OECD GOING DIGITAL TOOLKIT

POLICY NOTE

# The impact of data portability on user empowerment, innovation, and competition

OECD
BETTER POLICIES FOR BETTER LIVES

going digital

This Toolkit note was written by Christian Reimsbach-Kounatze and Andras Molnar. It was reviewed by the OECD Digital Policy Committee (DPC) and the OECD Working Party on Data Governance and Privacy (DGP). This paper was approved and declassified by written procedure by the OECD Digital Policy Committee on 22 February 2024 and prepared for publication by the OECD Secretariat.

This Toolkit note is a contribution to the OECD Going Digital project, which aims to provide policy makers with the tools they need to help their economies and societies thrive in an increasingly digital and data-driven world.

For more information, visit *www.oecd.org/going-digital*.

#GoingDigital

*Please cite this publication as:*

Reimsbach-Kounatze, C., A. Molnar (2024), "The impact of data portability on user empowerment, innovation, and competition" *Going Digital Toolkit Note*, No. 25

*Note to Delegations:*

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

DSTI/CDEP/DGP(2022)12/FINAL.

# Table of Contents

## Tables



## Figures



## Boxes

# The impact of data portability on user empowerment, innovation, and competition

Data portability has become a tool for enhancing access to and sharing of data across digital services and platforms. It can empower users to play a more active role in the re-use of their data and can help stimulate competition and innovation by fostering interoperability while reducing switching costs and lock-in effects. However, the effectiveness of data portability in enhancing competition depends on the terms and conditions of data transfer and the extent to which competitors can make use of the data effectively. Additionally, there are potential downsides: Data portability measures may unintentionally stifle competition in fast-evolving markets where interoperability requirements may disproportionately burden SMEs and start-ups. And by enabling data transfers to multiple destinations, data portability can also increase digital security and privacy risks. The latter underlines the importance of trust in the providers of digital services or platforms for the adoption of data portability. This Toolkit note presents the following five dimensions essential for designing and implementing data portability frameworks: 1) sectoral scope; 2) beneficiaries; 3) type of data; 4) legal obligations; and, 5) operational modality, and provides an overview of ongoing government and private sector initiatives in this domain.

Data portability is the ability of users – both natural or legal persons – to request that a data holder[1] transfer, to them or a specific third party, data[2] concerning that person in a structured, commonly used and machine-readable format on an ad hoc or continuous basis (OECD, 2021[1]). This capability can empower users to actively manage and re-use their data across various digital services and platforms.[3] Data portability can also enable interoperability that in turn can facilitate communication between systems, typically through interoperable technical specifications including standards and application program interfaces (APIs) – the software specifications used for data transfers between digital services.

As data portability provisions become increasingly common in legal frameworks, significant implementation challenges remain: In the right circumstances, data portability has the potential to boost competition, foster data-driven innovation, and broaden consumer choice. However, it also poses the risk of creating unintended disincentives for investments in data and adversely affecting market structures in specific scenarios. Additionally, transferring data to third-party entities that are beyond the control and purview of the original data holder introduces new layers of risk in terms of privacy, intellectual property rights (IPR), unethical uses of data and digital security. The intensifying complexity of the landscape, coupled with implementation challenges, can exacerbate legal uncertainties, especially concerning liabilities. This can also fuel trust issues and reluctance among users to embrace data portability initiatives.

[1] This toolkit note adheres to the definitions of the OECD (2021[19]) Recommendation on Enhancing Access to and Sharing of Data. Therefore, the term "data holder" is used as a more general term than "data controller", the latter being specific to holders of personal data per the OECD (OECD, 2013[58]) Recommendation concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (hereafter, the "OECD Privacy Guidelines"). Data holders "refers to organisations or individuals who, according to applicable laws or regulations, are competent to decide on granting access to or sharing data under their control, regardless of whether or not such data are managed by that organisation or individual or by an agent on their behalf." (OECD, 2021[19])

[2] The term "data" is understood as "recorded information in structured or unstructured formats, including text, images, sound, and video." This includes, but is not limited to, personal data which, in line with the OECD Privacy Guidelines, "refers to information relating to an identified or identifiable individual (data subject)". (OECD, 2021[19])

[3] Data portability aligns well with the individual participation principle of the OECD Privacy Guidelines. According to this principle individuals "should have the right to obtain from a data controller, or otherwise, confirmation of whether the controller has data relating to them [and] to have communicated to them, data relating to them within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to them" (OECD, 2013[58]).

## Mapping approaches to data portability

Data portability initiatives vary significantly across jurisdictions in terms of their nature, purpose, scope (i.e. who has the right to have data ported and what data can be ported), technical and legal requirements, and implementation. While there are significant differences, some data portability arrangements and initiatives share some commonalities that reflect common approaches to data portability. The following five key dimensions (identified in OECD, 2021[1]) can be used to categorise data portability arrangements and initiatives. Combined, they provide a taxonomy that can be used for mapping and analysing data portability initiatives in the private and public sectors (see Annex):

- Sectoral scope, including whether they are sector-specific or horizontal and thus directed potentially at all data holders across all sectors.
- Beneficiaries, including whether only natural persons (i.e. individuals) or also legal persons (i.e. businesses) have a right to data portability.
- Type of data that is subject to data portability arrangements, including whether data portability is limited to personal data and whether it includes volunteered, observed or derived data.
- Legal obligations, especially the extent to which data portability is voluntary or mandatory and if the latter, whether data portability consists of an ex ante regulatory measure or an ex post enforcement action.
- Operational modality, or modalities of data transfer reflecting the extent to which data transfers are limited to or include ad hoc (one-time) downloads of data in machine-readable formats (regarded as "data portability 1.0"), ad hoc direct transfers of data to another data holder ("data portability 2.0"), or real-time (continuous) data transfers between data holders that enables interoperability between their digital services ("data portability 3.0").

Other dimensions could be used to categorise data portability arrangements, which, although pertinent, are not the central focus of the initiatives presented in the Annex. For example, data portability initiatives could also be classified based on whether data portability consists of an ex ante or an ex post regulatory measure. Contrary to the ex ante measures outlined in the Annex, ex post measures are typically specific to competition enforcement, and are typically invoked by a regulator or the relevant court as a remedy once a breach of antitrust laws is identified. (Box 1; see also OECD, 2021[2])

Box 1. Data portability as (*ex post*) competition enforcement remedy

Data portability is often considered one of the ex ante regulatory measures that complement competition law remedies in policy discussions on competition issues (CMA, 2020[2]) (ACCC, 2020[3]) (HDMC, 2020[4]). Data portability can also be considered as an ex ante measure in merger reviews. However, the large majority of such cases tend to focus on requiring merging firms to license (bulk) data access instead of data portability as defined in this report (FTC, 2014[5]).

