TECHNICAL NOTE

CGAP

COMBINING OPEN FINANCE AND DATA PROTECTION FOR LOW-INCOME CONSUMERS

February 2023

David Medine and Ariadne Plaitakis

ACKNOWLEDGMENTS

The authors would like to thank the following CGAP and World Bank colleagues: Stephen Rasmussen for overseeing this effort; Xavier Faz, Fredesvinda Fatima Montes, and Will Cook for peer review; Stefan Staschen for helping conceptualize this work; and Ivo Jenik, Maria Fernandez Vidal, Yasmin Bin-Humam, and Arisha Salman for their feedback.

The authors would also like to thank the many experts who contributed to this Technical Note, provided feedback, shared their experience, and worked with CGAP through the CGAP Data Project's Expert Advisory Group, including Chapin Flynn, Mastercard; Buhle Goslar, JUMO; Sonia Jorge, Global Digital Inclusion Partnership; Ivan Mortimer-Schutts, World Bank/IFC; and Faith Reynolds, the Finance Innovation Lab.

Consultative Group to Assist the Poor
1818 H Street NW, MSN F3K-306
Washington DC 20433
Internet: www.cgap.org
Email: cgap@worldbank.org
Telephone: +1 202 473 9594

RIGHTS AND PERMISSIONS

CONTENTS

SECTION I Overview 1

Introduction 1

Background 2

Key Entities in Open Finance 3

Data Protection Can Develop Consumer Confidence in Open Finance 4

Open Finance vs Data Protection Entities 5

Impact of Gender on the Use of Open Finance 7

How Regulatory Frameworks Can Protect Customer Data 7

Timing for Introducing Data Protection Regulation 9

Who Should Regulate Data Protection? 9

Which Open Finance Data Is Out of Scope for Data Protection? 10

SECTION II Basic Data Protections to Support Inclusive Open Finance 11

Consumer Control Over Data 11

Responsible Use of Data 21

Data Security 23

SECTION III Data Protection Implementation 26

Recordkeeping 26

Liability Allocation 27

Complaints Resolution 27

SECTION IV Conclusion 29

APPENDIX A Open Banking and Data Protection Laws and Regulations 30

APPENDIX B Glossary 32

Bibliography 34

SECTION I

OVERVIEW

Introduction

Consumers' money and their digital financial data are both often locked inside banks. But historically it has been easier for consumers to withdraw their money than their data. In many cases, consumers had no right to withdraw their digital financial data at all, let alone direct that it be shared with third parties. Today, we see a rise in financial technology companies (fintechs) providing new financial tools based on consumer data, including the ability to initiate payments and make informed choices based on financial advisory services. Yet sharing bank-stored consumer data with third parties like fintechs has proved challenging. As a result, competition has been stifled and consumers are often left with fewer financial services choices at higher prices.

However, a new era is emerging that legally empowers consumers to:

- Direct that their data be moved from one bank to another bank or a third party, such as a fintech. This type of data sharing is known as "open banking."
- Better harness, share, and apply their financial data in order to access additional types of financial services. Consumers may now have the ability to move their data from a variety of financial institutions beyond banks (e.g., insurers, pension funds) to other similar entities or to third parties—including fintechs. This type of data sharing is known as "open finance." Open finance includes open banking and is the focus of this CGAP Technical Note.
- Move their financial and nonfinancial data from one company to another (e.g., a travel operator, energy provider, social media platform) for a variety of purposes—including access to financial services. This type of data sharing is known as "open data."

The goal of this type of data sharing is to promote competition, which leads to the development of innovative financial products and services that benefit consumers. However, the resulting digital ecosystem is more complex due to the extensive new movement of sensitive consumer financial data between a wide variety of participants for multiple purposes. Consumers across every income range have been asked to place their trust and confidence in the ecosystem. But they are concerned about whether their data will be used for unauthorized or fraudulent purposes; handled irresponsibly or not in their best interest; or used and shared beyond their control by other open finance participants far removed from them and their original providers.

Successfully addressing these concerns is critical to the widespread adoption of open finance. Research has shown that "trustworthy data ecosystems are core to public trust"[1] and "consumers are more willing to share data

1 Ada Lovelace Institute 2022.

when they believe a firm is acting in their best interests."[2] Research also suggests that regulation, including data protection, is a key component of those ecosystems.[3]

This CGAP Technical Note offers guidance for financial, data protection, and competition regulators and authorities on how to address data protection concerns in an open finance world. If these issues are not addressed, wary low-income consumers in emerging and developing markets (EMDEs) may be inhibited from taking advantage of all that open finance has to offer. In particular, the goal of data protection is to support open finance to expand financial inclusion for low-income consumers while ensuring their data is kept safe and used for their benefit. This note assumes that basic data protection provisions must be in place to create a safe and sound open finance regime. It elaborates on what those provisions entail and how they can be addressed within law and regulation.

The note builds on CGAP's previous work in data protection and open finance.[4] CGAP's work showed the importance low-income people in EMDEs place on data protection and privacy related to financial services,[5] including those services fueled by data accessed through open finance. CGAP's research further identified comprehensive data protection regulatory frameworks as one of twelve critical design elements of an open finance regime that could benefit low-income populations. However, Plaitakis and Staschen (2020) noted that this is a challenging prerequisite to fulfill in the context of EMDEs as they may not have fully developed data protection legal frameworks. That observation inspired this Technical Note. Additionally, forthcoming CGAP work identifies data protection as one of the foundational elements of inclusive data ecosystems.

Section I of this note provides background on the importance of data protection to open finance and laws that can provide such protection. Section II is a guide to benchmarking whether basic data protections are in place in a legal framework, as informed by various data protection and open finance laws around the world. To provide a diversity of approaches to open finance, this note examines the open finance and data protection laws of Australia, Brazil, the European Union, India, Nigeria, and the United Kingdom.[6] These approaches include giving consumers control over their personal information, having mechanisms in place to ensure the responsible use of data, and implementing security measures to prevent unauthorized access to or use of data. Section III addresses some of the practical challenges of implementing data protection laws and regulations within open finance. Finally, Section IV concludes that data protection is critical to developing trust and confidence in open finance. It also offers a word of caution on creating an open finance system that is so complex that consumers are reluctant to participate in it.

Background

Open finance, which includes open banking, holds tremendous promise for unbanked and underbanked consumers in EMDEs. Specifically, it gives them the ability to exercise greater control over personal information and make their data work for them. Breaking the grip that large banks and other financial institutions have on data creates many possible channels through which innovative uses of data can benefit these consumers. It can allow them to save more easily, provide them with access to suitable credit products, and help them to control their finances, obtain better deals, and manage debt.[7] More than open banking, open finance provides the underbanked with a data sharing mechanism that uses their limited banking and/or payments history to expand access to a broader suite of financial services. Open finance is particularly

2 Reynolds and Chidley 2018, citing Ipsos MORI for Open Banking Ltd, Data minimization and user privacy amongst consumers and SMEs, 2018.

3 Ada Lovelace Institute 2022.

4 See Plaitakis and Staschen (2020) on open finance. The CGAP blog series on data protection can be found at: https://www.cgap.org/blog/series/data-privacy-and-protection.

5 Fernandez Vidal and Medine 2019; Fernandez Vidal 2020.

6 For India, the authors reviewed a draft law.

7 Plaitakis and Staschen 2020.

helpful to unbanked consumers because it enables the transfer of data from nontraditional financial sources (e.g., mobile money accounts) to more traditional financial institutions. This helps unbanked consumers to access previously inaccessible formal financial services. The value open finance brings can be expanded if it transitions open data. For example, making data on utility and telecom transactions available to financial institutions (e.g., banks) will allow them to serve previously ineligible customers.

Key Entities in Open Finance

Under open finance, consumers would be able to direct the transfer of their data from an FSP they do business with (i.e., the "data holder"—an entity that holds or possess consumer data) to an FSP or TPP they would like to do business with (i.e., the "data user"—an entity that uses consumer data). Data transfers facilitate a variety of actions: opening and operating credit and debit cards; extending MSME credit; accessing suitable and appropriate personal loans; opening deposit, savings, and checking accounts; and other finance-related actions. Other TPPs, such as fintechs, can make use of existing data to offer more targeted and innovative services and products, such as financial advice, savings sweepers, and utility switching services.[8] In addition to bringing new provider entrants into the banking sphere, open finance would promote competition among existing banks and FSPs, ideally resulting in lower transaction costs and more value-added products and services.

Under an open finance regime, data is transferred from the data holder to the data user for the benefit of the consumer (the "data subject"). Transfers can be performed directly by the data holder. However, in some cases another entity (i.e., a data intermediary or a series of data intermediaries) handles consumer requests and ultimately makes transfers to data users. This gives the intermediary the responsibility of controlling or processing sensitive personal financial data. It is thus important that all parties (i.e., data holders, data users,

BOX 1. Open Finance Primer: Key Terms and Definitions

OPEN FINANCE

Open finance is the sharing of consumer data from banks and financial services providers (FSPs) with other FSPs and/or third-party providers (TPPs) such as fintechs, with the consent of the customer. Although payment initiation is often introduced in the same legislative framework as open finance, it is not essential to the functioning of open finance and therefore is not part of the definition.

OPEN DATA

Open data is the exchange of consumer data between private-sector institutions—including financial institutions and nonbank financial institutions such as mobile money issuers, utility providers, and telecoms—and other such institutions, with customer consent.

Although customer transaction data sharing is at the heart of our definition of open finance schemes, the majority of these schemes regulate access to three main types of data:

Generic services data. Publicly available information on specific financial services, such as product pricing and locations of ATMs, agents, and branches. Generic services data is not personally identifiable data.

Customer data. Customer data is a customer's personally identifiable data required for account opening and administrative purposes, including registration/know your customer (KYC) data.

Transaction data. A customer's personally identifiable transaction data includes balances, purchase amounts and dates, and transaction counterparty identity.

Source: Adapted from Plaitakis and Staschen 2020.

8 A savings sweeper is a tool that calculates savings potential, then transfers funds to a savings account if that is found to be beneficial to the consumer.

and data intermediaries) protect the data they handle so it is securely transmitted and only used for legally and contractually permissible purposes.

The nature of the intermediaries that handle data in open finance jurisdictions can vary. For instance, India created the account aggregator (AA) category for entities whose role is to act as a trusted and impartial intermediary. AAs serve as the pipes through which data flows. They also manage consumer consent. When a consumer consents to a transfer, the AA reaches out to the data holder and securely transmits data to the data user.[9] AAs are barred from seeing, storing, analyzing, or using customer data. AAs must be licensed to act as an intermediary and are regulated by India's central bank.[10]

By contrast, the revised European Union payments directive that regulates open finance—the Second Payment Services Directive (PSD2)—requires certain data holders (banks and payments institutions) to share certain data with specific data users based on the data subject's consent.[11] The data can be directly shared between a data holder (e.g., a bank) and a data user (e.g., another FSP). The data can also be shared with a TPP that acts as both data intermediary and data user on behalf of the data subject. PSD2 also introduced two types of TPPs: account information service providers (AISPs) that use data to provide customers with an aggregated view of their accounts and offer recommendations on new services[12] and payment initiation service providers (PISPs) that initiate payments on behalf of consumers.[13] AISPs only have permission to "read" accessed data and are only required to register with the authority. AISPs under PSD2 can actively provide financial advice, monitor spending, compile information for a consumer's credit application, and provide a dashboard with an aggregate view of information from multiple accounts.[14] Thus, AISPs do not act as passive AA intermediaries. PISPs, on the other hand, have permission to "read" and "write" accessed data and transfer funds so they can initiate payment transactions. But PISPs must operate with regulatory authorization.[15]

Australia takes a similar approach to intermediaries. Pursuant to its open finance law, Australia published guidelines for accrediting TPPs that can receive and use customer data from data holders,[16] as well as rules for accredited intermediaries that can receive and transmit customer data to accredited individuals.[17]

Data Protection Can Develop Consumer Confidence in Open Finance

Faith Reynolds, the former Independent Consumer Representative of the U.K. Open Banking Implementation Entity, notes that "[s]haring data may allow new convenient and personalised services, but it comes at a cost to data privacy and control over how that data is used. It may give rise to new feelings of disempowerment as complex chains of providers sharing data and offering various parts of a service reduce transparency and clarity about liability."[18] Importantly, Reynolds observes that "consumer experts acknowledge that as people confront those complexities, it's possible

9 Datwani and Raman 2020.

10 Reserve Bank of India 2016b.

11 PSD2 2015, Article 67.

12 Ibid, Articles 4(16) and 33.

13 Ibid, Article 4(18).

14 Ibid, Articles 4(16) and (19).

15 It is important to note that "write access" means a TPP can change the base data it has access to. It follows that any errors or mishaps concerning the data a TPP has write access to are more significant than errors relating to data it only has "read access" to. It is therefore not surprising that data and consumer protection provisions concerning such data are much more restrictive. For example, PSD2 stipulates that certain forms of payment initiation require three-factor authentication. Payment initiation, however, is out of the scope of this Technical Note and thus these data and consumer protection provisions have not been addressed.

16 Australian Competition & Consumer Commission 2022. See Australia Competition and Consumer Act 2010.

17 Australian Competition & Consumer Commission 2020.

18 Reynolds 2017, p. 19.

that they will stick with what they know and trust. Complexity may undermine the ability of Open Banking to really disrupt the market."[19]

Addressing data protection is critical to the adoption of open finance, particularly for low-income and excluded people in EMDEs. While expanded data flows will benefit all consumers, they must be accompanied by a data protection framework. A data protection framework establishes basic rules regarding who can do what with customer data and under what circumstances. It includes the rights and obligations of the parties involved and remedies in cases of failure. In the absence of such a framework, data behavior is either regulated by private contract or data protection is left unregulated. When left to private contract, consumers are vulnerable as they are typically the weaker party. When unregulated, consumers are exposed to the risk of abuse, fraud, and exploitation. According to the Basel Committee on Banking Supervision, "[d]ata privacy laws can provide a foundation for an open banking framework."[20]

A data protection framework is also key to promoting customer trust, which in turn promotes consumer uptake and responds to customer privacy preferences. Such preferences are particularly important for poor customers in EMDEs. CGAP's work on data protection has focused on how data protection can benefit low-income people.[21] It concludes that the consumer consent model for data privacy and protection is broken and it is time for a new data paradigm whereby FSPs and data collectors take greater responsibility for protecting customer data.[22] More recently, CGAP conducted behavioral research in India and Kenya to test the extent to which poor consumers care about financial privacy. The research demonstrated that poor consumers care deeply about the privacy of their financial information and are willing to pay a premium for financial products that protect their data—even during a pandemic.[23] If open finance succeeds, with the proper protections in place it can pave the way for broader exchanges of data in nonfinancial sectors of the economy (i.e., open data) and provide even more consumer benefits. However, if data is not protected, consumers could easily lose trust and confidence in open finance and even their existing banking relationships.

