Open finance policy considerations

OECD

Please cite as: OECD (2023), *Open finance policy considerations*, OECD Business and Finance Policy Papers, OECD Publishing, Paris, https://doi.org/10.1787/19ef3608-en.

Open finance enables the sharing of, and access to, financial sector data. This paper analyses the benefits, risks and implementation challenges of Open finance and provides policy recommendations for the safe and successful implementation of such data-sharing frameworks in finance. It considers the impacts of providing access to customers' financial data and how to do this responsibly and safely, with due consideration for data privacy. The paper also discusses other consumer safeguards, notably related to consent and liability. Finally, it considers whether there is a need to support the development of technical infrastructure to promote data interoperability.

Foreword

This paper analyses benefits and risks of Open finance frameworks, discusses the main challenges to implementing such data sharing schemes, with due consideration to data privacy, and considers policy recommendations for the safe and successful implementation of such data sharing frameworks in finance.

The paper has been drafted by Iota Kaousar Nassr and Giuseppe Bianco under the supervision of Fatos Koc from the Division of Capital Markets and Financial Institutions of the OECD Directorate for Financial and Enterprise Affairs and Clarisse Girot from the Digital Economy Policy Division of the OECD Directorate for Science, Technology and Innovation. Eva Abbott and Andreia Furtado provided editorial and communication support.

The paper supports the work of the OECD Committee on Financial Markets, chaired by Aerdt Houben. and the OECD Committee on Digital Economy Policy, chaired by Yoichi Iida. It was first discussed by the Expert Group on Finance and Digitalisation, chaired by Aerdt Houben, and the Working Party on Data Governance and Privacy in the Digital Economy, chaired by Barbara Bucknell, in April 2023. This paper was approved and declassified by the OECD Committee on Financial Markets on 6 October 2023 and by the Committee on Digital Economy Policy by written procedure on 27 October 2023. It was prepared for publication by the OECD Secretariat. The authors gratefully acknowledge valuable input and constructive feedback provided by Delegates.

Table of contents

FIGURES

Executive summary

Data sharing arrangements in Open Finance[1] build on existing data sharing frameworks in Open Banking and expand data access and sharing to data sources beyond payment data (OECD, 2023[1]). This includes other areas of financial activity such as savings, credit, insurance, pensions and investments. Open Finance includes the sharing, access and reuse of personal and non-personal data for the purposes of providing a wide range of financial services (European Commission, 2022[2]). In addition to providing a secure and privacy-preserving framework where customers can consent to third parties accessing their data, Open Finance, similar to Open Banking, allows third parties to initiate payments, transactions or taking other related actions on the customers' behalf. There is no real separation between Open Banking- and Open Finance-related frameworks, and they can co-exist depending on the use cases.

Open Finance arrangements have multiple complementary objectives with common themes around: improving financial products and services; fostering customer empowerment and choice also about the use of their data; promoting innovation; and encouraging competition, all objectives found across OECD countries' frameworks. In terms of potential benefits, the development of new innovative products and services based on data access could improve customer choice in the wider financial space beyond banking and payments. The promotion of innovation can have a knock-on positive effect on competition conditions in financial services, especially through the de-monopolisation of data.

The potential benefits of Open Finance can only be achieved if these frameworks are built with safeguards in place to protect consumers, financial services providers, and markets, from old and newly emerging risks. These relate to: inappropriate data usage and handling; other risks to consumers; operational risks; risks to fair competition and possible systemic risks for specific types of use cases.

In particular, the wider sharing and reuse of personal data raise concerns for privacy and security. The offer of additional, tailor-made services relies on the availability of more personal data, sometimes across borders. Risks include the use of data for other purposes than those communicated to the customer, as well as data breaches and other incidents, which may also affect sensitive categories of data. Such perceptions of privacy risks are widely shared among financial consumers.

Open Finance frameworks need to be sufficiently attractive to participating firms and consumers to flourish in a sustainable manner. This means that three main pre-conditions may need to be satisfied[2]: (i) the right incentives need to be in place to attract participation from financial institutions and third-party providers (TPPs); (ii) customers need to have confidence in the safety, reliability, and fairness of the framework, and effectively reap tangible benefits from such frameworks; and (iii) some minimum level of technical interoperability must exist for data and infrastructure enabling data sharing (alongside regulatory interoperability among different frameworks).

[1] In the absence of a common typology of different Open Finance data sharing arrangements, the term Open Finance is used herein as a term broadly encompassing any Open Finance data sharing arrangements.

[2] Pre-conditions discussed herein are necessary, but not sufficient, conditions for such frameworks' success.

Satisfying the above pre-conditions dictates some design choices for Open Finance frameworks. The defining choice about any data sharing framework relates to the introduction of mandatory requirements based on regulatory action or voluntary data sharing arrangements themselves based on bilateral or multilateral contractual agreements between participants. There is no superior approach between the two, but it is important to consider that the drivers of data sharing arrangements will depend to a large extent on the chosen approach.

Under both approaches, but particularly in the case of voluntary schemes, the existence of the right incentives for participants is of paramount importance for the successful implementation of any data sharing frameworks. Incentives are needed to counter the costs that incumbents may need to pay for the development and maintenance of application programming interfaces (APIs) or other connecting interfaces for data sharing, and for the general upgrade of their systems to allow for the sharing of data in a digital format that can be used in such infrastructure. Examples of possible incentives can take the form of reciprocal data sharing and/or economic compensation. Non-economic incentives may also need to be considered for TPPs, for instance, associated with the quality and format of data received and the alleviation of technical friction.

Whether the implementation of an Open Finance framework is successful or not will depend to a large extent on user uptake. This, in turn, will depend on the level of trust that consumers will have in such frameworks and in the usefulness of the products or services built on data sharing. Key factors to build such trust are that: consumers need to be aware of their rights, first and foremost their right to consent or not to the opening up of their data; and they need to be made aware of, and be comfortable with, the conditions of such data sharing. In this respect, clear prior distribution of responsibilities and liabilities between all the parties involved with regard to the conditions of collection, processing and sharing of data is essential. This includes all aspects regarding processing, sharing, and storage of data including access, data quality, assessment of privacy and confidentiality risks, exercise of rights, as well as cyber security breaches. Overall, data sharing frameworks will need to be designed in a way that produces tangible benefits to individual users, with a view to incentivise take up and maximise the success of such frameworks.

Although the general objectives of data sharing and data protection frameworks, both in terms of protecting users and promoting innovation, are shared, in practice their interplay can raise complexities. Depending on the circumstances, regulations can be complementary and converge or they may include similar or identical expressions, but attribute different meanings to them. A data sharing framework may also broaden or introduce data protection provisions that would not be required otherwise, for instance where the general data protection legislation is less prescriptive or where the texts do not fully overlap. Furthermore, data privacy and security tasks are commonly split across different regulators under data sharing frameworks. These difficulties must be identified and remedied through co-operation between the actors involved, regulators, industry, and end users.

The long-term success of Open Finance may also depend on the level of interoperability achieved so as to support data sharing between service providers across different sectors and different countries (e.g. industry-led development of API standards) as well as on the existence of digital identities (ID).

1 Introduction

Open Finance could be described as the next stage in the evolution of Open Banking data sharing arrangements. Building on existing frameworks, Open Finance expands data access and sharing to data sources beyond payment data, while also including other areas of financial activity.

The results of the 2022 OECD Survey (OECD, 2023[3]) showcase the gradual evolution of Open Banking-related frameworks towards an expanded set of data types and other parts of the financial – and non-financial – sector, in what is being described as Open Finance. While this evolution is taking place at different paces, common themes appear across different OECD and partner economies approaches and experiences, and common risks and implementation challenges remain to be addressed.

Building on the results of the OECD Survey (OECD, 2023[3]) and the 2022 workshop "Data Portability in Open Banking: Privacy and Other Cross-cutting Issues", this paper provides further analysis on benefits and risks of Open Finance data sharing frameworks; analyses main challenges to the implementation of such schemes, including around incentives, governance, standards, and data protection; and provides some policy considerations on how to best address these challenges. The paper includes assessment of the benefits and risks of access to customers' financial data in a responsible and safe manner, particularly through the privacy lens; and discusses other consumer safeguards that need to be in place, particularly around consent and liability attribution. The paper also discusses whether there is a need to support the development of technical infrastructure that will promote data interoperability, without undermining the technology neutral approach to regulation that most OECD countries endorse.

2 Benefits and risks of Open Finance

Data sharing frameworks[3] in place, such as in Open Banking, are reported by OECD countries to have been producing positive impacts on customers and financial services, fostering innovation, increasing competition, lowering costs, and delivering better customer experiences (OECD, 2023[1]). The objective of extending Open Banking frameworks to more data sources and to the wider financial sector is to amplify potential benefits to customers, improving products, services and competition conditions in wider financial markets. However, such enhanced data sharing and usage may give rise to challenges and risks for customers and participating firms, in particular related to data privacy, security, and data misuse.

This Chapter provides an analysis of the possible benefits of Open Finance and corresponding risks arising from this type of framework, particularly when it comes to data privacy considerations.

Objectives and potential beneficial impact of Open Finance

The potential benefits of data sharing frameworks have been well established and documented (European Commission, 2018[4]; UK CMA, 2023[5]; OECD, 2023[6]; Banco Central do Brasil, 2023[7]; OECD, 2023[8]). Open Finance arrangements have multiple objectives with common themes around improving financial products and services and fostering customer empowerment and choice about their data; promoting innovation; encouraging competition, and these multiple objectives are found across the OECD countries' frameworks (OECD, 2023[1]). In the European Union (EU), for example, a broader data strategy aims to create a single market for data that will allow it to flow freely within the EU and across sectors for the benefit of businesses, researchers and public administrations, and will include non-financial sectors (e.g. medicine, transportation, public services) (European Commission, 2022[9]).

The development of new innovative products and services on the basis of data access could improve customer choice in the wider financial space beyond banking and payments. This relates to greater diversity of products available; enhanced personalisation when it comes to individually tailor-made solutions[4]; less costly products[5] when data use or reuse allows for efficiencies to be reaped; or extension of services to previously underserved parts of the population (e.g. credit scoring of SMEs). In the latter case, Open Finance frameworks can effectively promote financial inclusion for underserviced or financially excluded people.

Open Finance can offer new opportunities to inform consumers and support their decisions to subscribe to these services, for example, through facilitating comparison or to help when switching between financial

[3] For the purposes of this report, frameworks refer to laws and regulations applicable to data sharing, and arrangements may also involve bilateral/multilateral contractual arrangements in the absence of legal/regulatory frameworks.

[4] Open Banking and Open Finance can be a way to deliver hyper-personalisation, involving a combination of alternative and conventional data sources and the use of behavioural science to deliver services, products and pricing tailored to the needs of individual customer at any point in time.

[5] Indeed, lower prices have been observed in several OECD countries for specific financial services (e.g. lower fees) (OECD, 2023[1]).

products and services. Client empowerment is being sought as financial services customers gain control over their data and decide on which data they provide under such data sharing arrangements. Benefits can also feature potential use cases of packaging financial data for consumers in a helpful way which is easier to understand for consumers. Some examples include financial management for businesses, tax estimation and future in- and out-goings and ways for them to browse between loan/credit offerings by different providers. New applications built on data access can help customers keep to budgets, reduce unnecessary expenditures, switch products or providers ('shop around'), minimise fees/charges and make better-informed decisions. Open finance frameworks can be beneficial to customers including by reducing the bureaucracy and friction, by providing a more seamless and smooth process for switching services/ providers, thus reducing the time and the effort it would usually take.

The promotion of innovation can have a knock-on positive effect on competition conditions in financial services, in particular through the de-monopolisation of data. Open Finance frameworks encourage the emergence of TPPs, such as FinTech start-ups, to offer existing services in a different way, or to provide new services to customers on the basis of data access. The impact of such frameworks on the FinTech industry can already be observed in regard to both growth and diversity of companies active in several OECD countries (OECD, 2023[1]). The emergence of new participants could also be expected, as was the case in the Open Banking frameworks in certain jurisdictions (account information service providers or aggregators), while such frameworks could also result in greater and closer co-operation between banks and other financial institutions on the one hand and FinTechs and other TPPs on the other.

Box 2.1. Open Finance use cases

The establishment of Open Banking and other data sharing frameworks has contributed to the emergence of various active use cases in a large number of areas within the financial services space, primarily found in the payment space (e.g. payment account information services, aggregation services, as well as payment initiation services).

Open Finance is expected to allow for new or improved financial products and services and a higher level of personalisation of services offered to consumers across a wider range of financial services or products. These could expand the already available products built on payment account information, such as enhanced credit scoring tools or wealth management applications, alternative payment services, product comparison or debt management tools.

Examples of use cases include:

- Personal financial management dashboards;
- Pension dashboards, enabling customers to access data about all their pensions (occupational, workplace, personal and state) in one place;
- Creditworthiness assessments with improved accuracy and/or allowing for credit scoring in 'thin file' customers without prior credit history or collateral;
- Improved financial advice and support, including improved risk management or tax optimisation;
- Aggregation of insurance services data into a single location to perform financial projections, risk assessments, and cash flow projections. These calculations assist with identifying the appropriate insurance products and the appropriate duration of these products, based on the consumers' specific needs;
- Bespoke and on-demand insurance;
- Easier switching between products or providers;
- Building of artificial intelligence and machine learning models that can be used as a basis for financial services, including for example more accurate risk management;
- Sweep accounts through variable recurring payments (moving funds between customer accounts when triggers occur);
- Utilities or public administrations sending payment requests without the need for card provider intermediaries (e.g. HM Revenue and Customs in the United Kingdom);
- Energy-related and climate data feeding into financial services.

Source: (European Commission, 2022[2]), (Capgemini, 2023[10])

Key risks and challenges of Open Finance

The potential benefits of Open Finance can only be achieved if Open Finance frameworks are built with safeguards in place to protect consumers, financial services providers, and markets from the variety of risks arising from such activity. These risks can be attributed to different parties in the ecosystem (users, TPPs, etc.) and/or concern some or all of them. Overall, these risks relate to: inappropriate data usage

and handling; privacy leakage and unauthorised surveillance; other risks to consumers; operational risks; risks to fair competition, and possible systemic risks for specific types of use cases.

Inappropriate data usage and handling

Open Finance frameworks must address all the underlying risks of inappropriate data handling or misuse, given the quantity and diversity of data subject to sharing, use and re-use in such frameworks, and the complexity of sharing mechanisms, both in terms of regulatory frameworks, and in terms of operational mechanics (infrastructure level). The frameworks must take into account the diversity and the sophistication of these risks, which are of various types and concern all parties involved in the Open Finance ecosystem.

