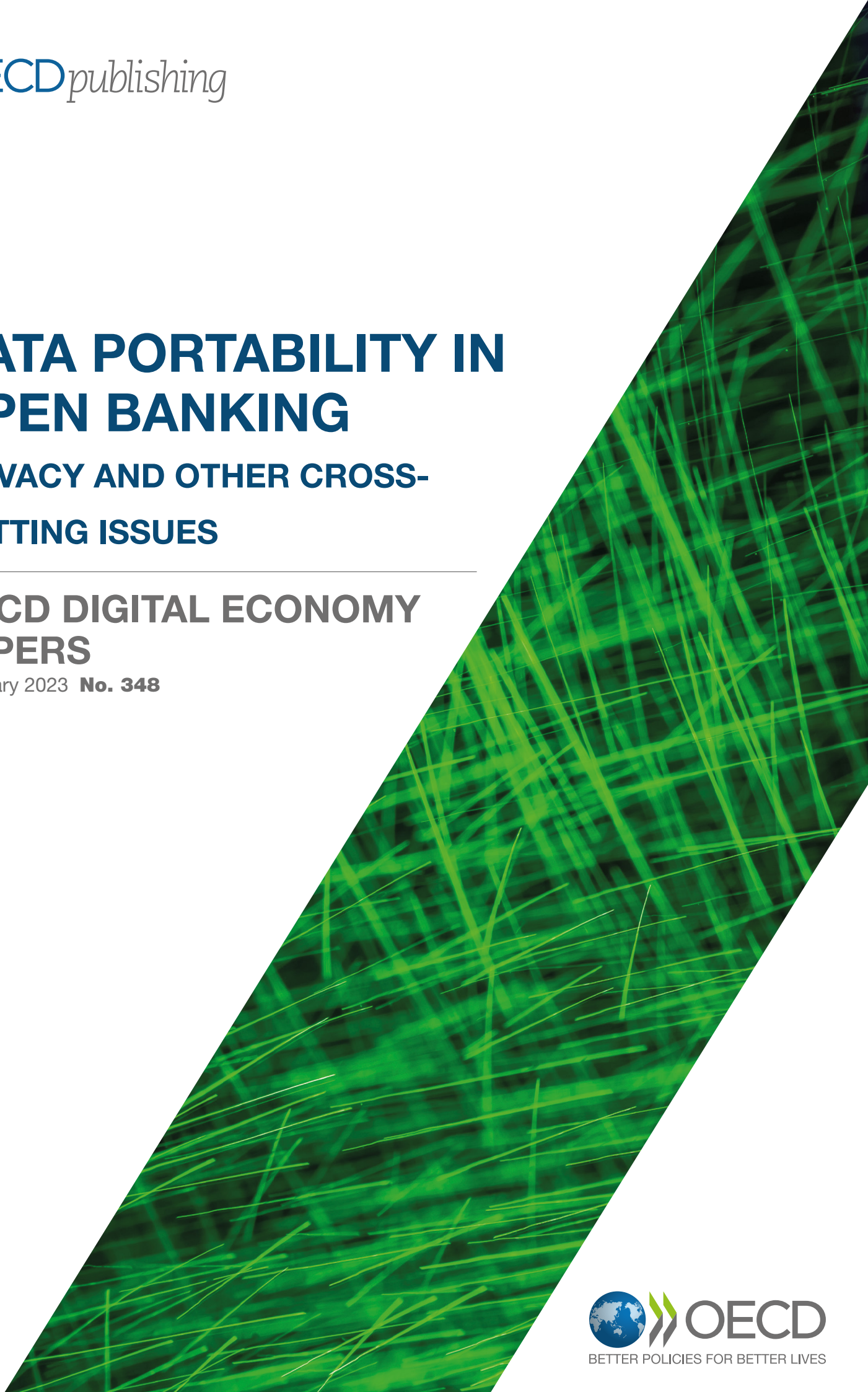
OECD publishing

# DATA PORTABILITY IN OPEN BANKING

## PRIVACY AND OTHER CROSS-CUTTING ISSUES

OECD DIGITAL ECONOMY PAPERS

February 2023 **No. 348**



OECD
BETTER POLICIES FOR BETTER LIVES

## Foreword

This report presents a summary of the main points emerging from the virtual workshop 'Data Portability in Open Banking: Privacy and Other Cross-Cutting Issues', which was organised by the OECD jointly with the Future of Privacy Forum and the Israel Tech Policy Institute and held on 16 and 17 March 2022. It was drafted by Giuseppe Bianco and Andras Molnar (OECD Secretariat). Panellists reviewed the draft and provided input.

The summary follows the structure of the workshop, and focuses on the four main issues that were addressed. Namely: i) data-driven innovation in banking: the state of play of open banking; ii) data portability and inclusion as the economic and social rationales for open banking; iii) privacy, consent and liability in open banking; and iv) co-operating among regulators, nationally and internationally. The Annex contains the workshop agenda.

The summary was prepared under the aegis of the OECD Committee for Digital Economy Policy (CDEP), with input from delegates of the Working Party on Data Governance and Privacy in the Digital Economy. It was approved and declassified by CDEP by written procedure on 9 December 2022 and prepared for publication by the OECD Secretariat.

*Note to Delegations:*

*This document is also available on O.N.E under the reference code:*

*DSTI/CDEP/DGP(2022)11/FINAL*

This document, as well as any data and map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

# Table of contents

# Executive Summary

Open banking initiatives employ consent-based data portability tools to improve user access to financial information and services. Such initiatives seek to empower users to unlock the potential of their data, while also preserving privacy and security. On 16 and 17 March 2022, the OECD, together with the Future of Privacy Forum and the Israel Tech Policy Institute, held a virtual workshop on 'Data Portability in Open Banking: Privacy and Other Cross-Cutting Issues'. This workshop brought together private and public experts from a wide variety of countries, and provided an opportunity to explore open banking and the opportunities and challenges it can bring.

This summary sets out the main findings of the workshop, which include:

- Open banking can offer significant benefits. It can empower consumers and promote greater financial inclusion in the banking sector. It can help users play an active role in the sharing and re-use of their financial data across digital services, online platforms, sectors and borders. It can also enhance innovation and help in the development of financial products that can reach the "underbanked".
- At the same time, the open banking ecosystem presents risks. For example, data sharing through portability and interoperability may open up the possibility of data breaches, and when data is shared across multiple parties it can raise privacy concerns. Reconciling data protection obligations and open banking frameworks remains a challenge in many jurisdictions, and there is lingering uncertainty about how open banking and other data sharing frameworks interact with data protection and privacy regimes.
- Open banking is happening in practice in several jurisdictions, and several governments have created legal frameworks and technical mechanisms to facilitate it. Different approaches have been taken, from those grounded in regulation (e.g. in the European Union and Israel) to market-driven approaches based on voluntary collaboration and reciprocity (e.g. Singapore). Furthermore, the use of industry-wide API standards and a focus on customer experience can ensure high customer uptakes (e.g. in the United Kingdom).
- Three policy objectives are at stake in open banking: i) financial stability and integrity, ii) privacy and consumer protection, and iii) efficiency and competition. The complexity of the trade-offs among these policy objectives raises the need for national and international coordination among different financial and non-financial regulators.

Trust and efficiency are essential in making the open banking system work in practice. In order to achieve this, regulators and policy makers may need to explore new models of regulatory co-operation between systems and across borders. This is likely to be necessary in reducing fragmentation in standards and ensuring more clarity on the relationship between data protection laws and open banking laws. Robust data protection and privacy regimes are needed to capitalise on the promises of open banking, while mitigating any risks. Looking forward, the OECD could consider how cross-sectoral cooperation between financial, competition and data protection authorities could help further open banking.

# *Data Portability in Open Banking: Privacy and Other Cross-Cutting Issues*

## Summary of main points[1]

## 1. Background

Open banking is a set of initiatives by governments and industry to implement data portability and improve users' access to financial information and services, while preserving privacy and security. The overall goal of open banking is to empower users and to unlock the potential of their data. Open banking is defined as the sharing and leveraging of customer-permissioned data by banks with third-party developers and firms to build applications and services, including for example those that provide real-time payments, greater financial transparency options for account holders, marketing and cross-selling opportunities (Basel Committee on Banking Supervision, 2019[1]).

Thus, customers obtain the ability to access data, grant data permissions, or share data with third parties for various services and financial benefits. Because of these benefits, open banking is at the forefront of supporting financial inclusion, increasing competition in the financial sector, and encouraging responsiveness to consumer needs through innovation, while providing meaningful privacy protections and data rights to a diverse set of consumers over their sensitive financial data.

### Opportunities and challenges of open banking

In open banking, consumers and businesses can benefit from evolving business and technology solutions to better manage their finances. Examples include: improving aggregation of information held in different accounts and institutions, giving consumers both a better overview of their financial status and the option of involving a host of applications to analyse the data and provide financial advice and cost-reducing recommendations; supporting the innovation of the financial sector through the development of wider services to reduce costs, ease transactions, and promote financial planning; and serving the unbanked who do not have access to traditional banking services. Initial evidence suggests a positive impact of open banking initiatives on competition: for example, since the Retail Banking Market Investigation Order 2017 (CMA, 2017[2]) and the Payment Services Regulations 2017 (UK, 2017[3]) entered into force, approximately 300 third parties have joined the open banking ecosystem in the United Kingdom, as of August 2022 (UK Open Banking, 2022[4]).

Although these initiatives started rolling out in countries like the United Kingdom and others around 2017, they are infused with a renewed sense of urgency due to the strains the COVID-19 pandemic has laid on economies globally. The pandemic has induced the requirement for lockdowns and social distancing, which have increased reliance on digital financial services (The Economist Intelligence Unit and Temenos, 2020[5]) through digital means, payments could occur and financial support could reach those in need, without physical contact (Agur, Martinez Peria and Roch, 2020[6]). To face the economic downturn due to the COVID-19 pandemic, more businesses have turned to open banking. Thanks to open banking, micro, small and medium-sized enterprises have improved their accounting and cash flow forecasting capabilities, and this clearer view of their financial performance has helped them to stay in business (Italian Presidency

of the G20 and G20 Global Partnership for Financial Inclusion, 2020[7]). For example, of the small businesses surveyed in the United Kingdom that had started using open banking providers since March 2020, 90% stated that their decision was a direct result of COVID-19.[2] Furthermore, there is an increase in data from open banking being used to provide credit, as lending providers can assess creditworthiness more accurately and tailor funding solutions (Open Banking Implementation Entity and Ipsos MORI, 2020[8]).