Generally, ex post competition remedies have several advantages over ex ante regulatory measures. These include minimal compliance costs due to targeted enforcement, greater flexibility, and coverage over all types of data when used for facilitating data sharing (OECD, 2020[6]). The unpredictability inherent in the development of digital markets and the potential benefits of digital innovations amplify the significance of these advantages. Against this backdrop, ex ante regulation that applies to all market participants can impose overbroad restrictions or costs on markets that ultimately do not exhibit competition concerns, potentially stifling innovation unnecessarily (JFTC, METI, MIC, 2019[7])

However, when faced with systemic competition issues common in the digital economy, governments have begun to consider complementary ex ante regulatory measures. Fast moving markets in the digital economy can generate adverse competition effects that may cause large-scale harms before competition law investigations and interventions are completed. In addition, efforts to investigate may be hampered if potential competitors also rely on services offered by the dominant platform and are reluctant to co-operate with investigators. This situation is compounded by the intricate networks of value chains and digital transactions which may challenge the ability to demonstrate adverse impacts on competition and consumer welfare (CMA, 2020[2]) (HDMC, 2020[4]) (HDMC, 2020[8]).

In response to competition concerns stemming from the unique characteristics of digital platforms, governments are considering ex ante measures focusing on the governance of platform operators and data-related remedies such as data portability. As these measures can fundamentally impact competition, careful consultation with stakeholders and long-term analysis and monitoring are needed (CMA, 2020[2]). Additionally, enhancing data portability is being explored to increase consumer control over data and reduce barriers to entry and expansion.

Source: (OECD, 2021[9])

### *Sectoral scope*

There is a major distinction between general cross-sectoral data portability approaches (sometimes also referred to as horizontal approach) and sectoral or sector-specific approaches. General cross-sectoral approaches include privacy and data protection frameworks such as the European Union's General Data Protection Regulation (GDPR), the GDPR of the United Kingdom, the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA) as well as other cross-sectoral data governance frameworks such as the Digital Markets Act (DMA) and the EU Data

Act, (see further details about data portability initiatives in the Annex). Conversely, sectoral approaches are most frequently used for critical infrastructure and cover e.g. financial services (open banking and the EU Second Payment Service Directive of November 2015 [PSD2]), transportation and mobility (the EU Regulation on Motor Vehicles of May 2018), energy (e.g. EU Electricity Directive of 2019) and health care (e.g. HIPAA).

Australia's Consumer Data Right (CDR) is also mainly used for critical infrastructures, although it can be best classified as a hybrid approach in this respect. The CDR is implemented at a sectoral level based on requirements defined with market participants (primarily in infrastructural sectors such as energy, banking and telecommunications). However, it is a horizontal framework that ensures a common approach across sectors. Following the CDR's strategic assessment, the CDR is moving towards 'targeted datasets' (Australian Government, 2022[10]). The strategic assessment identifies 'open finance' as the likely next priority area to expand the CDR. Open finance is anticipated to include datasets from across sectors, including general insurance, superannuation, merchant acquiring and non-bank lending service providers.

Horizontal data portability initiatives in the past have focussed on a specific type of data, mainly personal data. In an analysis of the legal framework on data portability in the European Union (EU), CERRE (Streel, Kramer and Senellart, 2020[11]) shows that horizontal data portability initiatives focus either on personal data or non-personal data with competition law being the exception in many respects. On the other hand, sector-specific data portability initiatives usually cover a range of data types. This has changed with the introduction of the EU DMA as well as the EU Data Act which incorporate data portability provisions that complement Art. 20 GDPR on the right to data portability (Table 1).

Table 1. EU legal frameworks for data portability and sharing

| | Personal data | Non-personal data | All data |
|---|---|---|---|
| Horizontal | Art. 20 GDPR – Right to data portability | Art. 16 Digital Content Directive – Obligations in the event of termination | Art. 6(9-11) DMA – Obligations for gatekeepers to provide data portability |
| | | Art. 6 Free Flow of Non-personal Data Regulation – Porting of data | Chapter II Data Act – B2C and B2B data sharing with a focus on the Internet of Things |
| Sector-specific | Art. 66(4) and 67(3) – Second Payment Service Directive (PSD2) | | |
| | Art. 61 Regulation on Motor Vehicles (2018) – Access to vehicle diagnostic, repair and maintenance data | | |
| | Art. 23(2) New Electricity Directive | | |

It is important to recognise that both, horizontal and sectoral approaches to data portability, can co-exist, although there are compelling reasons to adopt one over the other. For instance, sector-specific approaches can better address the specific legal, organisational and technical requirements of individual sectors, given that requirements for data transfers may vary by both data type and sector. Cross-sectoral approaches may on the other hand facilitate data sharing across sectors more effectively. This becomes possible as certain industries may not have sufficient incentives to develop a sector-specific data-sharing framework on their own. Furthermore, sector-specific approaches may create asymmetries. In these cases, certain businesses may act as data "gatekeepers", while others may be required to share their data. As an illustration, the revised PSD2 enables non-banks to access consenting clients' payments data when they are authorised as third-party providers. However, banks are not given similar access to the comparable data sets, which could lead to unfair competition (de la Mano and Padilla, 2018[12]; Di Porto and Ghidini, 2020[13]; Kerber, 2021[14]).

Given the difference in their sectoral scope, combined with their various objectives, such as privacy and data protection, consumer empowerment, innovation and competition support and enforcement, data portability measures may require cross-agency co-operation among different regulators and policymakers. This includes in particular co-operation between enforcement authorities in charge of competition, privacy and consumer protection. Other regulatory domains may also be concerned where data portability is implemented at a sectoral level (e.g. open banking). Co-operation across policy perspectives will be particularly valuable in terms of avoiding unintended consequences of data portability measures and developing the most suitable oversight approach. Further, given experience with these measures is limited, the sharing of lessons learned across regulators and jurisdictions will prove particularly valuable. Initiatives like the United Kingdom's Digital Regulation Cooperation Forum and Australia's Digital Platform Regulators Forum are noteworthy in this context, serving as platforms to enhance coordination and collaborative efforts among regulatory entities, addressing the multifaceted challenges and opportunities presented by digital platforms. That said, governments still need to plan which regulator will have primary oversight of respective initiatives to ensure efficiency, streamlined processes and beneficial outcomes.

