitive tendencies of the data economy where the size of the data pool determines competitive strength[14] and where technology firms like Amazon, Google and others have foregone profits for years to build dominant platforms. At the core are network effects, including economies of scope and scale, leading to the potential for industry dominance. At the extreme, data-driven industries are particularly subject to 'winner takes all outcomes', with the potential for significant benefits followed by significant negative externalities. As the leading example, American tech and data markets have tended towards oligopoly or monopoly over time,[15] a process which seems to have occurred

Markets in Financial Instruments and Amending Directive 2002/92/EC and Directive 2011/61/EU, 2014 O.J. (L 173) 349.

[13] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC, 2014 O.J. (L 257) 73.

[14] *See* Simonetta Vezzoso, *Fintech, Access to Data, and the Role of Competition Policy*, *in* COMPETITION AND INNOVATION (Scortecci, & Bagnoli eds., 2018).

[15] *See* Tim Wu, *The Master Switch: The Rise And Fall Of Information Empires* (Vintage 2011) (arguing that American information industries tend to press towards monopolies); *see*

in China as well. Both jurisdictions have allowed commercial enterprises to acquire control of large consumer and other data pools. The core asset of those platforms is their pool of data from shoppers and merchants. Once this data pool is assembled it can be used for targeting advertising, undercutting prices, offering new tailored services faster to more clients, and/or data analysis in all markets where superior information benefits profits.

Legal competition/antitrust scholars argue that where investors reward growth over profit, predatory pricing becomes highly rational and striving for dominance, even where this is costly, is a worthwhile strategy since it ensures monopoly rents due to control over the essential infrastructure on which their rivals depend: 'This dual role also enables a platform to exploit information collected on companies using its services to undermine them as competitors.'[16] This has prompted the policy demand to treat data as a product, since information and data, although different from traditional goods and services, pose problems familiar to competition/antitrust law, such as monopolistic behaviour and collusion.[17] Treating data as a product

also Ariel Ezrachi & Maurice E. Stucke, *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy* (Harvard University Press 2006) (discussing the promise and perils of technology-driven competition).

[16] *See* Lina M. Khan, *Amazon's Antitrust Paradox*, (2017) 126 Yale L.J. 710; K. Sabeel Rahman & Lina Khan, *Restoring Competition in the U.S. Economy*, *in* UNTAMED: HOW TO CHECK CORPORATE, FINANCIAL, AND MONOPOLY POWER 18, 18 (Nell Abernathy, Mike Konczal & Kathy Milani, eds., 2016) (arguing that the potential harms from dominance of platform firms include lower income and wages for employees, lower rates of new business creation, lower rates of local ownership, and outsized political and economic control in the hands of a few); *see also* Australian Competition & Consumer Comm'n, *Digital Platforms Inquiry: Preliminary Report* (2018), https://www.accc.gov.au/system/files/ACCC%20Digital%20Platforms%20Inquiry%20-%20Preliminary%20Report.pdf

[17] *See* Mark R. Patterson, *Antitrust Law in the New Economy: Google, Yelp, LIBOR, and the Control of Information* (Harvard University Press 2017) (arguing in favour of conceptualizing information and user and use data as a product, since information and data although different from traditional goods and services, poses problems familiar to antitrust law, such as monopoly and collusion).

becomes a particular consideration in avoiding potential reductions in innovation and therefore in long-term growth and development. (The economics of data is explored in Chapter 7 by Vikram Haksar and Yan Carrière-Swallow.)

These debates are increasingly important in the EU, the US and other countries, even China.

Open banking applies these insights to financial services where the controller of client data controls access to the client, and thus can impede or facilitate access of clients to new services.

In essence, open banking facilitates greatly increased levels of democratization of finance by enabling participants to simply, swiftly and safely provide their raw financial data to competitors of their current financial services provider.[18] This should support the growth of many new competitors in financial services. Most financial ecosystems are dominated by a relatively small number of very large banks or, in the case of China, very large tech companies providing financial services. Open banking should result in a far greater range of product offerings and ecosystem participants. These new participants will not be burdened with legacy systems and many will utilize more cost-efficient decentralized systems.

B. Countering Pro-concentration Effects

Three data-related factors together may lead to friction in the market for financial services that prevents private ordering from leading to socially optimal outcomes, in the sense that market forces ensure competition

---

[18] *See* Christopher C Nicholls, *Open Banking and the Rise of FinTech: Innovative Finance and Functional Regulation* (2019) 35 Banking & Fin. L. Rev. 121, 123.

among services providers. These factors are traditional economies of scale, data-driven economies of scale, and network effects.[19]

In this regard, Open Data (or Open Finance) is a two-edged sword. While the EU (with GDPR and PSD2) has required the financial industry to develop appropriate systems for data management and limited the use the industry can make of pooled data (thereby reducing the advantages of traditional financial institutions through their data pools), it has also driven the standardization of data processes outside of finance – potentially making for a larger data pool and enabling new entrants to potentially access more data of their individual customers. In other words, data are now more freely accessible and transferable than ever before. Large technology companies know well how to make use of the new rights to data transfer – much more so than do new entrants with access to customers limited by budgets and resources. This could prompt utterly unexpected results. While PSD2 and GDPR were originally designed to curtail the power of data behemoths, the eventual outcome of these two groundbreaking initiatives may well be less competition as there will be a greater concentration of data in the hands of the few.[20] As a result, it may be necessary for regulators to impose open data requirements only on firms with a potentially dominant position, regardless of whether they are financial institutions or tech firms.

[19] DA Zetzsche, RP Buckley, DW Arner, & JN Barberis, *From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance*, (2018) 14(2*)* New York Univ. J. L. & Bus. 393.

[20] *See* DA Zetzsche, DW Arner, RP Buckley & RH Weber, *The Evolution and Future of Data-Driven Finance in the E.U.*, (2020) 57 Common Mkt. L. Rev. 331.

C. The European Big Bang in Data-Driven Finance

Financial integration in Europe has evolved as a result of a series of major policy, legislative and regulatory strategies and initiatives, developed and implemented since the 1980s.[21] These have included the 1986 Single European Act,[22] which established the key formative plan for integration in the context of the single market and which was also one of the triggers for the financial reforms in the United Kingdom known as 'Big Bang';[23] the 1992 Maastricht Treaty[24] establishing the EU as well as the structure of the single market and the single currency; the 1995 White Paper on enlargement;[25] European Economic and Monetary Union ('EMU') in 1999 combined with the 1999 Financial Services Action Plan;[26] the 2001 Lamfalussy Report;[27] the 2009 de Larosière Report in the aftermath of the

[21] For the evolution of the EU Single Financial Market, the role of financial regulation and implications for global finance, *see* Emilios Avgouleas & Douglas W. Arner, *The Eurozone Debt Crisis and the European Banking Union: "Hard Choices", "Intolerable Dilemmas" and the Question of Sovereignty*, (2017) 50 Int'l L. 29; Douglas W. Arner & Ross P. Buckley, *Redesigning the Architecture of the Global Financial System*, (2010) 11 Melb. J. Int'l L. 185; Rolf Weber & Douglas W. Arner, *Toward a New Design for International Financial Regulation*, (2007) 29 U. Pa. J. Int'l Econ. L. 391.

[22] 1987 O.J. (L 169).