Open Finance vs Data Protection Entities

As Box 2 notes, "data subjects," "data holders," "data intermediaries," and "data users" are the primary entities in open finance, although certain jurisdictions use different names for these functions. A data subject is the person identified in the data, although sometimes this designation is complicated (e.g., a joint account involving more than one person's data). Data holders are institutions that originally stored the data and are responsible for sending it to an accredited data intermediary and/or data user at the consumer's request.[24] Data intermediaries and data users, which must be accredited in some jurisdictions, can receive and use consumer data.[25] Data holders and data users could jointly establish data transfer systems which, under certain circumstances, would make them jointly responsible for how those systems operate.[26]

Contrary to open finance where key entities are largely defined by the role they play in the transfer of data, key entities in data protection laws and regulations are defined with a focus on their ability to make decisions about data processing. For example, they include "data controllers" under GDPR (the European Union's data

19 Ibid, p. 22.

20 Basel Committee on Banking Supervision 2019.

21 CGAP 2022.

22 Medine and Murthy 2020.

23 Fernandez Vidal and Medine 2019; Fernandez Vidal 2020.

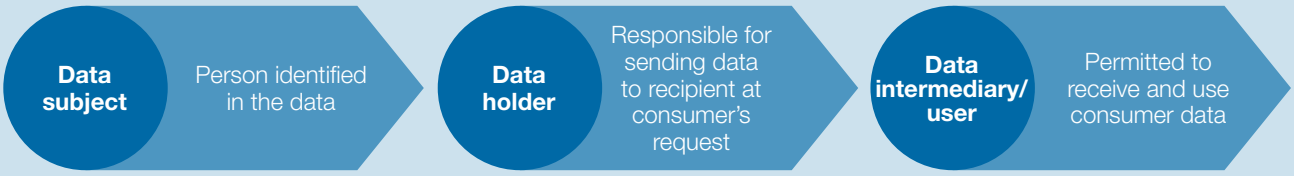
24 OAIC, CDR Participants; Australia Competition and Consumer (Consumer Data Right) Rules 2020.

25 A common characteristic of open finance regimes. One example is Australia's rules for accreditation, OAIC 2022. As previously noted, AAs in India may only transmit data.

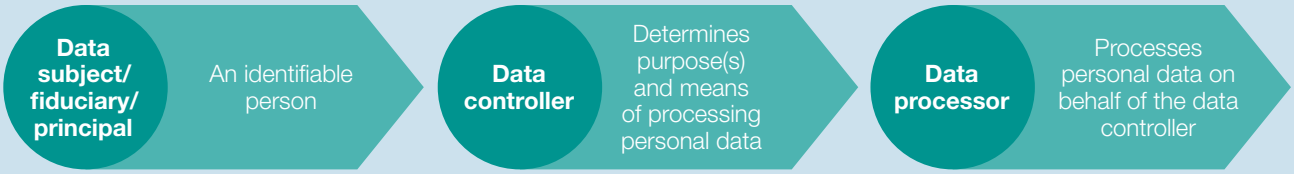
26 GDPR 2016, Article 26.

BOX 2. Similarities between Key Terms for Open Finance and Data Protection

Open finance



Data protection



protection law)[27] and "data fiduciaries" under the draft India Digital Personal Data Protection Bill.[28] Such laws also apply to entities that process data ("data processors") on behalf of firms that make processing decisions.[29] Under these laws, consumers may be referred to as "data subjects" or "data principals."[30]

In the context of open finance, both data holders and data users are likely to be considered data controllers/ fiduciaries. Under laws modeled on GDPR, entities such as AAs in India that transmit but are not permitted to access data are more likely to be considered data processors.[31] Under these GDPR-type laws, it is the duty of data controllers (in the open finance context, data holders and users) to only use processors that sufficiently guarantee they will implement the necessary measures to ensure data is protected.[32] The processor is typically bound by contract to adhere to GDPR requirements. The responsibility to oversee such data in the hands of unrelated parties may fall on the national data protection authority[33] or other government agencies with the appropriate jurisdiction.

Terms used in open finance frameworks and data protection regulations (e.g., data user, data processor) do not necessarily overlap. In some cases, a data user may

27 GDPR 2016, Article 4(7). Under GDPR, processing is broadly defined to include "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."

28 Draft India Digital Personal Data Protection Bill, 2022, Section 2(5). See also India Personal Data Protection Bill 2019, Section 3(13); India Report of the Joint Committee on the Personal Data Protection Bill, 2019. On August 3, 2022, the Indian government withdrew the Personal Data Protection Bill from legislative consideration with an indication that a revised bill would be reintroduced in the future. See also Economic Times 2022. On November 18, 2022, the Indian Ministry of Electronics and Information Technology (MeiTY) published a draft Digital Personal Data Protection Bill, 2022, and Explanatory Note for public comment.

29 GDPR 2016, Article 4(8); Draft India Digital Personal Data Protection Bill 2022, Section 2(7); India Report of the Joint Committee on the Personal Data Protection Bill, 2019, Section 3(17).

30 GDPR 2016, Article 4(1); Draft India Digital Personal Data Protection Bill 2022, Section 2(6); India Report of the Joint Committee on the Personal Data Protection Bill, 2019, Section 3(16).

31 Reserve Bank of India 2016b: Section 45-IA of the Reserve Bank of India Act, 1934.

32 GDPR 2016, Article 28(1).

33 Basel Committee on Banking Supervision 2019, p. 11.

follow another entity's directions and is therefore a data processor under data protection law. In other cases, the data user may have authority, through the consumer's consent, to make decisions about how the data should be used, thus making that entity the data controller. In each case it is necessary to conduct both an open finance and a data protection legal analysis to determine an entity's status and obligations.[34]

Impact of Gender on the Use of Open Finance

Open finance poses both challenges and opportunities for women. Historically, women have been excluded from the formal financial system for various reasons. These include partial or complete lack of literacy, insufficient access to technology, distrust in the formal financial system, and limited time on their part. As a result, women often have less financial data that can be accessed or leveraged through open finance tools. This suggests they may be less likely to benefit from the opportunities open finance has to offer. However, open finance has the potential to provide women with opportunities that do not currently exist. For instance, while some women may have transaction data that can provide access to valuable financial tools and advice, it currently is not collected from data holders nor transmitted to data users. Open finance would require firms holding such data to transmit it upon request, thus providing women with the financial history they need to enter the formal financial system. A woman's right to data access is also a valuable tool for identifying potentially discriminatory data user behaviors such as credit denial. Movement from open finance to open data will expand the set of data sources that include women's information and thus bring more women into the fold.

It is also crucial to ensure that women are comfortable and willing to share their data. When determining whether to share data, there must be an assessment of whether the data will be protected and used for their benefit. Preliminary results from a study in India reveal "that women consider [certain types of data as] personal and would be less willing to share with financial service providers, such as information on savings, loans, government transfers that they receive and ATM pins," even if it were economically beneficial. The study's research manager concluded that "[s]ubstantially increasing the usage of financial services among women requires digital financial services providers to appreciate women's needs, coping mechanisms, and intrinsic privacy preferences."[35] Given the opportunities open finance and open data provide for women, further research on women's willingness to share personal financial data is an essential next step in encouraging their participation in open finance.

How Regulatory Frameworks Can Protect Customer Data

It is important to note that consumers' open finance data can be protected through different channels. A jurisdiction may have comprehensive data protection legislation in place that cuts across all sectors, such as the European Union's General Data Protection Regulation (GDPR).[36] Alternatively, data protection legislation or regulations such as the financial privacy law in the United States[37] may only target financial institutions. Specific open finance or open banking laws may also incorporate data protection provisions. A general open data law with financial sector-specific requirements is another option.[38] As discussed below, multiple laws may apply to aspects of open finance in some jurisdictions,

34 According to the European Data Protection Board 2020a, p. 8, "[d]epending on specific circumstances, payment service providers [under PSD2] could be a controller or processor under the GDPR."

35 Chugh 2022.

36 GDPR 2016.

37 See, for example, U.S. Congress, Gramm-Leach-Bliley Act.

38 See Australia Competition and Consumer Act 2010, Section 56EC, reconciling which aspects of the Privacy Act 1988 apply to open finance; Australia Competition and Consumer (Consumer Data Right) Rules 2020, Schedule 3, provisions relevant to the banking sector.

FIGURE 1. Different Legal Bases for Open Finance and Data Protection

General data protection (DP) law that applies to open finance:

Pro: Level playing field for market participants
Con: Provisions do not take into account specific issues raised by open finance

Open finance (OF) law that covers data protection issues:

Pro: Tailored to open finance context
Con: Potential lack of level playing field for entities that may compete but not be covered by open finance law

General data protection law and **separate open finance law:**

Pro: Have laws that require data sharing as well as data protections
Con: May have conflicting definitions and provisions as the two laws were not designed to work together

***Additional option:** An open data law that has open finance-specific provisions to address the flow of financial data

leaving uncertainty as to which law governs and where laws overlap or create conflict. Figure 1 illustrates some of the different legal options for open finance and data protection (DP). It also lists pros and cons and shows the interplay between different types of laws.

When regulators adopt open finance, they need to decide whether their current data protection laws sufficiently protect consumers from the data risks of open finance—regardless of whether these data protection provisions are contained in comprehensive legislation or are simply found in sector-specific legislation. In specific cases, a jurisdiction may decide to adopt both open finance and data protection laws to cover data protection issues because a data protection law without accompanying financial sector-specific regulations is sometimes insufficient.[39] For example, Kenya's Central Bank concluded that "[e]ven with the enactment of the Data Protection Act, 2019, it is likely unauthorized use of a customer's data in digital payments is undermining trust unless strong safeguards and financial sector data protection regulations are developed and enforced."[40] The Central Bank also stated in its National Payment Strategy that it would seek to see the emergence of a comprehensive data protection framework that is tailored for digital payments and in line with its payments mandate.[41]

As Section II discusses in greater detail, each country needs to assess how best to protect open finance consumer data, considering its existing legal structure and willingness to adopt new laws. A one-size-fits-all approach does not exist as the design of new legislation depends on each country's existing data protection rules and its approach to open finance. In addition, these types of laws may be implemented by regulations issued by bodies such as a central bank, a data protection authority, or other regulators such as a competition authority. Another consideration is whether the data

39 See Central Bank of Kenya 2020, p. 27.
40 Central Bank of Kenya 2022, p. 51.
41 Ibid.

protections put in place should vary depending on the data's use, for example, loans vs financial advice vs know your customer (KYC) onboarding.[42]

To enhance consumer trust and confidence in the absence of laws and regulations, open finance participants can volunteer to mutually agree to industry standards or enter into contractual data protection provisions. For example, the worldwide mobile industry trade association, GSMA, established a mobile money certification program that includes a data protection component. It is designed to "enhance trust with local regulators, attract commercial business partners and merchants, encourage other financial institutions to integrate, and assure customers that their rights are protected."[43] Depending on the structure of similar efforts, as a practical matter they can become as standardized and enforceable as national laws and regulations.[44]

Timing for Introducing Data Protection Regulation

In the context of open finance, it is essential that comprehensive data protection laws and regulations are in place. However, identifying the right time to introduce them is important since open finance is relatively new and evidence on how it works at scale is limited. The premature application of data protection regulation on open finance providers can pose risks, given the impact of regulation on cost, competition, and innovation. Thus, the impact of regulation should be carefully considered prior to its implementation. For instance, a potentially negative consequence of regulation is that only larger FSPs can afford to comply and smaller entrants are shut out—the very entities open finance was designed to encourage. Compliance exemptions for smaller entities may be a possible solution. There is also the risk that large players become disincentivized from serving the lower end of the market since compliance costs bear more heavily on low-value accounts and transactions. Risk may be mitigated with digital transactions because the marginal cost of serving each low-income customer, including compliance obligations, could be minimal. Despite the risks of prematurely introducing regulation, incorporating data protection is integral to the long-term success of open finance as it will help allay consumer concerns about the collection, use, and disclosure of sensitive financial data.

Who Should Regulate Data Protection?

Designing a regulatory approach for open finance is complex. In so doing, it is important to take into account both the complexity of jurisdictional mandates and the burden that would be placed on resource-limited regulators in EMDEs. A country's enforcement and regulatory regime[45] determines who is responsible for promulgating regulations and promoting compliance related to data protection. The responsibility lies with one or more of the following: the data protection authority or information commissioner,[46] a consumer protection agency,[47] standard setting bodies,[48] or a financial regulator. In some cases it may be unclear which entity is responsible; in others, authorities could have concurrent jurisdiction. Thus, it is important to identify jurisdictional mandates for data protection and open finance. If concurrent jurisdiction exists, an agreement between the authorities should be established. Further, to ease the burden of developing and enforcing a new regulatory scheme and responding to consumer

42 To prevent money laundering, KYC onboarding requires FSPs to identify clients and verify their identity (Watts, Medine, and De Koker 2018).

43 See the GSMA Mobile Money Certification: https://www.gsma.com/mobilefordevelopment/mobile-money/certification/.

44 Self-regulatory organizations could work to convince governments to establish safe harbors for firms that voluntarily comply with these standards. Adherence would lower compliance risk for companies that choose to participate in the safe harbor.

45 PSD2 2015, Article 22(1), "Member States shall designate as the competent authorities responsible for the authorisation and prudential supervision of payment institutions"; Article 23, supervisory functions; Article 25, judicial review of authority decisions.

46 See, for example, Australia Treasury Laws Amendment (Consumer Data Right) Act 2019, Section 56EQ(1).

47 Ibid, Section 56EZ.

48 In Australia, CSIRO Data61 2022.

complaints, regulators can consider leveraging technology such as regulatory technology (regtech: the application of information technology to enhance regulatory and compliance processes) and supervisory technology (suptech: the use of technology for regulatory, supervisory, and oversight purposes). Considering a country's legal and technological environment, regulators may also decide to phase in data protections over time. Bhaskar Chakravorti, Dean of Global Business at the Fletcher School at Tufts University, noted "data…is just plain complicated."[49] His observation succinctly captures the complexity of data—an asset that needs a set of regulations that address this complexity to ensure customer privacy and protection.