### *Beneficiaries*

Most data portability initiatives tend to focus on individuals as the only beneficiary of the right to data portability. This reflects the common rationale of most data portability initiatives, specifically the desire to empower individuals, notably consumers. It is especially the case with privacy and data protection frameworks that include a data portability right, such as the GDPR and the CCPA/CPRA.

However, more recent initiatives also allow users more broadly (including organisations) to request that a data controller transfer their data to the user or to a third party. Australia's CDR, for instance, extends the right to certain businesses. More

specifically, the legislation defines one of its three categories of actors as "CDR consumers", which can include individuals and businesses. CDR consumers can hold rights to access data held by data holders (the other category of actor) and direct that data be shared with accredited data recipients (the third category of actor).

Similarly, the EU Free Flow of Non-Personal Data Regulation, promotes data portability of non-personal data in business-to-business (B2B) relationships. "The Regulation instructs the Commission to contribute to the development of EU Codes of conduct to facilitate the porting of (non-personal) data in a structured, commonly used and machine-readable format including open standard formats" (Streel, Kramer and Senellart, 2020[11]). The regulation aims, among other goals, to enable easier switching between cloud service providers for professional users. The European Commission has been working with stakeholders on "facilitating self-regulation in this area, encouraging providers to develop codes of conduct regarding the conditions under which users can move data between cloud service providers and back into their own IT environments" (European Union, 2018[15]).

To address apparent shortcomings in data portability and interoperability following the EU Free Flow of Non-Personal Data Regulation, the European Commission (2022[16]) proposed the Data Act (issued on 23 February 2022 and adopted on 27 November 2023). These shortcomings include both "the limited efficacy of the self-regulatory frameworks" and "the general unavailability of open standards and interfaces," as well as the need "to adopt a set of minimum regulatory obligations on providers of data processing services." (European Commission, 2022[16]) The Data Act has several relevant provisions on data portability, e.g., provision to further enable the switching between cloud and edge services and address existing lock-in effects (most notably Article 29). Significantly, the Act broadens the data portability rights to include not only individuals but also legal entities. It also aims to improve interoperability with regard to the building of common European data spaces, where necessary (European Commission, 2022[16]).

The Data Act is complemented by the Digital Markets Act (DMA) (adopted on 19 July 2022), which also includes data portability obligations in Article 6 (9-11). Besides individuals covered under Article 6(9) DMA, Article 6(10) DMA mandates access by business users to data associated with their use of the gatekeeper's services, while Article 6(11) DMA mandates access by "third-party online search engines" to "ranking, query, click and view data" (subject to anonymization for personal data) at fair, reasonable and non-discriminatory (FRAND) terms.

### *Data subject to data portability arrangements*

When data are subject to data portability arrangements it is commonly required that such data must be transferred "in a structured, commonly used, and machine-readable format". However, substantial variations can exist in data portability arrangements in respect to which data is deemed portable, beyond potential needs for further

clarification on what qualifies as a structured, commonly used, and machine-readable format.[4]

OECD work on data governance stresses the need to differentiate between the different types (OECD, 2015[17]; OECD, 2019[18]; OECD, 2021[19]) which is imperative in the context of data portability and for addressing various stakeholder interests. In the context of data portability, the OECD (2019[18]) distinguishes between:

- *Volunteered (or surrendered, contributed or provided) data* are data provided by individuals when they explicitly share information about themselves or others. Examples include entering credit card information for online purchases or creating a social network profile.
- *Observed data* are created where activities capture and record data. In contrast to volunteered data, where the data subject is actively and purposefully sharing its data, the role of the data subject in the case of observed data is passive; the data controller plays the active role. Examples of observed data include location data of cellular mobile phones and data on web usage behaviour.
- *Derived (or inferred or imputed) data* are created by data analytics processes, including data "created in a fairly 'mechanical' fashion using simple reasoning and basic mathematics to detect patterns" (OECD, 2014[20]). In this case, the data processor plays the active role. Data subjects typically have little awareness over what is inferred about them. Examples of derived data include credit scores calculated based on an individual's financial history.
- *Acquired (or purchased or licensed) data* are obtained from third parties based on commercial contracts or licences (e.g. when data are acquired from data brokers) or other non-commercial means (e.g. when data are acquired via open government initiatives). As a result, contractual and other legal obligations may affect the access, use and sharing of the data.

The above categories are not exclusive to one another, and other categorisations may be also pertinent depending on the context. This categorisation reflects the extent to which different stakeholders are involved in the creation of data and acknowledges that stakeholder involvement might take place at different times, including when

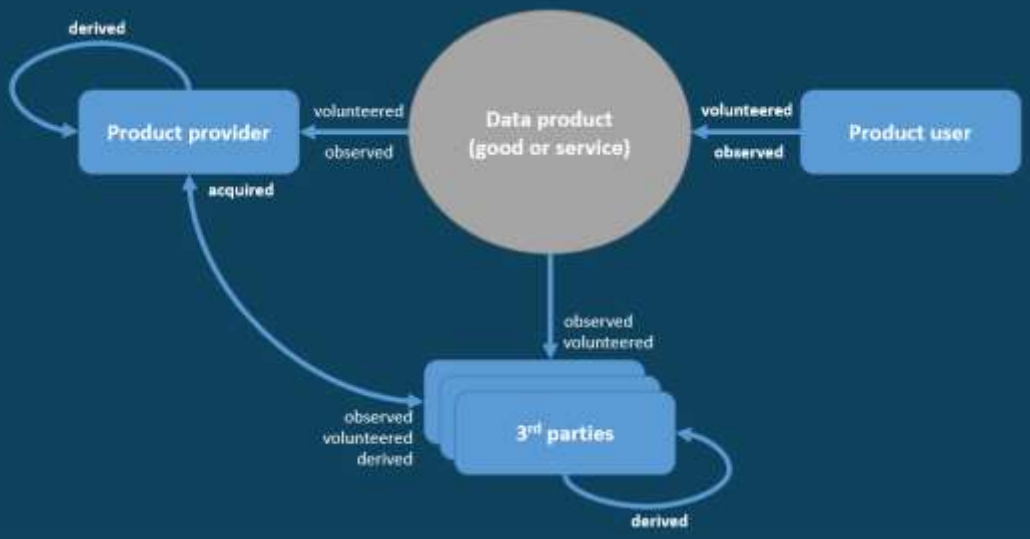
[4] See for example the cases brought by taxi "app drivers" against Uber and Ola Cabs in the Netherlands where the individuals invoked Article 20 EU GDPR, asking for their data to be received either via an API or a CSV file. However, the court, referring to Directive 2013/37/EU on the re-use of public sector information, ruled that "machine-readable" does not obligate the provision of data through these specific means. The court rejected the requests as the claimants did not justify why they needed additional (machine-readable) personal data to what they already had and didn't specify what additional data they required. (IAPP, 2022[25] citing Rechtbank Amsterdam, 2021[58] and Rechtbank Amsterdam, 2021[59]). See also Wong and Henderson (2019[55]) who made 230 real-world data portability requests based on Article 20 EU GDPR across a wide range of data controllers, showing that only 75% of data portability requests were successfully completed with some file formats not meeting the GDPR requirements.