Data integrity and quality is of paramount importance: the use of poor-quality data by TPPs (outdated, incorrect, flawed or incomplete data) is a source of risk for, among others, consumers as this use may result in questionable outcomes. This translates into sub-optimal or outright wrong product choice (e.g. wrong investment advice for the specific user profile; switching to an inferior product; or receiving wrong pricing).

The inappropriate use of certain data (e.g. around gender, ethnicity) may result in biased, discriminatory or unfair decision-making, ultimately harming through the overcharging or unjustified exclusion of some people from certain financial services (OECD, 2021[11]). It should be noted in this regard that some data can be used to infer other data, insights or individual attributes that can be considered as sensitive and therefore attract reinforced protection by law (for example, inferring gender by looking into purchasing activity data) (OECD, 2021[11]).

Additional risks related to the quality of data arise in the case of synthetic data or other proprietary datasets produced by TPPs on behalf of the customers, and which are controlled by the TPP. Synthetic data is artificial data generated from original data and a model that is trained to reproduce the characteristics and structure of the original data, with potential for enhanced privacy, lower cost and improved fairness. Issues arising in the creation and use of synthetic data include representative and completeness of data, and risks such as bias and discrimination e.g. in the use in artificial intelligence-driven models (OECD, forthcoming).

Other consumer risks

Risks of exclusion may also be due to the digital divide. The latter is understood as designating different levels of access and use of information and communication technologies (ICTs) and, most often, gaps in access and use of internet-based digital services (González Fanfalone et al., 2021[12]). The digital divide could be associated with limited infrastructure (e.g. broadband access)[6], gender or age differences between consumers, for instance.

Other consumer risks are similar to those arising in all digitally-enabled financial intermediation. They relate to the over-simplification of product comparisons and to sub-optimal product selection (OECD, 2020[13])[7] or to the lack of support for complex decisions, particularly for those customers with lower levels of financial and/or data literacy or awareness. For example, in the case of insurance products, market fragmentation

[6] The differences of broadband connectivity between countries are significant: for example, in 2019 the average rate of fixed broadband subscriptions per 100 inhabitants in G20 countries (19.6) was 2.6 times that of the rest of the world (7.5) (OECD, 2021[93]).

[7] Consumers may focus more on the price as the single criterion of their choice, under the false assumption that all contracts proposed have the same terms and conditions (e.g. exclusions, excesses, other services offered) and differ only in price. This becomes problematic for users when the aggregator does not provide clear information on all product features and exclusions in a consistent manner or does not explain the differences in cover that may drive the price differential.

may mislead the consumer about the ultimate insurer responsible for risk coverage (EIOPA, 2022[14]). Auto-switching services could lead to consumers becoming focused solely on price over other factors affecting suitability (FCA, 2019[15]).

Similarly, the availability of granular consumer data may also increase the use of price optimisation practices when setting insurance premia, which can lead to potentially unfair treatment of some groups of consumers (EIOPA, 2022[14]). This could be particularly concerning where the groups of consumers that suffer most are more vulnerable consumers (e.g. elderly, low income), or are suffering because of potentially unfair discriminatory practices.

Price differentials or outright exclusion can also occur in cases where consumers opt out of data sharing frameworks. Access, use and re-use of customer data needs to be done in a safe manner and with appropriate informed customer consent. Where customers choose not to allow TPPs to access their data, a 'privacy premium' may apply, with customers getting less advantageous pricing. Such privacy premia, i.e. excessive differentiation in pricing based on a consumer's willingness to share data, has been raised by certain consumer protection organisations and regulators (FCA, 2019[15]). Available empirical research has found evidence that participants presented with prominent privacy information are more likely than those in the other conditions to pay a premium to purchase from sites that have better privacy policies, whereas, in the absence of prominent privacy information, people purchase where price is lowest (Tsai et al., 2011[16]). Yet, there may also be a need for further studies to detail better the significance of such privacy premia.

A wider issue is the externalities that may occur when one data owner shares their data, and such sharing also reveals insights about other data owners who have not made their data available. Some customers' decision to share their personal information may allow the parties accessing the information to know more or better about others, who choose not to share their information (MacCarthy, 2011[17]; Choi, Jeon and Kim, 2018[18]). These externalities can reduce the value of non-shared data and could form the basis for price differentiation. Potential ways to avoid them include de-correlation techniques that reduce insights about data owners who have not shared their data, while maintaining valuable signals of data analysis; and the reasonable use of data (e.g. what data is reasonable for what processes; and what level of exclusion/differentiation is ethical).

Operational risks

Cybersecurity, privacy and operational risks and outright fraud are some additional risks in the discussion related to data management and usage. Such risks increase if financial service providers, including TPPs, do not have the appropriate security systems in place to protect customer data. Concerns about the security and wider operational resilience of participating firms are on the rise, given the operational changes to their IT systems required to support Open Finance, as well as increased complexity and interconnectedness of the relationships of parties involved (FCA, 2019[15]). Operational risks may also rise from poor governance, risk and process controls of participating firms. Operational risks and risks of fraud are also present in the initiation of payments, either where payments may be accidentally misdirected or in case of scams or financial crime (the latter being particularly important for the potential cross-border implications and the need for international alignment in approaches). Concerns arise when it comes to small FinTech companies that may not have sufficient defences to protect consumers against the abovementioned risks, due to their limited operational capacity.

Risks to fair competition

Fair competition risks relate to possible market dominance by certain actors, as well as risks of an unlevel playing field depending on the conditions of data sharing. To mitigate this particular risk to competition, the regulator has a critical role in maintaining a level playing field and ensuring equity and equality among

financial service providers, including both incumbents and new entrants, and consumers. BigTechs are the prime example of market participants who can leverage their access to vast sets of customer data, raising questions about possible anti-competitive behaviours and market concentration both in terms of unequal and unfair data access, and in terms of the operational aspect of service provision (e.g. cloud services) (OECD, 2021[11]). Similar concerns may arise when API aggregators dominate the market, imposing practices and pricing that may lead to the exclusion of small companies from participation. This, in turn, would hinder competition and disincentivise small firms and start-ups from establishing activity in this sector. Similarly, the lack of reciprocity in data sharing is a key consideration that may result in a lack of incentivisation of relevant data holders to fully participate in voluntary Open Finance-related arrangements. It should be noted that, ultimately, it should be up to the customer to decide which data is shared with whom.

Risks of changes in customer preferences away from data sharing also exist, for example through a change of culture and a subsequent shift in preferences towards privacy. This means costs incurred to build the infrastructure required, without having demand for the services. Over-estimating customer demand for data sharing and building an expensive data sharing/standards infrastructure could, in turn, increase the costs of doing business for firms (depending on who bears the cost), leaving a market less efficient and less competitive, with a data sharing infrastructure that customers end up not using. Commercial incentives, market forces and cost-benefit analyses can mitigate against this risk if incorporated properly.

Possible systemic risks

Concerns about potential systemic risk may arise in case of increased concentration in the market linked to the dominance of some firms benefiting from Open Finance, as well as in cases where it could have an impact on the resilience of financial institutions and the stability of their funding. The two scenarios are interlinked: firms using their dominance in an Open Finance environment may drive concentration in the market instead of diversification. Such dominance could reduce the resilience of financial institutions, either by affecting their profitability or by reducing their funding stability. Similar effects could be produced if incumbent financial institutions lose large parts of their funding base to new TPPs and/or if such TPPs provide bank-like services without operating under the regulatory framework for such services. Innovative solutions enabled by Open Finance, such as sweep accounts (see Box 3.1), which allow for the automated transfer of funds between customer accounts when triggers occur, could also have similar consequences for the funding of financial institutions in the scenario of a significant size of withdrawals happening simultaneously, with limited visibility for the financial institution to predict such fund moves. In addition, asymmetrical information access requirements could tip the market to the benefits of few, bigger players whose size and complexity could potentially create systemic vulnerabilities.

Data protection and privacy-related risks and challenges

With the sharing and reuse of larger sets of data among a wider number of entities that Open Finance allows, privacy risks become potentially prominent. This stands in stark contrast with cash payments, which guarantee full anonymity and need no personal data.

After the adoption of some form of Open Finance measures, problems affecting privacy and security arise. This can result in harm to individuals and organisations, hinder Open Finance implementation or create tension between different legal obligations (Future of Privacy Forum, 2022[19]). For example, due to single-factor authentication systems, some Japanese digital payment service providers have suffered serious privacy and digital security incidents (e.g. an unauthorised withdrawal from an open banking account due to a digital security vulnerability).

As Open Finance enables more online transactions to take place, frauds can also potentially increase. To combat such frauds, more checks are imposed, which in turn require the processing and combination of more data (CNIL, 2021, p. 41[20]). Consequently, more data are provided and shared among participants.

Furthermore, Open Finance, just like Open Banking, is intended to facilitate the provision of additional services for customers. To achieve such objective, the trend is to enrich payment data so that more services can be offered, for example reconciliation and billing automation (CNIL, 2021, p. 48[20]). The overall result is an increase in the volume and the cross-referencing of data in circulation, which heightens the risk for the privacy of individuals (Banque de France, 2022[21]). As data often travels across national boundaries, the enforcement of laws protecting privacy can become more difficult. In this respect, the OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy provides a basis to foster international co-operation among Privacy Enforcement Authorities to address the challenges of protecting the personal information of individuals wherever the information or individuals may be located (OECD, 2007[22]).

Different kinds of personal data processing are involved in Open Finance. Some of these data can be sensitive or pertain to special categories of data in the meaning of the OECD Privacy Guidelines or data protection legislations like the GDPR in the EU. This includes, for example, transaction data that can reveal information about membership of religious institutions, political parties or trade unions. For such data, data protection authorities can consider that data subjects have a reasonable expectation that their data will not be processed for other purposes (Huysmans, 2019[23]), and that strict compliance with the principles of necessity and proportionality is required for the legal provisions that govern the processing of such data (EDPS, 2023[24]).

Indeed, the risk could be that users' data shared with third parties is used for other purposes than those requested or that it is obtained through misleading tactics, especially by firms whose surveillance revenue models incentivise them to use and abuse consumer data (CFPB, 2022, p. 5[25]). This would lead to a lack of trust and a sense of powerlessness by consumers. In addition, customers may receive no or unclear notices, and thus not understand how their personal data is going to be used.

This is reflected in the public's perception of risk. Responses to a consultation launched by the European Commission indicate that 84% of the responders believe there are security and/or privacy risks in giving service providers access to their data. Also, 57% do not believe that financial service providers that hold their data always ask for consent before sharing that data with other financial or third-party service providers (European Commission, 2022[26]).

3 Implementation challenges and design choices

Open Finance frameworks need to be sufficiently attractive to participating firms and consumers in order to flourish in a sustainable manner. This means three main groups of pre-conditions need to be satisfied: (i) the right incentives need to be in place to attract financial institutions and TPPs; (ii) customers need to be able to trust and have confidence in the safety and fairness of the framework; and (iii) some minimum level of security and privacy-aware interoperability must exist for data and infrastructure enabling data sharing.

Satisfying the above pre-conditions dictates some design choices for Open Finance frameworks. The defining choice about any data sharing framework relates to the introduction of mandatory requirements based on regulatory action or voluntary data sharing arrangements built on the basis of bilateral contractual agreements between participants. This Chapter discusses some of the challenges to Open Finance implementation relating to: the incentivisation of participants; the strengthening of consumer trust, primarily through appropriate measures to ensure data security and privacy; the level of secure and privacy-preserving interoperability of data and infrastructure, including through harmonisation and standards; as well as the existence of portable digital identification. It discusses the difference in drivers of data sharing arrangements and analyses design choices affecting such drivers.

Voluntary and mandatory nature of data sharing

There are two main design approaches to data sharing frameworks in OECD countries: the market-led approach or voluntary framework (e.g. US, Switzerland), and the more prescriptive approach where data sharing is imposed by regulation (e.g. EU PSD2). There is no superior approach between the two, but it is important to consider that the drivers of data sharing arrangements will depend to a large extent on the chosen approach.[8]

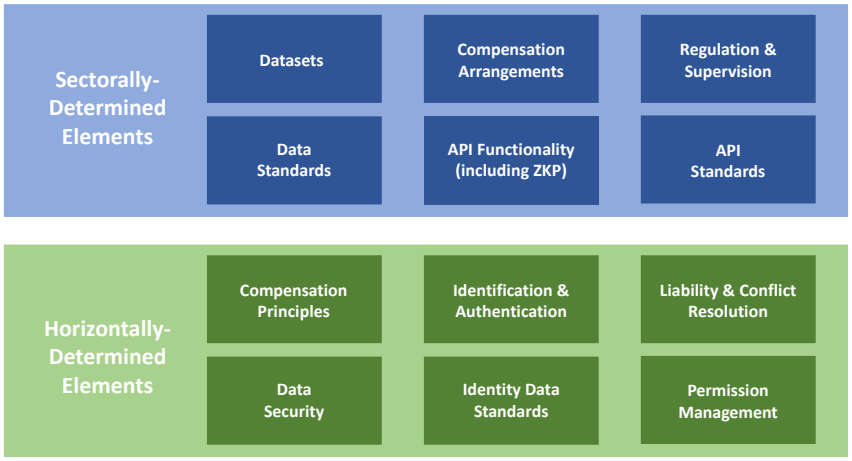
[8] At the time of writing of this report, the US Consumer Financial Protection Bureau (CFPB) proposed a Personal Financial Data Rights rule, aiming at accelerating a shift towards open banking and requiring companies to share data with other companies at the person's direction, for the person's own preferred purpose. The proposed Personal Financial Data Rights rule would protect the interests of both consumers and financial firms through robust protections to prevent unchecked surveillance and misuse of data; meaningful consumer control; a move away from risky data collection practices, and with fair industry standard-setting. Under the proposal, the requirements would be implemented in phases, with larger providers being subject to them much sooner than smaller ones. In addition, the community banks and credit unions that have no digital interface at all with their customers would be exempt from the rule's requirements. The proposed rule is the first proposal to implement Section 1033 of the Consumer Financial Protection Act, which charged the CFPB with implementing personal financial data sharing standards and protections. The CFPB intends to cover additional products and services in future rulemaking (CFPB, 2023[91]).

In countries or regions where data sharing initiatives are prescribed by regulation, the primary motivation for data holders to share data is the need to comply with the legal requirement.[9] This is the case, for example, of account servicing payment service providers (ASPSPs) in the EU, most commonly banks, which previously held the monopoly on payment account data and payment services. In the absence of mandatory regulatory frameworks, incumbents may be reluctant in opening up their data, especially if they consider the relative upside for them to be limited. Reciprocity in the sharing of consumer data between all market participants, which in turn would level the playing field, could also be one of the aims of data sharing frameworks, such as in Open Insurance frameworks (EIOPA, 2022[14]).[10]

In both cases, but particularly in the case of voluntary schemes, the existence of the right incentives for participants is of paramount importance for the successful implementation of any data sharing framework. Data holders incur ex-ante and ongoing costs to store, process, maintain and transfer data, and there may be a need to consider the fair and proportionate allocation of costs among participants in data sharing schemes. Incentives are needed to counter the costs that incumbents may need to pay for the development and maintenance of APIs or other connecting interfaces for data sharing, and for the general upgrade of their systems to allow for sharing of data in digital format that can be used in such infrastructure.