Open banking also has the potential to address financial exclusion, if properly designed (Plaitakis and Staschen, 2020[9]). Open banking ecosystems can reduce barriers to access, provide access to responsible credit, encourage informed financial behaviours, and enable participation in the global economy (Yazdanpanah, 2021[10]). Thus, open banking can assist in the inclusion of traditionally excluded categories, especially in emerging markets and developing economies with scarce (or non-existing) public credit information (Italian Presidency of the G20 and G20 Global Partnership for Financial Inclusion, 2020[7]). In addition, in Kenya and in other African countries, open banking is having a significant impact on instant payments and government payments (Soar and Mwago, 2020[11]).

Whilst open banking provides considerable benefits, it also involves significant challenges, which are exacerbated due to the importance and sensitivity of financial data. Data breaches related to the financial sector carry considerable risks for users, thereby requiring these initiatives to include digital security mitigation measures. Third-party application providers entering into the financial sector require the question of liability to be addressed. As other countries consider introducing open banking measures, the level of government oversight, the type of enforcement mechanisms, and the permitted use purposes of the data need to be defined.[3]

## Relevant OECD work

The OECD has been conducting relevant work in the area of open banking and data portability. Its Privacy Guidelines have been a cornerstone for data protection regulation in both member and non-member countries around the world. The recent review of their implementation has highlighted the importance of strengthening data subject rights such as data portability (OECD, 2013[12]). The OECD has also held a number of expert workshops to discuss data portability from both a privacy and a competition perspective (OECD, 2020[13]) (OECD, 2021[14]) (OECD, 2021[15]) (OECD, 2021[16]), and has published an analytical report (OECD, 2021[17]).

The OECD Financial Consumer Protection Policy Approaches in the Digital Age and its guidance on mobile and online payments are also relevant to open banking (OECD, 2014[18]). Furthermore, the OECD has examined open banking as part of its work on finance and digitalisation (OECD, 2019[19]).

## Objectives of the workshop

To bring these diverse perspectives together and to help advance the conversation, the OECD organised a two-day workshop jointly with the Israel Tech Policy Institute and the Future of Privacy Forum on 16 and 17 March 2022. The workshop brought together subject-matter experts from governments, privacy enforcement authorities, and competition authorities, banking regulators, international organisations, industry, civil society and academia. It explored some of the challenges of open banking and the strategies for promoting a mix of financial inclusion, robust competition, and strong protection for data subjects. In particular, it considered the need for co-operation among privacy, competition and banking regulators, and the difficulties this entails.

## 2. Data-driven innovation in banking: the state of play of open banking

***Short summary*** *– The current open banking landscape includes different approaches, ranging from regulatory to market-driven approaches. The regulatory approach of the EU focuses on the Payment Services Directive II (PSD2), and it is the first legal instrument to give customers access to data from their payment accounts through third parties. PSD2 requires banks to build up interfaces through which these third parties can securely access these accounts, without requiring a single API standard. In Israel, the Financial Information Service Law 2021 aims to open up different kinds of data signalling a move to "open finance". In the United Kingdom, the API standard adopted by the nine largest banks (as required by the Competition and Markets Authority) has become the generally accepted, industry-wide standard. This, together with a focus on customer experience, has ensured a high uptake. Non-regulatory approaches include Singapore's market-driven approach, which is based on voluntary collaboration, and the encouragement of uptake through reciprocity.*
*Future policies may extend to broader categories of data, aim to reduce fragmentation in standards, and ensure more clarity on the relationship between data protection laws and open banking laws.*

### Introduction

Pinar Ozcan (Academic Director, Oxford Future of Finance and Technology (Fintech) Initiative) recalled how different open banking initiatives have been in place in some countries for several years, or are currently being planned. Different policy-makers and agencies have taken (or are considering) different paths with regard to the need for legislation/regulatory action. The experience accumulated over the years can shed light on the difficulties encountered to balance data protection while promoting wider sharing of banking data.

Ozcan highlighted the challenges for open banking, such as the development of application programming interfaces (APIs), the extent to which data being shared is useful, and whether data sharing is enough to boost innovation and competition across markets.

### The regulatory-driven approach of the EU's Payment Services Directive 2

Larisa Tugui (Senior Policy Expert, Conduct, Payments and Consumers Unit, European Banking Authority) illustrated the experience of the European Union. The so-called Payment Services Directive II (PSD2) (EU, 2015[20]) represented a paradigm shift, as the first legal act to give consumers the right to access payment accounts through third parties. It is an example of a regulatory-driven initiative on open banking. The PSD2 has required banks to build up interfaces through which these third party can securely access these accounts, and prohibited screen scraping for accessing payment accounts.[4]

Challenges in the implementation of the PSD2 have been primarily related to the high-level nature of its text. The European Banking Authority (EBA) has played a crucial role, as it has adopted technical standards and guidelines. The EBA's Regulatory Technical Standards have defined how banks should build interfaces for third-party providers to receive data. The EBA has issued more than 200 Questions and Answers, and many own initiative opinions.

Both the PSD2 and the standards developed by the EBA are technology neutral. Banks can use APIs or allow third-party service providers to use the same interface that customers use. The option of developing a single API in the EU was explored by the EBA at the time of developing the Regulatory Technical Standards in 2016-2017. However, eventually the decision has been

made not to develop it, as it would not have been possible within the time limits set by the PSD2. In addition, market participants were considered technologically better equipped than public authorities to develop a single API. In the market, there has been widespread adoption of the "Berlin Group" standards for access to payment accounts, with around 75% of European banks that follow them (Berlin Group, n.d.[21]).[5]

However, fragmentation remains one of the main challenges, and raises issues for new entrants to the market. At this stage, APIs are improving, but some issues persist across EU Member States. There are also different levels of consumer uptake of third-party services across the EU.

On the bright side, new, innovative, and added-value services leveraging the PSD2 have been brought to the market and more than 400 non-bank third-party providers have been authorised in the EU under the PSD2 framework (many of which passport their services into other EU Member States). This points to the fact that the competition-enhancing objective of PSD2 has started to materialise. Furthermore, an increasing number of banks are themselves acting as third-party providers. This latter figure is not known because banks do not need to request a specific authorisation. Moreover, the introduction of security requirements, in particular strong customer authentication, has led to a reduction of fraud levels.

The European Commission has requested the advice of the EBA on the review of the PSD2 (European Commission, 2021[22]). One of the questions addressed the evolution from open banking to open finance. Tugui noted that, building on the experience gathered with the PSD2 implementation, a future framework on open finance would need to clarify what type of data can and cannot be accessed, how consumers can provide consent, and how incumbents should provide access to third-party providers. Additionally, such framework should empower and oblige supervisory authorities to enforce these requirements to ensure compliance, to the same standard and equally across the EU, and be carefully aligned with the GDPR.

## The market-driven approach of Singapore

Singapore is an example of a market-driven approach to open banking. Alan Lim (Head, FinTech Infrastructure Office, Monetary Authority of Singapore) noted that collaboration is particularly important in this model, where there is no mandated requirement for open banking and uptake is encouraged through reciprocity.

The Monetary Authority of Singapore (MAS) has established the Singapore Financial Data Exchange (SGFinDex), a public digital infrastructure that uses a national digital identity and centrally managed online consent system. SGFinDex allows data sharing through an infrastructure instead of bilateral connections. The infrastructure does not itself store data, but only works as a gateway. It enables individuals to access, through applications, their financial information held across different government agencies and financial institutions. Banks can support customers retrieve information from their bank accounts, insurers, etc., and use it for their holistic financial planning.

On the payments front, non-bank financial institutions can gain access to the banking systems' retail payments infrastructure. This allows for consumer-to-consumer transfers: with a mobile phone number, a person can transfer money to another person's e-wallet. This allows payment interoperability across platforms with participating fintechs and financial institutions.

A Financial Industry API Registry has also been introduced. It contains open APIs made available by financial institutions, which concern products, sales and marketing, servicing, and

transactions. Almost 1700 open APIs were available as of 2020 (Monetary Authority of Singapore, 2022[23]).

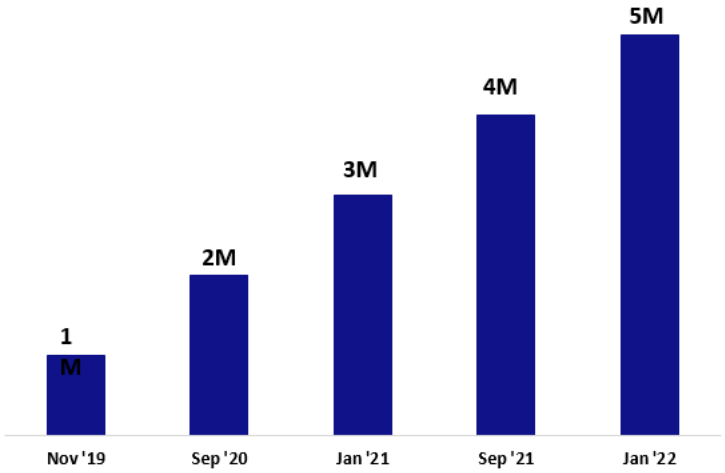
The MAS has also been promoting data sharing innovation through its participation in the API Exchange (APIX). It is a global, open-architecture platform that supports financial innovation and inclusion in Association of Southeast Asian Nations (ASEAN) and around the world. This marketplace and sandbox allows market players to connect with one another, design experiments collaboratively and deploy new digital solutions (Monetary Authority of Singapore, 2021[24]), with the ultimate goal of creating a more seamless and mobile outcome for consumers and market participants.

## The United Kingdom's experience with common standards

Richard Mould (Senior Policy Lead, UK Open Banking Implementation Entity) focused on the key features of open banking in the UK regulatory environment. The Competition and Markets Authority (CMA) was worried about a lack of competition in the banking sector. Therefore, in addition to the obligations stemming from the PSD2, the CMA required the nine largest banks in the United Kingdom to adopt the same API standard. This in turn provided a critical mass for a generally accepted, industry-wide standard. Such a common technical standard stands in contrast to the EU-wide context, where the EBA has not mandated a similarly unified standard across the continent.

The uptake of open banking in the United Kingdom has been considerable. At the end of 2021, there were more than 300 third-party service providers. In addition, from November 2019 to January 2022, the number of unique users grew from one million to five million (see Figure 1).