users (consumers and businesses) interact with a data product (good or service) such as a social networking service or a portable smart health device (OECD, 2019[18]). Data portability initiatives tend to focus primarily on volunteered data and to some extent on observed data. Some uncertainties remain on whether observed data should be subject to portability rights.

The European Data Protection Board (EDPB), which endorsed an opinion by the Article 29 Working Party (adopted on 27 October 2017), includes within the scope of "data provided by the data subject" both (i) data provided with the individual's consent, and (ii) data provided by the individual by virtue of the use of the service or the device, "from the observation of his activity" ("observed data"). However, it should not include personal data that are inferred or derived, which include personal data that are created by a service provider (for example, algorithmic results).

The right to data portability enshrined in Article 20 of the GDPR, for instance, only applies to personal data "provided by" the data subject under two specific legal bases for lawfulness of processing (i.e. data collected with consent, or where the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract).

Figure 1. Data products and the different ways data originate




*Note:* Arrows represent potential data flows between the different actors and a data product (good or service). The type of data is highlighted in bold to indicate the moment at which the data are created.
*Source:* (OECD, 2019[18]).

The Data Act of the EU broadens the scope of data portability to include a much wider range of data, offering a more comprehensive reach than Article 20 of the GDPR, which

focuses only on personal data. Not only does the Data Act cover both personal and non-personal data generated by the use of a product or service. The Act also specifies that both "actively provided" and "passively observed" data fall under the ambit of portability rights. Furthermore, it removes the limitation of scope based on the legal basis for data processing from just consent or contract as in the case of the GDPR, making the right applicable irrespective of the legal grounds for data processing. Moreover, the Act mandates the technical feasibility for third-party access to all types of data, going beyond the limited technical requirements set out in previous regulations.

In Australia's CDR, the relevant Minister designates the classes of data that will be available for data sharing in a specific sector, should the consumer wish to do so. Only 'volunteered' or 'observed data' is currently required to be shared. Depending on the industry, the type of data made available to consumers can differ significantly, reflecting sector-specific risks and requirements. For instance, in the banking sector data holders are required to share data on financial products such as credit and debit cards, deposit and transaction accounts, and data on mortgages. Data holders are able to share additional data on a voluntary basis.

### *Legal obligation and enforcement action*

The legal obligations surrounding data portability vary widely across jurisdictions and sectors, encompassing a range of approaches from voluntary frameworks to mandatory requirements. And when mandated, the mechanisms for enforcement can also differ considerably.

For example, the United Kingdom's midata initiative introduced in 2011 as voluntary frameworks granted authority under the Enterprise and Regulatory Reform Act 2013 to enforce compulsory regulations if voluntary measures proved insufficient. A similar approach to self-regulation is taken by the EU's Free Flow of Non-Personal Data Regulation, which requires businesses to adhere to "self-regulatory codes of conduct" monitored by the European Commission. Acknowledging the limitations of this self-regulatory framework, the European Commission later proposed the Data Act with mandatory portability provisions.

Data portability provisions in most cases carry a mandatory obligation, especially in privacy and data protection as well as sector-specific regulations, and these are typically backed by varying levels of oversight and enforcement. For instance, both the GDPR and the CCPA/CPRA establish obligatory data portability measures for entities under their jurisdiction. Singapore's Personal Data Protection Act (PDPA) was amended to include a new data portability obligation, which will come into effect with the issuance of forthcoming regulations. In Australia, the Consumer Data Right (CDR) requires data holders to share consumer data, but it gives consumers the discretion to opt in. The EU's Revised Payment Services Directive (PSD2) mandates third-party access to both account and payment transaction data. On the other hand, Japan's

Banking Act amendment leans towards a voluntary data portability arrangement, though (as of 2020) more than 70% of banks have chosen to adopt its open APIs.

Data portability regimes can also be classified based on whether data portability consists of an *ex ante* regulatory measure or an *ex post* enforcement action. Data portability measures tend to be of the former type, which the exception of those implemented in the context of competition enforcement mechanisms (OECD, 2021[21]). In the latter case, data portability may emerge as the subject of, or remedy to, a competition enforcement theory of harm. For this to occur, several conditions must be met, including the importance of the data or platform access, the lack of technically and legally feasible workarounds (such as data scraping), and the ability of firms with market power to benefit from the alleged misconduct.

Degrading data portability (or interoperability) could be anticompetitive, and could thus be considered an abuse of dominance. However, it may be challenging to assess the related theories of harm in cases in which there were no pre-existing portability or interoperability arrangements. Collusive arrangements among market participants to deter entry through selective interoperability may also arise. More broadly, data portability and interoperability may be considered as remedies in abuse of dominance cases or in merger proceedings to address fundamental market conditions giving rise to competition concerns. Competition authorities in some jurisdictions have also imposed or recommended portability and interoperability measures through market studies, market investigations and advocacy activities.

The benefit of addressing interoperability and portability through competition enforcement and market studies or investigations is the resulting focus on competition harms, and the source of those harms, such as a dominant firm. In addition, competition law remedies can be flexibly designed according to the situation of a given market, and adapted as the market evolves. However, these remedies will require substantial oversight, which may be a significant challenge for authorities to design and monitor.

Given these challenges, *ex ante* regulation may be a possible alternative approach, particularly when the regulation is tailored to a specific sector, and there is a sector regulator in place to provide surveillance and dispute adjudication. This approach may also be faster or more preventative than competition enforcement. Examples of a regulatory approach include data protection regulation, open banking (which has been used to enable multi-homing, shopping around, and mixing and matching), and proposed new measures focused on gatekeeper digital platforms.

### *Operational modality*

Data portability is commonly characterised by the provision of data in a structured, commonly used and machine-readable format. Nevertheless, the structured and machine-readable data can be provided to the user in several different ways. This typically includes (i) (ad hoc) downloads, whereby the data are stored (in a commonly

used machine-readable format) and made available online (e.g. via a website)[5]; as well as APIs, which enable service providers to make their digital resources (e.g. data and software) available over the Internet.