It should also be noted that there may be merit in establishing a horizontal basis that harmonises requirements for various elements of data access across sectors, in order to facilitate data sharing across sectors and ensure commonality in data access (DNB and AFM, 2023[27]) (see Figure 3.1). This can include: compensation principles, in case of economic incentives; data security; liability and conflict resolution, for example (DNB and AFM, 2023[27]).

Figure 3.1. Sets of sectorally and horizontally determined elements



Source: (DNB and AFM, 2023[27]).

Incentives: reciprocity of data sharing and compensation

Incentives play an important role in the success of data sharing frameworks. The OECD Recommendation on Enhancing Access to and Sharing of Data highlights the importance of providing coherent incentive mechanisms and promoting conditions for the development and adoption of sustainable business models and markets for data access and sharing (OECD, 2021[28]). Examples of possible incentives in Open

[9] In some jurisdictions, a consultative approach is adopted within such mandatory approach (e.g. Brazil), where the industry is actively consulted on the design of the mandatory framework.

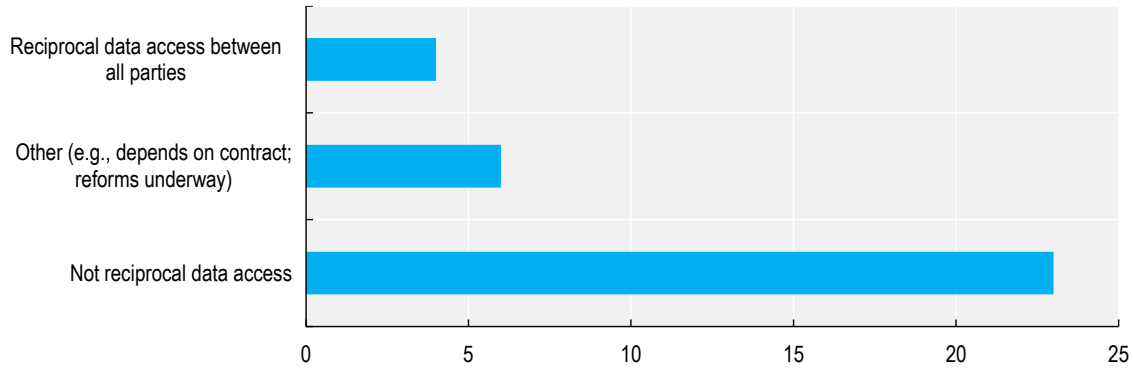
[10] It should be noted that, ultimately, it should be up to the customer to decide which data is shared with whom.

Finance can take the form of reciprocity of data sharing and/or economic compensation. Reciprocity, intended as reciprocal access to customer data between all parties under Open Finance data sharing frameworks, exists in a minority of the OECD countries that have data sharing arrangements in place (Figure 3.2) (OECD, 2023[1]). In other cases, reciprocity depends on the financial institution and the technology service provider relationship and/or on the contractual relationship between the relevant parties in such arrangement. Without reciprocity, banks and other incumbent firms have less of an incentive to invest in the delivery of infrastructure such as APIs. Even in case of regulatory requirements for data sharing and for the delivery of such infrastructure, the absence of any commercial incentives for firms may result in malfunctioning or underperforming data sharing infrastructure or in the lack of its maintenance. Both these sub-optimal results have been anecdotally reported by FinTechs as issues impeding their accessibility to data under existing arrangements.

Reciprocity in data sharing can constitute a powerful incentive particularly when it aims at being cross-sectoral, in other words when it extends beyond the financial sector. Cross-sectoral reciprocity is most valuable when it increases not just the amount, but also the variety of data to which (financial) entities have access. Moreover, cross-sectoral reciprocal approaches also increase the value of data sharing as they enhance the number and complexity of data sharing use cases. This is of particular relevance with respect to Internet of Things (IoT)-generated data, platform (BigTech) data, and utilities data (particularly useful for environmental, social, governance (ESG) objectives). It should be noted that, ultimately, it should be up to the customer to decide which data is shared with whom.

Non-economic incentives may also need to be considered for TPPs, and may involve the removal of friction and blockers to access to customer data. By way of example, TPPs requesting data from an ASPSP (bank), but with the obvious caveat of framework/arrangements in place and consumer protection. Some of these incentives could relate to the alleviation of technical frictions and others to the quality and format of data received, or whether it is standardised (e.g. error codes).

Figure 3.2. Reciprocity in access to customer data for all parties involved in data sharing



Note: Based on 34 responses to the OECD Survey.
Source: (OECD, 2023[1])

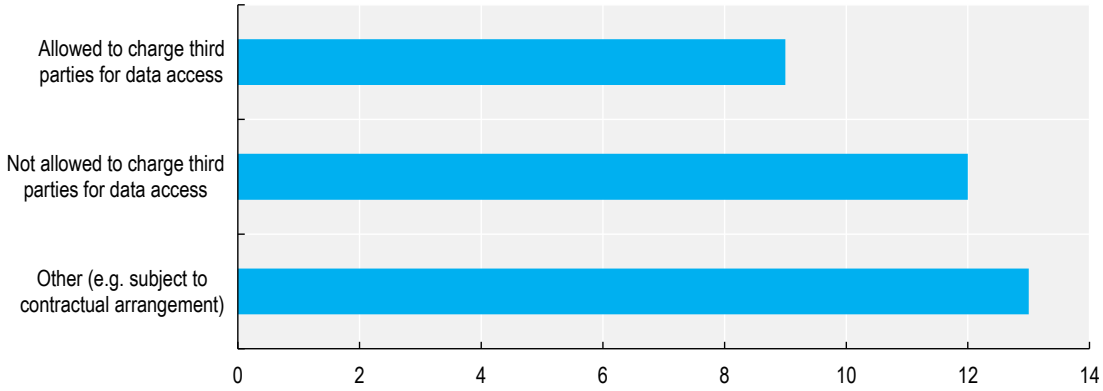
Economic incentives, such as compensation for data access, are another key issue that relates to the motivation for banks and other ASPSPs to open their data to TPPs and to face the cost associated with such access provision. There is currently great divergence in the way compensation is tackled in data sharing frameworks in OECD countries (Figure 3.3) (OECD, 2023[1]). In countries where data sharing is based on bilateral contractual arrangements, possible fees are defined alongside other terms in such contracts (e.g. Japan, US or tiered pricing system as in Brazil). In countries with explicit frameworks, fees are either fully prohibited (e.g. Chile) or allowed under certain circumstances (e.g. for 'premium' solutions).

In the EU framework, regulation prescribes banks and other ASPSPs to make their data available without compensation. Banks may not require contracts with – nor charge – the TPP to have account access. Data sharing free of charge responds indeed to limitations that SMEs (such as small FinTechs and other TPPs) may have in their ability to compensate banks and other ASPSPs for data. However, the success of Open Finance will also depend on having high quality APIs for the sharing of data and on firms having commercial incentives to invest and participate in the Open Finance ecosystem (EBA, 2022[29]). This includes, *inter alia*, incentives for financial institutions to develop high quality APIs as a foundation for Open Finance. To that end, the recent Open Finance proposal of the European Commission introduces compensation for data access. This will allow market participants to recover costs incurred by the requirement to provide technical interfaces for data access (APIs). In addition, based on the same proposal, SMEs acting as data users will be able to access customer data against a reduced compensation, capped at cost (Article 9(2) of the Data Act proposal) (European Commission, 2023[30]).

It should also be noted that there are exceptions to the free of charge rule for 'premium' solutions that can be charged, even under PSD2 in the EU context. In particular, the European Payment Council (EPC) is working on a SEPA Payment Account Access (SPAA) that also takes into account that ASPSPs are able to provide innovative 'premium' solutions (e.g. services that go beyond the PSD2 legal baseline) to TPPs, which can be charged. In that sense, such other data access, beyond payment account data sharing, is based on contractual arrangements. Pilots of new premium APIs are also envisaged in the UK, based on a multilateral commercial agreement (JROC, 2023[31])

A number of principles could be considered for the definition of a fair compensation scheme that would allocate costs fairly among participants while safeguarding fair competition (European Commission, 2022[2]). These would include the principle of proportionality so as not to impede smaller firms from accessing data, while also protecting against anti-competitive behaviours.

Figure 3.3. Charging third parties for data access



Note: Based on 34 responses to the OECD Survey.
Source: (OECD, 2023[1]).

Building customer trust: data protection and liability frameworks[11]

Whether the implementation of an Open Finance framework is successful or not will depend to a large extent on user uptake. This, in turn, will depend on the usefulness of the products or services built based

[11] Customer and consumer are terms used interchangeably in this report.

on data sharing and on the level of trust that consumers will have in such frameworks. Consumers will derive trust in the frameworks in large part based on the level of protection they feel they are afforded.

The OECD's approach to financial consumer protection is set out in G20/OECD High-Level Principles on Financial Consumer Protection (FCP Principles) (see Box 3.1). The FCP Principles can be applied to Open Finance frameworks and provide a structure to aid in the analysis of policy approaches to protect consumers and build their trust. While all the FCP Principles are relevant to the provision of Open Finance services as any other financial product or service for consumers, two of them are especially relevant to the policy considerations raised, i.e.:

FCP Principle 10 (Protection of Consumer Assets against Fraud, Scams & Misuse) specifies among other things that oversight authorities and financial services providers should develop and implement mechanisms to protect consumers' assets from *inter alia* digital security risks and should include "clear and transparent liability arrangements between financial services providers and consumers in the event of financial loss";

FCP Principle 11 (Protection of Consumer Data & Privacy) specifies that consumers' financial and personal information should be protected by mechanisms which *inter alia* "should define the purposes for which the data may be collected, processed, held, used and disclosed (especially to third parties), […] should acknowledge the rights of consumers regarding consenting to data sharing, accessing their data, being informed about breaches impacting their data, and seeking redress such as the prompt correction and/or deletion of inaccurate, or unlawfully collected or processed data."

Box 3.1. G20/OECD High-Level Principles on Financial Consumer Protection (updated in 2022)

The G20/OECD High-Level Principles on Financial Consumer Protection were originally endorsed by G20 Leaders in November 2011, and adopted by the OECD Council in the form of a Recommendation on 17 July 2012 (OECD, 2022[32]). The FCP Principles were comprehensively reviewed and updated over the course of 2021-2022 by the Task Force on Financial Consumer Protection (Figure 3.4)

Figure 3.4. G20/OECD High-Level Principles on Financial Consumer Protection (updated in 2022)

Source: (OECD, 2022[32])

The FCP Principles are the international standard for effective and comprehensive financial consumer protection frameworks. As a high-level standard, the FCP Principles are specifically designed and intended to be applicable to any jurisdiction and are cross-sectoral in nature (i.e. they can be applied to credit, banking, payments, insurance, pensions and investment sectors). Many countries, including all OECD, G20 and Financial Stability Board (FSB) jurisdictions, have adopted the FCP Principles in establishing or enhancing their financial consumer protection frameworks.

The updated FCP Principles specifically recognise the impact, opportunities and risks of digitalisation and technological advancements for financial consumers, included as a new cross-cutting theme relevant to each and all of the FCP Principles. Digitalisation in this context includes such things as considering the ways that consumers increasingly interact with digital financial products and services.

Overall awareness of consumers about data sharing arrangements varies. As data sharing happens at the back end of the product construction, the end user is not necessarily aware that the product is offered thanks to Open Finance. Payment initiation services are a great example of this: users may appreciate the innovative use case and the functionalities offered; however, they are not necessarily aware that this is made available thanks to a data sharing framework.

Nevertheless, consumers need to be aware of their right to consent or not to the opening up of their data, and they need to be comfortable with the conditions of such data sharing, in order to build trust around the framework. Financial services providers should ensure that requests for consent to collect, store and use personal data in relation to a financial product or service are clear and understandable in the interest of ensuring informed consent about their data at a relevant time and context.[12] Requests for consent should be as clear and understandable as possible and avoid language or terminology that are excessively legal, technical or specialised (OECD, 2020[33]). Recognising that consent-based models may be limited due to lack of consumer understanding or reading of terms and conditions in privacy notices, more needs to be done to ensure effective privacy, notably by adopting privacy by design, and especially data minimisation (OECD, 2020[33]) (see the next subsection below).

In addition, as with any digitally-enabled financial product, financial literacy efforts and consumer awareness campaigns are also important in order to convey the message around the importance of consent and the overall data rights of the user.

Clear liability attribution in case of data-related issues with respect to access, quality, privacy and confidentiality, processing, sharing, and storage of data as well as cyber security breaches can be conducive to building consumer trust. Attribution of liability is a complex matter that is often resolved on a case-by-case basis given the different authorities involved; any provisions of data sharing arrangements need to be consistent with existing data protection regimes and possible contractual arrangements that may be used for data sharing, depending on the case (OECD, 2023[1]). Attributing liability to the entities with which consumers directly interact may be particularly helpful to help them navigate this environment (Medine and Plaitakis, 2023[34]). Liability-related provisions need to also include frameworks for complaint handling and redress and dispute resolution mechanisms for out-of-court settlement of disputes (OECD, 2023[1]) and at the cross-border level. At the moment, rules around liability attribution are fragmented across regulatory jurisdictions, and any lack of clear liability frameworks may have an impact on consumer uptake and confidence, while further complicating any dispute resolution at the cross-border level (OECD, 2020[35]).[13]

Authorisation and/or other supervisory requirements for financial data intermediaries can also improve the level of comfort for consumers participating in Open Finance ecosystems. TPPs are required to be licensed to access consumer data[14] and/or initiate payments in most, but not all, OECD countries. As Open Finance frameworks can extend the type of services TPPs or similar actors can undertake, similar extensions may need to be considered to be applied to the terms of the authorisation of such participants (e.g. insurance brokerage).

[12] As set out in policy guidance developed by the G20/OECD Taskforce on Financial Consumer Protection relating to Protecting Consumers' Assets, Data and Privacy to support the implementation of the FCP Principles.

[13] The *Compendium of Effective Approaches for Financial Consumer Protection in the Digital Age* sets out examples of how policy makers and oversight authorities have worked to ensure that the application of arrangements for limitations on liability of financial consumers for fraudulent or unauthorised transactions extends to new types of mobile or online transactions (for example "push payments") (OECD, 2020[35]).

[14] With consumers' explicit consent.

The data protection angle to building trust

Open Finance frameworks raise a variety of data protection, privacy and security concerns. Consequently, ensuring high levels of data protection and security is a key objective for Open Finance frameworks.