### Figure 1. Number of unique open banking users in the United Kingdom




Source: Richard Mould, UK Open Banking Implementation Entity, presented at the workshop on "Data Portability in Open Banking: Privacy and Other Cross-Cutting Issues", 16 March 2022.

The first focus of open banking ecosystems in the United Kingdom has been on money management tools. These tools are designed to help customers make better financial decisions via a holistic approach to financial management. Secondly, open banking has allowed for the use of transactional data to enable better lending. The main benefit of using this information for lending decisions has been that the purchase of lending services has been improved. Furthermore, this has expanded lending opportunities: particularly consumers with no credit

history could access credit thanks to the use of historical transaction data. Conversely, in the past such customers may not have been granted loans because of the lack of relevant data.

Open banking has also brought further advantages. Small businesses have improved their accounting processes, with lower administrative burdens. The clear framework for data sharing mechanisms provided by open banking has replaced older technologies like screen scraping, which existed in a grey, less defined legal context. Moreover, open banking allows linking transactions more closely to a richer set of data. Therefore, companies that collect funds enjoy a lower reconciliation burden. In addition, open banking offers benefits in a number of specific consumer areas, for example it reduces human errors (e.g. the "fat finger" problem, a keyboard input mistake resulting in the transmission of the wrong information) in paying via open banking after filing taxes online.

The objective of consumer protection means that the regulator ensures banks do not put undue barriers in place between customers. Moreover, this objective has led the United Kingdom to also introduce Customer Experience Guidelines. For example, these standards concern dashboards, a common tool used in many industries to enable customers to manage their connections with service providers (Open Banking Implementation Entity, 2022[25]). Standards for consent and access dashboards ensure that customers stay in control. As a result, the industry is beginning to coalesce around commonly accepted terms for what "open banking" is. This uniform terminology helps institutions communicate with their customers.

As mandated implementation is about to be completed, the next steps may realise the potential of expanding into open finance, with data sharing across more financial products. Furthermore, open banking payments may be fully implemented. Finally, the new API infrastructure may be leveraged to reduce fraud by improving identity checking.

## The broad Israeli legislation

Daniel Hahiashvili (Head of Technology and Innovation Division, Central Bank of Israel) illustrated how the Financial Information Service Law 2021, adopted in November 2021, introduced a broad road map for open banking in Israel. It contains specific timetables for opening different kinds of data, with open banking coming into force in June 2022. Because of its breadth, this legislation is more akin to "open finance", in that it involves other parts of the financial system (e.g. securities).

The basic premises of the Israeli approach are that data is valuable as everything today is driven by data, and that data belongs to the customer. As more entities enter the market, the increased competition and innovation favour consumers. Furthermore, unbundling services and facilitating the collaboration between fintechs and banks can bring higher value for customers. As Israel has a concentrated banking system, the legislation has prioritised open finance to achieve an open eco-system with a variety of players, both existing and new ones.

The regulation mandates standards for the entire ecosystem, for data sharing on current accounts, savings, loans, securities, etc. Thanks to the development of API abilities, financial service providers and banks will be able to offer a wider variety of services, engage with a wider range of parties, and develop new products, such as account aggregation and easy financial product comparisons.

Open banking can unlock the potential for collaboration and partnerships between banks, fintechs, and other third parties. This can result in digital wallets, digital platforms for services, and marketplaces for multiple financial service offerings.

Dilemmas faced in the adoption of the legislation concern competition, with regard to what will drive new competition and what level of support should be provided to new fintechs. On oversight, questions embrace how to approach new entrants and their connections with the financial system, and whether the appropriate level and scope of supervision should focus on data protection or include wider consumer protection issues. Finally, on privacy, dilemmas are over a general or an explicit consent for data collection, the monetisation of data, and whether there should be a separate model for privacy in the financial sector.

### A view from the private sector

Fanny Solano (Head of Regulatory Affairs & Implementation Management, Caixa Bank) noted that third-party providers use banks as supporting platforms. Instead, all participants should be required to contribute to establishing and maintaining the new infrastructure, also in terms of costs. In addition, open data should be implemented across all sectors, to mix data from other sectors with financial data, and serve customers better.

Finally, challenges around open banking were noted. The issue of market concentration in banking/financial services has not been fully solved by PSD2 or other open banking initiatives. A lack of clear regulation, or clarity on the interaction between open banking and other regulations, can make innovation and competition more difficult, and has had to be addressed over time via guidelines and opinions. Ensuring that privacy and security needs are met and balanced with the benefits of open banking can also represent a challenge.

## 3. Data portability and inclusion as the economic and social rationales for open banking

***Short summary*** *– Open banking can empower consumers and promote greater financial inclusion for underserved populations. Open banking can reduce the switching costs for users between traditional banks and fintechs. It can also help enhance innovation, which in turn can advance the development of financial products that can reach the "underbanked".*
*Recognising the significant benefits of open banking, several governments have created legal frameworks and technical mechanisms to facilitate open banking. The United Kingdom's Open Banking Implementation Entity was established to agree, implement and maintain open and common banking standards in the country. Recent changes in Australia allow financial data to be shared with financial counsellors, meaning that vulnerable consumers in open banking can access assistance and expert advice.*
*However, despite the significant benefits of open banking, data sharing across multiple parties raises privacy concerns. In encouraging consumers to join open banking, it is important that the necessary data and privacy protections are in place.*

### Introduction

The second session, moderated by Ori Schwartz (Head of Competition Division, OECD), highlighted that open banking has the potential to promote greater financial inclusion in the banking sector and to empower consumers by reducing the cost of switching between traditional banks and fintechs. Third parties with consent from data subjects can access data that has historically been held by incumbents. This can promote innovation and enable the development of financial products that can reach underserved populations (i.e. the "underbanked"). However, whilst there are opportunities for greater consumer benefits, experts also noted that data sharing among multiple parties could raise privacy concerns.

## Challenges to providing greater financial inclusion

Ms Sheila Jambekar (Chief Privacy Officer, Plaid) noted in her presentation that there are three points of frictions that can undermine financial inclusion:

- *The "unbanked" and "underbanked" problem:* Historically, banking used a "one-size-fits-all" approach which inherently left out underserved populations, did not meet their needs or was too expensive for them to afford. However, open banking is able to challenge this system by for instance providing lower fees and overdraft protections. By giving consumers and businesses the opportunity to share their transaction history, open banking enables innovative landing platforms to build algorithms that can assess credit worthiness and provide loans. In particular, SMEs owned by minorities benefited largely from loans that were provided by fintech companies.
- *Difficulties for consumers to sign up for open banking services:* Consumers might find it difficult to switch from traditional banks to open banking services. However, if innovators can make it easier for consumers to port their data to open banking services, there is a greater chance that more consumers can sign up for these services.
- *Lack of trust in open banking services:* There are certain consumers who might be hesitant to sign up for open banking services, due to concerns about data breaches or privacy. In addition, there is a generational gap in using open banking services, as older generations are more hesitant to use open banking. In this regard, appropriate data and privacy protections can encourage consumers from a broader and more diverse background to join open banking and improve the overall open banking ecosystem.

## Australia's open banking ecosystem

Mr Paul Franklin (Executive General Manager, Consumer Data Right Division, Australian Competition and Consumer Commission) described in his presentation Australia's open banking ecosystem. The current open banking ecosystem has a variety of actors, and they have all contributed to the progressive take up of open banking in Australia. These actors include data holders, data recipients, and consumers. Data holders supply the data. Data holders include banks that are required to make data available to all customers. The demand side includes data recipients (such as banks and third parties that want to offer innovative services) and consumers. Data recipients have been reluctant to provide banking services before witnessing ubiquitous availability of data. In particular, banks prioritised compliance with data sharing obligations over competing in the market. Nevertheless, the number of data recipients is gradually increasing.

Mr Franklin noted that Australia's Consumer Data Right (CDR) was enacted in order to spur competition and innovation and to ensure that financial services are more affordable to consumers (Australian Competition and Consumer Commission, 2019[26]). Australia could largely avoid the challenges of "underbanking" or accessibility to financial services concerns, given that a large portion of the population is already enrolled in banking at birth. However, the country's policy recognizes that the existing banking ecosystem may not be easy to use and that it must address financial issues affecting vulnerable populations (e.g. to prevent arrears). In this regard, open banking can be a useful tool to provide financial services to vulnerable consumers. In addition, recent rule changes in Australia also permit the sharing of financial data with mortgage brokers and financial counsellors (known as "trusted advisors") that can support vulnerable

consumers by providing advice on loans and financial challenges these consumers might face in open banking. The CDR also sets out limits on data sharing that are relevant to open banking. Among these restrictions is the prohibition on screen scraping. This is a practice of providing a third party one's credentials to grant them access to a digital account and "scrape" the data from that interface and, in certain cases, to execute transactions on behalf of the consumer (OECD, 2021[17]).

There are several government entities that oversee Australia's open banking ecosystem. Under CDR, the Australian Consumer and Competition Commission (ACCC) has to i) establish and maintain a Register of Accredited Persons and Data Holders; ii) provide guidance to stakeholders about their rights and obligations under the CDR; iii) and take enforcement action (in a co-regulatory manner in collaboration with the Office of the Australian Information Commissioner). The Federal Treasury also plays a key role in open banking regulation. The Treasury's Data Standards Body has the responsibility to design, build and run the technology for data sharing.

## Open banking in the United Kingdom

In 2016, the United Kingdom's Competition Market Authorities (CMA) concluded an investigation into the retail banking market (Competition and Markets Authority, 2016[27]). The investigation followed previous interventions that had had limited impact in improving competition in the retail banking industry. In her presentation, Ms Sabrina Basran (Director, Competition and Markets Authority, United Kingdom) highlighted that the investigation focused on personal current accounts (PCA) and SME banking, with a particular focus on business current accounts and SME lending. The CMA found a number of competition concerns, including barriers to accessing and assessing information, barriers to switching, and incumbency advantages. In terms of remedies, the CMA required the nine largest banks in the United Kingdom to set up and fund an organisation, the Open Banking Implementation Entity. The Open Banking Implementation Entity was tasked with agreeing, implementing and maintaining open and common banking standards.

In the United Kingdom, the open banking ecosystem is reliable and resilient. There are three hundred and thirty regulated providers and roughly two thirds are third-party providers. The number of end users participating in open banking is also significant and growing exponentially. There were five million end users in total as of December 2022 and open banking is expected to reach sixty percent of the population by September 2023. Most of this growth has come from the open banking payment space.