[23] *See* Jamie Robertson, *How the Big Bang Changed the City of London For Ever*, BBC NEWS (Oct. 27, 2016), https://www.bbc.com/news/business-37751599[https://perma.cc/Q9B9-AUNH].

[24] Treaty on European Union, Feb. 7, 1992, 1992 O.J. (C 191).

[25] *Commission White Paper on Preparation of the Associated Countries of Central and Eastern Europe for Integration into the Internal Market of the Union*, COM (1995) 163 final (May 3, 1995).

[26] *Implementing the Framework for Financial Markets: Action Plan*, *Financial Services Action Plan*, at 16-27, COM (1999) 232 final (May 11, 1999).

[27] *Final Report of the Committee of Wise Men on the Regulation of European Securities Markets* (Feb. 15, 2001), https://www.esma.europa.eu/sites/default/files/library/2015/11/lamfalussy_report.pdf [https://perma.cc/27XB-M924].

2008 Global Financial Crisis;[28] and Banking Union in the aftermath of the 2010 Eurozone Crisis.[29]

We suggest in this section that 2018 and the implementation of four separate legislative reforms should be seen as a new Big Bang in the EU: one of data-driven finance and its regulation. We argue that the impact of the 2018 Big Bang will be transformative for European finance over the coming years and will be as important a milestone as those which have taken place before. However, unlike the list of developments in the preceding paragraph, Big Bang II has not been a carefully designed strategy to support further integration and evolution of finance in the EU.

Rather, the four legislative measures analysed in this part were all implemented for separate reasons, but their combined effect has been to give an extraordinary, unanticipated impetus to the digital transformation of finance in the EU. The measures are the digital regulatory reporting requirements particularly of AIFMD and MiFID II, the rigorous data protection of GDPR, the open banking regime introduced by PSD2 (particularly combined with the data portability requirements in GDPR), and the pan-European digital identity framework built pursuant to eIDAS. Each is considered in turn.

II. OPEN BANKING: PSD2

The Second Payments Services Directive ('PSD2') mandates 'open banking': that banks now will have to share customer data with third parties

[28] *Report of the High-Level Group on Financial Supervision in the EU* (Feb. 25, 2009), https://ec.europa.eu/economy_finance/publications/pages/publication14527_en.pdf [https://perma.cc/LMS3-NSP5].
[29] *See* Avgouleas & Arner, *supra* note 21.

– in many cases their new FinTech and BigTech, as well as traditional, competitors – when directed to do so by their customers, reinforcing the requirements of GDPR, discussed in Part III.[30]

Besides extensive and purely digital reporting to regulators (further reinforcing the RegTech cycle discussed below), PSD2 imposes to a certain degree 'open banking' requirements, whereby incumbent financial intermediaries must share client data with third parties, including potentially innovative new competitors.[31] By giving providers access to the clients' financial information, PSD2 opens the way for new banking products and services and facilitates customers moving from one financial service provider to another. With the EU functioning as first mover, other jurisdictions are considering whether and how to follow.[32] This renders the EU PSD2 experiment particularly valuable and significant not only in payments but also from the standpoint of the real impact of open banking and competition especially from non-traditional technology-focused competitors, including FinTechs and BigTechs.

---

[30] 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, 2015 O.J. (L 337) 35.

[31] *See generally* Markos Zachariadis & Pinar Ozcan, *The API Economy and Digital Transformation in Financial Services: The Case of Open Banking* (SWIFT Institute Working Paper No. 2016-001, 2017), https://ssrn.com/abstract=2975199; Peggy Valcke, Niels Vandezande & Nathan Van de Velde, *The Evolution of Third Party Payment Providers and Cryptocurrencies Under the EU's Upcoming PSD2 and AMLD4* (SWIFT Institute Working Paper No. 2015-001, 2015), https://ssrn.com/abstract=2665973; Fernando Zunzunegui, *Digitalisation of Payment Services* (Ibero-Am. Inst. L. & Fin. Working Paper No. 5/2018, 2018), https://ssrn.com/abstract=3256281; Oscar Borgogno & Giuseppe Colangelo, *Data, Innovation and Transatlantic Competition in Finance: The Case of the Access to Account Rule*, Eur. Bus. L. Rev. (forthcoming 2020), https://ssrn.com/abstract=3251584; Benjamin Geva, *Payment Transactions Under the E.U. Second Payment Services Directive (PSD2) – An Outsider's View*, (2019) 54 Texas Int'l L. J. 211.

[32] *See* Australian Open Banking Initiative, *Review into Open Banking in Australia: Final Report* (Dec. 2017), https://perma.cc/6QVD-U2R3

Such data will have been collected and digitized, repackaged for delivery to regulators and/or internal use and managed by new purpose-built systems, typically all at great expense and difficulty. PSD2 thereby sets the stage for the next level of the evolution of data driven finance: broad competition among incumbent and new participants.

A. PSD2's Open Banking Approach

PSD1[33] and its amending and complementary legislation adopted from 2007 through 2012[34] established the common European market in payment services with the Single Euro Payments Area ('SEPA') framework. PSD1 was a success, in harmonizing payment transactions throughout the EU single market, and in achieving significant market integration and related efficiencies in the commercial and consumer payment sector. When PSD2 was first discussed, the European payments sector was not in need of reform; but one recently completed successful reform project provided the background for advancing payments regulation, addressing the significant technical innovation since adoption of the PSD1 framework.[35] The reform

[33] *See* Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on Payment Services in the Internal Market Amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and Repealing Directive 97/5/EC, 2007 O.J. (L 319) 1.

[34] *See* Regulation (EC) No 924/2009 of the European Parliament and of the Council of 16 September 2009 on Cross-Border Payments in the Community and Repealing Regulation (EC) No 2560/2001, 2009 O.J. (L 266) 11; Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the Taking Up, Pursuit and Prudential Supervision of the Business of Electronic Money Institutions Amending Directives 2005/60/EC and 2006/48/EC and Repealing Directive 2000/46/EC 2009 O.J. (L 267) 7; Regulation (EU) No 260/2012 of the European Parliament and of the Council of 14 March 2012 Establishing Technical and Business Requirements for Credit Transfers and Direct Debits in Euro and Amending Regulation (EC) No 924/2009, 2012 O.J. (L 94) 22; Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on Consumer Rights, Amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and Repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, 2011 O.J. (L 304) 64.