Introducing strong safeguards for data protection and data security helps to build trust and provide control to users. Consequently, the parties to Open Finance frameworks must ensure compliance with all applicable data protection principles and rules in order to facilitate the uptake and use of digital financial products (World Bank Group; Ministry of Foreign Affairs of the Netherlands, 2021[36]), such as for Open Finance.

The protection of personal data is ensured by compliance with a series of global principles and concepts that have been codified by law and practice over time. These can be found in international standards such as the OECD Privacy Guidelines (OECD, 1980, 2013[37]), recognised as the global baseline for data protection, as well as in virtually all domestic and regional legal frameworks. The most relevant of these principles to ensure data protection in Open Finance frameworks, including the clarification of roles and data protection responsibilities, purpose limitation and related principles (including data minimisation and data retention), privacy by design and by default, accountability, and data security, are mentioned below.

Clarification of roles and data protection responsibilities. The roles of the entities involved in Open Finance (OECD, 2023[8]) need to be clearly identified from the perspective of data protection in order to determine who shall be responsible for compliance with different data protection rules, and how individuals can exercise their rights in practice. The OECD Privacy Guidelines, like most data protection laws around the world including the EU GDPR, use the terminologies of data controllers and data processors for this purpose (EDPB, 2020[38]). One or more parties decide on the purpose and the modalities of the processing of personal data and are defined as “data controllers” in some data protection legislations. A different party may process the personal data on behalf and under the authority of the data controller, and would be defined as “data processor”. Each party would have different obligations and responsibilities with regard to the processing of personal data, and needs to abide by existing privacy and data protection legislation.

Purpose limitation principle. The purpose for the collection and processing of personal data needs to be clearly determined. Such purpose cannot lie only in the objective to amass more data for potential future uses (CNIL, 2021, p. 56[20]). The purpose of collection and processing must not go beyond what is reasonably necessary to provide the product or service the customer has requested (CFPB, 2022, p. 40[25]). Sometimes the data sharing framework regulates the scope of, or the conditions for the potential use of data for other purposes. For instance, the Israeli Account Information Service Law provides that the use of data for statistical purposes related to the provision of an Open Banking service for other customers is subject to the customer’s explicit consent in writing (OECD, 2023[8]). Flowing from the purpose limitation principle, the principle of data minimisation requires that the collection and processing of personal data be limited to what is necessary in relation to the purposes for which it is processed. To minimise personal data processing, data controllers could use anonymisation or pseudonymisation[15] wherever possible (CNIL, 2021, p. 56[20]). In addition, data should be kept only for the time needed to fulfil the purpose for which the information was collected (data retention principle).

Privacy by design and by default. Open Finance frameworks should incorporate the concepts of privacy by design and by default. Privacy by design demands that technologies, processes, and practices to protect privacy be built into system architectures, rather than added on later as an afterthought (OECD, 2013[39]). Privacy by default entails that, when a product or service is made available to the public, the highest privacy settings should apply by default, without any manual input from the end user. Some proposals for Open

[15] Pseudonymisation consists in transforming data so that it can no longer be attributed to a specific data subject without resorting to additional information (CNIL, 2021[20]).

Finance frameworks already recognise the need to embrace and spell out privacy by design and by default (European Commission, 2022[2]).

Accountability. Accountability comprises the taking of responsibility for personal data use and a means to demonstrate this to other stakeholders, and encompasses the notion that the organisation is legally responsible for its data protection practices including before the judicial system (OECD, forthcoming[40]).[16] A privacy management programme should ensure the organisation's accountability, and include governance measures (e.g. internal oversight, organisational structure, process controls, definition of roles and responsibilities, and training for individual actors) and technical measures (e.g. access control to data). The programme should be tailored to the structure, scale, volume and sensitivity of the organisation's operations concerning personal data and rely on privacy risk assessments.

Data security. Data sharing regulations need to ensure that those entities that obtain users' data guarantee appropriate data security against risks such as loss or unauthorised access, destruction, use, modification or disclosure of data. This entails a duty of confidentiality, integrity and availability. The duty of confidentiality, in the Israeli Account Information Service Law, is spelled out as mandating account information service providers to maintain in confidence all information about the customer, including documents transferred to their possession and the contents thereof, and all other details referring to the activities it performed as part of the services it rendered to the costumer (article 23). Sometimes data sharing regulations impose on third parties the same safeguards that the financial institutions (from which the data originates) comply with. For example, in the US the Consumer Financial Protection Bureau is considering mandating third parties to comply with the Gramm-Leach-Bliley Act safeguards framework[17] that is applicable to financial institutions (CFPB, 2022, p. 46[25]).

It should be noted that there is strong convergence between data sharing frameworks and data protection regulations in limiting practices that may threaten data security, as the framing of data scraping exemplifies. Before the implementation of Open Banking frameworks, third parties would often use web scraping techniques. This consists of the collection of their customers' bank identifiers and their use to connect to their customers' online banking to retrieve account or transaction statements (CNIL, 2021, p. 65[20]). Screen scraping often comes in the form of user-not-present personal financial management services, which rely on frequent monitoring of balances and transactions to give warnings to consumers (e.g. of the fall in an account balance or of an unusually large transaction) (CFPB, 2022, p. 63[25]).

While web scraping is easy to implement and ensures accuracy of data, it features no revoking rights and requires that customers share their usernames and passwords (World Bank Group; Ministry of Foreign Affairs of the Netherlands, 2021[36]). Consequently, this technique presents risks for security and data storage. The third party, in theory, could access information other than that for which it had been authorised, the customer's credentials could be stolen or used for fraudulent purposes, and screen scraping makes it harder for the bank to distinguish between the customer and a third party, which impairs the bank's ability to identify fraudulent transactions (Pellitteri et al., 2023[41]).

In the EU, PSD2 has made APIs the default option and left screen scraping as a fallback mechanism when the services offered before the regulation came into effect cannot be guaranteed by only connecting to APIs (Unnax, 2022[42]). This move away from screen scraping has considerably increased data security (CNIL, 2021[20]). At the same time, this is convergent with the data protection regulation, as several

[16] Accountability can be complemented by a fiduciary duty whereby data controllers are required to act faithfully and diligently in their customer's best interests, not prefer their personal interests or the interests of another party over the interests of their customers or prefer the interests of one customer over another (Article 21 of the Israeli Account Information Service Law).

[17] For more information, see (Federal Trade Commission, 1999[88]).

concerns have been raised about the compliance of screen scraping practices with the GDPR (CNIL, 2020[43]), with fines issued by some data protection authorities in this respect (Lomas, 2019[44]).

Privacy-enhancing technologies. Privacy-enhancing technologies (PETs) are defined as a collection of digital technologies, approaches and tools that permit data processing and analysis while protecting the confidentiality, and in some cases also the integrity and availability, of the data and thus the privacy of the data subjects and commercial interests of data controllers (OECD, 2023[45]). Policy makers and privacy enforcement authorities (PEAs) are increasingly considering how to incorporate the latest generation of PETs, which are partly still in their infancy, into their domestic privacy and data protection frameworks. Technological and regulatory developments on PETs are important as they can help to address data privacy and security concerns in Open Finance frameworks and in digital finance applications more broadly. PETs would namely help to meet requirements in terms of data security and the implementation of the principles of privacy by design and data minimisation, among others. Examples of PETs that could be relevant to Open Finance include: privacy-preserving federated or distributed analytics[18]; encrypted data processing tools[19]; differential privacy[20]; and zero-knowledge proofs (ZKP)[21], which allow verifying information without requiring disclosure. It should be noted, however, that the robustness of these mechanisms and their performance may need additional innovations and rigorous testing to reach maturity, particularly for high-risk use cases in finance (OECD, 2023[46]).

Clarifying the interplay between data sharing frameworks and data protection regulations

Open Finance sits at the intersection of data protection and data sharing legislations or frameworks. Although these rules broadly share the objectives of protecting users while promoting innovation, their philosophies and backgrounds are different and therefore their cumulative application commonly raises complexities in practice. Clarifying the interplay between these rules is thus essential to provide the legal certainty, transparency, and trust which are needed to develop Open Finance solutions. This co-operation may also relate to the applicability of relevant rules and principles from the legal frameworks applicable in the field of artificial intelligence (AI), which themselves intersect with data protection frameworks on issues such as fairness, transparency and explainability, robustness, security and safety, and accountability. This clarification must be done in the context of regulatory co-operation, including, where appropriate, cross-border co-operation, in order to maximise the convergence and the interoperability of these frameworks.

On some aspects, data sharing frameworks can be complementary to general data protection regulations. Therefore, the data protection frameworks may govern elements that the data sharing framework does not specifically address, and vice versa. For example, data protection frameworks include the principles of purpose limitation and data retention, requiring that the collection of any personal data be limited to what is directly relevant and necessary to accomplish a specified purpose and be kept only for the period of

[18] Privacy-preserving federated or distributed analytics allows executing analytical tasks upon data that are not visible or accessible to those executing the tasks. In federated learning, for example, data are pre-processed at the data source, and that way only the summary statistics/results are transferred to those executing the tasks (OECD, 2023[86]).

[19] Encrypted data processing tools include homomorphic encryption, and multi-party computation including private set intersection. Encrypted data processing PETs allow data to remain encrypted while in use (in-use encryption) and thus avoiding the need to decrypt the data before processing. These tools have limitations (e.g. computation costs) (OECD, 2023[86]).

[20] Differential privacy "adds noise" to the raw data: it makes small changes to individual inputs to de-identify them, while maintaining the explanatory power of the data (OECD, 2023[86]).

[21] ZKPs refer to cryptographic protocols in which a prover can convince a verifier about a mathematical statement, for example, that the prover knows a piece of data that has specific properties. ZKPs are "proofs that convey no additional knowledge other than the correctness of the proposition in question" (Goldwasser, Micali and Rackoff, 1989[87]).

time necessary for such purposes. The purpose of the processing thus holds a central role, and the data controller must define and respect a retention period proportionate to the said purpose (CNIL, 2021, p. 61[20]). Sometimes, the data sharing framework itself includes specific safeguards pertaining to data retention. For example, the Israeli Account Information Service Law provides that consent for retaining the collected data for more than three years can be obtained only towards the end of the three-year period (OECD, 2023[8]). Similarly, the proposal for rulemaking in the US envisages to have a maximum period for the authorised third-party access, after which reauthorisation would be necessary (CFPB, 2022, p. 41[25]).

On some other aspects, data sharing frameworks and data protection regulations may include similar or identical expressions, but attribute different meanings to them. For example, the notion of consent may differ between data protection legislation and sectoral data sharing frameworks. Regarding Open Banking, for example, in the EU the sectoral regulation (PSD2) included consent as the agreement by a payment service user to a contractual condition with the third-party provider (OECD, 2023[8]). As a consequence, the bank is legally obliged to share the user's data with the third-party provider. However, consent under PSD2 does not amount to consent under the relevant data protection legislation (GDPR), which has different legal characteristics.[22] Thus, other legal bases available under the GDPR must be used by the data controller, such as contractual necessity and legal obligation. As to contractual necessity, the essential elements of the contract and the reasonable expectations of the parties involved will determine the scope of what is necessary data processing in relation to the provision of the payment service. Such inconsistencies between data sharing frameworks and data protection regulations are common also in other regions and sectors. While such inconsistencies can often be resolved (at least partially) through cross-sector regulatory co-operation, the legislation should allow relevant regulators to cooperate and exchange information as appropriate, which is not always the case.

Yet another possibility is that the data sharing framework introduces data protection safeguards that would otherwise not be required under applicable data protection provisions. This can occur where the general data protection legislation is less prescriptive or where the texts do not fully overlap. For instance, in the US there is no general, comprehensive data privacy law at the federal level (whilst specific pieces of legislation cover e.g. how federal agencies can collect and use data about individuals in their systems of records (the Privacy Act of 1974) or how financial institutions have to safeguard consumers' data (the Gramm-Leach-Bliley Act of 1999)). Consequently, there is no overarching accuracy requirement on the collection of data by authorised third parties at the federal level to-date (CFPB, 2022, p. 46[25]). The proposal for a rulemaking in this area, which includes data accuracy, may thus introduce a novel requirement with regard to Open Finance that would strengthen data protection.

The introduction of a data sharing framework can also provide an opportunity to broaden the scope of applicable data protection provisions. For example, currently in Australia most small businesses with a turnover of less than AU$3 million would not normally be subject to the Privacy Act (OAIC, n.d.[47]).[23] The Farrell Report (which has laid the foundations for the Open Finance legislation in Australia) recommended that all data recipients under Open Banking (which includes fintech start-ups) be subject to the legislation

[22] "Explicit consent under the PSD2 is different from (explicit) consent under the GDPR. Explicit consent under Article 94 (2) of the PSD2 is an additional requirement of a contractual nature" (EDPB, 2020[90]). Similarly, the European Data Protection Supervisor has stressed the need to clearly differentiate the permissions under the Proposal for a Regulation on payment services in the internal market and the Proposal for a Directive on payment services and electronic money services in the Internal Market (which will replace the PSD2) and the legal bases for processing of personal data under the GDPR (EDPS, 2023[24]). A recommendation to the same effect has been made with regard to the Proposal for a Regulation on a framework for Financial Data Access (EDPS, 2023[57]).

[23] To note, a recent review of the Privacy Act recommends removing the exception from the Act itself (Australian Government. Attorney-General's Department, 2022[83]).

on privacy (Deloitte, 2018[48]). As a result, if a small business wishes to be accredited under the Consumer Data Right system, it will be covered by the Privacy Act.

Where data sharing takes place across borders, the flow of personal data may be permitted subject to accountability requirements or it may require compliance with specific regulatory or policy frameworks (OECD, 2022[49]). Most often, these frameworks envisage the fulfilment of model contractual clauses, binding corporate rules, certifications, or codes of conduct. In some cases, flows of personal data may also be permitted to the extent that an adequacy decision has been taken by the relevant domestic authority with respect to the privacy framework in the destination country.

However, some implementations of data protection regulations could lead to potential issues, where a given jurisdiction proposes the localisation of payment data. This has been proposed about payment data of EU natural persons (Lemery and Steiner, 2020[50]) and motivated by concerns about sovereignty on payments as well as about compliance with the GDPR. However, the effect of data localisation on data protection would require further investigations. For example, data localisation measures requiring data to be exclusively stored in a particular country have been alleged to undermine systems designed to provide cross-border anonymity, or pseudonymity, given that several of such systems rely on data being stored on the users' devices (Svantesson, 2020[51]).