Nevertheless, in order to protect customer data, build trust and enable take-up, it is critical to have sufficient privacy and security safeguards. Accordingly, there are a number of measures in place to promote control and safety of data for open banking users in the United Kingdom. For instance:

- open banking security standards in the United Kingdom are industry-led, and financial institutions in open banking invest heavily in the resilience of their systems;
- only third-party providers are able to access account data that are regulated by the Financial Conduct Authority (FCA);
- the PSD2 and the United Kingdom Payment Services Regulations place a strong reliance on consent as the only gateway to data access, use of access and consent dashboard tools for consumers;
- an ombudsman has been established for redress;

- further FCA rules will be issued that clarify the level of required consumer authentication.

## Competition-driven rationales for, and implications of, open banking

Mr Giuseppe Colangelo (Jean Monnet Chair in European Innovation Policy, University of Basilicata) in his presentation focused on the competitive rationale for and implications of open banking. Mr Colangelo underlined that open banking may offer many benefits to society. These include the potential to reduce the legal and technical barriers that have made it difficult for customers to: i) access their information easily; ii) share information with third parties; iii) and switch to products and services offered by different financial institutions. The presence of these barriers hurts competition by creating customer inertia and allowing incumbents to reap economic benefits from customers.

In light of the potential benefits of open banking, governments around the world have created or have been involved in the creation of legal and technical mechanisms to facilitate open banking. For instance, the EU's PSD2introduced a data portability rule by forcing banks, with the consumer's consent, to share certain data with authorized third parties. There are proposals for data sharing that differ from the General Data Protection Regulation's concept of data portability. These proposals advocate for an in situ data right: rather than take data from the platform (or ex situ as portability implies) users have the right to use their data in the location where it resides. The European Parliament's amendments to the Digital Markets Act and the Data Act proposals both seek to introduce this in situ data right in legislation.

APIs are at the core of open banking frameworks. APIs are key enablers of interoperability, and facilitate the data flows that are necessary for open banking. However, despite this pro-competitive potential, there is currently no consensus amongst jurisdictions on who should define APIs or whether to standardise APIs. In the EU, for example, authorities refrained from mandating API standardization. Instead, banks were allowed to set their own data sharing interfaces or take part in standardisation initiatives. In this regard, Mr Colangelo emphasised that the PSD2 does relatively little to advance the core principle of data sharing. In particular, the PSD2 does not specify the form of data that must be provided to third parties and it does not envision steps to promote open APIs. Nevertheless, the European Commission has launched the Digital Finance Regulatory Payment Strategy which recognized the relationship between the lack of API interoperability and participation in open banking (European Commission, 2020[28]).

Despite the advantages of open banking, there are concerns about whether it will give rise to "big tech" monopolisation of the market if big tech were to give preferential treatment to their own products. Accordingly, within the Digital Markets Act there are several ex-ante provisions regarding vertically integrated platforms in finance. However, once API standardization issues have been addressed and consumers can switch to different providers, regulators should not seek to counter the emergence of new market concentrations. The rise of dominant players simply means that the provider has outcompeted other entities. Regulators should not view open banking as a failure if either legacy banks or big tech companies end up dominating the market, as this would be the result of competition— exactly what open banking is supposed to encourage.

## The challenges of implementing open APIs in Poland

Ms Karen Nadasen (CEO, PayU) defined open banking as the ability to access consumer-consented data from a bank or other financial institution, either i) to provide a product or service based on aggregated data or account information; or ii) to perform an action on behalf or for the consumer (e.g. payment instruction, switching account, or providing credit or loan service).

Prior to open banking coming to Poland, there were many payment services operating in that jurisdiction (e.g. credit and pay by link[6]). Most transactions were directly between people or entities' accounts (i.e. account-to-account market). Ms Nadasen described that PayU (which is a payment service provider to online merchants) implemented the APIs for nine banks in Poland. However, the standardization of APIs did not help PayU, because there were no user experience guidelines and there were significant differences between banks in this regard. Some of the user journeys were so long that they led to significant drop off, as consumers became frustrated with the amount of time it took to authorise the sharing of their data.

### A view from the private sector

Ms Cara Yara (Privacy Policy Manager, Meta) explained in her presentation that Meta joined the Data Transfer Project in 2018 to collaborate with industry partners to build data portability products that enable direct transfers between services (Data Transfer Project, 2022[29]). In addition, in 2020 Meta launched the Transfer Your Information tool that enabled Facebook users to transfer their Facebook photos, videos, posts and other data types directly to other document or photo cloud services.

In the metaverse, the interoperability of data transfer mechanisms will be just as important as it is for open banking. This interoperability could be enabled by "Web3" technologies, specifically through blockchain. Identity remains a major factor for financial inclusion and Ms Yara underlined that users of the metaverse will need easier access to identification. Whilst identification in the metaverse is not necessarily tied to a nation, Ms Yara pointed out that it will need to be recognized by nations.

## 4. Privacy, consent and liability in open banking

***Short summary*** *– Open banking helps users to play an active role in the sharing and re-use of their financial data across digital services, online platforms, sectors and borders. The collection or use of financial data in open banking requires the user's consent, and as such consent management is key for protecting the data of open banking users.*
*However, this can be difficult to implement. For instance, fragmentation in conventional financial systems in Japan means that applying consent management can be challenging. Whilst providers are keen to use financial data to offer a variety of services, they face difficulties using that data efficiently.*
*The open banking ecosystem also presents risks, as data sharing through portability and interoperability may expose the data to breaches. In addition, reconciling data protection obligations and open banking frameworks remains a challenge in several jurisdictions.*

### Introduction

The third session, moderated by Ms Audrey Plonk (Head of Digital Economy Policy Division, OECD), highlighted that data portability can be a tool to promote interoperability across different online platforms, increase consumer control over their data, enhance competition and innovation, and reduce switching costs and lock-in effects. It can empower users to play a more active role in the sharing and re-use of their data across digital services, online platforms, sectors and borders. In addition, open banking is an important example in the use of data portability. Thanks to open banking, data can be used more extensively than in "closed", traditional banking, and it can bring about significant benefits.

However, experts noted that open banking can also give rise to new risks. For instance, facilitating data flows and data sharing through data portability comes with significant digital security and privacy concerns, including the risk of personal data breaches.

## Privacy issues in Israel's open banking legislation

Mr Reuven Eidelman (Head of Legal Department, Privacy Protection Authority of Israel) explained that Israel in November 2021 enacted legislation regarding open banking, called "Account Information Service Law" (Government of Israel, 2021[30]). The law came into force in June 2022. The new law covers data protection issues, increasing customer control and transparency, and rules for consent and its withdrawal. The Israel Securities Authority (ISA) is tasked with supervising compliance with the law.

The first law in Israel that touched upon open banking was enacted in 2017 and primarily focused on the increasing competition in the banking system and screen scraping. After that, Israel enacted new legislation which primarily dealt with API technology, eventually allowing more customer control over their information. The Israeli Privacy Protection Authority was involved in the drafting effort.

Mr Eidelman noted that the Israeli privacy regime does not cover all issues related to the use of new technologies. In addition, as the GDPR does not apply in Israel, the country can create specific, stricter arrangements in its sectoral legislation, such as in the case of privacy issues. For instance, the legislation does not include a data portability principle, which allows more discretion to regulators.

Mr Eidelman highlighted some specific provisions of the Account Information Service Law, for instance:

- the collection or use of financial data requires the customer's explicit consent;
- 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;
- presenting other customers with identifiable data is prohibited, even under consent;
- prior to his/her consent, the customer will be provided with information about the nature of the service in a clear and concise language;
- consent for retaining the collected data for more than three years can be obtained only towards the end of the three-year period.

The Account Information Service Law also outlines that, in case of a data security breach, the Privacy Protection Authority is obliged to order the service provider to notify all data subjects whose privacy may be tangibly harmed by the breach. Furthermore, the service provider's regulator determines rules regarding risk management, digital security and the obligation to appoint officers in charge of data security. Finally, with regard to the use of joint accounts, a partner may express consent on behalf of both partners to the transmission of financial information to the third-party provider.

## Open banking in Japan from a financial regulatory perspective

Mr Ryosuke Ushida (Director for Strategy Development, FinTech and Innovation Office, Financial Services Agency, Japan) offered a financial regulator's perspective from Japan. This regulator has the responsibility of advancing open banking initiatives in the country. Mr Ushida highlighted that in 2016 the Japanese Banking Act was amended, requiring banks to open APIs to third parties (e.g. account aggregators and payment service providers). Nevertheless, since then, serious privacy and digital security incidents have taken place (e.g. an unauthorized withdrawal from an open banking account due to a digital security vulnerability). To address these challenges, the Financial Services Agency has tried to ensure a higher threshold for identity checks.

Consent management can be a challenge for Japanese banks, because conventional financial systems are fragmented. Providers are eager to use customer data to provide a variety of services, but due to the challenges of consent management they have difficulties efficiently using the data. Mr Ushida pointed out that whilst Japanese citizens' trust in banks is higher, they are worried about privacy and digital security risks.

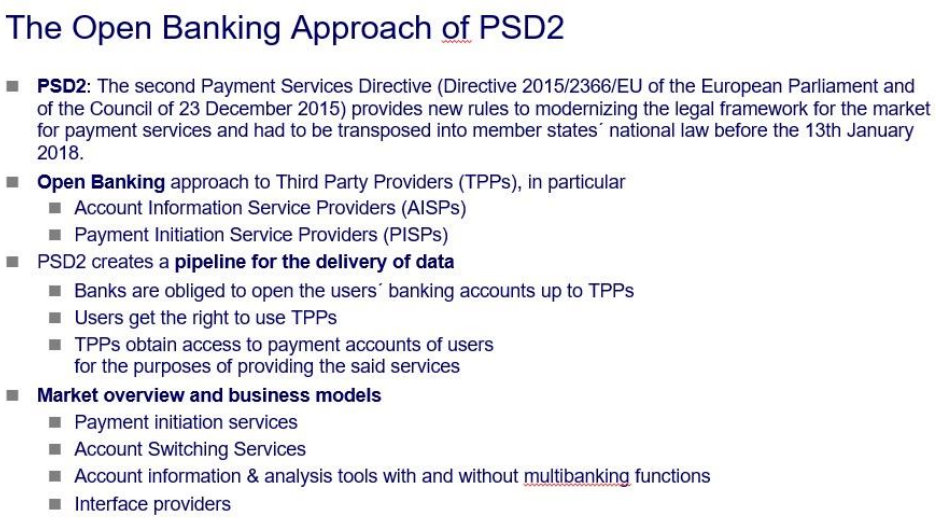
The Financial Services Agency carried out research on self-sovereign identity and decentralized (blockchain) solutions. Mr Ushida explained that the research has identified some advantages to adopting identity management schemes. In existing identity systems, some banks use analogue schemes, which are not necessarily suitable for appropriate data management and can be exploited for money laundering.[7] Mr Ushida noted that the Financial Services Agency is seeking a blockchain-based identity system to better protect privacy and to ensure data portability. He also explained the advantages and challenges of self-sovereign identity.