[35] *See* PSD2, Recital 3.

was premised upon the notion that '[s]ignificant areas of the payments market, in particular card, internet and mobile payments, remain fragmented along national borders' [36] and that the existing framework suffered from legal uncertainty, security risks and a lack of consumer protection. It was also difficult for payment service providers to launch innovative, safe and easy-to-use digital payment services.[37]

The European legislation sought to 'square the circle'. PSD2 sought to enable

> new means of payment to reach a broader market, [while] ensuring a high level of consumer protection in the use of those payment services across the [EU]. This should generate efficiencies in the payment system as a whole and lead to more choice and more transparency of payment services while strengthening the trust of consumers in a harmonised payments market.[38]

PSD2 also set out to address the security risks relating to electronic payments[39] as well as extraterritorial payment transactions.[40]

In order to achieve equivalent rules for equivalent transactions, regardless of the technology used, legal form employed or number of parties involved, and ensure equivalent protection for merchants and consumers,[41] PSD2 introduced a neutral definition of payment transactions.[42] Relating to that definition, the single license prudential framework for all 'payment

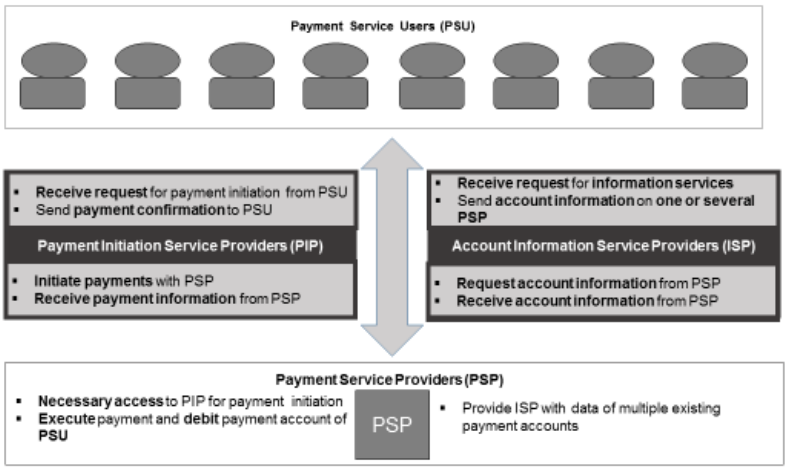
---

[36] *See* European Comm'n, *Consultation on Green Paper – Towards an Integrated European Market for Card, Internet and Mobile Payments* (2012).
[37] *See* PSD2, Recital 4.
[38] *See* PSD2, Recital 6.
[39] *See* PSD2, Recital 7.
[40] *See* PSD2, Recital 8.
[41] *See* PSD2, Recital 10.
[42] *See* PSD2, Art. 2.

institutions', i.e. providers of payment services unconnected to taking deposits or issuing electronic money, set out in PSD1 and refined and supplemented in PSD2, applies.

PSD2 responds, in particular, to new developments regarding internet payment services, such as payment initiation services[43] and account information services.[44] Both types of services 'play a part in e-commerce payments by establishing a software bridge between the website of the merchant and the online banking platform of the payer's account in order to initiate internet payments on the basis of a credit transfer'.[45]

Figure: Service Providers under PSD2



While both kinds of services are crucial in the modern payment services chain, each differs significantly from the other. In particular, '[w]hen exclusively providing payment initiation services, the payment initiation

[43] *See* PSD2, Art. 4(15). *See also* PSD2, Recital 29.
[44] *See* PSD2, Art. 4(16) and Recital 28.
[45] *See* PSD2, Recital 27.

service provider does not at any stage of the payment chain hold the user's funds'.[46] In turn, such a payment initiation services provider will not meet the definition and licensing requirement for payment institutions. However, '[w]hen a payment initiation service provider intends to provide payment services in relation to which it holds user funds, it should obtain full authorization [under PSD2] for those services'. [47] The same applies to account information services – they rarely hold the funds; it is the additional use of information that provides the benefits to clients. Both payment initiation services and account information services require direct or indirect access to the payer's account, or the account data, respectively. For providing its services, and even demonstrating its benefits to clients, the service provider must ask each client for consent to first access, and then to use the data.[48] This is the result of the GDPR's consent rule laid out above.

There are two ways to contact new clients. First, the service provider could identify the clients and seek their consent directly. But the service providers are new entrants, and they rarely know who the clients of a particular payment institution are, so they cannot seek consent in the absence of support by the payment institutions. Given that client contact is one of the payment institutions' core assets, they have little incentive to let new providers contact their clients.

Second, the service provider may tap into the existing data pool and contact the clients for consent directly if the payment institution is unwilling to support the provider. Under PSD1, bank confidentiality requirements prevented providers from doing so. PSD2 seeks to unlock the potential for

[46] *See* PSD2, Recital 31.
[47] *See id.*
[48] *See* PSD2, Art. 64.

innovation in payment services. Based on the recommendations provided by the Open Banking Working Group ('OBWG'),[49] PSD2 requires, in particular, that banks share customer data relating to payment services with technology firms. It does so by giving clients an ownership right over their data, and providing a specific use case for the data subject's data portability right granted by Article 20 of GDPR, thereby linking PSD2 to the GDPR.[50] In this way, PSD2 aims to create a pro-innovative environment with a high level of customer service, while simultaneously upholding the principles of cybersecurity, data protection *and* financial stability.

B. Transition to Data-Driven Finance

PSD2's central role in promoting 'open banking' is triggering the transition to data-driven finance in Europe. On the one hand, PSD2 allows technology firms to enter the payment markets. In light of incumbents' control over client data, and due to the limitation that payment institutions must share client data with certain additional (tech-driven) service providers, only where a new entrant meets that definition can it hope to gain access to client data. This alone inspires innovative firms to focus on development of value-added services, accelerating the development of data driven finance in Europe. Naturally, these entities will seek to keep their costs down and respond to regulatory responses like data sharing and liability requirements by technical means.

---

[49] *See* EBA Open Banking Working Group, *B2B Data Sharing: Digital Consent Management as a Driver for Data Opportunities*, (2018) 21, https://www.abe-eba.eu/media/azure/production/1979/eba_2018_obwg_b2b_data_sharing.pdf [https://perma.cc/7TNW-8J2K].
[50] *See* PSD2, Arts 66-67.

On the other hand, in the context of 'open banking', payment institutions must respond to PSD2 by providing data interfaces for third-party providers from which those providers can extract data of existing clients of the incumbents to provide value added services. This will increase competitive pressures: banks' only rational response to defend what is increasingly becoming their most valuable asset as the evolution of data-driven finance moves forward – client data – will be to enhance service levels and so avoid their clients seeking those value-added services elsewhere.

The costs for these additional value-added services will need to be kept as low as possible. The only way to do so will be to rely more heavily on technology, through advanced analytical tools and models which form the core of the evolution towards data driven finance. This process is then reinforced through the reporting obligations contained in PSD2 and elsewhere, thereby driving the consequential evolution.

While unintended, the outcome is nonetheless clear. Taking the process one step forward however is a system for making identification of customers easier, to enable them to more readily access financial services while also enhancing financial integrity through better customer identification and tracking). We analyse this in the next section. All of this enhances financial efficiency and benefits customers. It also makes it easier for new entrants to compete with established financial market participants and for customers to identify and transfer their data to innovative new entrants.

Nonetheless, we do not posit that the results of PSD2 will be all as expected. PSD2's objective is to enhance competition. Due to the data portability rights under PSD2, the door is open for large technology firms that know best how to use these data portability rights (which are not

identical to the data portability right under GDPR, which is designed to favour consumers) to enter financial services markets. While aiming at increased competition the outcome may well be the opposite: the concentration of data-driven services in the hands of a few technology firms that provide financial services as one aspect of their data-driven business models.