Contrary to ad hoc downloads, APIs can enable continuous real-time data portability and thus the smooth interoperability of the different actors, their technologies and services. In addition, data holders can implement several restrictions via APIs to better control the use of their data, including by enabling access based on the identity of API users, and the scale and scope of the data used. Last, but not least, a dedicated API may reduce the perceived necessity of 'data scraping' (or 'screen scraping'), which requires users to grant third parties' access to their online account to extract the data from the online interface and, in some cases, to execute transactions on the customer's behalf. Such activities may violate data holders' terms of use or the IPRs of third parties. Data portability regimes that take advantage of APIs may in this way increase the security of, and trust underpinning, data transfers, while minimizing the risk of copyright violations.[6]

The delay between the user's request and the transfer of data is another consideration through which data portability initiatives can be distinguished. For example, Article 12(3) of the GDPR requires that the original data holder provides the data subject with information on action taken in response to a request "without undue delay" and in any event within one month of receipt of the data subject's request. This one-month period can be extended to a maximum of three months for complex cases where the data subject has been informed about the reasons for such delay within one month of the original request. In contrast, the CCPA requires that businesses that receive a verifiable request from a consumer must:

> *promptly take steps to disclose and deliver, free of charge to the consumer, the customer's personal information (…) by mail or electronically, and if provided electronically, the information shall be in a portable and, to the extent technically feasible, readily useable format that allows the consumer to transmit this information to another entity without hindrance. (California Civil Code Section 1798.100[d])*

As another example, PSD2 provides that:

> *(t)he account servicing payment service provider shall: (…) (b) immediately after receipt of the payment order from a payment initiation*

[5] These formats may enable data syntactic portability, i.e. the transfer of "data from a source system to a target system using data formats that can be decoded on the target system" (OECD, 2019[18]). However, they do not guarantee data semantic interoperability, defined as "transferring data to a target such that the meaning of the data model is understood within the context of a subject area by the target".

[6] Data scraping can lead to copyright concerns as the scraped data may include copyright protected material, which when republished or used in a different context, may violate copyright laws. (Teresa Scassa, 2019[56]; CNIL, 2020[57])

> *service provider, provide or make available all information on the initiation of the payment transaction and all information accessible to the account servicing payment service provider regarding the execution of the payment transaction to the payment initiation service provider.*

Data portability arrangements may also distinguish the types of data recipients, in particular whether third-party data recipients need to be accredited to receive data. In Australia's CDR, for instance, third parties that can access CDR data directly from data holders must have demonstrated the implementation of particular digital security standards (OAIC, 2021[22]). To be able to receive consumer data directly from data holders, third-party data recipients must be accredited by the Australian Competition and Consumer Commission (ACCC). Once accredited, they are referred to as "accredited data recipients" (ADRs) or "accredited persons" and can "use a CDR brand mark to help consumers recognise that the business is able to receive their data securely and manage it in line with the rules and safeguards of the CDR system" (OAIC, n.d.[23]).

While common APIs can help address data portability challenges, their development and implementation typically requires coordination between market participants. The private sector obviously plays a pivotal role in shaping and implementing standards essential for effective data portability, including the development of APIs. Notably, in 2018, a consortium of tech companies such as Google, Meta, Microsoft, Apple, and Twitter (now X) proactively collaborated to launch the Data Transfer Project (DTP). This initiative aimed to develop a shared approach to data portability, a necessity in order to fully and effectually implement and effectuate the goals driven by regulations. Building on the work of the DTP, in 2022, a subset of its contributors – Google, Apple, and Meta - established the Data Transfer Initiative (DTI), a non-profit focused on furthering the same goals. Both these initiatives use existing APIs and develop service-specific adapters to streamline data transfers, encouraging a wider array of service providers to support portability and thereby fostering innovation and interoperability.

Some governments and regulators have leveraged this pivotal role of the private sector by establishing 'coordination entities' with private sector participation. For instance, the Competition and Markets Authority (CMA) in the United Kingdom collaborated with the nine largest banking institutions to establish the Open Banking Implementation Entity (OBIE). The OBIE has been instrumental in developing the API standards that guide the country's Open Banking initiative and that commentators have seen as one of the success factors of the initiative. In the context of Australia's CDR, the government established the Data Standards Body (DSB) to deliver open standards with the support of multistakeholder working groups for designing and testing these open standards. Similarly, the European Data Innovation Board (EDIB), as set out in Article 29 of the EU's Data Governance Act, works in tandem with the Data Spaces Support Centre (DSSC) and industry partners to foster the adoption of best practices and cross-sectoral data sharing standards.

# Data portability opportunities and challenges

## *Increasing competition and consumer choice*

From a competition perspective, data portability measures seek to address a broad range of concerns prevalent in online markets. These include consumer lock-in associated with network effects, anticompetitive conduct enabled by vertically integrated business models and conglomerate enterprises, demand-side concerns such as consumer inertia, and the exploitation of 'data feedback loops'[7] in reducing market contestability. Additionally, data portability can also leverage digital technologies to promote competition in specific sectors such as banking, energy and transportation to name a few. (OECD, 2023[24])

Data portability measures aimed at enhancing competition strive to lower user switching costs and reduce friction when adopting new services. Such measures could, in turn, stimulate competition by facilitating market entry for newcomers, especially in markets where individual-level data holds significant value and is needed for providing services. Further, the competition benefits of data portability may extend beyond the original market as the same data set can in theory fuel multiple applications beyond the markets in which the data were originally collected. Over the medium to long term, this may allow the development of firms outside a market to eventually challenge incumbents within the initial market. (OECD, 2021[21])

Data portability can enable the concurrent use of multiple services that might offer similar, complementary, or competitive functionalities (multi-homing). This may reduce customers' interest in switching services, even if their data are portable. (OECD, 2021[9]) However, even in scenarios where multi-homing diminishes the inclination of customers to switch services, the enhancement of interoperability achieved through real-time data exchanges between various online services, can still enhance competition. (OECD, 2021[21]) This enhancement can occur in two distinct manners: externally, *among* digital platforms (or ecosystems), by allowing users to preserve network effects on new services; and internally, *within* the same digital platforms (or ecosystems), by allowing users to mix and match different complementary services from different providers.