Mr Ushida also touched upon the challenge of where to store digital IDs. He noted three options: i) wallets; ii) cloud; or iii) with vendors. Some banks and experts do not want to store the data because of the associated risks. These parties believe it is better if individual customers possess their data, namely through self-sovereign identity. However, there are challenges for the adoption of self-sovereign identity, including the development of a trusted framework.

## Comparing the open banking legal framework and the GDPR

Ms Andrea Stubbe (Office of the North Rhine-Westphalia Commissioner for Data Protection and Freedom of Information – Member of the Financial Matters Subgroup, European Data Protection Board) focused her presentation on the interplay between the open banking legal framework (namely PSD2) and the data protection regime (namely GDPR). Ms Stubbe highlighted that the PSD2 provided new rules to modernise the legal framework for the market for payment services. Figure 2 provides an overview of the key points provided by Ms Stubbe on the PSD2.

**Figure 2. The open banking approach of PSD2**




Source: Ms Andrea Stubbe (Office of the North Rhine-Westphalia Commissioner for Data Protection and Freedom of Information – Member of the Financial Matter Subgroup, European Data Protection Board) presented at the workshop on "Data Portability in Open Banking: Privacy and Other Cross-Cutting Issues", 17 March 2022.

PSD2's version of "consent" differs from how the GDPR approaches that term. Under PSD2, users of a payment service that are authorizing data sharing with a third-party provider are actually agreeing to a contractual condition with the third-party provider, and the bank is legally obliged to share the data with the third-party provider. In this situation, GDPR-level consent has not been provided, and other legal bases under Article 6 GDPR apply (i.e. contractual necessity and legal obligation). What is "necessary" data processing to provide the payment service depends on the essential elements of the contract and the reasonable expectations of the parties to the contract.

For further processing of accessed data (for other purposes, such as automated creditworthiness assessments), third-party providers need a separate, specific consent aligned with the GDPR. When it comes to special categories of data under Article 9 GDPR (e.g. access to transaction data revealing health information), explicit consent may be required.

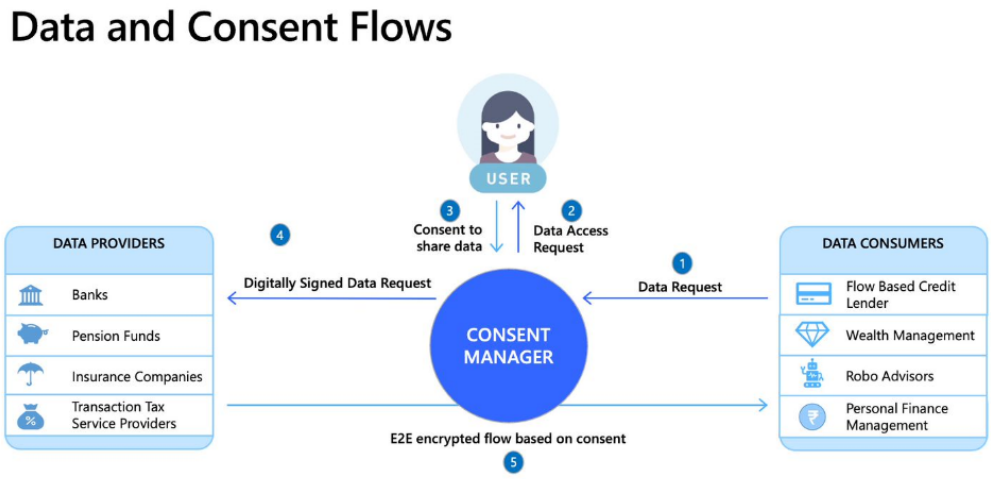
With respect to consent management and data dashboards, as long as consent is required, these tools can enable GDPR compliance, provided that these tools observe the conditions posed by Articles 4(11) and 7 GDPR (i.e. freely given, express, informed, unambiguous, etc.). The European Data Protection Board guidelines state that technical measures, such as encryption, should be implemented to ensure data minimisation and security. Recently, the European Commission presented the Data Act to make data more accessible. Banking associations welcomed the initiative, which promotes open finance.

## India's Data Empowerment and Protection Architecture

Mr Rahul Matthan (Partner, Trilegal) presented India's Data Empowerment and Protection Architecture (DEPA), which is a framework for data portability initiatives in the country. As India has a large number of digital payments, DEPA was first launched in the financial sector to foster open banking. DEPA aims to extend banking opportunities, including access to credit, to those

who are not served by traditional banking. Figure 3 below provides the design of data and consent flows in the open banking ecosystem:

### Figure 3. Data and consent flows in the open banking ecosystem




Source: Rahul Matthan (Partner, Trilegal) presented at the workshop on "Data Portability in Open Banking: Privacy and Other Cross-Cutting Issues", 17 March 2022.

The protection of privacy is central to the system. To this end, Mr Matthan noted that if consent flows are disaggregated from data flows, it is possible to achieve a better approach to privacy. In a traditional transaction, if a data consumer asks for evidence of the customer's income for the last six months, the individual will have to go to the bank and obtain their statement. Through the DEPA framework, no party has the full information about the transaction, except for the user. The consent manager is run by the private sector not by the government and there are five current licensees.

Mr Matthan explained that DEPA is a fully interoperable system that is accessible to multiple players. There is no need to obtain access for each provider as may be needed when using APIs: only a single consent management provider is needed. The uptake of the ecosystem is very high, just like it was in the digital payments movement. The DEPA framework can work across sectors, with some initiatives in the healthcare sector already surfacing as well.

## A view from the private sector

Ms Caroline Louveaux (Chief Privacy Officer, Mastercard) noted that Mastercard aims to empower an inclusive digital economy and considers open banking a key tool to achieve this objective. Ms Louveaux highlighted that data sharing is key for open banking and Mastercard's business model intends to support data sharing between participants in the payments' industry. She highlighted that Mastercard aims to connect fintechs to other third-party providers. In this regard, trust is essential to ensure uptake of these services. To achieve trust, promoting global interoperability and better alignment of regulations would be essential.

## 5. Co-operating among regulators, nationally and internationally

***Short summary*** *– Open banking revolves around three broad policy objectives: i) financial stability and integrity, ii) privacy and consumer protection, and iii) efficiency and competition. Different national approaches have also prioritised different interests: property/contract rights, human rights, and state rights. The complexity of the trade-offs among the different policy objectives raises a need for national and international coordination among different financial and non-financial regulators. At the domestic level, the United Kingdom's Digital Regulation Cooperation Forum brings together the privacy regulator with other three authorities. This has resulted in broad areas of alignment in practice on desired outcomes. However, such initiatives may be insufficient and, where alignment is not found, changes in primary legislation may be needed.*

*At the international level, the OECD could provide a forum for a dialogue among financial sector, competition and data protection authorities to enhance cross-sectoral understanding of trends in data policy strategies across different sectoral languages.*

### Introduction

Limor Shmerling Magazanik (Managing Director, Israel Tech Policy Institute) noted the cross-sectoral dimension of open banking, whose objectives pertain to data governance and privacy, competition, and banking regulation. Each sector regulator represents the public interest in a specific context.

As more sector-specific regulators will have to deal with data protection matters – in open banking and beyond –, a huge effort of coordination becomes necessary. These developments also raise the dilemma of whether to pursue a general data protection regulation or privacy protection arrangements specific to each sector.

### Domestic co-operation: the example of the UK Digital Regulation Cooperation Forum

Simon McDougall (Senior Fellow, Future of Privacy Forum; formerly Deputy Commissioner of the UK Information Commissioner's Office) highlighted that the intersection of data protection legislation and open banking raises novel challenges for regulatory coordination and oversight. Lessons from various approaches can provide important insights and help regulators draw best practices in their own frameworks.

There are a multitude of regulatory bodies that may have a role in open banking, including oversight of topics like data protection/privacy, competition, anti-money laundering, cybersecurity, consumer protection, and financial services. Each can have a role and the primary responsibility can be given to a non-privacy body as long as coordination is guaranteed.

For instance, in the United Kingdom, before the GDPR, the Information Commissioner's Office (ICO) did not have much contact with other UK regulators as data protection did not directly concern them. With the GDPR, the scope of data protection has become broader, and the ICO has acquired more powers.

Consequently, the ICO has become a horizontal regulator in a context with many vertical (i.e. sectoral) regulators. This makes negotiations between regulators a prerequisite for coordinated enforcement. Regulatory overlaps are common in complex environments such as open banking, digital identity, and facial recognition. They raise questions of management and how officials

within organisations communicate to their counterparts in other regulatory bodies. These challenges are not limited to financial services and open banking but exist in multiple sectors and raise numerous questions about the best way to create relationships between regulators and whether these relationships are bilateral or *ad hoc*.

Throughout the open banking ecosystem, the lack of systematic coordination is problematic. Since 2020, the ICO has engaged with other regulators through the Digital Regulation Cooperation Forum. This non-statutory body provides an institutionalised mechanism for cooperation among the ICO, the Competition and Markets Authority (CMA), the Office of Communications (Ofcom) and the Financial Conduct Authority.

Alignment stands out from the experience of the Digital Regulation Cooperation Forum. There are broad areas of alignment between regulators in practice as most desired areas and outcomes are the same, sometimes with different terms. Fairness, consumer autonomy, and economic growth are common to all authorities, but at times concealed by different concepts. Such differences may stem from the regulators' focus: for instance, the ICO is human-rights based, whereas the CMA is more interested in economic challenges. It is important to have formal meetings to work through these areas.

McDougall also noted that disagreement can arise between regulators. Thus, it is important to create procedures for handling conflict. The ICO has focused on information gateways and duties for regulators to consult and cooperate. When no agreement is found, each regulator simply fulfils its own statutory obligations. In these cases, primary legislation should intervene and address the obstacles. According to McDougall, the OECD is well placed to lead discussions on these topics.