The complexities inherent to clarifying the interplay between different rules, as exemplified above, clearly expose the crucial role of regulators in this area, and in particular their capacities for national and international co-operation. A point of note in this respect, however, is that Open Finance frameworks may task different regulators with different responsibilities. For example, under the Israeli Account Information Service Law, in case of a data security breach, the Privacy Protection Authority may order the service provider to notify all data subjects whose privacy may be tangibly harmed by the breach.[24] On the other hand, it is incumbent upon the service provider's regulator to determine rules regarding risk management, digital security and the obligation to appoint officers in charge of data security (OECD, 2023[8]).

Policy makers and oversight authorities responsible for financial consumer protection should liaise with data protection authorities – where they exist – to ensure understanding and application of data protection laws and regulations to financial services providers. This could include providing dedicated guidance to financial services providers to promote compliance. Capacities of regulatory co-operation are therefore indispensable in order to provide legal clarity and maximise the convergence and the interoperability of applicable frameworks. Such co-operation must make it possible to identify differences in scope, gaps, and variations in the interpretations of certain terms (e.g. the lack of clarity about the definition of personal data (Future of Privacy Forum, 2022[19])), or on the contrary enhance the potential synergies between different sets of rules and principles.

Policy makers and oversight authorities should therefore have in place arrangements to cooperate and share information with data protection authorities, e.g. via a memorandum of understanding or through legislative provisions enabling such information-sharing, at both national and international level (OECD, 2020[33]). The on-going review of the OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy aims to address the challenges of cross-sectoral co-operation (OECD, 2023[52]).

Consent and data subjects' rights

Consent plays a central role in Open Finance frameworks as it allows users to control how their financial data is shared in Open Finance, just as it is a central concept in modern privacy regimes. As well, it is important to underline that the protection of individuals is too often reduced to obtaining their consent but that consent is only one, albeit a crucial, component of a wider privacy architecture that should guarantee

[24] On data breach notification, see (Iwaya, Koksal-Oudot and Ronchi, 2021[92])

that personal data is protected in Open Finance frameworks, as discussed above. Overall, the role of consent is essentially an expression of the requirement to maintain the autonomy and control of the person over their data in the Open Finance ecosystem.

Consent is a cornerstone of all data protection legislations globally, although it plays a different role in different regimes. For instance, in laws following the models of the GDPR, consent is one of several so-called lawful bases for the processing of personal data. It must be obtained unless other lawful bases exist, for example when processing is necessary to comply with a legal obligation or if it concerns a purpose compatible with the purpose for which the data was initially collected. Data protection regimes may also or only require consent in circumstances in which personal information may be used or disclosed for a purpose other than the purpose for which it was collected. The collection of so-called 'sensitive data' (in jurisdictions where this category is recognised) or of children's data is also commonly subject to additional, reinforced consent requirements.

Open Finance frameworks may further specifically require the customer's consent to allow for the reuse of data, and thus complement the criteria laid down by data protection regulations, which can create challenges in practice. This is particularly the case with the PSD2, which states (specifically in Articles 66 and 67 thereof) that any purpose other than the provision of an account information service or a payment initiation service is not a compatible purpose for the providers of these services. The merchant must therefore obtain the data subject's consent to process this data for other purposes (unless such further processing is necessary to comply with a legal obligation) (CNIL, 2021, p. 61[20]). In particular, when accessed data can reveal special categories of data (e.g. health information or sexual orientation), explicit consent may be required (OECD, 2023[8]).

Data protection laws commonly provide conditions for consent to be valid. By and large all jurisdictions require that consent must be free and explicit, specific (or unbundled), informed, and unambiguous. Obtaining informed consent requires providing an appropriate degree of information to users. Therefore, this entails finding the right balance, with the aim of "educating and empowering consumers without confusing, scaring, or boring them" (McKinsey, 2017[53]). The design of online applications may make it easier to "capture" consumers' consent.[25] The duration of the validity of the consent also needs to be appropriate to the services at stake. For example, in the EU the consent to Open Banking services requires strong customer authentication every 90 days (EU, 2018[54]), although the European Banking Authority has recommended extending it to 180 days (EU, 2022[55]). In Open Finance frameworks, as services are less liquid than payments (e.g. mortgages, pensions), a longer time frame may be suitable.

However, limitations to the use of consent also need to be acknowledged. Consumers do not always read privacy and consent forms when they access online services and some of the language can be hard to understand even for educated consumers (World Bank Group; Ministry of Foreign Affairs of the Netherlands, 2021[36]). It can be thus helpful to specify that information about the nature of the service and the storage of the data should be provided to customers "in clear and brief language", as under the Israeli Account Information Service Law (Article 26(a) (Israel, 2021[56])).

In addition to consent, Open Finance could include a single location for users to review their personal data sharing. Thus, consumers could have a more transparent and direct oversight over the data shared, the time period, and the third parties (World Bank Group; Ministry of Foreign Affairs of the Netherlands, 2021[36]).

[25] This is the case with the prevalence of dark commercial patterns, which the OECD has defined as follows: "Dark commercial patterns are business practices employing elements of digital choice architecture, in particular in online user interfaces, that subvert or impair consumer autonomy, decision-making or choice. They often deceive, coerce or manipulate consumers and are likely to cause direct or indirect consumer detriment in various ways, though it may be difficult or impossible to measure such detriment in many instances" (OECD, 2022[94]).

Indeed, consent management and data dashboards can enable compliance with data protection legislation (notably by increasing transparency and control for individuals (EDPS, 2023[57])), but have to comply with the conditions provided therein (OECD, 2023[8]). For example, this entails that the consent should be given freely and be express and unambiguous. In order to enable consent dashboards or other permission management tools, horizontal agreements may be needed regarding reporting of data-transaction metadata (e.g. identity data user, data owner, data provider) (DNB and AFM, 2023[27]). Such dashboards could include cross-sectoral overviews of data access permissions in order to empower meaningful data control across sectors. Furthermore, the dashboard should not be designed in a way that would unduly influence users to grant or withdraw permissions (as prescribed in the proposal for an EU regulation on a framework for Financial Data Access (EU, 2023[58]) and as suggested by the European Data Protection Supervisor with regard to the revision of the PSD2 (EDPS, 2023[24])).

Consent management can be a challenge for banks as conventional financial systems are fragmented (OECD, 2023[8]). The existence and integration of digital ID schemes could help enhance user experience in Open Finance data sharing frameworks (see Section 0). To that end, the Japanese Financial Services Agency has conducted research on a blockchain-based identity system to better protect privacy and to ensure data portability.

Consent may also serve as an opportunity to teach consumers about their rights and responsibilities about their finances and their data. This can in turn help to enforce regulatory requirements and market discipline (OECD, 2023[8]).

Beyond consent, Open Finance frameworks need to take into account the rights of data subjects over their data, such as the rights to receive information and to object to the processing of their data. Indeed, transparency should be maintained along the data chain, and the data subject should be informed of the different personal data sources used to deliver a product. For example, if the data is shared for fraud prevention purposes, there should be general information provided to customers about the existence of such mechanisms. If the data controller detects anomalies or flags, it should contact the customer, who should be allowed to provide additional information. And when the data controller takes the decision to add the customer to a list of individuals presenting a fraud risk, with legal consequences (e.g. the inability to make payments), the data controller must send written and individual information, specifying the measures taken and giving the individual the opportunity to present its observations (CNIL, 2021, p. 67[20]).

In a similar manner, special attention should be given to automated decision-making based on personal data gathered in Open Finance. This could be the case of a refusal to process a transaction because of a score established automatically and without any human intervention (CNIL, 2021[20]). In particular, the GDPR (Article 22) provides the right, for the individuals concerned, not to be subject to a decision based solely on automated processing and producing legal effects concerning them or similarly significantly affecting them. Policy makers and oversight authorities should ensure that financial services providers employing automated decision-making models such as credit scoring take measures to mitigate against irresponsible or inappropriate outcomes, such as automatic refusals. Measures could include appropriately weighting all relevant variables and providing for human intervention, where appropriate (OECD, 2020[33]).

Beyond consent and data subjects' rights, policy makers, regulators and private sector organisations should consider the broader impact of data sharing and re-use, and the relationship between the protection of privacy and individual liberties, fundamental values and democracy. Some of the concerns in this area have been framed as ethical, to underscore the need to recognise the importance of issues that are complementary to regulatory or legal issues (e.g. fairness, respect for human dignity, autonomy, self-determination, human rights and the risk of bias and discrimination) (OECD, 2022[59]). Data ethics is referenced in particular in cases where the collection and processing of personal data will be legal under data protection law, but may generate moral, cultural and social concerns with potential direct or indirect adverse impacts on individuals or social groups. A wide range of data ethics frameworks have been developed recently by various jurisdictions, and tools such as Data Ethics Impact Assessments, Data

Review Boards and Data Ethics Seals may help organisations take responsible decisions about data use, and may be relevant also in the context of Open Finance.

Data portability

The existence of the right to data portability in data protection regulations may act to some extent as a forerunner for Open Finance frameworks. Data portability is understood as the ability of users to request that a data holder transfer, to them or to a third party, data about them in a structured, commonly used and machine-readable format (OECD, 2021[60]). Its scope in terms of categories of data is broader than Open Finance (as it is not confined to one sector) and could be helpful in the move from Open Finance to wider Open Data policies (Medine and Plaitakis, 2023[34]).

In the OECD Privacy Guidelines, the right to data portability can be inferred as an application of the individual participation principle. The latter provides that individuals "should have the right to obtain from a data controller, or otherwise, confirmation of whether the controller has data relating to them [and] to have communicated to them, data relating to them within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to them".

In other data protection regulations, the right to data portability is stated in more explicit and specific terms. For example, Article 20(1) GDPR provides the data subject with the right to "receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and […] the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided", under the conditions and within the limits spelled out in the provision. Importantly, the article encompasses the right to have the data transmitted from a data controller to another data controller.

In theory, data portability could allow users to put into practice Open Banking and Open Finance in the absence of specific frameworks. Customers could request banks (as data controllers) to transmit data concerning them to other data controllers such as Fintech start-ups, which could then provide additional services by leveraging the value of such data.

Generally, data portability is regulated such that it should be provided "at a charge, if any, that is not excessive" (OECD Privacy Guidelines) or free of charge (Art. 12(5) GDPR). This stems from the logic of facilitating the exercise of data subjects' rights, and may have a bearing on the overall balance of incentives of Open Finance frameworks.

At any rate, the actual implementation of data portability may require additional measures. Empirical research conducted after the entry into force of the GDPR showed that guidance materials, standards, codes of conduct as well as technological solutions such as open APIs were needed to improve the effective exercise of the right to data portability (Wong and Henderson, 2019[61]).

Further empirical research has highlighted that individuals cannot make use of direct data portability between data holders, in the absence of the necessary infrastructure (Kuebler-Wachendorff et al., 2021[62]). Indeed, the direct transfers between services raises considerable technical obstacles. These include lack of standardisation, compatibility and interoperability, as discussed below.

Furthermore, the right to data portability in data protection regulations typically does not provide the same granular level of control features that Open Finance frameworks include (Medine and Plaitakis, 2023[34]). This implies that customers may be unable to specify the details of data to be ported, and measures for the secure and timely transmission of data may not be spelled out.

Consequently, Open Finance frameworks can be an opportunity to design data sharing in a manner that effectively empowers users and protects their personal data. Data protection and liability frameworks need to be a core component of Open Finance to solve some of the issues highlighted above. To achieve this objective, regulatory co-operation among relevant authorities (chiefly those responsible for financial

services and for data protection) is crucial, and should take place as early as possible in the design and implementation of Open Finance frameworks.

Building interoperability by design: data and infrastructure enabling data sharing

The long-term success of Open Finance may depend on the level of interoperability achieved so as to support data sharing between service providers across different sectors and different countries.[26] Such interoperability can be achieved, *inter alia*, through some level of harmonisation of data formats and through the interoperability of interfaces used for data sharing (e.g. APIs). Data needs to be made available in a digital format and following specific formats in order to be usable. This means that a minimum level of standardisation may need to be considered to make data sharing and usage cost efficient. When it comes to interfaces used to access and share data (APIs), there is currently great fragmentation in the solutions available, which results in a lack of interoperability and increases the costs associated with participation in the Open Finance ecosystem.

There are currently limited examples of the existence of standards promoting or ensuring data interoperability in OECD countries, over and above the API standards mentioned in this Section. Initiatives are, however, being planned in some OECD countries, such as the United Kingdom, where the proposed smart data legislation would encourage smart data schemes to be interoperable with other open data initiatives in the UK. In other countries, standards on data interoperability apply only in cases of mandatory interoperability by financial institutions contemplated by law, mainly on network operation such as those relating to card payments, or outside the financial services space. In Australia, in the context of the Consumer Data Right legislation, data standards (including standardised APIs) are developed by the Data Standards Body to be made by the Data Standards Chair (OECD, 2023[1]).

Common standards for data interfaces are being promoted in some jurisdictions as enabling conditions for the development of Open Finance. Indicatively, in Switzerland, standards with broad national support and internationally compatible where appropriate are included as part of the Open Finance objectives, with a maximum of one recommended standard per business area (Federal Council of Switzerland, 2022[63]). Under the same objectives, open interfaces should also be based on common standards to the extent possible (Federal Council of Switzerland, 2022[63]).

The use of common standards for APIs could be considered as a way to reduce the costs involved in TPPs having to connect with multiple different ASPSPs' interfaces, and to maintain or update their connection across time. This may in itself be a barrier to entry for smaller SMEs and a challenge to the successful implementation of Open Finance and to the achievement of its objectives around the fostering of innovation. The benefits may be most prominent in the case of small entities who may otherwise need to pass costs incurred for connecting to different interfaces on to their clients. Examples of mandatory standards imposed by the authorities include the UK, where the UK Open Banking Implementation Entity (OBIE) was setting the standards.[27]

The role of aggregators in the absence of standardisation, and associated risks

Today, interoperability is facilitated through the use of API aggregators that integrate many different APIs and provide a single implementation point for TPPs, but also give rise to risks of market dominance in terms of competitive dynamics. Aggregators deliver a standardised API regardless of what APIs or services they integrate, allowing TPPs to connect to many different APIs without having to deal with the

[26] In this respect, the OECD Recommendation of the Council on Enhancing Access to and Sharing of Data recommends fostering where appropriate the findability, accessibility, interoperability and reusability of data across organisations, including within and across the public and private sectors (OECD, 2021[28]).

[27] https://standards.openbanking.org.uk/api-specifications/

configuration and formatting of data and interfaces, for a fee. Interoperable data sharing frameworks and API standards are also considerations for sound Open Insurance frameworks (EIOPA, 2022[14]).

While aggregators offer improvements to the Open Finance ecosystem, they pose risks for the financial services industry both in terms of data privacy and security (similar to the ones discussed in Section 4.3), and in terms of competition. Given that data aggregators' large scale and scope in accessing consumer financial data are beneficial for many parties, the market may allow for only a few large data aggregators (Alcazar and Hayashi, 2022[64]). This market structure could lead data aggregators to gain and exercise market power by charging higher fees to TPPs and smaller consumer financial institutions. Importantly, aggregators are not licensed entities in some economies, and therefore not directly supervised by authorities.