III. OPEN DATA: GDPR

The EU GDPR is the most important change in data regulation since the first Data Protection Directive of 1995,[51] not only in the EU but to a large extent globally. It has been – due to its exterritorial effect as stated in the Recitals and in Article 3(2) GDPR[52] – a game changer for data collection and processing in the EU and worldwide.[53]

EU financial regulatory reporting requirements – discussed in Part II and IV – have driven digitalization and datafication of finance and its regulation, causing an acceleration of the transition to data-driven finance in Europe's traditional financial services industry. GDPR – while impacting all sectors of the economy – has triggered a similar process in the collection, use, storage and protection of data in the financial sector. As financial regulation drove the digitalization of data, GDPR has driven spending on systems designed to appropriately manage that ever-increasing volume of data. Such spending is supporting digitalization and datafication

[51] *See* Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 [hereinafter 'GDPR'].
[52] *See* GDPR, Recitals 24-25.
[53] The interpretation of the notion of extraterritorial effect has been clarified by the European Data Protection Board. *European Data Protection Board (EDPB), Guidelines 3/2018 on the Territorial Scope of the GDPR* (Article 3) – Version for public consultation (2018), adopted on Nov. 16, 2018.

in the regulated financial industry and across the entire economy. We next consider GDPR in light of its role as a key driver of data-driven finance.

A. *Basic Principles of GDPR*

In the EU, Article 8(1) of the European Convention on Human Rights ('ECHR'), Article 8(1) of the Charter of Fundamental Rights of the European Union ('the Charter') and Article 16(1) of the Treaty on the Functioning of the European Union ('TFEU') together provide as fundamental rights and freedoms that everyone has the right to have their personal data protected.[54] An extensive regulatory framework has developed around this over time, with GDPR as the most important element. Specifically, GDPR imposes rules that seek to protect natural persons in relation to the processing of their personal data.[55]

According to the GDPR:

> '[r]apid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities.'[56]

[54] Svetlana Yakovleva, *Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade 'Deals'?*, (2018) 17 World Trade Rev. 477, 478; Consolidated Version of the Treaty on the Functioning of the European Union art. 16, Oct. 26, 2012, 2012 O.J. (C 326).
[55] *See* GDPR, Recital 1.
[56] *See* GDPR, Recital 6.

GDPR is thus a response to the substantial increase in cross-border flows of personal data between public and private actors across the European Union:[57]

> '[n]atural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and [is expected to] further facilitate the free flow of personal data within the [EU] and the transfer to [non-EU countries] and international organisations.'[58]

In addition, EU law calls upon national authorities in the EU Member States to cooperate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another EU Member State,[59] which is also a key focus of GDPR.

In this environment, and based on the premise that the creation of trust is a crucial precondition for further developing the digital economy across the European internal market,[60] GDPR seeks to ensure a high level of protection of personal data, through a 'strong and more coherent data protection framework in the [EU], backed by strong enforcement'.

GDPR is designed to be technology neutral, i.e. it does not depend on the techniques used for data collection and processing in order to prevent circumvention:[61]

> 'The protection of natural persons should apply to [any] processing of personal data by automated means, as well as to manual processing, if

[57] *See* GDPR, Recital 5.
[58] *See* GDPR, Recital 6.
[59] *See* GDPR, Recital 5.
[60] *See* GDPR, Recital 7.
[61] *See* GDPR, Recital 15.

> the personal data are contained or are intended to be contained in a filing system.'[62]

GDPR is restricted to data processing of personal data in connection with a professional or commercial activity (in contrast to an individual's household activity).[63] However, the controllers or processers of social media or other providers of software for household activities are subject to the GDPR.[64]

B. *Consent and Ownership*

The most important building block of the GDPR is that natural persons should have control of their own personal data. This right does not apply to legal persons, however, given that legal persons do not benefit from the fundamental rights granted by the ECHR, the Charter and the TFEU.[65] The key GDPR tool for control is the consent requirement stipulated by Article 6(1)(a) GDPR.[66] Natural persons must be clearly informed of the data collected as well as the purposes for which the personal data are used. According to Article 7(2) GDPR the request for consent must be presented in an intelligible and easily accessible form, using clear and plain language. Even where consent has been given, the circumstances under which consent has been achieved will be reviewed to remedy coercive pressure to achieve consent:

> 'In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject

[62] *See* GDPR, Recital 15.
[63] *See* GDPR, Art. 2.
[64] *See* GDPR, Recital 18.
[65] *See* GDPR, Art. 4(1).
[66] *See* GDPR, Recitals 40 and 42.

and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.'[67]

GDPR further provides considerable detail on how consent must be achieved:

'Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not

[67] *See* GDPR, Recital 43.

unnecessarily disruptive to the use of the service for which it is provided.'[68]

In addition, the data collected cannot be stored forever, but must be deleted in timeframes that relate to the objective for which the data was collected.[69] Following the Google Spain decision of the Court of Justice,[70] the GDPR further establishes a right to be forgotten upon request of the natural person (understood as withdrawal of consent), where the data have been unlawfully processed or where the personal data are no longer necessary for the purposes for which they were collected or processed.[71] This in many ways is targeting both the potentially undesirable impact of network effects and economies of scope and scale in data and their possible tendency toward undesirable natural monopolies.

The ownership approach embedded in the consent requirement is taken one step further with the data subject's right to data portability stipulated in Article 20 GDPR: Any natural person can ask the current data controller to transfer the data gathered, stored and processed to another controller in a structured, commonly used and machine-readable format without hindrance from the current controller. The right to data portability is driven by antitrust law considerations but is applicable irrespective of the existence of a data controller's dominant market position.[72] This approach is reinforced further specifically for the banking industry in the context of PSD2's open

---

[68] *See* GDPR, Recital 32.
[69] *See* GDPR, Art. 5(1)(c).
[70] *See* Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, 2014 E.C.R 317; *see also* Rolf H. Weber, *On the Search for an Adequate Scope of the Right to Be Forgotten*, (2015) 6 J. Intell. Prop., Info. Tech. & Electronic Com. L. 2.
[71] *See* GDPR, Art. 17(1).
[72] For further details see Rolf H. Weber, *Data Portability and Big Data Analytics*, (2016) 23 Concorrenza e Mercato 59, 66-70.

banking provisions. However, in fact, GDPR likewise imposes portability across the entire economy, not only in the context of payments, a subject we return to subsequently. (See Chapter 6 by Zee Kin Yeong and David Roi Hardoon for more reading on data portability and Singapore's approach.)

C. *Data Management and Compliance Requirements*

In addition to the mentioned fundamental principles, importantly in EU data protection law, the GDPR contains a number of specific data organization requirements. It furthers the use of pseudonymization of personal data as a measure to 'reduce the risks to the data subjects and help controllers and processors to meet their data-protection obligations'.[73] It also regulates the use of online identifiers[74] and imposes rules on tracing and profiling of users.[75] In particular, natural persons have the right to be subject to a decision by humans (in contrast to a decision based solely on automated processing, including profiling) where the decision produces legal effects, such as entering or termination of a contract, or denial of rights.[76]

Article 25 GDPR also introduces the requirements of 'privacy by design' and 'privacy by default'. These principles were originally developed and promoted by the Canadian Ontario Data Protection Commissioner, Ann Cavoukian.[77] Article 25(1) GDPR reads as follows:

> 'Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural

[73] *See* GDPR, Recital 28*; see also* GDPR, Recital 29.
[74] *See* GDPR, Recital 30.
[75] *See* GDPR, Arts 22-23
[76] *See* GDPR, Art. 22(2).
[77] *See* Ann Cavoukian, *Privacy by Design, The 7 Foundational Principles*, January 2011, www.privacybydesign.ca.

persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of the data subjects.'