Finally, the challenges of such regulatory cooperation are practical in nature. A regulator may face resources constraint when it has to understand the activities of another regulator with which it has to engage. If secondary objectives are added to a regulator's mandate, they can give rise to conflict with other objectives and to higher legal risks linked to the increased duties to be discharged.

## Data governance frameworks at the international level

Open banking, and data sharing more broadly, need coordination at the international level, alongside the domestic one. Frameworks that encourage data sharing raise novel challenges and are particularly important because technological advances have led to reduced costs of collecting and storing data. In particular, big techs are best-in-class at taking advantage of personal data as part of their business model, as they rely on the self-reinforcing nature of data analytics, network externalities and interwoven activities.

Juan Carlos Crisanto (Deputy Chair, Financial Stability Institute, and Head of Technology and Capacity Development, Bank for International Settlements) identified three broad categories of policy trade-offs with respect to open banking: financial stability and integrity, privacy and consumer protection, and efficiency and competition. Each of these trade-offs is interrelated, with goals realised by one (e.g. privacy) potentially creating tension or conflict with another (e.g. competition). For instance, privacy and consumer protection are sometimes in tension with efficiency and competition. Mandating that private providers have access to data for competition purposes may lead to the misuse of data. Moreover, when firms underinvest in technical compliance systems, access to data may lead to security concerns.

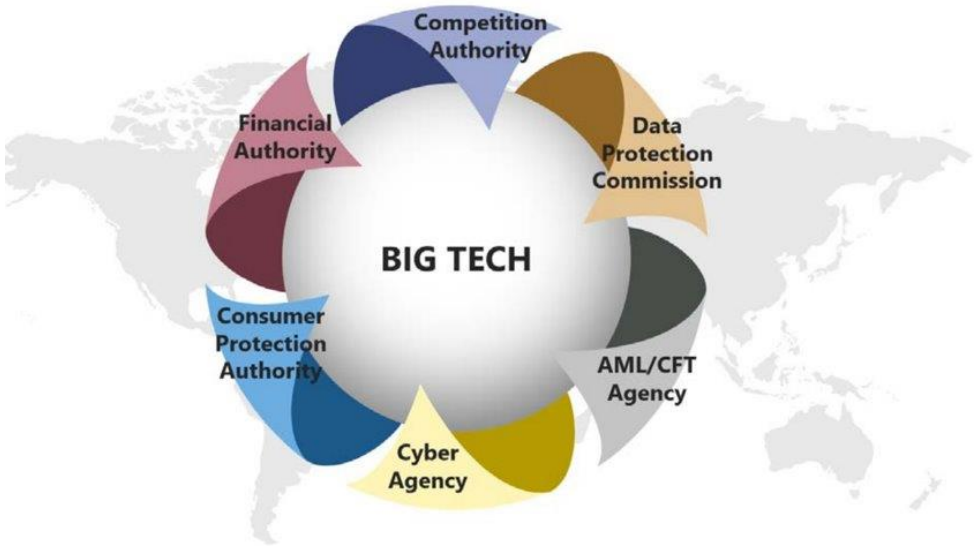
Likewise, from a banking perspective there are three policy frictions: 1) data infrastructure; what it looks like and who establishes it and has access to it; 2) how open banking interplays with the growing field of ethical data uses; and 3) what, if any, is the impact of the rise in power of Big Tech.

Public policy challenges arise from privacy trade-offs and lead to numerous issues for regulators and lawmakers. The value people attach to data privacy varies from country to country. Topics such as addressing heterogeneity in personal data, assessing the value of individual data points in a large data set, and defining ownership and control over data each presents incredibly complex questions that evade easy consensus.

However, well designed data governance frameworks can address some of these trade-offs. Crisanto noted that authorities are starting to put in place AI governance policies to promote an ethical use of data. There is also limited regulatory action on mitigating big tech market power. Clarifying rules and data policy principles like data portability, creating resilient data infrastructures, and setting up public infrastructure and data management protocols help support open banking implementation. Instruments to achieve this range from laws to non-binding frameworks. It is however difficult to find a cohesive data framework: different data frameworks are emerging but do not necessarily complement each other.

The inherent complexity of these policy trade-offs raises the need for national and international coordination among different financial and non-financial regulators (see Figure 4 which addresses Big Tech in particular (Carstens et al., 2021[31]). An organisation such as the OECD, the International Monetary Fund or the Financial Stability Board may initiate a dialogue among financial sector, competition and data protection authorities to facilitate an understanding of the trends in data policy strategies across different sectoral languages. Some authors have proposed a new Bretton Woods-style agreement for an updated international governance architecture around a Digital Stability Board (Fay and Medhora, 2021[32]) or an international agreement on common minimum principles for the data economy (Haksar et al., 2021[33]). In addition, with respect to big tech regulation, it is important to involve data protection and competition authorities (Knot, 2021[34]).

## Figure 4. Policy trade-offs provide a strong case for national and international co-ordination



Source: Juan Carlos Crisanto (Financial Stability Institute, Bank for International Settlements), presented at the workshop on "Data Portability in Open Banking: Privacy and Other Cross-Cutting Issues", 17 March 2022.

## Lessons from international regulatory co-operation

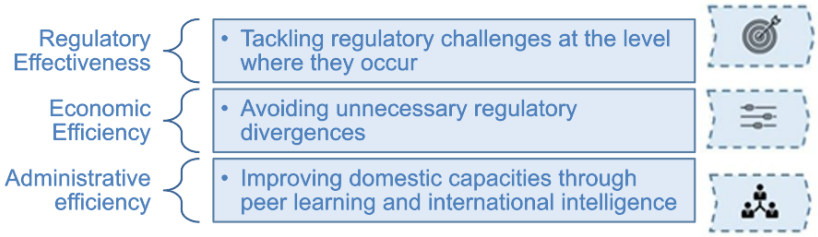
Marianna Karttunen (Policy Analyst, Regulatory Policy Division, OECD) highlighted the lessons that international regulatory cooperation can provide. Challenges from transboundary issues take many forms and emerge in a myriad of ways. Innovations of the fourth industrial revolution transcend physical, digital, and biological boundaries, and push the limits of national borders. Traditional institutional frameworks are no longer adapted to effectively keep up with these policy challenges, as they only have limited effectiveness: for instance, the global health system is as strong as its weakest link (OECD, 2020[35]). Additionally, regulatory fragmentation may lead to regulatory arbitrage and create barriers to innovation and trade (OECD, 2021[36]) (OECD, 2017[37]).

In finance, a survey of over 250 financial institutions senior management suggested that the costs of regulatory divergences are a barrier to international growth that amounts to more than $780 billion annually in costs to the global economy (IFAC and Business at OECD, 2018[38]). On average, regulatory divergences cost financial institutions from five to ten percent of their annual turnover and such costs are most material for the financial performance of smaller organisations. Furthermore, 73% of respondents reported an increase or substantial increase in costs related to divergent regulation over the previous five years (in the period 2013 to 2018).

Karttunen noted how open banking is a very telling example of the need for sharing, co-operation, and exchange of data between a range of actors of different legal natures and areas of activity, ultimately to offer better services to consumers. Only potential legal and data portability issues may prevent the actors that co-operate in offering open banking from being based in different countries. At the same time, this area calls for regulation to protect the public interest in light of the diversity of actors involved, the sensitivity of the content exchanged, and the need for protective yet innovation-enhancing regulatory frameworks.

Novel approaches to cross-border regulation have surfaced in recent years. These approaches view regulation as constrained by administrative factors beyond borders but with an eye towards identifying common solutions. The OECD Best Practice Principles on International Regulatory Co-operation provide basic tools for stakeholders to foster cooperation by adapting laws and regulations to an interconnected world (OECD, 2021[39]), and more recently the Recommendation of the OECD Council on International Regulatory Co-operation to Address Global Challenges gives further incentive to upscale regulatory frameworks with more resilience and leveraging of international flows (OECD, 2022[40]). Regulators should prioritize regulatory effectiveness, economic efficiency, and administrative efficiency when cooperating (see Figure 5). They should also consider all relevant international standards and frameworks for co-operation in a particular policy area and the multitude of multilateral fora that are active (OECD, 2012[41]). With particular regard to open banking, Karttunen highlighted the complementarity of international organisations for the exchange of experiences and international expertise, or for aligning approaches internationally, especially concerning the OECD, the Financial Stability Board and the Bank for International Settlements.

**Figure 5. Better regulation for a complex and interconnected world**




Source: Marianna Karttunen (Regulatory Policy Division, OECD), presented at the workshop on "Data Portability in Open Banking: Privacy and Other Cross-Cutting Issues", 17 March 2022.

Furthermore, the OECD Recommendation on Agile Regulatory Governance to Harness Innovation supports regulators in adjusting their regulatory management tools to ensure regulations are fit for the future. It helps to lay the institutional foundations to enable co-operation and joined-up approaches within and across jurisdictions. It furthers the development of governance frameworks to enable the development of agile and future-proof regulation. Finally, it recommends adapting regulatory enforcement strategies and activities to promote compliance, help innovators navigate the regulatory environment, and uphold public protection, including across jurisdictions (OECD, 2021[36]).

## Open banking and financial data governance

Douglas Arner (Professor in Law, University of Hong Kong) recalled that the digitization of finance presents very complex problems around the role of data in finance. The integration of finance into the platform economy has created novel business models and complex regulatory instruments to address particular issues with those models. However, policymakers have not always drafted laws and regulations with similar instruments in mind. There are real divergences in data governance for financial models that need addressing – examples are benefits and challenges of networks, platforms, datafication of finance, and data aggregation – because they have made regulating this space more challenging (Arner, Castellano and Selga, 2022[42]). The EU has regulated financial data in an extensive manner. Such EU regulatory "Big Bang", as Arner and colleagues call it in their writings (Zetzsche et al., 2019[43]), is made up of the PSD2, the second directive on markets in financial instruments (European Union, 2014[44]), the electronic identification regulation (European Union, 2014[45]), and the fifth anti-money laundering directive (European Union, 2018[46]) (Arner, Buckley and Zetzsche, 2022[47]).

Moreover, data governance differs between property-based, rights-based, and state-based approaches. Each of these approaches may create tension with how regulators operationalise data governance architectures and relate legal process to commercial activity. Financial data governance focuses heavily on the standardisation, storage, and transmission of data, and also covers non-personal financial data.