Standardised APIs

Making a specific API standard the legally mandatory standard of a country may not be in line with the principle of technology and business model neutrality, which is a cornerstone of financial services regulation across most OECD countries (OECD, 2023[1]). In addition, the enforcement of a single API standard would likely be difficult to implement and hard to regulate, while it would also possibly create barriers to adoption for certain market players (European Commission, 2022[2]). However, encouraging some sort of harmonisation of API standards could foster the user-friendliness of customer journeys and improve technical compatibility, as well as reduce costs associated with data access by FinTech start-ups. Increased standardisation driven by the industry can promote a level playing field and further encourage innovation and FinTech creation.

The development of standardised APIs could be industry-led. However, a mechanism for national authorities to potentially provide guidance and steer its development, could contribute to a clearer legal framework to be complied with by the industry (OECD, 2023[1]). Common API standards could be developed by the industry along the lines of existing initiatives, but with a view to reducing fragmentation in the standards available. Existing initiatives (e.g. the Berlin Group standards[28], STET standards[29], Financial Data Exchange (FDX) standards in the US) or national standards (e.g. Czech or Polish API standards) have been helpful in driving some level of interoperability of interfaces. Another example of national standards implementation is the National Open API Payment Standard (SNAP) in Indonesia, which aims to create a healthy, competitive and innovative payment system industry, while promoting integration, interconnectivity, and interoperability to increase healthy, efficient, and fair practices in a secure and reliable payment system.[30] Nevertheless, the API environment still remains fragmented.

Authorities could consider providing support to further standardisation efforts in order both to guide initiatives and to ensure that standardisation efforts are abiding by any legal requirements. The diversity of APIs despite industry-led standards renders market access, from a technical perspective, somehow cumbersome and costly for providers of account information services (AIS) and payment initiation services (PIS), as service providers have to deal with a relatively large diversity in the dedicated interfaces / APIs offered by ASPSPs (mostly banks) for accessing payment accounts (and the associated IT costs). Common standards may also create familiarity and convenience for end consumers, therefore helping to build customer trust, while they may also help innovative services come to the market faster (FCA, 2021[65]).

The discussion on standardisation should not be restricted to API specifications but also to data formats; operating practices, including consent management, authentication and identity management; security

[28] https://www.berlin-group.org/

[29] https://www.stet.eu/

[30] SNAP has been developed by Bank Indonesia in co-operation with payment system industry representatives covering: 1) Technical and Security Standards, Data Standards, and Technical Specifications, as published on the Developer Site (https://apidevportal.bi.go.id/snap/); and 2) Governance guidelines for interconnected and interoperable open API payments.

protocols and performance criteria. Standardisation may be required for specific core data fields, and guidelines for a common taxonomy could be developed by the industry, with an appropriate level of flexibility embedded into any such exercise (European Commission, 2022[2]).

The importance of interoperability is even more pronounced when it comes to cross-border data sharing. The lack of commonly accepted API standards may pose potential inefficiencies to participants or increase the fragmentation of the digital financial ecosystem (Ehrentraud et al., 2020[66]). Any API standards, if considered, would need to be developed in a way that promotes security, interoperability, efficiency and usability for all users and in a way that is compatible with relevant existing global standards (EIOPA, 2022[14]). This could ultimately lead to costs reduction and better consumer protection, facilitating scaling and enabling a secure and smooth access to consistent data sets across sectors (EIOPA, 2022[14]). Also, new technology could potentially supersede APIs in the future, and in that sense, regulations and policy approaches need to future-proof.

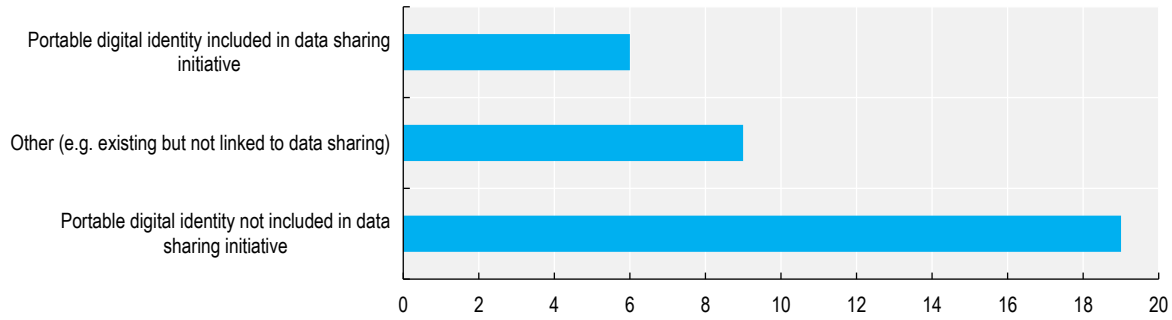
The importance of portable digital identity (ID) for Open Finance

The link between data access and digital identity (ID) is indispensable for the successful implementation of comprehensive Open Finance frameworks (OECD, 2023[1]) (Linda Jeng, 2022[67]). Identity underpins the entire financial system, and poor identity infrastructure opens the path to bad actors exposing consumers and businesses to important risks. Implementation of such frameworks is currently predicated on the data holder (primarily banks) identifying and verifying the individual requesting a transaction before the data is released. Fulfilling onboarding (KYC) and AML/CFT checks is one of the possible challenges particularly for cross-border activity, insofar as trusted cross-border ID verification mechanisms are not available.

The existence of portable IDs could significantly alleviate processes related to secure customer authentication in payment initiation involved in Open Finance frameworks. Enabling the use of digital IDs that provide a high level of assurance in data transactions could enable more efficient onboarding of new clients, while it would also make it possible for data owners to authenticate data transactions with different entities using a single set of credentials (DNB and AFM, 2023[27]). Horizontal guidelines on user experience and integration could promote a level data playing field.

Only a minority of countries with data sharing frameworks are employing portable digital IDs as part of their initiatives (Figure 3.5). However, efforts are underway in many parts of the world to address portable digital IDs. At the national level, the Czech Republic, Estonia and Finland have made progress (OECD, 2023[1]). Bank-IDs are another method for performing electronic identification in some OECD countries, e.g. in public sector e-services. At the regional level, in the EU, EIDAS 2.0 is being pursued to that end. Efforts are also underway by private sector participants, although any ID that is issued outside of government-issued credentials gives rise to additional risks.

Figure 3.5. Inclusion of portable digital ID in data sharing initiatives



Note: Based on 34 responses to the OECD Survey.
Source: (OECD, 2023[1]).

The existence of portable digital ID could act as a catalyst for cross-sectoral and cross-country data sharing to be operational. It can enable the secure connection between the entities participating in the ecosystem and ensure they can interoperate with each other. At the cross-border level, it can enable extensibility across vertical markets beyond finance, in 'Open Data' type of ecosystems (e.g. health, IoT).

The OECD has developed a Recommendation (OECD, 2007[68]) and a Guidance (OECD, 2009[69]) to assist countries in developing effective and compatible approaches to electronic authentication, at both the national and the international level. It has also undertaken work on digital identity management (OECD, 2009[70]) and has adopted a Recommendation on the Governance of Digital Identity (OECD, 2023[71]). It recognises that the governance, design and implementation of digital identity systems should be rooted in democratic values and respect for human rights. It also recommends treating user control, privacy and data protection as fundamental tenets of digital identity systems, and encouraging the adoption of privacy-by-design and privacy-by-default approaches.

In the absence of portable digital IDs, the implementation of data sharing is predicated on the fact that the bank (or other data holder) will correctly identify the individual making the transaction request before the data is released. Digitally native financial services present challenges to a patchwork system of largely paper-based identifiers and credentials issued by a variety of different entities, which are better suited for in-person transactions (Das, 2022[72]). Any security or operational weaknesses at the identity infrastructure opens the path to bad actors, fraud and cyber risk, with harmful impact on people and businesses. That is why the OECD Recommendation on the Governance of Digital Identity recognises security as foundational to the design of trusted digital identity systems, to ensure that digital identity solution providers and solutions comply with all relevant requirements, also to protect users from possible identity theft or alteration (OECD, 2023[71]).

Outside of government-issued credentials, there is considerable appetite from private entities (e.g. BigTech platforms) to offer derived credentials with varying levels of binding to government credentials and record systems. Government-issued digital identity credentials remain, however, the most credible way for people to access the formal economy, while closing gaps exploited by cybercriminals. Private-public collaboration could help governments modernise and virtualise physical identity credentials. In parallel, regional efforts are underway (e.g. in Europe with eIDAS 2.0 or in the US with states' issuance of digital IDs). Most recently, the concept of self-sovereign digital identity has been discussed particularly in the context of financial inclusion initiatives. Such identity consists of a lifetime portable digital identity, completely controlled by the individual, that does not depend on any central authority and can never be taken away (GPFI and World Bank, 2018[73]). When discussing digital ID at the company level, the Global Legal Entity Identifier (LEI) presents a global business passport under regulatory oversight (see Box 4.2).

Box 3.2. Global Legal Entity Identifier (LEI)

In 2020, the G20 called on the Financial Stability Board (FSB) to provide recommendations for a Global Legal Entity Identifier (LEI) and a supporting governance structure (FSB, 2022[74]). The LEI was endorsed by the G20 as a solution to identify counterparties in over-the-counter derivatives markets. There are over 200 jurisdictions where at least one LEI is registered.

The LEI is a worldwide unique identifier based on the ISO standard 17442, intended to identify parties in any financial transaction. It equips legal entities with a global, digital identity and enhances interoperability in digital finance applications and payments. As such, the LEI is part of the FSB's proposed enhancements to make cross-border payments more transparent, efficient and inclusive for all users. As an open and non-proprietary standard, it can facilitate more effective counterparty identification and verification on a global scale by providing a universally recognised identifier paired with essential entity data, rigorous verification processes and high data quality, which helps increase transparency and traceability. Furthermore, notable advancements have been made for the LEI in the CPMI ISO 20022 Harmonisation Consultation conclusion released in October 2023. The LEI is recognized as an equivalent identifier to the BIC for financial institution identification. Additionally, for entities involved in payment messages, name and postal address may be substituted by the LEI.

The Asian Development Bank and the African Development Bank indicated the usefulness of the LEI for creating a standardised, reliable, global identity to: (a) mitigate the risk for the correspondent bank-customer relationships being de-risked; (b) increase SMEs' access to finance in emerging markets by easing the flow of reliable information; and (c) promote development of FinTech platforms to reduce costs (ADB, 2019[75]; GLEIF, 2021[76]). As a global open data standard, LEI does not contain confidential (private) information; therefore, it does not pose confidentiality threats in respect of information exchange (FSB, 2022[77]).

The LEI is managed by the Global Legal Entity Identifier Foundation (GLEIF), established by the FSB in 2014 and tasked with supporting the implementation and use of the LEI. GLEIF continues to work with the FSB to further encourage the adoption of the LEI in identifying beneficiary and originator in cross-border payment messages. In the EU, the European Systemic Risk Board has called on the European Commission to create an EU legal framework for broader adoption of the LEI also for non-financial corporations and to consider the LEI in any new or amended legislation (European Systemic Risk Board, 2020[78]).

The Bank for International Settlements Committee on Payments and Market Infrastructure (CPMI) suggested the LEI as a unique identifier for precisely identifying the beneficiary and originator in payment messages in their Stage 2 report to the G20 (CPMI BIS, 2020[79]). As part of the implementation of the concluding Stage FSB report (FSB, 2020[80]), the LEI features prominently as a solution, as it is a digital unique identifier for identifying legal entities in payment transactions.

Specifically on open banking and payments, the FSB's focus on cross-border payments in order to meet the G20 Roadmap for Enhancing Cross-border Payments has led it to recommend exploring the enhanced the use of the LEI (FSB, 2023[81]). In support of the goals of the G20 Roadmap (endorsed by G20 Leaders in November 2020), the FSB deemed that the LEI could help make cross-border payment transactions faster, cheaper, more transparent, and more inclusive, while maintaining their safety and security. Subsequently, in 2023, the FSB asked GLEIF to collaborate with leading payments industry stakeholders to provide clarity, through examples, on how the LEI can deliver value within cross-border payment flows. GLEIF has been working with multiple partners to demonstrate the value the LEI brings to both nonfinancial corporates and financial institutions when transmitted in cross-border payment flows. As a result, five key use cases have been defined: (i) screening (watch lists and sanctions); (ii)

KYC and client onboarding; (iii) fraud detection and fight against vendor scams; (iv) e-invoice reconciliation; and (v) account-to-account validation.

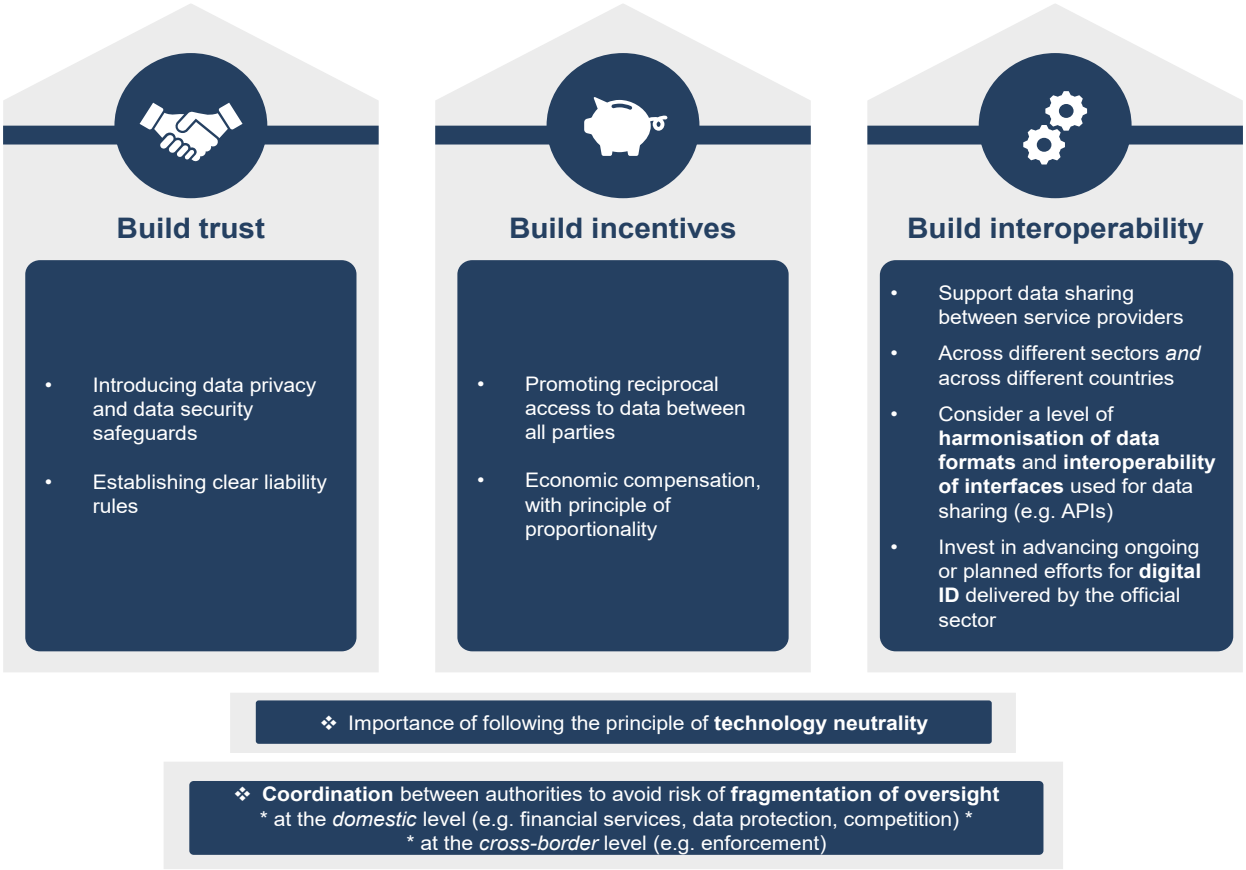
In parallel, a banking industry association which aims to develop frameworks and guidance for the management of financial crime risks has published its updated Payment Transparency Standards, which begin to identify how various capabilities within the ISO 20022 structure can be utilised to enhance payment transparency (The Wolfsberg Group, 2023[82]). The updated standards state that, to the fullest extent permitted by the payment market infrastructure, the payment-service-provider (PSP) of the payer (referred to within ISO 20022 as the 'debtor agent') should use the LEI or other equivalent reference codes to enhance the accuracy of identification information on relevant parties.