However, the effectiveness of data portability measures on competition could be constrained by several other factors, including those unrelated to data that nonetheless significantly impact the competitive capabilities of firms in data-driven markets. Limitations may arise, for instance, if the scope of the data is too narrow, if

[7] Data feedback loops refer to the self-reinforcing mechanisms in data-driven, multi-sided markets where the collection and reuse of data lead to improved services. These enhanced services attract more users, generating even more data and thereby further improving the service in a virtuous cycle. Such loops can significantly strengthen one side of a multi-sided market, reinforcing its market dominance (OECD, 2015[59]).

user-initiated data portability requests are not sufficient to generate economies of scale, if there are no existing or prospective firms that stand to benefit from the data, or if prevailing network effects limit the value of new digital services regardless of data sharing. (OECD, 2021[21]) These challenges may be compounded by consumer doubts or lack of understanding about the benefits from data portability (see section below on "Adoption and technical implementation challenges").

Additionally, when portability measures include data that required significant investments to obtain and use, including investments in complementary intangible assets such as skills and competences as well as organisational change, they may discourage or render inefficient the implementation of these measures, adversely affecting the development of a market. (OECD, 2021[9]) This could be in terms of data collection or deriving value from raw data through analysis and insights. This is inline with evidence suggesting that larger entities are more equipped than SMEs to undertake the essential investments for transforming data into productivity gains, thereby securing larger market shares. (OECD, 2022[25]) All this underscores that access to data, through mechanisms such as data portability, is a necessary but not sufficient condition for fostering competition in data-driven markets.

Further, data portability could create risks in terms of market transparency (potentially facilitating collusion) or enhancing incumbents' ability to collect even more personal data (both from rivals and consumers), since consumers may be more inclined to share data if they know they can be ported elsewhere. In cases where a dominant digital platform lacks substantial competition, including from potential new entrants, data portability measures may be more effective in stimulating competition in adjacent and complementary markets rather than in challenging the platform's dominance. (OECD, 2021[9]; OECD, 2021[21])

Consequently, when implemented solely to advance competition objectives, data portability measures may be most effective and appropriate in markets where (according to OECD, 2021[12]):

- Access to personal data provides tangible competitive advantages to recipient firms.
- A degree of competition is already present or is expected so that network effects and data-driven economies of scale do not completely preclude effective competition.
- The data in question are applicable to well-defined uses and available in a standardised format.
- The data do not entail substantial IPR or other ownership complexities; and/or
- Consumers are fully informed about their rights and about of the nature of the data to ported, and they are comfortable with and have trust in sharing the data in question between platforms.

Measures aimed at enhancing interoperability, for instance by enabling continuous data transfers can improve data utility for recipients and help consumers preserve network effects when switching services. (OECD, 2021[9]; OECD, 2021[21]) This can address some of the limitations associated with one-off (static) data portability arrangements. However, these measures are not without risks to competition and innovation. Without adequate oversight and careful design, they may entrench incumbent technologies, disincentivise data-related investments and innovation, and heighten risks for exclusionary conduct or tacit collusion.

For example, universal requirements to interoperate with all other services could be expensive with uncertain benefits including for small and medium-sized enterprises (SMEs) and start-ups. Such companies may bear a disproportionate burden, being mandated to ensure compatibility with every existing system in the market upon entry. (OECD, 2021[9]) Conversely, dominant market participants would be more likely to have the capital to invest in necessary systems, as well as to play a role in determining standards. Therefore, asymmetric approaches – for example through either competition enforcement or regulation – may be necessary to concentrate the obligations and burdens of data portability on large incumbents while avoiding the creation of entry barriers for new firms. (OECD, 2021[21])

### *Facilitating personal data flows and enabling informational self-determination*

The portability of personal data more specifically gives data subjects (i.e. the individuals that are identified or identifiable through personal data) the ability to exercise more control over their data. (OECD, 2021[9]) By allowing them to request data downloads or transfers, data portability can be a means to implement individual participation principles such as articulated in the OECD Privacy Guidelines. For individuals to effectively exercise this right, a prerequisite is an existing level of transparency; they to know what data is available about them, the nature of the data being transferred, the entities they are being transferred to, and eventually the duration for which the transfer will persist. This knowledge is crucial as it provides the basis for individuals to make informed decisions regarding what to download and whether to initiate data transfers. All these processes are that distinguish data portability from other data sharing approaches, where data transfer is typically initiated by the data holder or recipient instead of the data subject (or individual).

As a positive consequence of the competition benefits highlighted above, data portability can help address the power imbalance between consumers and digital service providers (OECD, 2021[9]). Specifically:

- The option to download their personal data from a data controller can contribute to more transparency and allow data subjects to determine whether they wish to take further action (such as correction or, to the extent granted by law, deletion).

- The option to transfer allows individuals to switch from a data controller with subpar privacy policies and practices and poor data management capabilities to one that is more trustworthy and better aligned with their privacy and data governance preferences. (See Luzsa et al., 2022[16])
- This capability also serves as a safeguard against data loss or unavailability, for example, if a provider ceases operations. Instead of losing their customer history, individuals could simply transfer their data to a new provider. These features collectively can enhance users' informational self-determination.[8]

While data portability holds promise for enhancing informational self-determination, its benefits are still not guaranteed. (Syrmoudis et al., 2021[26]; IAPP, 2022[27]; Kranz et al., 2023[28]). Success depends on the effective and secure implementation of the data request and transfer processes in line with privacy and data protection obligations and best practices. For example, the digital security protocols of the data recipient may be inadequate, or individuals may lack clear information about how their personal data and privacy will be safeguarded. Therefore, there must be clarity on the circumstances under which the data holder or the data recipient may be held liable for digital security and privacy breaches stemming from data portability transfers. (See next section on "Adoption and technical implementation challenges").

Clarity about responsibility and liability is crucial for data holders, recipients, and data subjects alike. (OECD, 2021[9]) Liability concerns span not only digital security breaches, privacy and IPR violations, but other risks such as poor data quality. These risks can also vary based on the data portability model, industry context, and whether data is transferred on a one-off basis or via a continuous feed. Once data are transferred, the original data controller's liability generally is expected to cease, shifting to the recipient. However, if the original data controller transfers incorrect or insecure data, they could still be held liable. Issues may also arise when third party information may be concerned. Enforcement mechanisms, which can include private lawsuits or regulatory penalties, therefore play a key role although they may vary based on the nature of the breach and the regulatory frameworks involved, making it essential for all parties to understand their responsibilities and potential liabilities.