Consequently, the enterprises are obliged to implement privacy-friendly technologies into their technical systems.

Furthermore, in case of using new technologies causing substantive privacy risks, controllers of data are bound by the obligation to undertake data protection impact assessments (as prescribed in Article 35 GDPR). In addition, the security of data processing has become a key issue of the GDPR. According to Article 31, controllers and processors are obliged to implement specific data security (technical and organizational) measures that should help to identify and mitigate the respective risks.

Cross-border data transfer has been a hotly debated issue for many years.[78] In respect of private enterprises, the GDPR has now introduced a set of rules for transfers of personal data to third countries or international organizations – such transfers are legitimate in case of a positive adequacy decision, the existence of appropriate safeguards (in contractual relations)

[78] *See* Rolf H. Weber & Dominic N. Staiger, *Transatlantic Data Protection in Practice*, 16-30 (Springer 2017); Erdem Büyüksagis, *Towards a Transatlantic Concept of Data Privacy*, (2019) 30 Fordham Intell. Prop. Media & Ent. L. J. 139, 170 et seq.

or the implementation of binding corporate rules (within corporate groups) pursuant to Articles 44-47 of GDPR.

In addition, there are also new rules for the public sector: The GDPR addresses significant issues for regulators, particularly in the context of cross-border sharing of information – a core element of both pre- and post-2008 international regulatory initiatives.[79] Technically, GDPR does not extend to public authorities such as those involved in public security and crime prevention,[80] tax and customs authorities, financial investigation units, or financial market authorities.[81] These public authorities are subject to more specific legal requirements the EU has adopted for crime prevention.[82] If such specific sectoral legislation does not exist, general data protection requirements tailor-made for public institutions apply.[83] However GDPR is nonetheless significantly impacting the practices of financial regulators and their interactions with the financial industry – which is subject to the requirements of GDPR – resulting in potential questions about the legality of submitting information to regulators about the activities of individual customers, such as in the context of AML or other financial

[79] *See* GDPR, Arts 50, 60-62.

[80] *See* GDPR, Recital 19.

[81] *See* GDPR, Recital 31.

[82] Directive (EU) 2016/680 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 by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data and Repealing Council Framework Decision 2008/977/JHA, 2016 O.J. (L 119) 89.

[83] *See* GDPR art. 60; *see also* Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the Protection of Individuals with Regard to the Processing of Personal Data by the Community Institutions and Bodies and on the Free Movement of Such Data, 2001 O.J. (L 8) 1. In addition, EU law provides for many specific provisions of data processing by public authorities in sectoral legislation. For instance, *see*, with regard to financial legislation, CRD IV, MiFID II, AIFMD, and PSD2.

regulatory reporting requirements.[84] These arise in particular with the interactions between EU financial institutions and data about EU natural persons and the possible transfer to non-EU regulators (such as those in the US).[85]

The detailed provisions of the GDPR are paired with severe enforcement mechanisms. On the liability side, any person who has suffered material or non-material damage as a result of an infringement of the GDPR has a right to compensation from any controller or processor who was handling her personal data, even without contractual relationships between the person and controller/processor.[86] At the same time, GDPR comes with heavy penalties, up to four percent of the total worldwide annual turnover of the corporate group to which the data controller or processor belongs.[87]

The early months of GDPR practice have left little doubt that the European data protection authorities are willing to impose sizable penalties.[88]

D. *Driving the Next Stage of Open Banking and Data-Driven Finance: Open Data*

In the context of European finance, GDPR's initial impact comes from its requiring financial intermediaries to reorganize their data processing as well as client data policies to meet the requirements of GDPR. The extensive details on personal data of individuals also require data categorization tools

---

[84] *See* Iana Rezlauf, *EU Framework for Handling Big Datasets Mixed of Personal and Non-personal Data*, (2020) 21(1) CRi 7.
[85] *Id.*
[86] *See* GDPR, art. 82(1).
[87] *See* GDPR, art. 83.
[88] *See* Charlie Osborne, *Facebook Could Face $1.63bn Fine Under GDPR Over Latest Data Breach*, Zero Day (Oct. 2, 2018), https://www.zdnet.com/article/facebook-could-face-billions-in-fines-under-gdpr-over-latest-data-breach/ [https://perma.cc/HU5D-AMWQ].

which allow for amendments and deletion after a given timeframe or upon the natural person's request.

Financial intermediaries have often collected large amounts of data from and about their customers, over long periods of time. However, in many cases, these data have not been used effectively, because they have been restricted to certain business units, lines, products or silos within individual firms.[89] Financial intermediaries are now obliged to build comprehensive systems for their data which address the collection, storage, use and protection of the data according to the principles of the GDPR. The process of digitalization combined with systemization to meet the requirements of GDPR has triggered a revolution in financial industry treatment of customer data, in the same way that MiFID II and its financial regulatory relatives have driven a revolution in financial industry collection and processing of business and regulatory data.

However, unlike the reforms which drive digitalization and datafication through the application of analytics to massive amounts of data – providing the impetus for data driven finance in Europe's traditional financial industry – GDPR instead creates barriers to centralization of individual customer data and its use, placing requirements on the financial industry to develop new systems of data management and also shifting control of many aspects of their data from financial and data intermediaries (which have collected it) to individual customers (who are its subject).

Arguably, this may impair fully data-driven business models. For instance, financial institutions cannot contact new clients for distribution or sales

[89] *See* Remarks by Luiz Awazu Pereira da Silva & Goetz von Peter, *Financial Instability: Can Big Data Help Connect the Dots?* (Nov. 29, 2018), https://www.bis.org/speeches/sp181203.pdf.

purposes after acquisition of data pools from third parties unless the clients are legal persons only or the clients have consented ex ante, or the data pools were assembled through web-based gathering of user data.[90] Furthermore, data pools relating to the past become increasingly unreliable for data analysis or risk management purposes to the extent that the GDPR's deletion requirements apply, removing some upfront benefits from greater data gathering activity. These deficiencies could be considered and remedied in the risk models, for instance by adding further security margins to 'old' or obviously deficient data pools, by mixing data from different sources, or applying filters. But all of this requires further sophistication in data gathering and processing methodology.

Another development is noteworthy. The GDPR's data processing rules also interfere in the internal organization of data intensive businesses, such as social media, health or financial institutions. This has also driven the standardization of data processes outside of finance – potentially making for a larger data pool and enabling new entrants to potentially access more data of their individual customers. Large technology companies know well how to make use of the new rights to data transfer – much better than do new entrants with access to customers limited by budgets and resources. This could prompt unexpected results: while originally designed to curtail the

[90] *See* Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 201) 37 (introducing a specific data protection regime governing electronic communications). This Directive is expected to be replaced by a so-called E-Privacy Regulation, coordinated with and simultaneously with the implementation of the GDPR. *See Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC*, COM (2017) 10 final (Jan. 10, 2017). However, political objections, particularly in respect of the proposed cookies rules, have caused a major delay and it is not yet clear when this Directive will come into force; nevertheless, it might influence the financial intermediaries in the future.

power of data behemoths the result of GDPR may be less competition from the greater concentration of data in the hands of the few.