Which Open Finance Data Is Out of Scope for Data Protection?

Open finance regimes often go beyond the personally identifiable data protected by data protection laws. They also cover aggregated[50] or de-identified data that is not reasonably identifiable after aggregation or de-identification. Examples include sharing aggregated data as required under the Mexican Fintech Law and sharing publicly available nonpersonal information about specific financial services, including product pricing and locations of ATMs, agents, and branches.[51] In the context of open finance, there is no need to address data protections for this type of data if it is not, in fact, personally identifiable. Similarly, when open finance data users no longer need certain personally identifiable information, procedures should be in place to de-identify, delete, or destroy and thus remove it from the scope of data protection legislation.[52] In some cases, a government agency such as a data standards office can establish standards to ensure that data is sufficiently de-identified.[53]

49 Chakravorti 2020.

50 See Comision Nacional Bancaria y de Valores 2021.

51 Open banking regimes in Brazil, Hong Kong, India, Malaysia, Mexico, Singapore, and the United Kingdom address sharing of generic product data.

52 Australia Competition and Consumer (Consumer Data Right) Rules 2020, Section 1.17.

53 See, for example, Australia Treasury Laws Amendment (Consumer Data Right) Act 2019, Section 56FA(1)(d).

SECTION II

BASIC DATA PROTECTIONS TO SUPPORT INCLUSIVE OPEN FINANCE

IF WIDELY ADOPTED, OPEN FINANCE will facilitate an unprecedented flow of data and thus improve and expand financial services delivery. In many countries, consumers who currently wish to use an app to aggregate financial information must authorize the app to access their accounts and engage in screen scraping[54]—despite the high risk of sharing account credentials. In an open finance regime, the use of more secure APIs ideally will dramatically increase the flow of data and address the security and technical challenges posed by screen scraping.

As Section I discussed, data protection, including data security, will play a fundamental role in the widespread adoption of open finance. Incorporating data protection into the complex open finance ecosystem will be a challenge. This section explores some of the data protection measures legislators and regulators have adopted.

Broadly speaking, consumers are concerned about three areas of data protection in relation to open finance, each of which is discussed below. The first area is control over who has access to their data and how it is used—even if they do not always exercise that control.[55] The two key components of consumer control include providing consumers with privacy notices and obtaining consumer consent. Second, rather than placing the burden on consumers, the law should require open finance ecosystem participants to use consumer data responsibly—ideally in the consumer's best interest. Responsible use can include data use restrictions, controls on cross-border data transfers, data localization, and permissible data usage. Third and finally, security is critical during data storage and transfer since financial data is often viewed as highly sensitive and prone to misuse in the wrong hands. Compromised data or a data breach can cause consumers to lose confidence in open finance. Thus, open finance regimes should incorporate the following data protection provisions if they are not already provided for in national legislation or sectoral regulation.

Consumer Control Over Data

This section examines different ways consumers can be given control over their data in an open finance environment. Specifically, it focuses on the role played by providing consumers with privacy notices and obtaining their consent. While some measures only cover the bare minimum any legal framework should provide, other provisions are more comprehensive and benefit

54 Screen scraping entails using a computer program to copy data from a website.

55 Grady, Montes, and Traversa 2018, p. 4.

the consumer. In the absence of data security, consumer data would be vulnerable to misuse, which could cause considerable harm to lower income consumers. The section concludes with a discussion of the critical role data security plays.[56]

NOTICE

A key data protection provision in any open finance framework relates to providing consumers with privacy notices. It is essential to educate potential consumers about when they are authorizing third parties to make payments from their accounts as opposed to authorizing access to account data. Notice is particularly important in open finance as consumer control starts with transparency and information, in other words, consumers knowing what is done with their data. The open banking pioneer Faith Reynolds astutely observes that "people already struggle to understand what data they are creating as part of daily life, let alone who owns it or how it's being used by digital companies."[57] Notices generally explain which data transfers consumers are authorizing and often serve as the basis for providing informed consent. Because open finance is a complex and novel concept to many, it is challenging to use notice as the basis for consent. The problem is exacerbated when a variety of data types are shared (e.g., data relating to loans, money transfers, remittances, payment cards) and potentially granular choices need to be made about which data fields to share (e.g., balances, payments history, transactions) with which recipients, how often, and for how long.

The Australian Data Standards Body, charged with developing open finance standards, has general recommendations related to notice. Its holistic set of recommendations serve as a guide for drafting privacy notices, as follows:

1. Avoid vague descriptions of data use.
2. Justify requests for data.
3. Indicate the time and effort required to provide consent.
4. Ensure language is written from a consumer perspective.
5. Make language clear, understandable, and accessible.
6. Give consumers a record of their data sharing agreement.
7. Educate consumers on how data can be used.[58]

Privacy notices should generally address consumer interest in a comprehensible open finance process[59] by informing them of:

1. Types of data held
2. How it is held
3. Purposes for which it is being held, used, or disclosed
4. Role of consent
5. Consumer access and correction rights
6. How complaints may be made about noncompliance with applicable data protection rules
7. Whether data will be sent out of the country
8. Types of recipients that will receive data, and, in the case of third-party service providers, potentially their data handling/privacy policies[60]
9. Deletion rights.[61]

When an intermediary only handles data transfers, it is helpful to give consumers an explanation of how the entity handles data disclosure, its accuracy, transfer security, and other data protections.[62]

56 Before open finance, customer information was typically accessed on a case-by-case basis. With open finance, as with data portability under GDPR, "an individual's lifetime of data with a service can be downloaded all at once," making security measures all the more important (Swire and Lagos 2013).

57 Reynolds 2017, p. 18.

58 Data61 2019a. See also Banco Central do Brasil 2020, Articles 10(1) and (2).

59 Consumer Policy Research Centre 2020.

60 See also Central Bank of Nigeria 2022, Section 11.1.1(b).

61 See, for example, Australia Treasury Laws Amendment (Consumer Data Right) Act 2019, Section 56ED(5). Additional disclosures are required under Australia's implementing regulations, including a statement of the consequences of the consumer withdrawing consent and information about de-identification. See Australia Competition and Consumer (Consumer Data Right) Rules 2020, Section 7.2 and GDPR 2016, Article 13.

62 See, for example, Australia Treasury Laws Amendment (Consumer Data Right) Act 2019, Section 56ED(6) and Australia Competition and Consumer (Consumer Data Right) Rules 2020, Section 4.11 (extensive disclosures).

Australia's consumer data standards program recommends that data users make the following consumer disclosures:

1. Why each data cluster is required[63] and how far back in time data will be accessed
2. How each data cluster will be used, including if inferences will be made, applications will be influenced, or if CDR (consumer data rights) data will influence how services/products are priced or provided
3. How data will be handled during and following the consent period, including who will access the data; that data will not be used for unrelated marketing purposes; and that outsourced providers will be bound by consent agreements
4. How data will be stored, including after revocation/expiry of consent
5. What will happen to CDR data following revocation/expiry, including redundant data
6. Any other use during or following the consent period.[64]

Notice can be challenging in countries where multiple languages are spoken and where consumers receive notices on devices that make it difficult to read, review, and save them. To be meaningful to consumers, open finance notices should be written in language that is easily understood. Legal language should be avoided. Moreover, limited levels of literacy—common among low-income people in EMDEs, particularly women and those with disabilities—can make it challenging for some consumers to review notices. Although literacy limitations are not widely prevalent in Australia, the Australian Consumer Policy Research Centre noted that:

> A key threat for inclusion and accessibility in the CDR ecosystem is the risk of creating two-tiered markets across the board. [W]ithout deliberate approaches or incentives to create inclusive access, consumers who are batting [sic] digital exclusion (often in combination with other vulnerabilities) may be excluded from obtaining benefits of CDR, while those who are digitally skilled and digitally connected have better access to new consumer products and services that might improve wellbeing but remain out of reach for consumers with less access to digital markets.[65]

Notices may also be broad in scope, which can result in situations customers do not expect, especially if they include a long list of permissible uses customers technically consented to. Consumers wishing to take advantage of an open finance data transfer may later find that they authorized use of their information for purposes unrelated to their transfer request as they did not carefully read the privacy notice they received. There is also the risk that lenders take unfair advantage of consumers by using shared financial data to offer services, such as unfavorable loan terms that they know the consumer is in a position to repay.[66] As McKinsey observed, "There is a fine line to walk: educating and empowering consumers without confusing, scaring, or boring them."[67]

Consumers should not be required to parse privacy notices to determine whether hidden data use authorizations lurk within them. Rather, legal protections against secondary or potentially unfair uses of data should be put in place. One option for preventing abuse is to limit use to the specified purpose (e.g., the requested goods and services of the data transfer and not any secondary uses[68]) or, as GDPR provides, to prohibit processing that is incompatible with the purposes for which information was collected.[69] The downside of limiting the use of data in a privacy notice could be that it inhibits providers from developing and promoting new innovative services whose terms may not have been disclosed in earlier privacy notices. This will pose a challenge to regulators that

63 The term "data cluster" is used to refer to a grouping of data under Australian consumer data rights (Australia Consumer Data Standards Glossary 2022) and with open banking in the United Kingdom (U.K. Open Banking Standard 2022b).

64 Data61 2019b, p. 42.

65 Consumer Policy Research Centre 2020, p. 32.

66 Reynolds 2017, p. 21.

67 Brodsky and Oakes 2017.

68 See Medine and Murthy 2020.

69 GDPR 2016, Article 5(1)(b); Brazilian General Data Protection Law (LGPD) 2018; PSD2 2015, Article 66(3)(g): Data may not be used, accessed or stored "for purposes other than for the provision of the payment initiation service as explicitly requested by the payer" and Article 67(2)(f).

wish to promote beneficial new services yet still impose reasonable use restrictions. Thus, two key questions are raised: how should data that was collected prior to open finance be handled and how should the possibility of new but unspecified future uses of open finance data be communicated in notices?[70]

Although many, if not most, consumers do not read privacy notices and often skip disclosures, notices play an important role in an open finance environment. They should be required[71] of parties that handle data, including data holders, entities that transfer data, and data users as they provide the basis for holding those parties accountable to the data protection standards they adopt.[72]

In the context of notice, it is important for consumers to understand how open finance works, to trust that their data will be handled responsibly by third parties, to understand how data flows through the system, and to be aware of redressal mechanisms. It follows that regulators should consider the following:

- In the early years of open finance, **offering general consumer education** on what open finance is, how it works, and how specific consumer data transfer requests are handled.
- **Providing consumers with clear information** on who receives their data and how it is protected is essential. CGAP research showed that consumers are particularly concerned about disclosure of their data to third parties.[73] Thus, alleviating these concerns is key to encouraging the adoption of open finance.
- Assurance that any information presented to consumers includes an **explanation of the journey customer data takes through the open finance system** and that this information is easy to understand.[74] Flow charts or other graphics in addition to the use of text can be beneficial. A rating service for data protection can also be offered.[75]
- **Ensuring that consumers are aware of available redress mechanisms** since they might be hesitant to use digital services if they do not feel empowered to fully exercise their rights.

A final element in relation to notice would include regulators advocating for real-time notifications to consumers on the movement of data—in part to verify that transmission was authorized.[76]

CONSENT

Even after providing consumers with notice, obtaining their consent is a critical but challenging next step in an open finance environment.[77] It is critical because consumers should and often want to control whether and when their data is shared, with whom, and for what purposes. Transfer of sensitive financial information is prone to misuse if sent to an unauthorized third party. While consent should be required to authorize data transfer,[78] obtaining informed consent continues to present numerous challenges.[79] Consumers experience "consent fatigue" due to the many daily interactions that call for consent—from mobile device apps to websites to internet of things (IoT) devices. Even if consumers want to make informed consent decisions, privacy notices are typically lengthy documents written in complex legal language that often grant providers broad use of data and only provide consumers with a take-it-or-leave-it choice. As the European Data Protection Board noted, "If

70 See Popoola and Oturu 2021.

71 See, for example, Australia Treasury Laws Amendment (Consumer Data Right) Act 2019, Section 56ED(3), maintenance of privacy policy required.

72 Susser 2019.

73 Fernandez Vidal and Medine 2019.

74 See also Central Bank of Nigeria 2022.

75 A private-sector example of a rating system is the Rating Assurance and Certification offered by Dataswift. See: https://docs.dataswift.io/deploy/rating-assurance-and-certification.

76 See, for example, Australia Treasury Laws Amendment (Consumer Data Right) Act 2019, Sections 56EH and 56EM(1). See also Central Bank of Nigeria 2022, Section 8.8.2.

77 Miller, Sullivan, and Montes 2021, p. 10.

78 See, for example, Australia Competition and Consumer (Consumer Data Right) Rules 2020, Section 4.3; GDPR 2016, Article 6(1)(a); PSD2 2015, Article 67: "explicit consent" required. See also FIGI 2022, pp. 21–22.