Over time and across jurisdictions, a number of open banking regulatory types have developed: prescriptive, facilitative, market-driven, and emerging. Similarly, there are different underlying interests being protected: property/contract rights, human rights, and state rights. The combination of the regulatory type and interest base further creates specific approaches. Examples are the differing approaches of the US (a contracts-based and market-driven approach) and the EU (a human rights-based and prescriptive approach). These approaches also need technological infrastructures, which could be federated or centralised. There is value in international organisations outlining different objectives and institutional structures, such as

memorandum of understanding, committees and supervisory colleges. Another debate concerns the option of entrusting existing institutions or creating a new one, for instance a digital stability board. Academia has provided analytics regarding trends, drivers, and goals for open banking.

### A view from the private sector

Kent Andrews (Senior Vice President, Regulatory Risk, Toronto-Dominion Bank Group (Canada), and Chair, Business at OECD Finance Committee) noted that the private sector sees the benefits of financial inclusion and digitisation. The market often jumps ahead of regulatory bodies in many respects, which can lead to unsafe or unclear practices. These activities can undermine confidence in the financial system. Regulators must learn how to make progress and promote interoperability without creating instability.

For open banking, legislative and regulatory changes take time to be implemented, and the different national experiences provide relevant lessons. Stakeholders need to foster cooperation between the public and private sectors both domestically and internationally. This is not unprecedented in financial services. For instance, the international implementation of the Basel II framework for banks showed a high degree of coordination of industry, national and international bodies. Both rules and principles were part of the framework, coordinated by the Basel Committee. It allowed for domestic discretion at national level, where appropriate, and featured impact studies, an approval process, and best practices. Similarly to the Basel II framework, open banking has a financial stability foundation, but is consumer-oriented.

According to Andrews, the way forward could be for the OECD, the Financial Stability Board, and the Bank for International Settlements to join in for cooperation. They could support international benchmarking and facilitate ongoing country and industry activities and innovations to realise the potential of open banking.

## 6. Conclusion

Steve Wood (Deputy Commissioner (Policy), UK Information Commissioner’s Office, and Chair, OECD Data Governance and Privacy Working Party) noted that open banking is an advanced and mature sector for data portability.

Like other multi-sector frameworks, it presents both opportunities and challenges. Examples of open banking and other approaches' promises include access to innovative products and services, improved customer control and engagement, financial inclusion, and greater data portability and accountability across the business landscape.

Participants from a variety of countries, industries, and regulators also recognised a variety of roadblocks that may frustrate the emergence of a well-functioning data sharing ecosystem, such as lingering uncertainty about how open banking and other data sharing frameworks interact with data protection and privacy regimes. Furthermore, the rise of Big Techs and major online platforms and their interactions with other technologies can give rise to further challenges.

It is now essential to make the system work in practice, to enable trust and efficiency. New models of regulatory cooperation should be explored, with the need to continue to learn and build, and scale to an international model. International interoperability between systems is necessary in many areas. It will make compliance easier for companies wishing to operate across borders. As proposed by several speakers, the OECD may play a role in this area and promote a dialogue among financial sector, competition and data protection authorities on data governance

frameworks. In particular, the Working Party on Data Governance and Privacy in the Digital Economy could initiate a work stream on cross-sectoral regulatory cooperation and leverage synergies both within the OECD and with other organisations.

# References


Agur, I., S. Martinez Peria and C. Roch (2020), "Digital Financial Services and the Pandemic: Opportunities and Risks for Emerging and Developing Economies", *IMF Special Series on COVID-19*, https://www.imf.org/-/media/Files/Publications/covid19-special-notes/en-special-series-on-covid-19-digital-financial-services-and-the-pandemic.ashx. [6]

Arner, D., G. Castellano and E. Selga (2022), *Financial Data Governance: The Datafication of Finance, the Rise of Open Banking and the End of the Data Centralization Paradigm*, University of Hong Kong Faculty of Law Research Paper No. 2022/08, http://dx.doi.org/10.2139/ssrn.4040604. [42]

Australian Competition and Consumer Commission (2019), *Consumer data right*, https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0#:~:text=On%2026%20November%202017%2C%20the,switch%20between%20products%20and%20services. [26]

Basel Committee on Banking Supervision (2019), *Report on open banking and application programming interfaces*, https://www.bis.org/bcbs/publ/d486.pdf. [1]

Berlin Group (n.d.), *About*, https://www.berlin-group.org/. [51]

Berlin Group (n.d.), *PSD2 Access to Bank Accounts*. [21]

Carstens, A. et al. (2021), "Regulating big techs in finance", *BIS Bulletin* 45. [31]

CMA (2017), *Retail Banking Market Investigation Order*, https://www.gov.uk/government/publications/retail-banking-market-investigation-order-2017. [2]

Competition and Markets Authority (2016), *Retail banking market investigation*, https://www.gov.uk/cma-cases/review-of-banking-for-small-and-medium-sized-businesses-smes-in-the-uk. [27]

Data Transfer Project (2022), *About us*, https://datatransferproject.dev/. [29]

EU (2015), *Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 200*. [20]

European Commission (2021), *Call for advice to the European Banking Authority (EBA) on the review of the payment services Directive (PSD2)*, https://ec.europa.eu/info/publications/211018-payment-services-calls-advice-eba_en. [22]

European Commission (2020), *Digital finance package*, https://finance.ec.europa.eu/digital-finance_en. [28]

European Commission (2017), *Payment Services Directive (PSD2): Regulatory Technical Standards (RTS) enabling consumers to benefit from safer and more innovative electronic payments*, https://ec.europa.eu/commission/presscorner/detail/en/MEMO_17_4961. [48]

European Union (2018), *Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32018L0843. [46]

European Union (2014), *Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU Text with EEA relevance*, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32014L0065. [44]

European Union (2014), *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG. [45]

FATF (2021), "Stocktake on Data Pooling, Collaborative Analytics and Data Protection", https://www.fatf-gafi.org/publications/digitaltransformation/documents/data-pooling-collaborativeanalytics-data-protection.html. [49]

Fay, R. and R. Medhora (2021), "A Global Governance Framework for Digital Technologies", *T20 Policy Brief*, https://www.t20italy.org/wp-content/uploads/2021/09/TF4-PB5-Fay-1.pdf. [32]

Government of Israel (2021), *Account Information Service Law*, https://www.isa.gov.il/sites/ISAEng/1485/LawsSupervision/Documents/HOK16122.pdf. [30]

Haksar, V. et al. (2021), "Toward a global approach to data in the digital age", *IMF Staff Discussion Note*, https://www.imf.org/-/media/Files/Publications/SDN/2021/English/SDNEA2021005.ashx. [33]

IFAC and Business at OECD (2018), *Regulatory Divergence: Costs, Risks and Impacts*, https://www.ifac.org/system/files/publications/files/IFAC-OECD-Regulatory-Divergence.pdf. [38]

Italian Presidency of the G20 and G20 Global Partnership for Financial Inclusion (2020), "MSME Digital Finance: Resilience and Innovation during COVID-19", *International Finance Corporation and SME Finance Forum*, https://www.gpfi.org/sites/gpfi/files/sites/default/files/5_IFC-SMEFF%20Report_MSME%20digital%20finance_Resilience%20and%20Innovation%20during%20COVID-19.pdf. [7]

Jeng, L. (ed.) (2022), *Open Banking, Open Data and Open Finance: Lessons from the European Union*, Oxford University Press, https://ssrn.com/abstract=3961235. [47]

Knot, K. (2021), *11th BIS Research Network meeting, 6-7 October*. [34]

Monetary Authority of Singapore (2022), *Financial Industry API Register*, https://www.mas.gov.sg/development/fintech/financial-industry-api-register. [23]

Monetary Authority of Singapore (2021), *API Exchange (APIX)*, https://www.mas.gov.sg/development/fintech/api-exchange. [24]

OECD (2022), *Recommendation of the Council on International Regulatory Co-operation to Tackle Global Challenges*, *OECD/LEGAL/0475* https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0475. [40]

OECD (2021), *Best Practice Principles on International Regulatory Co-operation*, OECD Publishing, https://doi.org/10.1787/a2507c21-en. [39]

OECD (2021), *Data portability, interoperability and competition*, https://www.oecd.org/daf/competition/data-portability-interoperability-and-digital-platform-competition-2021.pdf. [16]

OECD (2021), *Mapping Data Portability Initiatives, Opportunities and Challenges*, https://www.oecd-ilibrary.org/docserver/a6edfab2-en.pdf?expires=1660752451&id=id&accname=ocid84004878&checksum=87383B96E17D6660E498D94277736FD2. [17]

OECD (2021), *OECD Expert Workshop on Data Portability (internal document)*. [14]

OECD (2021), *OECD Webinar on Data Portability (internal document)*. [15]

OECD (2021), *Recommendation of the Council for Agile Regulatory Governance to Harness Innovation, OECD/LEGAL/0464*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0464. [36]

OECD (2020), *No policy maker is an island: The intenraitonal regulatory co-operation response to the COVID-19 crisis*, https://www.oecd.org/coronavirus/policy-responses/no-policy-maker-is-an-island-the-international-regulatory-co-operation-response-to-the-covid-19-crisis-3011ccd0/. [35]

OECD (2020), *OECD Online Expert Discussion in preparation for an OECD Workshop on Data Portability (internal document)*. [13]

OECD (2019), *Open banking: selected developments and issues (internal document)*. [19]

OECD (2017), *International Regulatory Co-operation and Trade: Understanding the Trade Costs of Regulatory Divergence and Remedies*, OECD Publishing, Paris, https://www.oecd-ilibrary.org/docserver/9789264275942-en.pdf?expires=1675943052&id=id&accname=ocid84004878&checksum=2B261D3F1B689CECD061E812D09A3116. [37]

OECD (2014), *Consumer Policy Guidance on Mobile and Online Payments*, https://www.oecd-ilibrary.org/docserver/5jz432cl1ns7-en.pdf?expires=1662315784&id=id&accname=ocid84004878&checksum=46CAA8582F344C9D31F14B945AFE36DD. [18]

OECD (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. [12]

OECD (2012), *Recommendation of the Council on Regulatory Policy and Governance, OECD/LEGAL/0390*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0390. [41]

Open Banking Implementation Entity (2022), *Dashboards Overview*, https://standards.openbanking.org.uk/customer-experience-guidelines/dashboards/about/latest/. [25]

Open Banking Implementation Entity and Ipsos MORI (2020), "Adapting to survive: UK's small businesses leverage open banking as part of their COVID-19 crisis recovery", https://www.openbanking.org.uk/news/adapting-to-survive-uks-small-businesses-leverage-open-banking-as-part-of-their-covid-19-crisis- [8]

recovery/#:~:text=Sharp%20increase%20in%20small%20business,direct%20result%20of%20COVID%2D19.