IV. EXTENSIVE, DIGITAL REGULATORY REPORTING OBLIGATIONS: SETTING THE STAGE FOR A MOVE FROM OPEN BANKING AND OPEN DATA TO OPEN FINANCE

Since the 2008 Crisis, in tandem with post-crisis international regulatory approaches, European regulators have imposed ever higher reporting obligations on financial intermediaries in an effort to combat systemic risk and address a range of integrity risks around money laundering, terrorism financing and competition scandals (in particular about LIBOR and foreign exchange trading). The most important regulatory initiatives in this regard include those for: banking, CRR/CRD IV (finalized in 2013 and effective in 2014); asset management, AIFMD (2011 / 2013); financial markets, MiFID II/MiFIR (2014 / 2018); market infrastructure, EMIR (2012 / 2013); payment services, PSD2 (2015 / 2018); and money laundering, AMLD5 (Anti-Money Laundering Directive 2018 / 2020).

These frameworks share a common focus related to international financial regulatory standards in the EU; and a common imposition of extensive reporting requirements upon the financial services industry. Regulators in the EU, by requiring financial intermediaries to report far more data on their decisions, activities and exposures, have triggered a revolution in Europe's regulated financial industry. Today, when faced with a proposed regulation, the financial services industry will demand sufficient time to build the necessary IT systems to implement it. The necessity of technological implementation of regulatory reporting requirements has forced intermediaries and their service providers to continually invest in the

development of their software and IT systems to ensure sufficient data are collected within their organization to meet reporting requirements, that these data are packaged and reported in the necessary structure and form, and that they flow from the supervised entities to the supervisors in the required manner.

This has also forced regulators and supervisors to develop data management systems capable of receiving and processing the volume of data being generated and delivered. This process of digitization of reporting and related compliance requirements across both intermediaries and regulators has led to a RegTech ‘revolution’ in the European financial services industry.

In addition, as the industry has digitized, and standardized data has been collected across the global operations of individual firms, it has begun to focus on better using the data being collected, to both reduce compliance costs and generate new opportunities. This is the process of datafication: the application of analytics tools to digital data, i.e. the fundamental process of digital financial transformation and the evolution of data-driven finance in the traditional financial services industry.

In addition, as supervisors have been deluged with ever-increasing volumes of data, in digitized standard forms, supervisors have also had to enhance their data analytics tools. Once their analytics tools are enhanced, supervisors can handle even more data (and in turn, tend to ask supervised entities to collect and transmit even more of it, triggering another RegTech cycle).

As an example, when fund managers were required by the AIFMD in 2011 to report extensive data on investment strategies in a purely digital

manner,[91] there was an outcry from small and mid-size firms arguing they would be disadvantaged relative to the large fund managers. Time has solved this problem. Seven years later the data stream from fund managers via national competent authorities ('NCA's) to the European Securities and Markets Authority ('ESMA') flows smoothly. We expect the same with regard to other regulatory initiatives if sufficient implementation time is granted; the latest example being the MiFID II implementation with its extensive reporting requirements and extraterritorial impact.

This development, examined elsewhere,[92] is central to the process of Europe's digital financial transformation because this regulatory evolution has forced the financial services industry (and its regulators) to digitize data collection and regulatory reporting comprehensively.

V. DIGITAL IDENTITY: TYING THE PIECES TOGETHER

A. Towards Cross-border ID

The eIDAS Regulation (eIDASR) was adopted in 2014 to provide mutually recognized digital identity for cross-border electronic interactions between European citizens, companies and government institutions. Member states can notify the European Commission of their national form of eID. Other member states have been able to recognize these forms voluntarily since 2015, and have had to do so since 2018.[93] When an eID is ultimately

---

[91] *See* Dirk A. Zetzsche & David Eckner, *Investor Information and Reporting,* in THE ALTERNATIVE INVESTMENT FUND DIRECTIVE (Zetzsche, ed., 2018).

[92] *See* Veerle Colaert, *RegTech as a Response to Regulatory Expansion in the Financial Sector* (June 2018) (unpublished manuscript), https://ssrn.com/abstract=2677116 [https://perma.cc/UM37-4GMS]; https://ssrn.com/abstract=2677116; Rodrigo Zepeda, *The 2018 Big Bang* (Aug. 30, 2017), https://ssrn.com/abstract=3029145 [https://perma.cc/E7SA-QZR6].

[93] *See* R. Bastin, I. Hedea & I. Cisse, *A Big Step Toward the European Digital Single Market*, DELOITTE (2016) at 70-77, https://www2.deloitte.com/lu/en/pages/about-

recognized throughout the EU, an individual can use it in any member state.[94] The eID is assigned a certain level of assurance based on its security specifications, and this allows states to determine the services in relation to which it may be used.[95]

This system does not make redundant individual sovereign forms of identity. However, it does allow national forms of digital identity to be recognized throughout the EU, and thereby enables any EU citizen or entity so identified to enter into transactions digitally.

Rather than introducing a pan-European ID card system, which would have doubled the work for Member States, the eIDASR has sought to ensure people and businesses can use their own national eIDs to access public services in other EU countries where eIDs are available. The goal has been to create a European internal market for e-trust services by ensuring that eIDs work across borders, and have the same legal status as traditional paper-based processes.[96] Use cases include submitting tax declarations, enrolling in a foreign university, remotely opening a bank account, setting up a business in another member state, and bidding for tenders.

Prior to eIDASR many different national standards for eIDs, independent from coordinated EU policy, were developed within EU member states. The eIDASR does not harmonize those standards, but focuses on their technical interoperability. By mandating that member states and eID providers meet

---

deloitte/articles/inside/inside-issue13.html [https://perma.cc/68LH-VS3B].

[94] *Id.*

[95] *Id.*

[96] *See* Regulation (EU) 910/2014, of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC, 2014 O.J. (L 257/73) [hereinafter 'eIDAS Regulation'].

certain identification obligations (including that the person identification data uniquely represents the person to which it is attributed and that online authentication is available),[97] the eIDASR is designed to create trust.

B. eIDASR as an Open Standard

The eIDASR is a useful model for eID projects since it provides, in principle, an open standard not limited to EU jurisdictions.[98] Every national ID system that wants to connect to the eIDAS system can do so.[99] Connecting to the eIDASR does not require reform of national eID standards. Rather, by defining nodes (so-called 'eIDAS connectors') that provide the cross-border links between other countries' systems and one's own system, any country could link to the eIDAS identification system in the EU/EEA, resulting – potentially – in a global eID network.[100]

While adopted in 2014, the implementation of eIDASR took some time, with public eID systems taking the lead.[101] However, in November 2017 the first private sector-run national eID scheme was notified to the European Commission by Italy, connecting all eIDs created by that private enterprise to the European eID network.[102] This enables Italian citizens and businesses to use their SPID [*Italian eID*] credentials to access public services in other member states.[103]

---

[97] *See id.*, Art. 7, at 87.

[98] Douglas W. Arner, Dirk A Zetsche, Ross P. Buckley, & Janos N. Barberis, *The Identity Challenge in Finance: From Analogue Identity to Digitized Identification to Digital KYC Utilities*, (2019) 20 European Bus. Org. L. Rev. 55, 67.