79 See Medine and Murthy 2020.

obtained in full compliance with the GDPR, consent is a tool that gives data subjects control over whether or not personal data concerning them will be processed. If not, the data subject's control becomes illusory and consent will be an invalid legal basis for processing, rendering the processing activity unlawful."[80]

Following are some of the issues to consider when evaluating consent in the context of open finance. First, data protection laws typically define consent, often in similar ways in different jurisdictions. Laws such as GDPR,[81] Brazil's General Data Protection Law,[82] and Australia's Privacy Principles[83] have adopted definitions which state that consent must generally be freely and voluntarily given, unambiguous, express, informed, specific, and easily withdrawn. In the context of open finance law, Australia's CDR Rules[84] provide a similar definition of consent, as do Brazil's open banking regulations.[85]

In the open finance context, certain steps can enhance the likelihood of obtaining meaningful consent. Research by CGAP, Dalberg, and the Future of Finance Dvara Initiative revealed that many people who cannot read or write prefer more visual, verbal, or video forms of consent they can easily understand without relying on others.[86] Another option is to include a consent process that is separate from other parts of customer agreements (e.g., on a separate page or screen).[87] Under Brazil's open banking regulations, consent cannot be obtained based on a standard customer agreement or the use of a pre-filled form, and consent must be express—not implied.[88] In the account aggregator context, India has begun to employ an alternative approach to consent, the Data Empowerment Protection Architecture (DEPA), under which:

> The [data] subject needs to enroll with a consent manager (CM), and in so doing provides a list of approved data providers/controllers to the consent manager. When a data subject seeks service from a data user the data user initiates a data transfer request, which is submitted to the CM. The data user chooses a template from a suite of templates designed for this—specifying the purpose of the data transfer, the specific data that are needed to satisfy that purpose and the duration for which they will be retained—and picks the data request format that meets the requirements of the request. Only after the data subject has provided the consent for sharing data does the CM submit this request to the data providers. After verifying the request, the data provider transfers the data through an end-to-end encrypted flow to the consent manager, who shares the data with the data user.[89]

In conjunction with consent managers, nonprofit trusted intermediaries or privacy representatives could help consumers navigate a complex, digitally driven world. Intermediaries could take the form of an app that provides guidance on privacy settings, provides warnings about firms with unsafe privacy practices, and helps guide the

80 European Data Protection Board, 2020b, p. 13. See also Miller, Sullivan, and Montes 2021.

81 Under GDPR 2016, Article 4(11), consent "means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."

82 Under the Brazilian General Data Protection Law 2018, Article 5(XII), consent is the "free, informed and unambiguous manifestation whereby the data subject agrees to her/his processing of personal data for a given purpose."

83 Australia's Privacy Principles guidelines, Section B.35, states that "the four key elements of consent are: the individual is adequately informed before giving consent, the individual gives consent voluntarily, the consent is current and specific, and the individual has the capacity to understand and communicate their consent." For a fuller discussion of consent in Australia, see Australian Privacy Principles 2019.

84 See, for example, Australia Competition and Consumer (Consumer Data Right) Rules 2020, Section 4.9: Consent given by a CDR consumer to collect and use CDR data is a) voluntary, b) express, c) informed, d) specific as to purpose, e) time limited, and f) easily withdrawn.

85 Banco Central do Brasil 2020, Article 2 (VIII): "A free, informed, previous and unequivocal manifestation of will, made through electronic channels, by which a customer agrees to the sharing of data or services for specific purposes."

86 CGAP, Dalberg, and Dvara 2017.

87 See, for example, GDPR 2016, Article 7(2): "If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language."

88 Banco Central do Brasil 2020, Article 10(3).

89 Tiwari, Sharma, Shetty, and Packer 2022.

BOX 3. When Open Finance Consent Meets Data Protection Consent

Open finance may exist in a legal environment where both data protection and open finance laws or regulations are in effect. In some situations, it is not clear which law or regulation applies, especially since entities may be involved with payment instructions and information flows that are subject to both laws. This potentially presents compliance challenges. PSD2, the revised European Union payments directive that regulates open finance, notably requires "explicit consent" under certain circumstances but does not define the term.[a] As a result, a question arose about how the PSD2 requirement that "[p]ayment service providers shall only access, process and retain personal data necessary for the provision of their payment services, with the explicit consent of the payment service user"[b] relates to GDPR explicit consent requirements for use of sensitive data or profiling.[c] The European Data Protection Board concluded that explicit consent has different meanings under PSD2 and GDPR. The Board found that explicit consent means contractual consent under PSD2, noting that payment services are always provided on a contractual basis. Under this interpretation, contracts must make consumers aware of the purposes for which their data will be processed and consumers must explicitly agree to those contractual provisions. These clauses should be distinguishable from other portions of the contract. Therefore, consent under PSD2 is viewed as an "additional requirement of a contractual nature" and not the same as GDPR's explicit consent.[d]

This example offers a lesson on how it is helpful to harmonize obligations under data protection and open finance laws when possible. In this case, it was beneficial to have a governmental entity that could provide compliance guidance where the interplay between the two laws was unclear. In jurisdictions where such an entity does not exist, definitional discrepancies can pose a challenge.

a. PSD2 2015, Article 67(2)(a): Account information services may only be provided based on the user's explicit consent.

b. Ibid, Article 94(2).

c. GDPR 2016, Articles 9(2)(a) and 22(2)(c).

d. European Data Protection Board 2018. Reaffirmed in European Data Protection Board, 2020a, p. 15: "Explicit consent under the PSD2 is different from (explicit) consent under the GDPR."

deletion of information that no longer needs to be held by third parties.[90]

Consent mechanisms can be dictated by legal and/or regulatory requirements or in combination with voluntary technical standards, such as those found in the U.K. Open Banking Standard.[91] As the open finance approach expands to other sectors (e.g., open data), a common approach to consent provision may also benefit consumers. As customers become familiar with their options, they will no longer carry the burden of having to figure out each provider's approach to consent.[92]

To avoid an endless consent process and to keep the consumer engaged, consent may be limited to a number of factors such as a specific time frame (e.g., one year),[93]

90 See Medine and Murthy 2020.

91 U.K. Open Banking Standard 2022a.

92 Reynolds 2019: "Using the same construct for consent and authentication across sectors has several benefits, including the ability to create a coherent security, liability and redress regime for consent and data. The more familiar the consent journey for consumers, the easier it is to understand, engage with and build trust in. A fragmented protection regime with multiple consent journeys does not build trust and is likely to lead to consumer frustration."

93 See, for example, Banco Central do Brasil 2020, Article 10(1)(III): Compatible with the purposes for which it was given but limited to 12 months. A longer period of validity may be permissible when successive payment transactions are involved. Article 10(6). See also Central Bank of Nigeria 2022, Appendix 1: Consent must be time bound.

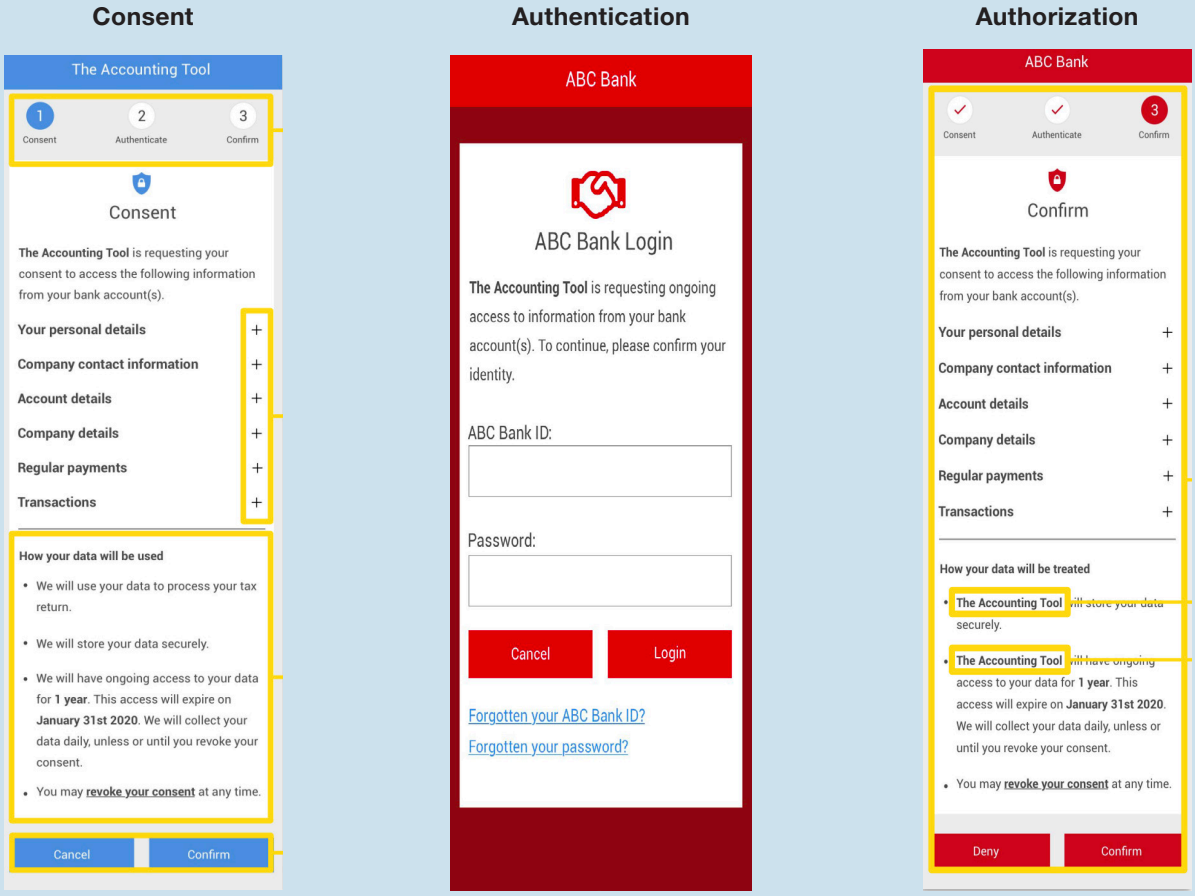
BOX 4. Granularity of Obtaining Consent

Open finance consumers may have banking relationships across multiple banks, as well as multiple accounts within a single bank (e.g., loans, payment services, credit cards) and relationships that span years or decades. When consumers consent to data transfers, they typically want to authorize not just the transfer of any and all information on file but instead specify:

1. Which account(s) to transfer from
2. Type of information to be transferred
3. Transaction time period(s) of information covered
4. Whether it is a one-time or recurring transfer.[a]

Capturing detailed consent potentially requires consumers to go through several smartphone screens and multiple options (see image below) to specify which information their request covers and how they wish to exercise control over the flow of their data.[b] There may be a variety of reasons for a data transfer request, such as for a credit application, comparing a competitor's financial products, tax preparation, or financial advisory services—all of which may need to be specified along with the data types required for each purpose. The process could be an even greater challenge for people in EMDEs with limited literacy or without a smartphone. It is important to strike the right balance between usability and protection as it will have implications on adoption.

Each step of the process may entail going through multiple screens, even with a smartphone.[c]



a. See, for example, Australia Competition and Consumer (Consumer Data Right) Rules 2020, Section 4.11. See also Central Bank of Nigeria 2022: When giving consent, consumers must provide the type of access, duration and tenor of the consent, frequency of access, and whether the consent applies to collection of anonymous and de-identified data analysis.

b. See, for example, Australia Consumer Data Standards 2019, pp. 8–13.

c. Data61 2019a, pp. 52–71.

loss of a TPP's authority to participate in open finance, or withdrawal of consent.[94] While consent time limits may serve a valuable purpose, they should not preclude offering services that require ongoing access to account information, such as monitoring accounts to alert consumers before they go into overdraft or are charged a late fee.[95]

It is important for consumers to have the ability to revoke consent at any time[96] and to have their request promptly take effect.[97] Unless easily performed, revocation is not a meaningful right. Consumers should be given the ability to use the same medium to revoke consent as they used to provide it. For example, if the consumer gave consent online, they should be able to revoke it online.[98] The Australian Data Standards Body recommends providing consumers with access to nondigital revocation channels as well. In a survey it conducted, many people would first use nondigital means of revocation, especially by phone and in person, because they felt that one-on-one and face-to-face interactions would lead to more accountability and request fulfillment.[99]

Consumers should also be informed of the consequences of revocation, including whether all previously shared data is erased or only future data transfers are discontinued. This could also mean that previously collected information may continue to be used if de-identified and no longer linked to a specific person.[100]

Under Brazil's open banking regulations, banks cannot suggest to customers who have consented to participate in open banking that they revoke their consent—except in cases of suspected fraud. This is possibly because banks that do not want customers to participate in open finance may encourage them to revoke information-sharing consent,[101] limiting the reach and benefits of open finance. The regulations also prohibit banks from setting up obstacles to data sharing, including asking consumers for additional authorizations or validating their consent, which would inhibit their customers' participation in open finance.[102]

Because financial information is considered sensitive data under some national data protection laws, heightened standards may be applied to open finance data, including explicit consent and a narrower set of permissible uses.[103] For instance, processing sensitive data is prohibited under GDPR unless it meets one of ten exceptions, such as where there is explicit consent or it is necessary to protect the vital interests of the data subject.[104]

94 See, for example, Australia Competition and Consumer (Consumer Data Right) Rules 2020, Sections 4.13 and 4.14. In such cases, the consumer should be given notice of the time period for expiration of consent.

95 Plaitakis and Staschen 2020, p. 9.

96 See GDPR 2016, Article 7(3); Banco Central do Brasil 2020, Article 15: Revoke any time through "secure, agile, precise, and convenient procedures."

97 Banco Central do Brasil 2020, Article 15(3): Revocation effective within one day for payment initiation and immediately otherwise.

98 See GDPR 2016, Article 7(3): "It shall be as easy to withdraw as to give consent"; Banco Central do Brasil 2020, Article 15(1): "Option for revoking consent through at least the same service channel by which it was granted, if said channel still exists."

99 Data61 2019a, p. 4.

100 Asrow 2022, p. 37.

101 Banco Central do Brasil 2020, Article 15(2).

102 Banco Central do Brasil 2020, Article 28; Miller, Sullivan, and Montes 2021, p. 22.

103 See, for example, the withdrawn India Personal Data Protection Bill 2019, Section 3(36)(i): "Personal data, which may, reveal, be related to, or constitute…financial data" is considered "'sensitive data'"; the draft India Digital Personal Data Protection Bill 2022 does not create categories of sensitive information. GDPR does not list financial data as being sensitive (GDPR 2016, Article 9[1]).

104 GDPR 2016, Article 9.

BOX 5. Consent Complications

Third-party data. Complications can occur when a third party's data is intermingled with the requesting consumer's data held by a data holder (e.g., joint accounts, authorized users, etc.). For example, the law may not give one accountholder the right to delete a joint accountholder's data.[a]

Silent party data. Silent party data is that which relates to a party that is not the customer of a data holder. For example, protecting the identity and data of the party receiving a check or money transfer from the customer can be a challenge. A data transfer would result in disclosure of the silent party's transactions to a third party, namely the data user and possibly a TPP. It is often not practical to obtain the silent party's consent. Nonetheless, the European Data Protection Board concluded that under GDPR, such transfers are permissible in the legitimate interest of the data holder or data user if transfers are necessary and proportional, as long as they do not interfere with the fundamental rights and freedoms of the silent party.[b]

Repeat consent requests. Complications may also occur when a TPP makes a data transfer request on a consumer's behalf or handles the actual transfer of data from a data holder to a data user. Such TPPs may repeatedly contact multiple financial entities on behalf of consumers. Even with a high volume of requests, it is important that the responsibility to comply with consent, security, and other open finance data protections be imposed on data-holding financial entities. To ensure that a transfer is properly authorized, in some cases the data holder may be required to obtain consent directly from the consumer before responding to TPP requests.