Plaitakis, A. and S. Staschen (2020), "Open Banking: How to Design for Financial Inclusion", *CGAP/World Bank Working Paper*, https://www.cgap.org/sites/default/files/publications/2020_10_Working_Paper_Open_Banking.pdf. [9]

Soar, A. and V. Mwago (2020), "Open banking in Africa after COVID-19", *DLA Piper Insights*, https://www.dlapiper.com/fr/canada/insights/publications/2021/04/africa-connected-issue-6/open-banking-in-africa-after-covid19/. [11]

The Economist Intelligence Unit and Temenos (2020), "Open banking: revolution or evolution?", https://www.temenos.com/wp-content/uploads/2021/02/Temenos-Open-banking-VFinal-1.pdf. [5]

UK (2017), *The Payment Services Regulations*, https://www.legislation.gov.uk/uksi/2017/752/contents/made. [3]

UK Open Banking (2022), *Regulated Providers*, https://www.openbanking.org.uk/regulated-providers/. [4]

US Government (2021), "Executive Order on Promoting Competition in the American Economy", https://www.whitehouse.gov/briefing-room/presidential-actions/2021/07/09/executive-order-on-promoting-competition-in-the-american-economy/. [50]

Yazdanpanah, A. (2021), "The Promise of Open Banking in Driving Financial Inclusion in Africa", *CNBC Africa*, https://www.cnbcafrica.com/2021/the-promise-of-open-banking-in-driving-financial-inclusion-in-africa/. [10]

Zetzsche, D. et al. (2019), *The Future of Data-Driven Finance and RegTech: Lessons from EU Big Bang II*, University of Hong Kong Faculty of Law Research Paper No. 2019/004, http://dx.doi.org/10.2139/ssrn.3359399. [43]

## Notes

[1] At the OECD, the workshop was organised by the Digital Economy Policy Division, in cooperation with the Competition Division, the Financial Markets Division and the Regulatory Policy Division. Part of the summary builds on a workshop report drafted by the Future of Privacy Forum's (FPF) Policy Counsels, Sebastião Barros Vale, Daniel Berrick, Hunter Dorwart, Lee Matheson, in consultation with Israel Tech Policy Institute (ITPI) Managing Director, Limor Shmerling Magazanik, and FPF Senior Fellow, Zoë Strickland.

[2] The 'Small Business Financial Landscape' study, commissioned by the Open Banking Implementation Entity, asked 500 small business decision makers (defined as has having 2-49 employees) about the financial decisions they have taken since March 2020 to support their businesses in response to the COVID-19 pandemic (Open Banking Implementation Entity and Ipsos MORI, 2020[8]).

[3] For example, in the US, in July 2021, the Biden Administration issued an executive order on promoting competition in the American economy (US Government, 2021[50]). Among its proposed measures, it encouraged the Consumer Financial Protection Bureau to consider rulemaking to facilitate the portability of consumer financial transaction data.

[4] Screen scraping is a technique consisting of accessing the data through the customer interface with the use of the customer's security credentials, which allows third-party providers to access customer data without any further identification vis-à-vis the banks (European Commission, 2017[48]).

[5] The 'Berlin Group' is a pan-European payments interoperability standards and harmonisation initiative with the primary objective of defining open and common standards in the interbanking domain (Berlin Group, n.d.[51]).

[6] Pay by link is a technology that allows customers to make payments by sending them a web payment link.

[7] Conversely, the Financial Action Task Force has highlighted that, by pooling more data, financial institutions can improve their abilities to detect money laundering and terrorist financing (FATF, 2021[49]).

# ANNEX: Agenda

## Wednesday, 16 March 2022

| | |
|---|---|
| 12.30 – 13.00 | ***Meeting registration and check-in*** |
| 13.00 – 13.10 | **Opening and welcome remarks**<br>• Andrew Wyckoff, Director, Science, Technology and Innovation Directorate, OECD<br>• Jules Polonetsky, CEO, Future of Privacy Forum |
| 13:10 – 14:30 | **Session 1: Data-driven innovation in banking: the state of play of open banking**<br>*Open banking initiatives have been in place in some countries for several years, or are currently being planned. Different policy-makers and agencies have taken (or are considering) different paths with regard to the need for legislation/regulatory action. Furthermore, the experience accumulated over the years can shed light on the difficulties encountered to balance data protection while promoting wider sharing of banking data. The first session will explore banking regulators' and industry's views around the following questions:*<br>• *What were the aims and expectations for the jurisdiction's open banking initiative when it was launched?*<br>• *To what extent have the outcomes matched the initial ambitions?*<br>• *Have banking services become more unbundled?*<br>• *What challenges has open banking raised for regulation and enforcement?*<br>**Moderator:** Pinar Ozcan, Academic Director, Oxford Future of Finance and Technology (Fintech) Initiative<br>**Speakers:**<br>• Larisa Tugui, Senior Policy Expert, Conduct, Payments and Consumers Unit, European Banking Authority<br>• Alan Lim, Head, FinTech Infrastructure Office, Monetary Authority of Singapore<br>• Richard Mould, Senior Policy Lead, UK OBIE<br>• Daniel Hahiashvili, Head of Technology and Innovation Division, Central Bank of Israel<br>*Open discussion*<br>*Lead discussant: Fanny Solano, Head of Regulatory Affairs & Implementation Management, CaixaBank* |

| | |
|---|---|
| 14:30 – 14:40 | ***Break*** |
| 14:40 – 16:00 | **Session 2: Data portability and inclusion as the economic and social rationales for open banking**<br>*Data portability brings benefits for competition and for consumers' autonomy, which is one of the key principles of data protection. Open banking is deemed an effective application of data portability. It is considered a tool to address low rates of switching and high prices for banking services. In addition, open banking is expected to make financial services more inclusive. Several years after the adoption of some open banking initiatives, it is important to assess the existing evidence to gauge the effects that have resulted from the regulatory or private initiatives implemented. This panel session will consider the following questions:*<br>• *Have customers (especially consumers) made full use of open banking? If open banking has not been user-led, what could explain such lack of traction among users?*<br>• *Are data privacy and security playing a role as competitive advantages for service providers that are committed to them?*<br>• *What players benefit more from open banking? Big players or smaller ones?*<br>• *Has open banking improved financial inclusion?*<br>**Moderator:** Ori Schwartz, Head of Competition Division, OECD<br>**Speakers:**<br>• Sheila Jambekar, CPO, Plaid<br>• Paul Franklin, Executive General Manager, Consumer Data Right Division, Australian Competition and Consumer Commission<br>• Sabrina Basran, Director, UK Competition and Markets Authority<br>• Giuseppe Colangelo, Jean Monnet Chair in European Innovation Policy, University of Basilicata<br>*Open discussion*<br>*Lead discussants:*<br>*Karen Nadasen, CEO, PayU*<br>*Cara Yara, Privacy Policy Manager, Meta* |

## Thursday, 17 March 2022

| | |
|---|---|
| 12.30 – 13.00 | **Meeting Registration and Check in, 2nd day of Meeting** |
| 13:00 – 14:20 | **Session 3: Privacy, consent and liability in open banking**<br>*Open banking implements data portability in the banking sector. This implies that data circulate in a wider ecosystem than in traditional, "closed" banking. This is deemed to be positive for the data subject's empowerment, by making the right to portability effective and easier to exercise. However, the wider circulation of personal data potentially may also raise risks for privacy and security. This session will explore the following questions:*<br>• *What privacy and security concerns does open banking raise? Is consent an effective basis for processing personal data in this area?*<br>• *Are current laws and regulations sufficient to protect privacy in open banking initiatives?*<br>• *How can trusted digital identity frameworks be designed?*<br>• *Is the sharing of data on payments and other transactions taking place across borders? Are there specific challenges linked to such cross-border sharing of data?*<br>**Moderator:** Audrey Plonk, Head of Digital Economy Policy Division, OECD<br>**Speakers:**<br>• Reuven Eidelman, Head of Legal Department, Privacy Protection Authority, Israel<br>• Ryosuke Ushida, Director for Strategy Development, FinTech and Innovation Office, Financial Services Agency, Japan<br>• Andrea Stubbe, Office of the North Rhine-Westphalia Commissioner for Data Protection and Freedom of Information – Member of the Financial Matters Subgroup, European Data Protection Board<br>• Rahul Matthan, Partner, Trilegal<br>*Open discussion*<br>*Lead discussant: Caroline Louveaux, Chief Privacy Officer, Mastercard* |
| 14:20 – 14:30 | ***Break*** |
| 14:30 – 15:50 | **Session 4: Co-operating among regulators, nationally and internationally**<br>*Open banking pursues objectives that pertain to data governance, competition, and banking regulation. Likewise, by its very nature, open banking gives rise to risks in all these different sectors. The regulatory* |

| | |
|---|---|
| | *and enforcement frameworks need to take into account this cross-sectoral dimension and allocate powers and responsibilities accordingly. This panel session will be devoted to the following questions:*<br>• *How can we improve the consistency of policy developments across data protection, competition and financial regulation?*<br>• *What difficulties do national authorities experience in overseeing open banking, also across borders?*<br>• *What is the ideal allocation of powers and responsibilities among different regulatory authorities at the domestic level? Should one authority be entrusted with exclusive powers?*<br>• *How can we ensure effective cross-sectoral co-operation at the international level?*<br>**Moderator:** Limor Shmerling Magazanik, Managing Director, Israel Tech Policy Institute<br>**Speakers:**<br>• Simon McDougal, Senior Fellow, Future of Privacy Forum<br>• Juan Carlos Crisanto, Deputy Chair of the Financial Stability Institute and Head of Technology and Capacity Development, Bank for International Settlements<br>• Marianna Karttunen, Policy Analyst, Regulatory Policy Division, OECD<br>• Douglas Arner, Professor in Law, University of Hong Kong<br>*Open discussion*<br>*Lead discussant: Kent Andrews, Senior Vice President, Regulatory Risk, Toronto-Dominion Bank Group (Canada), and Chair, Business at OECD Finance Committee* |
| 15:50 – 16:00 | **Closing remarks**<br>Steve Wood, Chair, OECD Working Party on Data Governance & Privacy, and Deputy Commissioner, Information Commissioner's Office, UK |