Source: GLEIF, Gianluca Riccio (Chair of the Business at OECD Finance Committee).

4 Policy considerations

There are two main design approaches to the data sharing frameworks in OECD countries: the market-led approach or voluntary framework (e.g. Japan, US, Switzerland), and the more prescriptive approach where data sharing is imposed by regulation (e.g. EU PSD2). Each of the approaches fits the idiosyncrasies of the corresponding economies and is considered equally effective in delivering the objectives of such frameworks. However, shared pillars may need to be considered to ensure a successful transition from Open Banking data sharing arrangements towards Open Finance (Figure 4.1). Where Open Banking frameworks are in place, Open Finance can gradually build on these frameworks by expanding towards data and sectors that are most meaningful for consumers and drive innovative product creation, as dictated by market forces. A phased approach with an extensive consultation of stakeholders could be considered by jurisdictions planning an Open Finance framework, for a smoother, gradual expansion towards cross-sectoral data sharing. Cost-benefit analyses may be considered where policy makers decide to intervene through policy action to promote such transition.

Figure 4.1. Pillars for successful implementation of Open Finance data sharing frameworks



Source: OECD.

Any data sharing should follow the principle of technology neutrality that OECD members apply in financial regulation, with the same activities and same risks being addressed by the same rules, regardless of the technological means used. Risks arising from Open Finance, whether old or new, need to be carefully analysed. Among these, policy makers may need to closely monitor the level of competition among data aggregators.

As highlighted in the paper, the implementation of comprehensive privacy and data protection safeguards is crucial to the proper functioning and uptake of Open Finance. Introducing safeguards for data protection and data security is particularly important to effectively protect personal data, to induce a sense of control among users and thus to build trust. This entails clearly defining roles in accordance with data protection rules, for example for "data controllers" and "data processors" as per the terminology adopted by some legislations; and allocating responsibilities with respect to the principles of purpose limitation and related principles (including data minimisation and data retention), privacy by design and by default, accountability, and data security which can be found in international standards. Governance, ICT controls and data governance and data protection requirements can promote the safety of data sharing by financial data intermediaries.

The OECD Privacy Guidelines and the G20/OECD High-Level Principles on Financial Consumer Protection provide reliable guidance to policy makers in this respect. Privacy-enhancing technologies can complement organisational and legal measures to allow for data processing and analysis while protecting the confidentiality, and in some cases also the integrity and availability, of the data. Furthermore, at the national level, consistency between data protection laws and Open Finance frameworks is needed to provide the legal certainty, transparency, and trust to develop Open Finance solutions.

Consumer education can contribute to the build-up of trust by consumers alongside the promotion of privacy and data protection. Consumer education can promote awareness with implications for implementation and uptake of Open Finance data sharing frameworks. Some consumers may not understand the products and services and/or may be unwilling to share their data if they lack awareness of the safeguards in place to protect them. The same applies to the use of digital ID and has important implications to the successful uptake of such tools (see below).

Formal consent plays a central role in Open Finance as it allows users to exert control over the flow of their financial data. It needs to be free and explicit, specific (or unbundled), informed, and unambiguous. Consent to data sharing that is reiterated on a periodic short-term basis could further promote the objectives of this instrument. To be truly given, an appropriate degree of information must be provided to users, including a clear identification of user data that can be shared (e.g. raw data rather than processed data). Parties involved in data sharing should avoid processing user data for purposes other than performing explicitly requested services by the user. It should be noted, however, that consent has its own limitations and practical challenges. Consent management and data dashboards can enable better compliance with data protection legislation. Consent is only one component of a wider privacy architecture which Open Finance should encompass, and which also includes the rights of data subjects over their data, such as the rights to receive information and to object to the processing of their data.

Data portability features in several data protection regulations and is understood as the ability of users to request that a data holder transfer, to them or to a third party, data about them in a structured, commonly used and machine-readable format. Its existence may act to some extent as a forerunner for Open Finance frameworks. However, its actual implementation requires additional measures and does not provide the same granular level of control features that Open Finance frameworks include.

Coordination will be required between authorities with jurisdiction over parts of Open Finance activities, particularly given the cross-sectoral nature of such frameworks, to avoid fragmentation of oversight (e.g. financial supervisors, data protection authorities and competition authorities). Collaboration protocols may be considered around information exchange and co-operation of authorities

involved in Open Finance frameworks.[31] The emergence of new entrants providing both financial and non-financial services or falling outside the perimeter of the financial supervisor will also need to be further analysed.

Coordination at the international level will be important for the oversight of cross-border data sharing activities. Coordination at the cross-border level could be challenging on many levels, e.g.: legal (liability, property rights over data); technical (e.g. different data standards, different data vocabularies due to language differences); and at the enforcement level (given possible differences in legal frameworks). The OECD has in place a Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy (OECD, 2007[22]), and its ongoing review (OECD, 2023[52]) will also address cross-sectoral aspects, which are important to maximise the convergence and the interoperability of these frameworks.

The right incentives need to be in place for participants in Open Finance frameworks, to counter the costs that incumbents may need to pay for the development and maintenance of APIs or other connecting interfaces for data sharing, and for the general upgrade of their systems to allow for sharing of data in digital formats that can be used in such infrastructure. Examples of possible incentives[32] can take the form of reciprocity of data sharing and/or economic compensation. Reciprocal data access to customer data between all parties in finance exists in the minority of OECD countries where data sharing arrangements are in place (OECD, 2023[6]). Without reciprocity for all parties involved in data sharing, incumbent firms may have less of an incentive to invest in the delivery of infrastructures such as APIs. Even in case of regulatory requirements for data sharing and for the delivery of such infrastructure, the absence of any commercial incentives for firms may result in underperforming data sharing infrastructures or in the lack of their maintenance (which may lead to malfunctioning). Both of these sub-optimal results have been anecdotally reported by FinTechs as issues impeding their accessibility to data under existing arrangements.

To that end, reciprocal access to data between all parties under Open Finance ecosystems may need to be promoted. Policy makers of jurisdictions where data sharing is mandatory on a free basis may consider allowing for reasonable economic compensation for data access under fair compensation schemes in order to allocate costs fairly among participants while safeguarding competition. This would include the principle of proportionality so as not to impede smaller firms from accessing data, while also protecting against anti-competitive behaviours. This could involve, inter alia, encouraging the industry to develop guidance or best practices on the content of compensation schemes e.g. in relation to the metrics to be adopted to determine a fair and proportionate remuneration. In addition, relevant policies and data sharing frameworks should be designed with the aim of producing tangible benefits to individual users, with a view to incentivising uptake and maximising the success of such frameworks. Financial or other benefits propositions will result in a significantly higher willingness to share payments data, too.

The long-term success of Open Finance may depend on the level of interoperability achieved to support data sharing between service providers across different sectors and different countries. Such interoperability can be achieved, *inter alia*, through some level of harmonisation of data formats and through the interoperability of interfaces used for data sharing (e.g. APIs). Today, interoperability is facilitated through the use of API aggregators that integrate many different APIs and provide a single implementation point for TPPs, but also give rise to risks of market dominance in terms of competitive dynamics.

[31] The European Data Protection Supervisor has highlighted the importance of a clear legal basis for the exchange of relevant information between data protection authorities and the authorities that are competent for the compliance of Open Finance frameworks (EDPS, 2023[24]; EDPS, 2023[57]).

[32] The relevance of data for financial institutions and other participating parties should also be noted as important, representing most part of their goodwill.

The development of standardised APIs could be industry-led, but with a mechanism for national authorities to potentially provide guidance and steer its development, to contribute to a clearer legal framework to be complied with by the industry. In the absence of standards around APIs, participating firms in such ecosystems are required to connect and integrate different APIs. This can both be technically complex and require an investment in time, cost and technical capabilities that may not be readily available to smaller players (e.g. SMEs, FinTech start-ups). The inability to integrate the different APIs may obstruct their ability to access data, thereby preventing them from benefiting from such frameworks.

Common API standards could be developed by the industry along the lines of existing initiatives, but with a view to reducing fragmentation in the standards available. Authorities could consider providing support to further standardisation efforts to both guide initiatives and to ensure that standardisation efforts are abiding by any legal requirements.

The existence of portable digital IDs could act as a catalyst for cross-sectoral and cross-country data sharing to be operational. It can enable the secure connection between the entities participating in the ecosystem and ensure that they can interoperate with each other. At the cross-border level, it can enable extensibility across vertical markets beyond finance, in 'Open Data' type of ecosystems. Policy makers could consider investing in advancing ongoing or planned efforts for digital identities delivered by the official sector, particularly in light of considerable appetite from private entities to offer derived credentials with varying levels of binding to government credentials and record systems.

Policy makers may also consider promoting efforts to measure the impact of data sharing frameworks, noting that the ultimate impact on innovation, competition and value-added services based on data sharing is difficult to quantify. This shall include measuring and close monitoring of risks generated by such frameworks. Currently, measurement usually occurs through direct or intermediate impact measures, such as API calls, number of TPP licenses issued, and number of consumers who (claim to) have made use of Open Finance-related services. Indicatively, and as a first step, policy makers could encourage entities required to provide data to report activity based on API calls (type of API, duration of sharing, data recipient) with a view to mapping out the data sharing universe, based on which further impact analysis can be pursued. Such analysis could also help determine which sub-sectors of Open Finance-type of arrangements would benefit the most from such frameworks based on cost-benefit analyses.

References

ADB (2019), “Trade and the Legal Entity Identifier | Asian Development Bank”, https://www.adb.org/publications/trade-legal-entity-identifier (accessed on 6 November 2023). [75]

Alcazar, J. and F. Hayashi (2022), “Data Aggregators: The Connective Tissue for Open Banking, Kansas Fed”. [64]

Australian Government. Attorney-General’s Department (2022), *Privacy Act Review. Report 2022*, https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf. [83]

Banco Central do Brasil (2023), *Open Finance*, https://www.bcb.gov.br/en/financialstability/open_finance (accessed on 30 October 2023). [7]

Banque de France (2022), “From open banking to open finance”, https://www.banque-france.fr/en/intervention/open-banking-open-finance. [21]

Capgemini (2023), *HMRC becomes the first tax authority in the world to launch open banking payments | Capgemini*, https://www.capgemini.com/news/client-stories/hmrc-becomes-the-first-tax-authority-in-the-world-to-launch-open-banking-payments/ (accessed on 7 March 2023). [10]

CFPB (2023), *CFPB Proposes Rule to Jumpstart Competition and Accelerate Shift to Open Banking | Consumer Financial Protection Bureau*, https://www.consumerfinance.gov/about-us/newsroom/cfpb-proposes-rule-to-jumpstart-competition-and-accelerate-shift-to-open-banking/ (accessed on 30 October 2023). [91]

CFPB (2022), *Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights. Outline of Proposals and Alternatives under Consideration*, https://files.consumerfinance.gov/f/documents/cfpb_data-rights-rulemaking-1033-SBREFA_outline_2022-10.pdf. [25]

Choi, J., D. Jeon and B. Kim (2018), “Governance of Platform Markets in the ’Big Data’ Era”. [18]

CNIL (2021), *When trust pays off: today’s and tomorrow’s means of payment methods facing the challenge of data protection*, https://www.cnil.fr/sites/default/files/atoms/files/cnil-white-paper_when-trust-pays-off.pdf. [20]

CNIL (2020), “La réutilisation des données publiquement accessibles en ligne à des fins de démarchage commercial”, https://www.cnil.fr/fr/la-reutilisation-des-donnees-publiquement-accessibles-en-ligne-des-fins-de-demarchage-commercial. [43]

CPMI BIS (2020), “Committee on Payments and Market Infrastructures Enhancing cross-border payments: building blocks of a global roadmap Stage 2 report to the G20”, http://www.bis.org (accessed on 25 October 2023). [79]

Das, H. (2022), *Prepared Remarks of FinCEN Acting Director Himamauli Das During the FDIC-FinCEN Digital Identity Tech Sprint Demonstration Day | FinCEN.gov*, https://www.fincen.gov/news/speeches/prepared-remarks-fincen-acting-director-himamauli-das-during-fdic-fincen-digital (accessed on 8 March 2023). [72]

Deloitte (2020), *The future of retail banking*, https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/financial-services/deloitte-uk-hp-the-future-of-retail-banking.pdf. [84]

Deloitte (2018), “Open banking. Privacy at the epicentre”, https://www2.deloitte.com/content/dam/Deloitte/au/Documents/financial-services/deloitte-au-fs-open-banking-privacy-epicentre-170718.pdf. [48]

DNB and AFM (2023), “Financial data access Position Paper DNB and AFM”. [27]

EBA (2022), *Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2)*. [29]

EDPB (2020), *Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR*, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202006_psd2_afterpublicconsultation_en.pdf. [90]

EDPB (2020), *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf. [38]