Multiple parties. Multiple parties are often involved in open finance transfers (e.g., the data holder, the data user, and a data intermediary). This raises the question of whose responsibility it is to obtain consumer consent.[c]

a. See, for example, Australia Treasury Laws Amendment (Consumer Data Right) Act 2019, Section 56BD(3).

b. GDPR 2016, Article 6(1)(f); European Data Protection Board 2018. See also European Data Protection Board 2020a, Section 4.2, p. 16. Note that PSD2 2015, Article 94, references existing EU data protection law requirements.

c. In India this task is assigned to intermediaries known as account aggregators. See Reserve Bank of India 2016b, Section 6.2: "Account Aggregator shall perform the function of obtaining, submitting and managing the customer's consent."

ACCESS, CORRECTION, AND DELETION

Consumers should have the right to access their own data to seek correction of inaccurate, incomplete, or untimely information—especially when their data is the basis for decisions on whether accounts can be opened or credit extended.[105] Depending on the circumstances, it may be necessary for either the data holder or the data user to conduct an inquiry into data accuracy based on a consumer's correction request.[106] It is in the consumer's interest that inquiries be conducted expeditiously (e.g., within 10 days).[107] A delay in response to a correction request can cause the consumer to be denied a loan or lose other financial opportunities. Once an inquiry is conducted, the data holder can either correct the disputed data or issue a statement that the data is accurate, up to

105 See, for example, Australia Treasury Laws Amendment (Consumer Data Right) Act 2019, Sections 56BC(1)(a) and 56ED(4); GDPR 2016, Articles 15 and 16. In addition, consumers may be given the opportunity to not be subject to automated decision making, such as through algorithms. Consumers may also have the right to have a person intervene in the decision so they can express their views and contest it. See, for example, GDPR 2016, Article 22; Brazilian General Data Protection Law 2018, Article 6(IV). Access may also be a useful tool to identify potentially discriminatory actions by financial institutions, Brazilian General Data Protection Law 2018, Article 6(IX), including, for instance, possibly differing treatment for men and women in making lending decisions.

106 See, for example, Australia Treasury Laws Amendment (Consumer Data Right) Act 2019, Sections 56EP(1) and (2).

107 See, for example, Australia Competition and Consumer (Consumer Data Right) Rules 2020, Section 7.15(b).

date, complete, and not misleading.[108] Once the inquiry is complete, the consumer should be notified of the outcome of their request.[109] If data is corrected, the corrected data should be sent to former data users to the extent reasonably possible[110] so the consumer no longer suffers from past inaccuracies.[111] Precedent for this approach can be found under some credit reporting laws.[112]

If consumers no longer wish to have their information held by a data user, they should be able to request that it be deleted.[113] TPPs or data users holding the data should act promptly to delete it.[114] However, this right may be limited in cases where data users are required by law to retain data, such as in the context of tax and accounting rules, court orders, or when data users are the subject of legal proceedings.[115] When deletion requests can be honored, data holders should be required to securely dispose of or de-identify data where possible.

In practice, it may be difficult to give consumers the ability to exercise these data rights. One option is to require that all financial institutions and entities acting as TPPs provide online dashboards so consumers can manage their requests in a timely manner, track disclosures, delete redundant data, and provide/withdraw consent.[116] Taking into consideration the limited IT capacity of some smaller entities in EMDEs, it may be more realistic to require financial institutions above a certain size threshold to provide dashboards and those below it to voluntarily do so.

Another open banking option the U.K. Financial Conduct Authority has considered is the provision of a single consent portal for each consumer. The portal would log every company the consumer has shared data with and allow the consumer to recall data they no longer want to share. Portals could "facilitate firms in differentiating in terms of privacy, by enabling consumers to see more clearly the implications of differing privacy policies."[117]

108 Ibid, Section 7.15(b)(ii).

109 Ibid, Section 7.15(c).

110 See, for example, GDPR 2016, Article 19.

111 See, for example, Australia Treasury Laws Amendment (Consumer Data Right) Act 2019, Section 56EN(4); GDPR 2016, Article 5(1)(d): Data is to be "kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay"; Brazilian General Data Protection Law 2018, Article 6(V).

112 U.S. Federal Reserve Board 2022, p. 4.

113 See, for example, Australia Competition and Consumer Act 2010, Section 56BAA(1): "Delete all or part of the CDR data in response to a valid request by a CDR consumer for the CDR data to be deleted"; GDPR 2016, Article 17(1): "Data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay."

114 See, for example, GDPR 2016, Article 17(1).

115 See, for example, Australia Competition and Consumer Act 2010, Section 56BAA(2).

116 See, for example, Australia Competition and Consumer (Consumer Data Right) Rules 2020, Sections 1.14 and 7.9. See also Banco Central do Brasil 2020, Article 23: Required standardized interface for sharing.

117 Open Finance Working Group on Incentives 2019.

BOX 6. Data Portability

Data portability, as defined by the GDPR, is the right of consumers to obtain their data from data controllers (data holders) in a structured, commonly used, machine-readable format.[a] It includes the express right to have data directly transmitted from one controller (data holder) to another (data user).[b] A small test of portability took place in the European Union just as GDPR went into effect. The results were discouraging, with only approximately 75 percent of requests successfully completed and financial entities experiencing a number of technical challenges.[c] Some countries have recently included data portability provisions in proposed[d] or existing data protection laws.[e]

While data portability is broader in scope than open finance in terms of types of data that can be transferred, the right to portability could provide many of the same benefits to consumers in countries without open finance laws. Additionally, broad portability provisions could allow countries with open finance laws to move from open finance to open data without the need for additional legislation. However, portability laws typically do not provide the same granularity on control features as open finance regimes. As a result, many of the provisions discussed here may be unavailable to consumers in jurisdictions with portability laws but without open finance. For example, consumers may not be able to specify details about which data should be transferred, for what purposes, and over what duration; they may lack the ability to revoke consent; measures to ensure secure and timely data transmission may be missing, and proper authentication of consumers and data users may not be required.[f] Thus, a portability right may not be enough to bring about desired data flows in the way open finance can. The advantage of an open finance regime is the organization and standardization of the data transfer process so the customer does not need to deal with the varying procedures required by each data holder and data user for portability.

a. GDPR 2016, Article 20(1).

b. A number of countries have recently included data portability provisions in proposed or adopted data protection laws. See, for example, GDPR 2016, Article 20(2).

c. Wong and Henderson 2019. See also Kuebler-Wachendorff, Luzsa, Kranz, et al. 2021. Three years after GDPR took effect, the authors found the portability right was little known and only implemented in a fragmented manner.

d. Between November 17, 2020, and January 17, 2021, sections 72 and 120 of Canada's proposed Digital Charter Implementation Act, 2020 Bill C-11, underwent public consultation (Canada House of Commons 2020). On June 16, 2022, the Digital Charter Implementation Act 2022 Bill C-27, was given a first reading with identical provisions on data portability (Sections 72 and 123) (Canada House of Commons 2022). See Olijnyk 2022.

e. The Singapore Parliament passed amendments to its Personal Data Protection Act 2012 (PDPA) on November 2, 2020, adding a portability provision. See Hopland, Dorwart, and Zanfir-Fortuna 2020b. On October 27, 2020, Rwanda adopted a data protection law that reportedly contains portability provisions (Rwanda Law 2021). By contrast, New Zealand's recently amended Privacy Act does not include portability provisions (Hopland, Dorwart, and Zanfir-Fortuna 2020a).

f. Authentication refers to verifying an individual's identity.

Responsible Use of Data

Open finance and data protection regimes may both permit and, in some cases, restrict data usage based on considerations other than consent. These restrictions and permissions are fundamental data protection provisions for any open finance regime and are based on the idea that data should be used responsibly by data holders, users, and intermediaries.

RESTRICTING DATA USAGE

The regulator should clearly set out circumstances where it may be appropriate for a data holder to refuse to transfer data, even when the consumer has consented to it. This includes situations where the data holder reasonably believes the transfer could result in physical or economic harm (e.g., fraud) or could adversely impact the security and integrity of the data holder's information systems.[118] For example, under PSD2, access requests can be denied for "objectively justified and duly evidenced reasons" relating to potential unauthorized or fraudulent access. In such cases, the data holder must immediately inform the national authority responsible for open finance and provide justification for denial. The objective is twofold: to deter data holders from unilaterally refusing transfers and disrupting the open finance process and to allow regulators to monitor data holder compliance. Yet even well-drafted regulation can be circumvented. For example, at the start of the implementation of PSD2, many TPPs complained that banks rejected access requests simply to create friction that would discourage consumers from using open banking tools. Even if the national authority subsequently found rejection by a bank abusive, the damage was already done as the transaction was blocked and the consumer dissuaded.

Customers should generally have the right to object to data processing and usage (vs revoking consent for data transfer, as discussed above) even if they consented in the past. At any time, customers should be able to object to how their personal data is used, particularly if it is being used for marketing purposes.[119] The right to object to data processing is particularly important in the context of open finance since data subjects "may have reservations and lack of trust in the notion of their personal data being shared with third parties."[120] In certain circumstances, countries may even restrict TPPs from seeking consent to use data for profiling and marketing.[121]

In addition to restricting data usage, certain jurisdictions appropriately limit the amount of a customer's data that can be legally collected and used. The concept of "data minimization" generally calls for collecting only the information needed and keeping it only for as long as necessary to fulfil the purpose for which it was collected.[122] In the context of open finance, data minimization comes into play when a data user requests information on behalf of a consumer.[123] In this case, the data user may not collect more data than is necessary for service provision nor use or keep it for longer than is reasonably needed to provide the requested product or services.[124] For instance, if a fintech offers a payment initiation service, it likely would not be necessary to collect a decade's worth of loan repayment history from the consumer's current bank. Similarly, if a consumer wanted to open a savings tracker, the need for detailed records of prior checking account transactions might not be justified. However, if personal financial management services are offered, it may be necessary to collect and retain information on all of a consumer's accounts going back 12 months or more.[125] Not only does data

118 See, for example, Australia Competition and Consumer (Consumer Data Right) Rules 2020, Section 4.7.

119 See, for example, GDPR 2016, Article 21.

120 Popoola and Oturu 2021.

121 See, for example, Australia Competition and Consumer (Consumer Data Right) Rules 2020, Section 4.12.

122 See GDPR 2016, Article 5(1)(c): "Adequate, relevant and limited to what is necessary in relation to the purposes" for which the data are processed; Article 5(1)(e): "Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed" and Article 13(2)(a); Brazilian General Data Protection Law 2018, Article 6(III); Central Bank of Brasil 2020, Article 13(3).

123 See, for example, Australia Competition and Consumer (Consumer Data Right) Rules 2020, Section 1.8: When a consumer asks an accredited person to provide goods or services to the consumer and providing those goods or services requires the use of the consumer's banking data.

124 Ibid, Section 1.8; PSD2 2015, Article 67(2)(f): "Not use, access or store any data for purposes other than for performing the account information service explicitly requested by the payment service user, in accordance with data protection rules."

125 Plaitakis and Staschen 2020, pp. 8–9.

minimization reduce a consumer's decision-making burden, it dampens the risk of cyberattacks and misuse since data is only kept as long as necessary.

Another policy option for regulators to consider is to restrict which data may be shared for specific use cases. For example, PSD2 limits the data that can be shared or accessed by PISPs for payment initiation. Only a "yes" or "no" response is permitted when verifying that the customer has sufficient funds to cover a particular payment.[126] Restrictions like these may also have social policy objectives, such as limiting the data that can be accessed or shared for credit scoring.

As open finance systems and associated APIs are designed, it makes sense that they be required to employ a "privacy by design" approach[127] that builds in privacy features.[128] This type of design approach is particularly relevant in EMDEs as it shifts the compliance burden onto providers, which are often better positioned to take on compliance than the consumers they serve.

CROSS-BORDER DATA TRANSFERS

This section flags some of the issues with cross-border data transfers and highlights important related data protection considerations. As a technical matter, personal data can easily flow into and out of a country via the internet. The question of whether open finance data protections should legally restrict the flow of such data requires consideration of the type of data being transferred, the purpose of the transfer, and protections put in place for the transferred data. A central rationale for open finance is to promote choice and competition among banks and to promote new market entrants. However, while the intention of open finance may be to promote competition with existing domestic banks and innovative FSPs within a country, this policy rationale may not always extend to competition that comes from banks and FSPs located or headquartered outside the country. In some cases, data protection may be a pretext for protecting domestic banks from foreign competition.

To the extent data is permitted to leave a country, open finance laws can specify whether they apply to data concerning its citizens that is held outside the country.[129] In such cases, there may be requirements to notify consumers of transfers and data users may be subject to laws that provide similar and enforceable data protections.[130] In 2017, Scott Farrell, a consultant appointed by the Australian Treasurer to conduct a review of the country's proposed Open Banking regime, recommended that express consumer consent be required before personal data is sent out of the country.[131] However, this requirement could negatively impact cloud computing and render it inefficient if some (but not all) customer data can be stored in the cloud.

DATA LOCALIZATION

Data localization laws that restrict a company's ability to transfer data out of the country could negatively impact open finance. In some cases, the rationale for these restrictions is that transfers to foreign countries could present risks if such countries do not have data protection laws in place. Another concern is that regulators might lose their supervisory access to the data if it is stored outside the country. However, these concerns can be addressed by putting into place mechanisms that permit data flows while still ensuring that data is protected and supervisors do not lose access, thus preserving the benefits to competition that exist under an open finance regime. Such mechanisms

126 PSD2 2015, Article 65(3).

127 Information Commissioner's Office 2021.

128 See, for example, GDPR 2016, Article 25(2).

129 See, for example, Australia Treasury Laws Amendment (Consumer Data Right) Act 2019, Section 56AO(1): Subject to some exceptions, "the CDR provisions extend to acts, omissions, matters and things outside Australia."