That said, risks exist that extend beyond legal liabilities. For example, data portability could result in the excessive collection and sharing of personal data even when privacy and data protection requirements are met. Service providers and other relevant actors may gain additional abilities to process and analyse previously inaccessible personal data, thereby enhancing their profiling capabilities which could adversely affect fundamental rights and freedoms. (Van der Auwermeulen, 2017[29]) This may exacerbated by higher risk that these actors may be incentivised to take advantage of vulnerable consumers, such as the elderly and very young consumers, who in turn

[8] For example, when Google's social networking service, Google+, was shut down in 2019 due to low usage and data privacy issues, users had a grace period to download their data, after which they lost access to their posts, images, and other shared content.

may feel pressured to provide more data than is beneficial for them (BEUC, 2022[30]; OECD, 2023[31]).

For instance, an insurance company could demand access to a consumer's social media data through a data portability regime as a precondition for service. Or a company may sell a fitness tracker at a discount if consumers agree to share health data in return, leading to consumers in economically challenging situations being at risk of giving away privacy protection due to economic considerations. Such practices might lead to a resurgence of excessive data collection practices. Therefore, it is crucial to emphasise the importance of the OECD Privacy Guidelines' principles such as data collection limitation and purpose specification to name just a few, and the need for data practices that support these principles, including through e.g. the use of privacy-enhancing technologies. (OECD, 2023[32])Lastly, the right to data portability has significant ramifications for data holders' ownership and control rights over collected data. By granting individuals (and legal persons) a right of data portability, the original data holder's ability to exclusively monetise or otherwise commercially exploit the data that is subject to data portability is typically limited, potentially opening it up for use by competitors. While the intent is to reduce lock-in and increase competition through data sharing in accordance with users' preferences, and the laws and regulations, implementing this presents its own set of challenges as discussed in the next section.

### *Adoption and technical implementation challenges*

Data portability initiatives have seen mixed success in terms of adoption, and this success often hinges on the distinctive approaches in their implementation, particularly with respect to their operational modality but also related practical aspects such as user experience, and the availability of third-party service providers that can leverage data portability.

There is empirical evidence to suggest that the varying degrees of success of data portability initiatives are also closely tied to user capabilities. More specifically, users possessing proficient technical abilities, especially those who value privacy, are more inclined to exercise their right to data portability. (IAPP, 2022[27]; Kranz et al., 2023[28]) This challenge is particular pertinent situations where users are expected to navigate and manage the data transfer process, typically through web interfaces or APIs, or where some data are presented in formats that are incomprehensible to the average person. In the latter, this can lead to lack of sufficient understanding of the nature of the data to be transferred, and of the implications for the user's own rights and that of third parties.

Despite growing legislative support for data portability in certain privacy and data protection frameworks, for instance, adoption by individuals is still facing significant challenges, primarily due to the lack of awareness and understanding. The European Commission acknowledged this challenge in its assessment of two years of application of the EU GDPR, emphasising in respect to Art. 20 of the EU GDPR that "[t]he right to

data portability has a clear potential, still not fully used". (European Commission, 2020[33]) This is in line with findings from Luzsa et al. (2022[34]) according to which only 26% of respondents surveyed in Germany in 2020 were aware of their right to data portability, with not even 7% indicating to have exercised this right. Approximately 25% of respondents indicated that, despite their intentions to switch providers due to concerns related to trust, privacy, and security, they ultimately did not transfer their data to a new service. The main barriers identified encompass concerns over loss of social contacts, loss of data and content, and lack of knowledge or experience with service switching.

This contrasts with initiatives such as open banking, where substantial advancements and adoption have been demonstrated. (OECD, 2023[24]; OECD, 2023[35]) In the United Kingdom, for instance, more than 4 million users consumed open banking services in 2022 with a noticeable rapid increase in the number of payments and API requests were made via the initiative. In December 2023, 1.3 billion requests were successfully made via open banking APIs, 30% more compared to December 2022, and up to 70% more compared to December 2021. In April 2024, the number of requests increased further to 1.4 billion (up to 26% more compared to April 2023).[9]

The relative success of open banking initiatives can be attributed to several factors. In these frameworks, consumers mostly engage with organisations providing value-added services based on the consumers' data, obtained through data portability mechanisms. Consequently, the intricate processes of data transfer are conducted behind the scenes by the organisations, requiring consumers mainly to provide access credentials to the original data holder and consent for the data transfer, thereby minimising technical complexities for the consumers.

Moreover, the development and promotion of standardised APIs for interoperability by a 'coordination entity' such as the OBIE have played a crucial role (OECD, 2023[24]; OECD, 2023[35]). This collaborative effort, involving the United Kingdom's nine largest banking institutions, facilitated smoother interactions among various stakeholders, reduced integration and interoperability challenges, and enabled innovations by third parties. Such innovations have enriched user experience including by alleviating technical burdens on consumers and streamlining their interaction with financial services as highlighted above.

That said, the moderate complexity and structured nature of the financial data being handled has been a contributing factor as well. The data involved in open banking, such as transaction details, account balances, and other financial particulars, are generally well-structured, and thus conducive to be shared securely and seamlessly across platforms via standardised APIs. This stands in contrast to the broader scope of personal data that can be transferred based on the right to data portability of privacy and data protection frameworks and that can range from tabulated data and

[9] See www.openbanking.org.uk/api-performance/ (last accessed 19 June 2024)

text to pictures, videos and other multimedia content.[10] It can be challenging to successfully write software that applies general frameworks to a broad range of data types, as demonstrated by progress made so far by, e.g., the Data Transfer Project (DTP), an open source platform for personal data portability.

## Conclusion

Data portability, as evidenced by the growing body of legislation, stands out as a promising instrument for enhancing access to and sharing of data across digital services and platforms. Data portability initiatives aim to empower users, enhance their self-determination, and/or foster competition and innovation. However, prevailing legislation vary significantly in their emphasis on either user empowerment and self-determination or competition and innovation; and in their applicability, whether cross-sectoral or sector-specific. Furthermore, the current status quo, where data portability rights are largely dormant, in particular within privacy and data protection frameworks, may necessitate further considerations by policy makers and regulators to bridge the gap between legislative intention and practical realisation.

While privacy and data protection frameworks like the GDPR (including in the EU and the United Kingdom) primarily focus on empowering individuals and enhancing informational self-determination through data portability provisions, other legal regimes such as Australia's Consumer Data Right (CDR), the EU's Digital Markets Act (DMA), and Digital Services Act (DSA), along with sector-specific regulations like open banking in the United Kingdom and the early "My Data" initiatives in the United States place greater emphasis on using data portability to foster consumer choice, competition and innovation. These legislative nuances in the specific objectives of data portability initiatives reflect the evolving perspective on data portability's multi-faceted impact – both on individual rights and market dynamics.