[99] *Id.*

[100] *Id.*

[101] *Id.*

[102] *Id.*

[103] *See First Private Sector eID Scheme Pre-Notified by Italy Under eIDAS*, Shaping Europe's Digital Future, EUROPEAN COMMISSION (Dec. 7, 2017), http://bit.ly/2DmVQtV

C. Towards an e-ID-Based Data Ecosystem

The eIDASR lays the foundation for a service-oriented ID base and for the establishment of electronic know-your-customer ('eKYC') utilities in Europe. The European Commission's Consumer Financial Services Action Plan,[104] aims to 'work with the private sector to explore how they could use electronic identification and trust services for checking the identity of customers'.[105] In particular, Action Item 11 states: 'The Commission will facilitate the cross-border use of electronic identification and know-your-customer portability based on eIDAS to enable banks to identify customers digitally.'[106] Such eKYC utilities are a major innovation that promise substantial reductions in customer on-boarding costs for providers, and substantial increases in the integrity of on-boarding processes as nefarious customers are limited in their capacity to shop around for a friendly and compliant, or perhaps inept, financial services provider. (The concept of digital identity is explored further in Chapter 12 by Greg Kidd.)

VI. EVOLVING APPROACHES TO OPEN BANKING, OPEN DATA AND OPEN

[https://perma.cc/N9XJ-Z4DM].

[104] *See* European Commission, *Consumer Financial Services Action Plan: Better Products, More Choice* (March 23, 2017), *https://eur-lex.europa.eu/resource.html?uri=cellar:055353bd-0fba-11e7-8a35-01aa75ed71a1.0003.02/DOC_1&format=PDF* [https://perma.cc/M4FX-X28Q]. The Action Plan draws on previous work, such as a commissioned study asking for connection eIDAS and the consumer financial services sector. *See* European Commission, Directorate-General for Financial Stability, Financial Services and Capital Markets Union, Study on the Role of Digitalization and Innovation in Creating a True Single Market for Retail Financial Services and Insurance (July 2016), https://ec.europa.eu/info/sites/info/files/study-digitalisation-01072016_en.pdf [https://perma.cc/2KAN-VQJG] [hereinafter 'European Commission, Digitization and Innovation'].

[105] Press Release, *European Comm'n, Consumer Financial Services Action Plan: Better Products and More Choice for European Consumers* (Mar. 23, 2017), https://ec.europa.eu/commission/presscorner/detail/en/IP_17_609.

[106] *See* European Commission, Digitization and Innovation, *supra* note 104.

Individually and in combination, it is clear that these four separate EU initiatives – payments and open banking, data protection and open data, financial regulation, and digital ID – all independently drive forward the digitization and the datafication of finance in the EU Single Market, for both market participants and regulators. Together they also are driving the next stage of evolution of the European financial sector. While the process is still evolving, based on the legal infrastructure now in place, the final outcomes are likely to see incumbent financial market participants, innovative FinTechs, BigTechs, digital finance platform providers and others increasingly competing with one another using ever-broader, and more highly analysed, data sets. While client relationships were incumbents' core assets in the past, control over large volumes of data now replaces them.

In addition to their impact within the European Union, each of these discrete sets of regulatory reforms are also effective extraterritorially in many aspects, for firms and others engaging in financial services with EU customers or dealing with EU customer data. Thus, particularly the impetus for development as a result of the combination of initiatives in the EU is provoking global responses, and in many cases development of related strategies and significant expenditures in compliance and implementation of necessary IT and other systems.

It is also clear that the policy concerns that have driven the development of these four EU pillars are driving an increasing range of other jurisdictions around the world to consider how best to approach the intersection of data, finance and regulation. Beyond the EU, the world is currently providing a

laboratory of different environments in which data-driven finance can operate and evolve.

In the US, a uniquely relaxed approach to privacy and data protection based on a market-based understanding of customer ownership coupled with an overriding distrust of state use of personal data has empowered a huge range of data applications that are increasingly raising concerns, particularly with the emergence of increasingly dominant data players such as Google, Facebook and Amazon.[107]

In the EU, we see the converse approach with the GDPR representing, so far, the global high point of data protection and rigorous information reporting requirements. This has meant the demand for RegTech in the EU is currently outstripping the capacity to generate the IT needed. However, when such systems designed to ensure individual control of data are combined with a distrust of public sector use of consumer data, particularly as is now being seen with US BigTech, a very different possible future emerges.

China has seen a similar pattern of BigTech emerging. In China, BigTech is already increasingly dominating finance.[108] Somewhat ironically given China's history, the private sector, in the form of Tencent and Alibaba, have led the evolution of data amalgamation and use, including by establishing national identification systems to underpin their payments and other

[107] *See* David McLaughlin, *Why Were Facebook, Amazon, Apple, and Google Allowed to Get So Big?* FORTUNE (Mar. 16, 2019), http://fortune.com/2019/03/16/google-amazon-antitrust-laws/ [https://perma.cc/V2LC-R7KQ].
[108] *See* Louise Lucas, *The Chinese Communist Party Entangles Big Tech*, FIN. TIMES (Jul. 19, 2018), https://www.ft.com/content/5d0af3c4-846c-11e8-a29d-73e3d454535d.

systems, and the burgeoning superstructure of other financial services applications being built upon them.[109]

India has adopted a comprehensive strategy around digital transformation and the development of data-driven finance through digitization and datafication, termed 'India Stack,'[110] which is described in greater detail in Chapter 11 by Haksar, Carrière-Swallow and Patnam. As the foundational element, Aadhaar is a government-driven, national biometric database and identification system which has empowered financial inclusion and provided the technological foundation for a whole range of innovations.[111] In many ways, India's top-down, state-led approach to designing digital infrastructure is the countermodel of the market driven approaches of the US and China.

India's strong centralized agenda to support digital financial transformation certainly demonstrates the potential of approaching data-driven finance strategically.[112] China's path to data-driven finance has been entirely different, and emerged from the largely unfettered market activities of a small number of major tech firms, often with close state relations, but without any overriding national strategy prior to 2015-2016.[113]

---

[109] *See* Gabriel Wildau, *China Unveils Digital ID Card Linked to Tencent's WeChat*, FIN. TIMES (Dec. 27, 2017).

[110] *See* IndiaStack, *What is IndiaStack?* (last visited June 6, 2019), https://www.indiastack.org/%20about/.

[111] *See* Unique Identification Authority of India, Government of India, *What is Aadhaar?* (last updated Jan. 24, 2019), https://uidai.gov.in/my-aadhaar/about-your-aadhaar.html [https://perma.cc/X7YK-L5J6].

[112] *See* DW Arner, J Barberis & RP Buckley, *FinTech, RegTech and the Reconceptualisation of Financial Regulation*, (2017) 37 *Northwestern J. Int'l L. & Bus.* 371.

[113] The very rapid growth in Ant Financial and other firms prompted the People's Bank of China to take steps to slow down developments and better manage potential risks in 2015-16. *See* Weihuan Zhou, Douglas W. Arner & Ross P. Buckley, *Regulation of Digital Financial Services in China: Last Mover Advantage*, (2015) 8 Tsinghua China L. Rev. 25.

In both the US and China, free transferability of data has allowed acquisition of large pools of data, reflected in the emergence of a small number of very large firms based on network effects and economies of scope and scale for data. The outcome is both impressive and fearsome: For instance, while datafication of finance has outstripped other (seemingly more developed) countries, the market dominance of China's three digital finance superfirms, Baidu, Alibaba and TenCent (the 'BATs'), have led to antitrust inquiries in China.