130 See, for example, Australia Treasury Laws Amendment (Consumer Data Right) Act 2019, Section 56EK(1); GDPR 2016, Article 45: "Transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country…in question ensures an adequate level of protection"; or alternative bases for international transfers (e.g., GDPR 2016, Article 47 [binding corporate rules] and Article 49 [derogations for specific situations]). Note that the Schrems II Decision cast doubt on available cross-border transfer mechanisms (Court of Justice of the European Union 2020).

131 Commonwealth of Australia 2017, p. 56.

could include security measures that require encryption of data in transit and storage regardless of where the data is located, including in cloud servers in other countries.[132] Financial supervisors could then be permitted access regardless of the data's location. Another option would be to permit data to leave the country but require that a mirror copy be kept within its borders, although this might impose additional data storage costs. While Indonesia initially required that copies of data be retained in the country, it later relaxed the requirement for financial institutions whose regulator could access the data.[133]

PERMISSIVE DATA USAGE

While consent is often the basis for use and disclosure of personal information under data protection laws, it is frequently not the only basis and is sometimes not required at all. For instance, disclosures may be permitted or required by law based on a court order or government reporting requirements.[134] For example, in the case of credit reporting, protections such as use limitations and accuracy requirements are tradeoffs for consumer data collection—often without consumer consent.[135] Another basis for disclosure is for contractual purposes. For instance, GDPR permits processing without consent when it is necessary to perform a contract. This consent exception is relevant to open banking since transfers usually require contracts. However, under GDPR, processing for contractual purposes is subject to GDPR use limitation provisions even if consent is not required. As the European Data Protection Board (EDPB) concluded:

> GDPR provides for the purpose limitation principle, which requires that personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. When assessing whether [a contract] is an appropriate legal basis for an online (payment) service, regard should be given to the particular aim, purpose, or objective of the service….[136]

Thus, data uses beyond what is necessary are usually based on consent. GDPR also permits processing to comply with legal obligations, including those imposed by open banking legislation;[137] to protect the vital interests of the consumer; to perform a task in the public interest; or for the legitimate interests of the data holder.[138] Under PSD2, European Union countries "shall permit processing of personal data by payment systems and payment service providers when necessary to safeguard the prevention, investigation, and detection of payment fraud."[139] However, such uses must also be carried out in accordance with GDPR.[140]

Data Security

Data security is critical as consumers begin to develop trust and confidence in open finance. In many ways it starts by confirming that consumers are who they say they are. Otherwise, identity thieves could impersonate consumers, steal their data, and use it to provide account access or cause other harms to legitimate consumers.[141] Depending on the jurisdiction, appropriate and available authentication measures should be required, which might include biometric identifiers and multi-factor

132 Baur-Yazbeck 2018.

133 Assegaf, Husein, and Sirie 2019.

134 See Popoola and Oturu 2021.

135 IFC 2012; World Bank 2011.

136 European Data Protection Board 2020a, p. 10.

137 GDPR 2016, Article 6(1)(c). See also European Data Protection Board 2020a, p. 12.

138 GDPR 2016, Article 6(1).

139 PSD2 2015, Article 94(1).

140 While PSD2 refers to the predecessor European Union data protection directive, it is now interpreted as applying to GDPR since the prior directive has been repealed. See European Data Protection Board 2018.

141 See also FIGI 2022, p. 22, "high risk of fraud"; Central Bank of Nigeria 2022.

authentication.[142] For instance, under GDPR, a data controller may confirm a requester's identity before responding to a request for additional information if it has reasonable doubt about the requester's identity as signaled by the data controller's system, algorithm, or AI.[143] Clear requirements should be established on who has the duty to authenticate the consumer, consumer agents that make data requests, and data users as well. If an individual engages in materially misleading or deceptive conduct designed to convince a data holder they are someone else making a request or providing consent, such conduct should be legally punishable.[144]

On the other hand, to preserve the efficiency of information flow, reduce costs, and develop user-friendly services in low-risk situations, authentication exemptions may be appropriate for low-value transactions (i.e., those less than EUR 30),[145] recurring transactions,[146] trusted beneficiaries,[147] contactless payments under EUR 50,[148] or certain types of information requests (e.g., account balances).[149]

It may be appropriate to accredit data users along similar lines, taking into account the risk they pose, types of data transferred, and data uses.[150] For example, the draft Nigerian Open Banking Guidelines state that only certain participants can access certain data, based on categorization of the data's risk (sensitivity).[151]

Accreditation procedures could include renewal and transfer as well as suspension or revocation if open finance or data protection requirements are not followed.[152] A register of accredited providers could be maintained and made publicly available so consumers can identify them.[153]

In cases where open finance laws have yet to be adopted, consumers interested in financial management tools sometimes turn to providers that aggregate their financial data through screen scraping. The process gives providers account access credentials for financial institution websites, potentially resulting in unauthorized transactions on consumers' accounts. As open finance frameworks move away from screen scraping toward using APIs, account security will see great improvements since TPPs are able to collect data directly from data holders through APIs.[154]

As the availability of open finance increases, a system will emerge where multiple parties handle the ever-increasing amounts of sensitive financial information. Basic security requirements should be established for all open finance system participants, including end points and intermediaries.[155] Requirements could include encryption for data that is in transit and at rest, and that data be transferred via secure API-enabled banking services.[156] A duty could be imposed to employ reasonable risk-based

142 See, for example, PSD2 2015, Articles 4(30), 52(2)(b), 97, and 98; European Banking Authority 2019: Two-factor authentication mandated; Banco Central do Brasil 2020, Articles 16 and 17: Institutions are required to adopt procedures and controls for authentication, taking into account the level of risk and type of data. See also Central Bank of Nigeria 2022, Section 11.2: Two-factor authentication and credentials of the end user.

143 GDPR 2016, Article 12(6).

144 See, for example, Australia Treasury Laws Amendment (Consumer Data Right) Act 2019, Section 56BN. See also Sections 56BO and 56CC: Falsely representing one is accredited is an offense.

145 Commission Delegated Regulation of PSD2 2017, Article 16.

146 Ibid, Article 14.

147 Ibid, Article 13.

148 Ibid, Article 11.

149 Ibid, Article 10.

150 See, for example, Australia Treasury Laws Amendment (Consumer Data Right) Act 2019, Section 56BH(1).

151 See also Central Bank of Nigeria 2022, Appendix II, Section 3.0.

152 See, for example, Australia Treasury Laws Amendment (Consumer Data Right) Act 2019, Section 56BH(1)(e).

153 Ibid, Section 56CE.

154 OECD 2020, p. 14; Wolberg-Stok 2022, p. 21.

155 See, for example, PSD2 2015, Article 67(2)(b): Duty to ensure that payment services user credentials are not accessible to others and that they are transmitted using safe and efficient channels.

156 See, for example, Australia Competition and Consumer (Consumer Data Right) Rules 2020, Schedule 2; Central Bank of Kenya, p. 60: "[The Central Bank of Kenya] will facilitate development of appropriate API standards and mandate robust but secure data sharing. The use of secure APIs by digital financial providers makes it easier for third parties, mainly fintechs that offer tailored, innovative solutions, to connect in a seamless, fast and secure manner."

security measures to protect data[157] and properly dispose of data that is no longer needed or necessary to retain.[158] The bottom line in an open finance environment is "the risk for Data Controllers is multiplied and entities looking to participate must bear this in mind and put in place the necessary measures."[159]

The government and consumers affected by security breaches should be duly notified. In addition, consumers should be made aware of the steps they can take to protect themselves. The consumer's primary contact or the entity "responsible" per the open finance framework (e.g., data holder, TPP, data user) is generally required to provide the breach notification unless the law designates that one entity provides breach notifications on behalf of all other entities.[160]

157 See, for example, Australia Treasury Laws Amendment (Consumer Data Right) Act 2019, Section 56EO(1); GDPR 2016, Articles 5(1)(f) and 32; Brazilian General Data Protection Law 2018, Article 6(VII); PSD2 2015, Articles 95(1) and (2).

158 See, for example, Australia Treasury Laws Amendment (Consumer Data Right) Act 2019, Section 56EO(2).

159 See Popoola and Oturu 2021.

160 See, for example, Australia Treasury Laws Amendment (Consumer Data Right) Act 2019, Section 56ES; PSD2 2015, Articles 73, 74, 89, and 90; Central Bank of Kenya 2020: Considering "timely, full and accurate reporting."

SECTION III

DATA PROTECTION IMPLEMENTATION

GIVING CONSUMERS CONTROL over their data and adopting laws and regulations that govern the responsible use of data are critical steps in establishing consumer trust and confidence in open finance. However, these measures will only be effective if they are implemented with appropriate oversight and effectively enforced by regulators and enforcing authorities. For example, Australia's Consumer Data Rights Law authorizes penalties of up to A$10 million for data violations.[161] Brazil's data protection law imposes fines of up to 2 percent of revenue for the prior financial year, topping off at a maximum of R$50 million per infraction.[162]

Additional sanctions in Brazil include public disclosure of infractions, blocking or deleting personal data that was the subject of an infraction, suspension of operation of the database for up to six months until infractions have been corrected, and partial or total prohibition of activities related to data processing. The United Kingdom's implementation of PSD2 allows the Financial Conduct Authority to impose penalties, seek injunctions to comply with regulations, and order restitution.[163]

The following provisions help implement open finance data protections.

Recordkeeping

For purposes of accountability and to limit improper access to data, procedures should be imposed to require recordkeeping on who requested data, who provided it and to whom, and the associated dates of those actions.[164] Records could be made available to consumers and entities charged with open finance oversight and enforcement.[165] Data holders and data users could be required to regularly report data requests and complaints received to the relevant government oversight entity.[166] In the United Kingdom, each data holder makes this information public in aggregate form in an effort to hold firms publicly accountable. In Brazil, the open banking governance body publishes the data in aggregate form for the same reason.[167]

161 Australia Treasury Laws Amendment (Consumer Data Right) Act 2019, Section 56BN(3).

162 Brazilian General Data Protection Law 2018. Under PSD2 2015, Article 103, E.U. Member States establish rules on applicable penalties when transposing the Directive into national law.

163 U.K. Payment Services Regulations 2017, Sections 111, 113, and 114.

164 See, for example, Australia Competition and Consumer (Consumer Data Right) Rules 2020, Section 9.3; GDPR 2016, Articles 5(2), 24, and 30; Brazilian General Data Protection Law 2018, Article 6(X); PSD2 2015, Article 21. See also Popoola and Oturu 2021.

165 See, for example, Australia Competition and Consumer (Consumer Data Right) Rules 2020, Sections 9.5 and 9.6.

166 Ibid, Section 9.4.

167 See, for example, Barclays 2022 and Monzo 2022 in the United Kingdom and the Open Finance Brasil Dashboard 2022 in Brazil.

Liability Allocation

When things go wrong, consumers should at a minimum understand who bears the risk of loss due to fraud, data compromise, failure to properly authenticate data requests, or transmission to the wrong bank. Imposing liability on system participants can provide greater incentives to protect data. For instance, under PSD2, parties are responsible for the acts of their agents.[168] One option is to make each entity responsible for the data it handles. For example, prior to transferring the data, a data holder is responsible for ensuring the consumer has truly consented and that the data user is who they purport to be (e.g., based on evidence of accreditation if required in that jurisdiction). The data user is then liable if it loses or inappropriately uses the data. TPPs would be responsible for the secure handling of data and transmission to the correct entity upon consumer request.

Imposing full liability on entities consumers directly interact with will make the liability structure easier for consumers to navigate. This is because it is difficult for consumers to determine which of the many entities that handle their data is legally culpable. This approach is especially useful in EMDEs where a large proportion of the population may have difficulty claiming indemnity rights due to literacy and other concerns. For example, in PSD2, the liability requirement makes banks liable for reimbursing customers even if unauthorized transactions originate from the relationship between the user and a third party.[169] In such cases, the entity the consumer deals with could then, through contractual arrangements it has put into place, resolve liability among the business interests should consumer redress be necessary. Another example of the approach is found in the Nigerian Data Protection Regulation (NDPR), which requires each party to a data processing agreement to ensure that the other party has no record of data protection violations and requires them to abide by the NDPR. Furthermore, under the NDPR, data controllers are liable for violations committed by third parties that handle customer data, thus creating a strong incentive for open banking participants to vet all parties.[170]

Complaints Resolution

Consumers with problems related to open finance should have access to a convenient, easy-to-use complaints process for dispute resolution. The process includes reimbursement to customers who should not be held responsible for direct losses resulting from unauthorized transactions unless they acted fraudulently or with gross negligence. One option is to create a voluntary mechanism where participants agree to adhere to a code of best practices, including how to handle cases and whether cases can be taken to mediation, adjudication, or arbitration. Complaints can be directly handled by the entity that allegedly caused the problem or, as in Japan, by a private body responsible for handling customers' open banking complaints. In Singapore, the Personal Data Protection Commission facilitates complaints between customers and providers. India has an Ombudsman Scheme for Digital Transactions.

Since consumers in EMDEs may be less confident or capable of raising complaints with providers or private bodies due to literacy issues, the role of consumer associations in helping handle complaints and dispute resolution should be considered. In the Philippines, for example, the consumer association Laban Konsyumer collects and shares consumer complaints directly with the central bank.[171] Regulators can create official channels that allow consumer associations to support complaints resolution in open finance disputes.

Another option is for regulators in EMDEs to use social media messaging platforms or mobile apps to directly

168 PSD2 2015, Article 20(2). See also Australia Treasury Laws Amendment (Consumer Data Right) Act 2019, Section 56EY: Consumers may bring an action for loss or damages "against any person involved in the contravention," although it is not clear if this is intended to make parties liable for their agents.

169 See Plaitakis and Staschen 2020, pp. 6–13.

170 See Popoola and Oturu 2021.

171 Duflos, Griffin, and Valenzuela 2021.

receive consumer complaints. Bangladesh, Colombia, Ghana, Peru, and the Philippines have recently taken this innovative approach to complaints resolution.[172] However, certain barriers diminish the potential of social media as a complaints resolution channel since many government agencies have yet to confer legitimacy on its use for public policy processes. Government agencies need to develop resources and capabilities for social media monitoring and analysis if they are to effectively resolve consumer complaints related to open finance.[173]

Open finance rules can give consumers the opportunity to seek review of compliance issues before a tribunal, such as a court, and provide other internal and external alternative dispute-resolution processes.[174] Rules violations can be punishable through the imposition of civil penalties.[175] One option is to permit class action lawsuits against firms involved in open banking.