EDPS (2023), *Opinion 38/2023 on the Proposal for a Regulation on a framework for Financial Data Access*, https://edps.europa.eu/system/files/2023-08/2023-0730_d2425_opinion_en.pdf. [57]

EDPS (2023), *Opinion 39/2023 on the Proposal for a Regulation on payment services in the internal market and the Proposal for a Directive on payment services and electronic money services in the Internal Market*, https://edps.europa.eu/system/files/2023-08/2023-0729_d2434_opinion_en.pdf. [24]

Ehrentraud, J. et al. (2020), “Policy responses to fintech: a cross-country overview”, http://www.bis.org/emailalerts.htm. (accessed on 26 September 2020). [66]

EIOPA (2022), “Open Insurance: Accessing and Sharing Insurance-related Data”, https://doi.org/10.2854/013491. [14]

EU (2023), *1. Proposal for a Regulation of the European Parliament and of the Council on a framework for Financial Data Access and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010, (EU) No 1095/2010 and (EU) 2022/2554. COM(2023) 360 final*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023PC0360. [58]

EU (2022), *Final Report on amending RTS on SCA and CSC under PSD2*, https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Draft%20Technical%20Standards/2022/EBA-RTS-2022-03%20RTS%20on%20SCA%26CSC/1029858/Final%20Report%20on%20the%20amendment%20of%20the%20RTS%20on%20SCA%26CSC.pdf. [55]

EU (2018), *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 o*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018R0389. [54]

European Commission (2023), *Adequacy decision for safe EU-US data flows*, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721 (accessed on 17 July 2023). [89]

European Commission (2023), *Impact Assessment Report. Proposal for a Regulation on a framework for Financial Data Access and amending Regulations...*, https://finance.ec.europa.eu/system/files/2023-06/230628-impact-assessment-financial-data-access-regulation_en.pdf. [85]

European Commission (2023), *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a framework for Financial Data Access and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010, (EU) No 1095/2010 and (EU) 2022/2554*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023PC0360 (accessed on 17 July 2023). [30]

European Commission (2022), *European data strategy*, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en (accessed on 27 February 2023). [9]

European Commission (2022), "Factual summary report PSD2 and open finance public consultation", https://ec.europa.eu/info/law/better-regulation/. [26]

European Commission (2022), *Report on open finance - Report of the Expert Group on the European Financial Data Space*, https://finance.ec.europa.eu/publications/report-open-finance_en (accessed on 27 February 2023). [2]

European Commission (2018), *Payment services: Consumers to benefit from cheaper, safer and more innovative electronic payments*, https://ec.europa.eu/commission/presscorner/detail/en/IP_18_141 (accessed on 30 October 2023). [4]

European Systemic Risk Board (2020), "Recommendation of the European Systemic Risk Board on identifying legal entities (ESRB/2020/12)", https://www.fsb.org/wp- (accessed on 25 October 2023). [78]

FCA (2021), *FS21/7: Open finance – feedback statement | FCA*, https://www.fca.org.uk/publications/feedback-statements/fs21-7-open-finance-feedback-statement (accessed on 8 March 2023). [65]

FCA (2019), "Call for Input Open Finance". [15]

Federal Council of Switzerland (2022), "Open finance objectives in Switzerland". [63]

Federal Trade Commission (1999), *Gramm-Leach-Bliley Act | Federal Trade Commission*, https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act (accessed on 17 July 2023). [88]

FSB (2023), "G20 Roadmap for Enhancing Cross-border Payments: Priority actions for achieving the G20 targets", https://www.fsb.org/wp-content/uploads/P091023-2.pdf (accessed on 25 October 2023). [81]

FSB (2022), *Legal Entity Identifier (LEI) - Financial Stability Board*, https://www.fsb.org/work-of-the-fsb/market-and-institutional-resilience/post-2008-financial-crisis-reforms/legalentityidentifier/ (accessed on 25 October 2023). [74]

FSB (2022), "Options to Improve Adoption of The LEI, in Particular for Use in Cross-border Payments: Options to Improve Adoption of The LEI, in Particular for Use in Cross-border Payments", http://www.fsb.org/emailalert (accessed on 6 November 2023). [77]

FSB (2020), *Enhancing Cross-border Payments: Stage 3 roadmap - Financial Stability Board*, https://www.fsb.org/2020/10/enhancing-cross-border-payments-stage-3-roadmap/ (accessed on 7 February 2023). [80]

Future of Privacy Forum (2022), "Developments in Open Banking. Key Issues from a Global Perspective", https://fpf.org/wp-content/uploads/2022/08/FPF-Open-Banking-Report-R2-Singles.pdf. [19]

GLEIF (2021), "The LEI: The Key to Unlocking Financial Inclusion in Developing Economies Plus: A Spotlight on Africa". [76]

Goldwasser, S., S. Micali and C. Rackoff (1989), "The knowledge complexity of interactive proof systems", https://people.csail.mit.edu/silvio/Selected%20Scientific%20Papers/Proof%20Systems/The_Knowledge_Complexity_Of_Interactive_Proof_Systems.pdf (accessed on 6 February 2023). [87]

González Fanfalone, A. et al. (2021), *Bridging connectivity divides*, OECD Going Digital Toolkit Notes, No. 16, https://doi.org/10.1787/6915b504-en. [12]

GPFI and World Bank (2018), *G20 Digital Identity Onboarding*, https://www.gpfi.org/sites/gpfi/files/documents/G20_Digital_Identity_Onboarding.pdf (accessed on 8 March 2023). [73]

Huysmans, X. (2019), "Direct marketing based on payment transaction data under GDPR?", https://www.linkedin.com/pulse/direct-marketing-based-payment-transaction-data-under-xavier-huysmans/. [23]

Israel (2021), *Account Information Service Law*, https://www.isa.gov.il/sites/ISAEng/1485/LawsSupervision/Account_Information_Service/Documents/HOK16122.pdf. [56]

Iwaya, S., E. Koksal-Oudot and E. Ronchi (2021), *Promoting comparability in personal data breach notification reporting*, OECD Digital Economy Papers, No. 322, https://doi.org/10.1787/88f79eb0-en. [92]

JROC (2023), *Recommendations for the next phase of open banking in the UK*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1150988/JROC_report_recommendations_and_actions_paper_April_2023.pdf (accessed on 16 June 2023). [31]

Kuebler-Wachendorff, S. et al. (2021), "The Right to Data Portability: conception, status quo, and future directions", *Informatik Spektrum*, https://doi.org/10.1007/s00287-021-01372-w. [62]

Lemery, S. and R. Steiner (2020), "Mise en oeuvre d'une politique de localisation des données critiques de paiement en Europe. Rapport à Monsieur le Ministre de l'Economie et des Finances", https://www.economie.gouv.fr/files/files/directions_services/cge/donnees-paiement.pdf. [50]

Linda Jeng (2022), *Open Banking*, Oxford University Press, https://doi.org/10.1093/OSO/9780197582879.001.0001. [67]

Lomas, N. (2019), "Covert data-scraping on watch as EU DPA lays down 'radical' GDPR red-line", https://techcrunch.com/2019/03/30/covert-data-scraping-on-watch-as-eu-dpa-lays-down-radical-gdpr-red-line/. [44]

MacCarthy, M. (2011), "New Directions in Privacy: Disclosure, Unfairness and Externalities", https://papers.ssrn.com/abstract=3093301 (accessed on 18 July 2023). [17]

McKinsey (2017), "Data sharing and open banking", https://www.mckinsey.com/industries/financial-services/our-insights/data-sharing-and-open-banking. [53]

Medine, D. and A. Plaitakis (2023), *Combining Open Finance and Data Protection for Low-Income Consumers*, https://www.cgap.org/sites/default/files/publications/20230216_Medine_TN_OpenFinanceDataProtection.pdf. [34]

OAIC (n.d.), *Privacy guidance for organisations and government agencies: Small business*, https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/organisations/small-business. [47]

OECD (2023), "Central Bank Digital Currencies (CBDCs) and democratic values", *OECD Business and Finance Policy Papers*, No. 31, OECD Publishing, Paris, https://doi.org/10.1787/f3e70f1f-en. [46]

OECD (2023), "Data portability in open banking: Privacy and other cross-cutting issues", https://doi.org/10.1787/6c872949-en. [8]

OECD (2023), "Emerging privacy enhancing technologies", http://www.oecd.org/going-digital. (accessed on 17 July 2023). [86]

OECD (2023), *Emerging privacy-enhancing technologies: Current regulatory and policy approaches*, https://doi.org/10.1787/bf121be4-en. [45]

OECD (2023), *Recommendation of the Council on the Governance of Digital Identity, OECD/LEGAL/0491*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0491. [71]

OECD (2023), *Review of the 2007 OECD Recommendation on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy (Internal document)https://one.oecd.org/official-document/DSTI/CDEP/DGP(2022)2/REV2/en*, https://one.oecd.org/official-document/DSTI/CDEP/DGP(2022)2/REV2/en. [52]

OECD (2023), *Shifting from open banking to open finance: Results from the 2022 OECD survey on data sharing frameworks | en | OECD*, https://www.oecd.org/finance/shifting-from-open-banking-to-open-finance-9f881c0c-en.htm (accessed on 21 May 2023). [6]

OECD (2023), "Shifting from open banking to open finance: Results from the 2022 OECD survey on data sharing frameworks", *OECD Business and Finance Policy Papers*, No. 24, OECD Publishing, Paris, https://doi.org/10.1787/9f881c0c-en. [3]

OECD (2023), *The shift from Open Banking to Open Finance: Results from the 2022 OECD survey on data sharing frameworks - Google Search*, https://www.google.com/search?q=The+shift+from+Open+Banking+to+Open+Finance%3A+Results+from+the+2022+OECD+survey+on+data+sharing+frameworks&rlz=1C1GCEB_enFR969FR969&oq=the+shift&aqs=chrome.1.69i57j69i59l2j46i175i199i512j0i512l3j69i60.2000j0j7&sourceid=chrome&ie=UTF-8 (accessed on 7 February 2023). [1]

OECD (2022), *Dark commercial patterns*, OECD Digital Economy Papers, No. 336, https://doi.org/10.1787/44f5e846-en. [94]

OECD (2022), *Expert Workshop on Data Ethics: Balancing Ethical and Innovative Uses of Data (internal document)*, OECD, https://one.oecd.org/official-document/DSTI/CDEP/DGP(2022)1/en. [59]

OECD (2022), *Fostering cross-border data flows with trust*, https://doi.org/10.1787/139b32ad-en. [49]

OECD (2022), *Recommendation of the Council on High-Level Principles on Financial Consumer Protection [OECD/LEGAL/0394]*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0394. [32]

OECD (2021), *Artificial Intelligence, Machine Learning and Big Data in Finance Opportunities, Challenges and Implications for Policy Makers*, https://www.oecd.org/finance/artificial-intelligence-machine-learningbig-data-in-finance.htm. (accessed on 22 August 2022). [11]

OECD (2021), *Bridging digital divides in G20 countries*, https://doi.org/10.1787/35c1d850-en. [93]

OECD (2021), *Mapping Data Portability Initiatives, Opportunities and Challenges*, https://www.oecd.org/publications/mapping-data-portability-initiatives-opportunities-and-challenges-a6edfab2-en.htm. [60]

OECD (2021), *Recommendation of the Council on Enhancing Access to and Sharing of Data, OECD/LEGAL/0463*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0463. [28]

OECD (2020), *Financial Consumer Protection Policy Approaches in the Digital Age: Protecting Consumers' Assets, Data and Privacy*, https://www.oecd.org/daf/fin/financial-education/Financial-Consumer-Protection-Policy-Approaches-in-the-Digital-Age.pdf. [33]

OECD (2020), *Compendium of Effective Approaches for Financial Consumer Protection in the Digital Age*, https://www.oecd.org/daf/fin/financial-education/financial-consumer-protection/Effective-Approaches-FCP-Principles_Digital_Environment.pdf. [35]

OECD (2020), “Regulatory and Supervisory Framework for Insurance Intermediation”. [13]

OECD (2013), *The OECD Privacy Framework*, https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. [39]

OECD (2009), *OECD Guidance for Electronic Authentication (2007)*, https://www.oecd.org/sti/ieconomy/49338232.pdf. [69]

OECD (2009), “The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers”, *OECD Digital Economy Papers, No. 160*, https://doi.org/10.1787/222134375767. [70]

OECD (2007), *Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy, OECD/LEGAL/0352*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0352. [22]

OECD (2007), “Recommendation of the Council on Electronic Authentication (OECD/LEGAL/0353)”, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0353. [68]

OECD (forthcoming), *Privacy Guidelines. Implementation Guidance. Chapter on Accountability*. [40]

OECD (1980, 2013), *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD/LEGAL/0188*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188. [37]

Pellitteri, R. et al. (2023), “L’Open Banking nel sistema dei pagamenti: evoluzione infrastrutturale, innovazione e sicurezza, prassi di vigilanza e sorveglianza”, https://www.bancaditalia.it/pubblicazioni/mercati-infrastrutture-e-sistemi-di-pagamento/questioni-istituzionali/2023-031/N.31-MISP.pdf. [41]

Svantesson, D. (2020), “Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines”*, OECD Digital Economy Papers*, No. 301, OECD Publishing, Paris, https://doi.org/10.1787/7fbaed62-en. [51]

The Wolfsberg Group (2023), *Wolfsberg Group Payment Transparency Standards*, https://db.wolfsberg-group.org/assets/13422898-fba1-44b3-9679-a8c7406e9e78/Wolfsberg%20Group%20Payment%20Transparency%20Standards%202023.pdf. [82]

Tsai, J. et al. (2011), *and Egelman, Serge and Cranor, Lorrie Faith and Acquisti, Alessandro, The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, https://doi.org/10.1287/isre.1090.0260. [16]

UK CMA (2023), *Millions of customers benefit as Open Banking reaches milestone - GOV.UK*, https://www.gov.uk/government/news/millions-of-customers-benefit-as-open-banking-reaches-milestone (accessed on 30 October 2023). [5]

Unnax (2022), “The State of PSD2 in Spain in 2022: Does Scraping Still Have a Place?”, https://www.unnax.com/psd2-scraping-account-aggregation-services/#:~:text=A%20year%20before%2C%20the%20European,only%20connecting%20to%20PSD2%20APIs. [42]

Wong, J. and T. Henderson (2019), “The right to data portability in practice: exploring the implications of the technologically neutral GDPR”, *International Data Privacy Law*, https://doi.org/10.1093/idpl/ipz008. [61]

World Bank Group; Ministry of Foreign Affairs of the Netherlands (2021), “The Role of Consumer Consent in Open Banking”, https://openknowledge.worldbank.org/bitstream/handle/10986/37073/P1705050aeb8e704f088260f228802b73b8.pdf?sequence=1&isAllowed=y. [36]