A. Data Regulation vs. Financial Regulation

As mentioned, existing regulation will need to be reshaped to better accommodate the demands, and potential, of the rise of open finance, particularly through interactions with data protection regulation. Budgets for IT, cybersecurity and IT risk will all need to grow substantially and even more rapidly than in the past, in the private sector and particularly for regulatory and supervisory bodies.

In addition, however, there is a more fundamental question regarding regulatory approaches to data-driven finance. To date, the impact of laissez-faire approaches to data regulation can be seen in the US and China, both of which are now characterized by the dominance of their data sectors by small numbers of participants. In both cases, this has arguably been facilitated by few limits on individuals transferring ownership and control of data to BigTech firms, which in turn have benefited from network effects and economies of scope and scale in its amalgamation and use.

This affects financial law's objectives and hence the remits of supervisors. Where the power is in the data we recommend financial regulators address the new systemic risk stemming from concentration of data in the hands of a

few technology firm. This risk mirrors the traditional systemic risk represented by banks that are too-big-to-fail or too-connected-to-fail. In turn, we support market structure-related interventions which aim to maintain the independence of, and choice among, critical infrastructure providers as well as data portability rights in favour of financial customers. The measures that result may look similar to existing antitrust approaches, based on a financial law rationale: systemic risk.

B. Towards Open Finance?

The EU experience highlights how, as financial systems digitize, it is necessary to carefully consider approaches to financial regulation, cybersecurity, data protection, digital identity and competition. The approaches taken in different jurisdictions will be driving forces in financial and economic development and innovation in the 21st century.

While financial intermediaries have often collected large amounts of data, over long periods of time, these data were not used effectively.[114] Digitalization combined with systemization to meet the GDPR's data governance requirements has triggered a revolution in the treatment of customer data, in the same way that MiFID II and its financial regulatory relatives have driven a revolution in financial industry collection and processing of business and regulatory data.

Partly contradictory, GDPR creates barriers to centralization of individual customer data and their use, placing requirements on the financial industry to develop new data governance standards and also shifting control, at least

[114] *See* da Silva & Goetz von Peter, *supra* note 89.

in name, of their data from intermediaries (which have collected it) to individual customers (who are the subject).

Finance has long been an information industry,[115] but financial regulation and data regulation evolved in distinctive non-interactive legal silos, based on very different underlying principles and policy objectives. How the financial sector and regulators come to terms with the interaction of these separate rulebooks will determine in many ways the future of data-driven finance in Europe and around the world.

Limitations on pooling and restrictions on cross-border storage and use of data are also encouraging significant research and spending on new systems of data aggregation and analysis which do not require individual data access, but rather are based on query-only or decentralized structures. These are driving innovation in data systems and analytics.

Thus, while regulation limits data-driven finance it also drives the process forward in new ways through its focus on the use, collection, storage, transfer and protection of data.

The transformative role of FinTech around the world highlights how finance, data and technology are now all tethered one to the other.[116] As such, regulatory approaches in each area will interact with approaches taken in other areas. The European Union provides a vivid example of this through the interaction of key legislation such as MiFID2, GDPR, PSD2

[115] Finance is only now slowly evolving from an information, into a data, industry. Historically information resided in parts of a bank and was not shared efficiently across the institution let alone analysed and applied effectively.

[116] *See generally* European Banking Authority, *Report on the Prudential Risks and Opportunities Arising from FinTech* (2018); European Banking Authority, *Report on the Impact of Fintech on the Incumbent Credit Institutions' Business Model* (2018).

and eIDAS. This combination of regulatory approaches and policies will continue to push forward data-driven finance in the European Union.

As other jurisdictions around the world are increasingly forced to consider the interaction of financial regulation, data protection, and cybersecurity in the context of their own cultural and political environments, the experience of the EU will provide major lessons for policy and regulatory choices.

VII. TAKE AWAY: THREE LESSONS

In this chapter, we argue that a series of clearly motivated but uncoordinated projects played a crucial role in shaping Europe's financial ecosystem to make it more open to innovation by data-driven financial services providers of an increasing range of forms. However, what the EU did without an overarching roadmap, other jurisdictions may – and we argue should – do so purposefully through careful development of coordinated legal and regulatory approaches to finance, data and their interaction. In this regard the EU presents an interesting and still evolving case study, relevant to every other jurisdiction in the world. In the EU, the road to data-driven finance has benefited from a robust rule of law environment (that ensures the viability of long-term investments), a strict approach to data privacy (that grants data portability rights to individuals rather than service providers), a willingness to use regulation to drive evolution of markets and societies, and an approach aiming at 'controlled' rather than 'cutthroat' capitalism.

In this respect the EU approach was enabled by a 'traditional' cultural bias against data commercialization. This political and social environment was further supported by the European Commission and the European regulatory authorities (particularly ESMA and the European Banking

Authority) playing a strong central role in developing regulatory frameworks to address key policy challenges around data and finance. Were it not for these new central EU financial regulators being able to extend their activities without long-standing bureaucratic legacy issues, few steps towards data-driven finance – outside of select jurisdictions such as the United Kingdom and Luxembourg – may have been possible in the practice of financial supervision.

Europe's experience with its four separately designed policy and regulatory frameworks considered here will have a very important determinative impact on the structure of data-driven finance in Europe and in global financial markets, particularly as other jurisdictions consider how best to balance the objectives of data protection and financial regulation while supporting innovation, efficiency and financial stability, and many of them look for role models. This will be driven by the familiarity of many institutions with the EU framework from having to implement its requirements for their European operations and because of its extraterritorial reach. The change from extending finance on the basis of what an institution knows directly about its customer to extending it on the basis of data analytics drawing upon huge pools of data is profound, with the potential for both highly positive as well as highly negative outcomes as this evolution plays out across Europe and the world.

In looking at these issues, based on experiences to date, we would suggest a number of central lessons. The first is that finance, data and technology are now intertwined as a result of a long-term process of digitalization and datafication of finance in developed markets (a process that is likewise happening rapidly in emerging and developing markets). As a result,

RegTech, the use of technology for compliance, monitoring, enforcement, and system design in financial regulation, will continue to increase.

The second clear lesson is that each society must grapple with its own approach to data and its role in their future. These discussions will involve not only questions of finance and data regulation but also of social regulation and competition/antitrust regulation. As we have shown, different societies can have very different views on this issue and on the governance and economic systems they prefer in their futures. Everywhere, however, these issues will need to be addressed and the choices made, because otherwise globalization and network efforts will likely mean that decisions taken abroad will dictate the outcomes in markets around the world. While there appears to be a strong divergence in the use of data by governments, there appears to be an increasing consensus around the desirability of placing limits on the use of data by the private sector.

The third lesson is that because of the integration of data and finance, when designing financial regulatory systems and seeking to regulate data it is necessary to consider the implications of the interaction of data and finance. As can be seen from the EU experience, conflicts between objectives and rules should be considered ex ante. One area where this is particularly important is in choices about whether to pursue open banking and digital ID strategies. At this point, the EU experience is at an early stage but it will influence the approach taken in many other jurisdictions. European success or failure will echo around the world.