BOX 7. Misuse of Account Access Privileges by the Data Aggregator, Plaid

The data aggregator Plaid was sued in a 2020 consumer class action suit filed in U.S. federal court.

The suit alleged the company obtained user financial account login credentials through an interface designed with the same look and feel of a user bank account login screen when, in fact, username and password were being provided to Plaid.[a] These access credentials were allegedly used to obtain more financial data than was authorized or needed by a user's app. Plaid enables connections for "5,000 mobile and web-based apps that consumers use to make payments, transfer money, pay bills, manage their personal finances, make investments, and apply for loans, among other finance-related activities."[b] In July 2022, the court approved Plaid's agreement to settle the case without admission of liability.[c] The case highlights the potential of TPPs such as Plaid to misuse account access privileges for their own benefit by collecting, for example, more data than is authorized or necessary to provide their services. It also highlights the importance of challenging TPP practices in court.

a. Wolberg-Stok 2022, p. 19.

b. In re Plaid, Inc. Privacy Litigation 2022; Order Granting Final Approval of Class Action Settlement 2022.

c. Ibid.

172 Ibid.

173 Ibid.

174 See, for example, Australia Treasury Laws Amendment (Consumer Data Right) Act 2019, Section 56BJ, 56BW–56BY, and 56DA; GDPR 2016, Article 79; PSD2 2015, Articles 101–102.

175 See, for example, Australia Treasury Laws Amendment (Consumer Data Right) Act 2019, Sections 56BL, 56EU, and 56EV. See also Popoola and Oturu 2021: "Considering the implementation of open banking's greater risk of resulting in a breach, it is important that participants take necessary steps to ensure absolute compliance with the provisions of the Regulation so as to avoid penalties."

SECTION IV

CONCLUSION

OPEN FINANCE ENTAILS CREATING a new digital ecosystem that enables unprecedented expansion in the use and flow of personal information. It holds tremendous promise for low-income consumers who are underbanked or excluded from the financial system but it also creates new risks. Open finance enables consumers to check account balances, review transactions, make payments, get financial planning advice, obtain loans, and easily move accounts from banks to competitive FSPs that offer more products and services at lower costs—all in real time. It can mean more products at lower costs through multiple and easy-to-access channels, and remote onboarding for low-income people.

Open finance stakeholders need to reassure consumers that their sensitive financial and transaction data will be protected and only used for legitimate, reasonable purposes, thereby ensuring that these services are worthy of consumers' trust and confidence. Data misuse or compromise could see many consumers deciding to remain on the sidelines of digital financial services. Thus, a key element of open finance is to create a legal and regulatory structure that facilitates information sharing but also provides critical data protections. The addition of data protection provisions that underpin open finance can be a complex task, given the interplay between the open finance scheme and data protection rules. This will prove challenging as open finance expands to countries with overburdened regulators and FSPs that operate on tight margins. Accordingly, this note lays out the data protections that would help develop consumer trust and confidence in open finance by identifying connections and potential choices regulators can make to incorporate adequate protections into open finance regimes. As recommended throughout, basic data protections should be adopted alongside the introduction of open finance. Over time, regulators can build on existing protections by considering the addition of the other provisions discussed in this note.

With appropriate data protections, open finance can empower low-income consumers to take charge of the financial data they generate and make it work for them.

APPENDIX A

OPEN BANKING AND DATA PROTECTION LAWS AND REGULATIONS

The following list is not exhaustive and may not include all open finance and data protection laws and regulations for the countries noted.

Country	Legislation	Regulation
Australia	• Treasury Laws Amendment (Consumer Data Right) Act 2019, No. 63, 2019 (CDR Law) • Competition and Consumer Act 2010	• Competition and Consumer (Consumer Data Right) Rules 2020 made under Section 56BA of the Competition and Consumer Act 2010, Registered February 20, 2022 (CDR Rules) • CDR Accreditation Guidelines, Version 4, December 2022 • Australian Privacy Principles Guidelines
Brazil	• Brazil General Data Protection Law (LGPD), Federal Law No. 13,709/2018 (amended by Law No. 13,853/2019)	• Banco Central do Brasil, Regulation on Open Banking, Joint Resolution No. 1 of May 4, 2020
Canada	• Canada's proposed Digital Charter Implementation Act, 2020, Bill C-11; proposed Digital Charter Implementation Act, 2022, Bill C-27	
European Union	• 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 (PSD2)	• 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 (PSD2 Regulation) • 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) (GDPR) • EDPB Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR Version 2.0 Adopted on 15 December 2020

Country	Legislation	Regulation
India	• Draft India Digital Personal Data Protection Bill, 2022 • Draft India Personal Data Protection Bill, 2019 (withdrawn)	• Master Direction—Non-Banking Financial Company—Account Aggregator (Reserve Bank) Directions, 2016 • Directions Regarding Registration and Operations of NBFC—Account Aggregators under Section 45-IA of the Reserve Bank of India Act, 2016 • Reserve Bank of India, Directive 2017-18/153, April 6, 2018, Storage of Payment System Data
Mexico	• Ley Para Regular Las Instituciones de Tecnología Financiera	
New Zealand	• Privacy Act 2020	
Nigeria		• Central Bank of Nigeria, Draft Operational Guidelines for Open Banking in Nigeria, May 2022 • NITDA Nigeria Data Protection Regulation 2019 • Central Bank of Nigeria, Regulatory Framework for Open Banking in Nigeria, February 2021
Rwanda	• Law relating to the protection of personal data and privacy	
Singapore	• Personal Data Protection (Amendment) Bill 2020	
United Kingdom		• Payment Services Regulations 2017
United States	• Gramm-Leach-Bliley Act	

APPENDIX B
GLOSSARY

The definitions provided in this glossary are general and are not intended to track the laws of any specific country.

Term	Definition
Account aggregator (AA)	A nonbanking financial company category created by the Reserve Bank of India in 2016. AAs securely transfer financial data from data holders to data users based on customer consent.
Account information service provider (AISP)	Third-party AISPs provide customers with consolidated online information about their financial accounts with other payment services providers.
Application programming interface (API)	A set of routines, protocols, and tools for building software applications. In the context of this note, APIs are the conduit for data transmission between two parties.
Consumer data right (CDR)	Under Australian law, the right of a consumer to access his or her own data or to share it with an accredited data recipient to whom the consumer has given access permission.
Customer data	Personally identifiable customer information that can be used for data on account opening and use, including registration, KYC, and customer due diligence (CDD) data.
Customer due diligence (CDD)	CDD involves identifying a client and verifying the client's identity by checking his or her identity documentation or data and, where appropriate, conducting background and beneficial ownership checks.
Customer transaction data	Data from a customer's bank or payment account(s) that show the customer's transaction history.
Data controller/ data fiduciary	A person or company that determines the purposes and means of personal data processing.
Data holder	An entity that holds or possesses customer data.
Data intermediary	An entity that processes data on behalf of another organization or mediates the flow of data from a data source to a data user.
Data portability	The ability of a data subject to download a full set of their data and "port" or share it with whomever they choose.
Data principal/ data subject	A person to whom data relates.
Data processor	An individual or company that processes personal data on behalf of a data controller.
Data user	An entity that uses the data relating to a data subject to perform a service.
Financial services provider (FSP)	An entity that provides financial services to consumers and other businesses.

Term	Definition
Fintech	A technologically-enabled innovation in financial services ("financial technology") that could result in new business models, applications, processes, or products, with an associated material effect on financial markets and institutions and the provision of financial services.
Open banking	A framework in which banks share financial product data and/or certain customer-specific data with other financial sector stakeholders. The sharing of customer-specific data is based on request by, and consent of, the consumer.
Open data	A framework for data sharing that goes beyond financial services to include the sharing of telecom, utilities, health, social media, and/or other types of data.
Open finance	A framework in which financial sector players, including insurance, investment, and pension providers, share financial product data and/or certain customer-specific data with other financial sector stakeholders. The sharing of customer-specific data is based on request by, and consent of, the consumer.
Payment initiation	A third-party service that facilitates the initiation of customer payments.
Payment initiation service provider (PISP)	A third-party service provider that allows a consumer to make a payment from their bank account directly to the merchant, typically by establishing an electronic payment link between payer and online merchant via the payer's online banking module.
Savings sweeper	Calculates what a consumer can save and when, based on their financial history, then automatically transfer those funds to a dedicated savings account.
Screen scraping	The action of using a computer program to copy data from a website.
Third-party provider (TPP)	A non-account-servicing payment services provider that is licensed or registered to provide a service to customers of account-servicing payment services providers, such as payment/transaction initiation, account aggregation, and customer acquisition services.

BIBLIOGRAPHY

Ada Lovelace Institute. 2022. "Who Cares What the Public Think? U.K. Public Attitudes to Regulating Data and Data-driven Technologies." Ada Lovelace Institute, 5 May. https://www.adalovelaceinstitute.org/evidence-review/public-attitudes-data-regulation/

Asrow, Kaitlin. 2022. "Defining Data Rights and the Role of the Individual," in *Open Banking, edited by Linda Jeng. U.S.: Oxford University Press, March.* https://doi.org/10.1093/oso/9780197582879.003.0003

Assegaf, Ahmad, Zacky Husein, and Muhamad Sirie. 2019. "Indonesia: Government Relaxes Data Localisation Requirement." Mondaq, 6 November. https://www.mondaq.com/data-protection/861082/government-relaxes-data-localisation-requirement

Australia Competition and Consumer Act 2010. No. 51, 1974. Compilation No. 139, 5 October 2021. https://www.legislation.gov.au/Details/C2021C00528

Australia Competition and Consumer (Consumer Data Right) Rules 2020, made under section 56BA of the Competition and Consumer Act 2010. *Compilation No. 7, 1 February 2022. Schedule 3.* https://www.legislation.gov.au/Details/F2022C00187

Australia Treasury Laws Amendment (Consumer Data Right) Act 2019. No. 63, 2019. https://www.legislation.gov.au/Details/C2019A00063

Australian Competition & Consumer Commission. 2020. "ACCC Makes Accredited Intermediary Rules." Consumer data right (CDR), 9 November. https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0/accc-makes-accredited-intermediary-rules

Australian Competition & Consumer Commission. 2022. "Consumer Data Right Accreditation Guidelines." Version 4, December. www.cdr.gov.au/sites/default/files/2022-12/CDR-Accreditation-guidelines-version-4-December-2022.pdf

Australia Consumer Data Standards. 2019. CX Workshop: Consumer Control, 22 October. https://consumerdatastandards.gov.au/sites/consumerdatastandards.gov.au/files/uploads/2019/10/CX-workshop-_-Consumer-control-presentation.pdf

Australia Consumer Data Standards Glossary. Consumer Data Right Support Portal. Webpage viewed September 2022. https://cdr-support.zendesk.com/hc/en-us/articles/900002911746-Glossary)

Australian Privacy Principles. 2019. Office of the Australian Information Commissioner, 22 July. https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-b-key-concepts

Banco Central do Brasil. 2020. Regulation on Open Banking. Joint Resolution No. 1 of May 4, 2020. https://www.bcb.gov.br/content/config/Documents/Open_Banking_CMN_BCB_Joint_Resolution_1_2020.pdf

Barclays. Open Banking. Webpage viewed September 2022. https://www.barclayscorporate.com/solutions/corporate-banking-solutions/digital-banking-services/corporate-open-banking-service/performance-availability-metrics

Basel Committee on Banking Supervision. 2019. "Report on Open Banking and Application Programming Interfaces." Basel: Bank for International Settlements, November. https://www.bis.org/bcbs/publ/d486.pdf

Baur-Yazbeck, Silvia. 2018. "3 Myths About Data Localization." Blog. Washington, D.C.: CGAP, August. https://www.cgap.org/blog/3-myths-about-data-localization

Brazilian General Data Protection Law (LGPD), Federal Law No. 13,709/2018, Article 6(I) (access) and 18(III) (correction). August 14, 2018, amended by Law No. 13,853/2019, effective September 18, 2020. http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm#art65

Brodsky, Laura, and Liz Oakes. 2017. "Data Sharing and Open Banking." McKinsey & Company, 5 September. https://www.mckinsey.com/industries/financial-services/our-insights/data-sharing-and-open-banking

CGAP. "New Approaches to Data Privacy and Protection." Washington, D.C.: CGAP. Webpage viewed September 2022. https://www.cgap.org/topics/collections/new-approaches-data-privacy-protection

CGAP, Dalberg, and Dvara. 2017. "Privacy on the Line." Dalberg, November. https://dalberg.com/wp-content/uploads/2017/11/Privacy-On-The-Line-Final-161117_1.pdf

CSIRO Data61. Commonwealth Scientific and Industrial Research Organisation, Australia. Webpage viewed September 2022. https://data61.csiro.au

Canada House of Commons. 2020. Bill C-11. Second Session, Forty-third Parliament. 69 Elizabeth II, 2020. First Reading, November 17. https://parl.ca/DocumentViewer/en/43-2/bill/C-11/first-reading

Canada House of Commons. 2022. Bill C-27. First Session, Forty-fourth Parliament, 70–71 Elizabeth II, 2021–2022. First Reading, June 16. https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading

Central Bank of Kenya. 2020. "Kenya National Payments System Vision and Strategy, 2021–2025." Nairobi: Central Bank of Kenya, December. https://www.centralbank.go.ke/wp-content/uploads/2020/12/CBK-NPS-Vision-and-Strategy.pdf

Central Bank of Kenya. 2022. "Kenya National Payments Strategy, 2022–2025." Nairobi: Central Bank of Kenya, February. https://www.centralbank.go.ke/wp-content/uploads/2022/02/National-Payments-Strategy-2022-2025.pdf

Central Bank of Nigeria. 2022. "Operational Guidelines for Open Banking in Nigeria." Exposure Draft. Lagos: Central Bank of Nigeria, May. https://www.cbn.gov.ng/Out/2022/CCD/OPERATIONAL GUIDELINES FOR OPEN BANKING IN NIGERIA_ APPROVED EXPOSURE DRAFT.pdf

Chakravorti, Bhaskar. 2020. "Why It's So Hard for Users to Control Their Data." Harvard Business Review, 30 January. https://hbr.org/2020/01/why-companies-make-it-so-hard-for-users-to-control-their-data

Chugh, Beni. 2022. "Making Digital Finance Work for Women." Blog. The Economic Times, 8 March. https://bfsi.economictimes.indiatimes.com/blog/making-digital-finance-work-for-women/90052605

Comision Nacional Bancaria y de Valores. 2021. Ley Para Regular Las Instituciones de Tecnología Financiera. Mexico City, 20 May. https://www.cnbv.gob.mx/Normatividad/Ley%20para%20Regular%20las%20Instituciones%20de%20Tecnolog%C3%ADa%20Financiera.pdf

Commission Delegated Regulation of PSD2. (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). Official Journal of the European Union. 27 November 2017. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0389&from=EN

Commonwealth of Australia. 2017. "Review into Open Banking: Giving Customers Choice, Convenience and Confidence." (Farrell Report). The Australian Government the Treasury,

December. https://treasury.gov.au/sites/default/files/2019-03/Review-into-Open-Banking-_For-web-1.pdf

Consumer Policy Research Centre. 2020. "Stepping Towards Trust: Consumer Experience, Consumer Data Standards, and the Consumer Data Right." CPRC: Melbourne, August. https://consumerdatastandards.gov.au/sites/consumerdatastandards.gov.au/files/uploads/2020/09/20200902_CPRC-Report-1_Publication.pdf

Court of Justice of the European Union. 2020. Schrems II Decision. Judgement of the Court. ECLI:EU:C:2020:559. Luxembourg, 16 July. http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en

Data61. Consumer Data Standards. 2019a. "Phase 1: CX Report (Data61 Report)." 20 February. https://consumerdatastandards.gov.au/engagement/reports/reports-cx/phase-1-cx-report-2

Data61. Consumer Data Standards. 2019b. "Design to Thrive. Design to Bias, Phase 1: CX Report." 20 February. https://consumerdatastandards.gov.au/sites/consumerdatastandards.gov.au/files/uploads/2019/02/Consumer-Data-Standards-Phase-1_-CX-Report.pdf

Datwani, Leena, and Anand Raman. 2020. "India's New Approach to Personal Data-Sharing." Working Paper. Washington, D.C.: CGAP, July. https://www.cgap.org/sites/default/files/publications/2020_07_Working_Paper_India_New_Approach_Personal_Data_Sharing.pdf

Duflos, Eric, Mary Griffin, and Myra Valenzuela. 2021. "Elevating the Collective Consumer Voice in Financial Regulation." Working Paper. Washington, D.C.: CGAP, March. https://www.cgap.org/sites/default/files/publications/2021_03_WorkingPaper_Collective_Consumer_Voice_updated.pdf

Economic Times. 2022. "India's Five-Year Wait for a Data Law Continues." Economic Times Tech, 5 August. https://economictimes.indiatimes.com/tech/newsletters/ettech-unwrapped/indias-five-year-wait-for-a-data-law-continues/articleshow/93379149.cms?from=mdr

European Banking Authority. 2019. EBA-Op-2019-06, "Opinion of the European Banking Authority on the Elements of Strong Customer Authentication under PSD2." EBA, 21 June. https://www.eba.europa.eu/sites/default/files/documents/10180/2622242/4bf4e536-69a5-44a5-a685-de42e292ef78/EBA%20Opinion%20on%20SCA%20elements%20under%20PSD2%20.pdf

European Data Protection Board. 2018. Letter from European Data Protection Board to Sophie in 't Veld, 5 July. https://edpb.europa.eu/sites/edpb/files/files/news/psd2_letter_en.pdf

European Data Protection Board. 2020a. "EDPB Guidelines 06/2020 on the Interplay of the Second Payment Services Directive and the GDPR." Version 2.0, adopted on 15 December 2020. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202006_psd2_afterpublicconsultation_en.pdf

European Data Protection Board. 2020b. "Guidelines 05/2020 on Consent under Regulation 2016/679." Version 1.1, adopted on 4 May 2020. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

Fernandez Vidal, Maria. 2020. "Data Privacy Concerns Influence Financial Behaviors in India, Kenya." Blog. Washington, D.C.: CGAP, 29 September. https://www.cgap.org/blog/data-privacy-concerns-influence-financial-behaviors-india-kenya

Fernandez Vidal, Maria, and David Medine. 2019. "Is Privacy Good for Business?" Focus Note. Washington, D.C.: CGAP, December. https://www.cgap.org/research/publication/data-privacy-good-business

GDPR (General Data Protection Regulation). 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. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Grady, Rosamund, Fredesvinda Montes, and Marci Traversa. 2018. "Financial Consumer Protection and New Forms of Data Processing Beyond Credit Reporting." Discussion Note. Washington, D.C.: World Bank, November. https://documents1.worldbank.org/curated/en/677281542207403561/pdf/132035-WP-FCP-New-Forms-of-Data-Processing.pdf

Hopland, Caroline, Hunter Dorwart, and Gabriela Zanfir-Fortuna. 2020a. "A Deep Dive Into New Zealand's New Privacy Law Extraterritorial Effect, Cross-order Data Transfers Restrictions and New Powers of the Privacy Commissioner." Washington, D.C.: Future of Privacy Forum, 8 December. https://fpf.org/blog/a-deep-dive-into-new-zealands-new-privacy-law-extraterritorial-effect-cross-border-data-transfers-restrictions-and-new-powers-of-the-privacy-commissioner/

Hopland, Caroline, Hunter Dorwart, and Gabriela Zanfir-Fortuna. 2020b. "Singapore's Personal Data Protection Act Shifts Away from a Consent-Centric Framework." Washington, D.C.: Future of Privacy Forum, 18 November. https://fpf.org/blog/singapores-personal-data-protection-act-shifts-away-from-a-consent-centric-framework/

IFC (International Finance Corporation). 2012. "Credit Reporting Knowledge Guide." Washington, D.C.: IFC. https://documents1.worldbank.org/curated/en/873561468320947849/pdf/941600WP0Box380IC00credit0reporting.pdf

India Digital Personal Data Protection Bill, 2022. https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Potection%20Bill%2C%202022_0.pdf

India Personal Data Protection Bill, 2019. Bill No. 373 of 2019 (withdrawn). http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

India Report of the Joint Committee on the Personal Data Protection Bill, 2019. Presented to Lok Sabha 16 December 2021. https://www.medianama.com/wp-content/uploads/2021/12/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf

Information Commissioner's Office. 2021. "Data Protection by Design and Default." Wilmslow, U.K.: 1 January. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/

In re Plaid, Inc. Privacy Litigation, Case No. 4:20-md-03056. United States District Court for the Northern District of California. https://www.plaidsettlement.com/frequently-asked-questions.php

Kuebler-Wachendorff, Sophie, Robert Luzsa, Johann Kranz, et al. 2021. "The Right to Data Portability: Conception, Status Quo, and Future Directions." *Informatik Spektrum* 44, pp. 264–272, 6 July. https://doi.org/10.1007/s00287-021-01372-w

Medine, David, and Gayatri Murthy. 2020. "Making Data Work for the Poor." Focus Note. Washington, D.C.: CGAP, January. https://www.cgap.org/research/publication/making-data-work-poor

Miller, Margaret, Clare Sullivan, and Fredesvinda Montes. 2021. "The Role of Consumer Consent in Open Banking: Financial Inclusion Support Framework." Technical Note. Washington, D.C.: World Bank Group, December. https://openknowledge.worldbank.org/bitstream/handle/10986/37073/P1705050aeb8e704f088260f228802b73b8.pdf?sequence=1&isAllowed=y

Monzo. Performance of our App and Open Banking Services. U.K.

Webpage viewed September 2022. https://monzo.com/service-information

OAIC (Office of the Australian Information Commissioner). CDR participants. Webpage viewed September 2022. https://www.oaic.gov.au/consumer-data-right/cdr-participants

OECD. 2020. "Personal Data Use in Financial Services and the Role of Financial Education: A Consumer Centric Analysis." https://www.oecd.org/finance/Personal-Data-Use-in-Financial-Services-and-the-Role-of-Financial-Education.pdf

Olijnyk, Zena. 2022 . "New Federal Privacy Legislation Likely Won't Come Until New Commissioner Is Named." Canadian Lawyer, 2 May. https://www.canadianlawyermag.com/practice-areas/privacy-and-data/new-federal-privacy-legislation-likely-wont-come-until-new-commissioner-is-named-fasken-lawyers/366241

Open Finance Brasil Dashboard. Webpage viewed September 2022. https://dashboard.openbankingbrasil.org.br/

Open Finance Working Group on Incentives. 2019. "Advice from 'The Open Finance Working Group on Incentives' to the FCA." FCA.org.uk, December. https://www.fca.org.uk/publication/documents/incentives-advisory-group-open-finance-advice-note.pdf

Order Granting Final Approval of Class Action Settlement, James Cottle, et al., v. Plaid Inc. 20 July, 2022. https://angeion-public.s3.amazonaws.com/www.PlaidSettlement.com/docs/Order+Granting+Final+Approval+of+Class+Action+Settlement.pdf

PSD2 (Payment Services Directive 2). 2015. 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. Official Journal of the European Union, 25 November. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN

Plaitakis, Ariadne, and Stefan Staschen. 2020. "Open Banking: How to Design for Financial Inclusion." Working Paper. Washington, D.C.: CGAP, October. https://www.cgap.org/research/publication/open-banking-how-design-financial-inclusion

Popoola, Mubaraq, and Davidson Oturu. 2021. "The Effect of Nigeria's Data Protection Regime on Open Banking." Aelex, Mondaq.com, 12 May. https://www.mondaq.com/nigeria/privacy-protection/1067744/the-effect-of-nigeria39s-data-protection-regime-on-open-banking

Reserve Bank of India. 2016a. Directions Regarding Registration and Operations of NBFC— Account Aggregators under Section 45-IA of the Reserve Bank of India Act, 1934. https://www.rbi.org.in/Scripts/bs_viewcontent.aspx?Id=3142

Reserve Bank of India. 2016b. Master Direction—Non-Banking Financial Company—Account Aggregator (Reserve Bank) Directions, updated 23 November 2022. https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10598

Reserve Bank of India. 2018. Storage of Payment System Data. Directive 2017-18/153, 6 April. https://src.bna.com/D5n?_ga=2.123343947.1131408265.1575749815-1922557974.1575749815

Reynolds, Faith. 2017. "Open Banking: A Consumer Perspective." Barclays.com, January. https://home.barclays/content/dam/home-barclays/documents/citizenship/access-to-financial-and-digital-empowerment/Open-Banking-A-Consumer-Perspective-Faith-Reynolds.pdf

Reynolds, Faith. 2019. "What Future Governance Arrangements Should Be in Place for Open Banking, Open Finance, and Open Life?" LinkedIn, 19 July. https://www.linkedin.com/pulse/what-future-governance-arrangements-should-place-open-faith-reynolds/?trk=public_profile_article_view

Reynolds, Faith, and Mark Chidley. 2018. "Consumer Priorities for Open Banking." openbanking.org.uk. https://www.openbanking.org.uk/wp-content/uploads/2021/04/Consumer-Priorities-for-Open-Banking-report-June-2019.pdf

Rwanda Law relating to data protection and privacy. 2021. Year 60, Official Gazette No. Special of 15 October 2021. https://www.minijust.gov.rw/fileadmin/user_upload/Minijust/Publications/Official_Gazette/_2021_Official_Gazettes/October/OG_Special_of_15.10.2021_Amakuru_bwite.pdf

Susser, Daniel. 2019. "Notice After Notice-and-Consent: Why Privacy Disclosures Are Valuable Even If Consent Frameworks Aren't." *Journal of Information Policy, Volume 9, pp. 37–62.* https://doi.org/10.5325/jinfopoli.9.2019.0037

Swire, Peter, and Yianni Lagos. 2013. "Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique." 72 Maryland Law Review 335, 31 May. http://dx.doi.org/10.2139/ssrn.2159157

Tiwari, Siddharth, Sharad Sharma, Siddharth Shetty, and Frank Packer. 2022. "The Design of a Data Governance System." BIS Papers No. 124. Basel: Bank for International Settlements, May (revised July). https://www.bis.org/publ/bppdf/bispap124.pdf

U.K. Open Banking Standard. 2022a. London: Open Banking Limited. Webpage viewed September 2022. https://standards.openbanking.org.uk/

U.K. Open Banking Standard. 2022b. Permissions and Data Clusters for AIS Journeys. London: Open Banking Limited. Webpage viewed September 2022. https://standards.openbanking.org.uk/customer-experience-guidelines/account-information-services/permissions-and-data-clusters/latest/

U.K. Payment Services Regulations 2017, Sections 111, 113, and 114. https://www.legislation.gov.uk/uksi/2017/752/contents/made

U.S. Congress. Gramm-Leach-Bliley Act. Title V. 15 U.S.C. § 6801 et seq. Federal Trade Commission. https://www.ftc.gov/legal-library/browse/statutes/gramm-leach-bliley-act

U.S. Federal Reserve Board. "Credit Reports and Credit Scores." Washington, D.C.: Board of Governors of the Federal Reserve System. Webpage viewed September 2022. https://www.federalreserve.gov/creditreports/pdf/credit_reports_scores_2.pdf

Watts, David, David Medine, and Louis De Koker. 2018. "Customer Due Diligence and Data Protection: Striking a Balance." Blog. Washington, D.C.: CGAP, 9 August. https://www.cgap.org/blog/customer-due-diligence-and-data-protection-striking-balance

Wolberg-Stok, Andres. 2022. "Open Banking Ecosystem and Infrastructure: Banking on Openness," in *Open Banking, edited by Linda Jeng, Chapter 1. U.S.: Oxford University Press, April.* https://doi.org/10.1093/oso/9780197582879.003.0002

Wong, Janis, and Tristan Henderson. 2019. "The Right to Data Portability in Practice: Exploring the Implications of the Technologically Neutral GDPR." *International Data Privacy Law, Volume 9, Issue 3, pp. 173–191, August.* https://doi.org/10.1093/idpl/ipz008

World Bank. 2011. "General Principles for Credit Reporting." Open Knowledge Repository. Washington, D.C.: World Bank, September. https://openknowledge.worldbank.org/bitstream/handle/10986/12792/701930ESW0P1180ting0pub010028011web.pdf?sequence=1&isAllowed=y

World Bank. 2022. "Technical Note on Open Banking: Comparative Study on Regulatory Approaches." January. https://openknowledge.worldbank.org/handle/10986/37483

CGAP members as of July 2022


CGAP
cgap.org