However, the variations between existing data portability initiatives, in particular within the same jurisdiction, can introduce legal uncertainties for market participants tasked with implementing these measures. These variations not only pertain to the specific purpose of the initiative, but to the initiatives' scope as well – including who has the right and can request data porting, under which legal basis, and what type of data can be ported, in particular in cases when third party data are involved. These complexities are exacerbated by uncertainties around liabilities, specifically the circumstances under which both the data holder and the data recipient may be held accountable and liable for breaches of privacy or intellectual property rights (IPR). Coupled with the lack of awareness and competence of users in respect to their rights and how to exercise these rights, this can prevent the effective adoption of data portability.

[10] See Wong and Henderson (2019[55]) highlighting the different types of data and their various formats involved in the context of their 230 real-world data portability requests made based on Article 20 EU GDPR.

Considering above challenges, data portability initiatives may require complementary measures to achieve their policy objectives. These could include raising public awareness about the purpose and scope of these initiatives. Specific attention may also be required to clarify the circumstances under which data holders or data recipients may be held liable for rights violations. Central to navigating these complexities and ensuring successful adoption of data portability is also the trust users place in digital service providers or platforms. This trust is the foundation for users' willingness to share and transfer their data and is thus a pivotal element for the success of data portability initiatives. Thus, in efforts to raise awareness, measures put in place to enhance digital security and protect privacy and IPR need to be highlighted.

Clear guidance on implementing data portability measures may also be needed. The observed dichotomy between the uptake of the right to data portability under privacy and data protection frameworks and e.g. open banking initiatives yields crucial insights for the effective implementation of data portability frameworks. This discrepancy cannot be attributed to the differences between sector-specific and cross-sectoral initiatives or the type of legal frameworks. Rather, it points to the importance of the operational modality of data portability initiatives. This includes, most notably, the role of standardised approaches to data transfers, whose development and adoption typically necessitate coordination and advocacy.

Other practical factors, including enhanced user experiences and the availability of third-party service providers that can leverage data portability, also appear to be crucial as they can alleviate potential skill barriers while delivering high value through good user experiences, thereby accelerating acceptance and adoption of data portability. However, to substantiate this perspective, more robust empirical evidence on consumer preferences regarding data portability is needed, specifically to better understand whether and what forms of portability are truly desired by users.

Evidence based on the initiatives assessed so far suggests that coordinated efforts, facilitated by governments where appropriate, may also be required to ensure successful adoption of data portability. This could involve, the help of governments to specify interoperability requirements where appropriate, and to encourage the development and adoption of common APIs and standards. The establishment of 'coordination entities' responsible for promoting the development and/or adoption of these common standards together with best practices has been a well-noted practice among some governments to foster the adoption of data portability. This is exemplified by the Open Banking Implementation Entity (OBIE) seen in open banking in the United Kingdom and the Data Standards Body (DSB) established in the context of Australia's CDR.

In this context, strengthening cross-agency enforcement co-operation and coordination becomes another essential element for the success of data portability initiatives, and 'coordination entities' can also provide a platform for such co-operation and coordination. This is illustrated by the EDIB, which consists of

representatives of national authorities designated under the EU DGA, including but not limited to the European Data Protection Board and the European Data Protection Supervisor, but also other bodies and business representatives with specific sectoral expertise. Cross-agency co-operation is crucial given that data portability initiatives address issues at the intersection of competition, privacy and consumer protection at least. Other regulatory domains may also be concerned where data portability is implemented at a sectoral level (e.g. open banking). As data portability initiatives may span multiple regulatory domains, governments need to plan which regulator will have primary oversight of the initiative to ensure efficiency, streamlined processes and beneficial outcomes. Against this backdrop, the OECD work in reviewing and possible revising the OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy is poised to be highly relevant and instructive in this context.

Lastly, implementation costs should not be underestimated. These may be one-time expenses for setup rather than ongoing costs, covering areas like technical development, consent management, and legal fees. Nevertheless, even these one-time expenditures can prove to be substantial, posing considerable financial strains particularly for SMEs and start-ups, and potentially hindering their ability to integrate data portability effectively within their operational frameworks. Trusted data intermediaries (TDIs) can potentially lower these costs while also enabling compatibility, interoperability and providing enhanced user experiences with high value-added services. Yet, the growing role of TDIs could centralise existing data schemes with negative effects on competition, privacy, and consumer protection. Future OECD work will provide more insights into the challenges and opportunities presented by these emerging intermediaries.

In conclusion, data portability has evolved from its initial conceptual stages into a nuanced regulatory instrument, underpinned by the changing modalities of data transfer, which have remarkably affected its practical use. The annex outlines this progression: from 'Data Portability 1.0,' which involves one-time data downloads, to 'Data Portability 2.0,' focused on ad-hoc data transfers, to the most recent stage, 'Data Portability 3.0,' which emphasises real-time transfers for interoperability. The diversity of these approaches across and within jurisdictions, as well as by the private sector, underscores not only the complexity of implementing data portability but also indicates that a one-size-fits-all approach may not be suitable. This diversity, however, also provides a substantial opportunity for governments and regulators to engage in mutual learning and to pursue cross-jurisdictional and multi-disciplinary co-operation and co-ordination.

# Annex. Selection of data portability initiatives in the private and public sector

The Annex provides a taxonomy that can be used for mapping and analysing data portability initiatives in the private and public sectors.

## Data Portability 1.0: Ad hoc data downloads

### *The midata initiative of the United Kingdom*

Responsible entity: Government of the United Kingdom

Description: In 2011, the United Kingdom introduced its "midata" Data Portability Initiative (then "mydata") as part of a broader consumer empowerment strategy (BIS, 2011[36]). When launched, the government claimed it was "the first time globally there has been such a government-backed initiative to empower individuals with so much control over the use of their own data" (OECD, 2015[17]). The programme was initially rolled out in anticipation that release of transaction data would stimulate innovation and the expansion of third-party choice engines such as price comparison websites (BIS, 2012[37]).

- *Beneficiaries and data types*: midata seeks to give consumers access to the electronic information that companies hold about their transactions in a machine-readable and portable format. This "transaction data" includes, for instance, information collected about an individual's browsing history and purchases when logged in to a particular website (BIS, 2012[38]). However, purchases made with a "guest" account entailing no user registration, or information about complaints or other such communications with service providers, would not constitute individual transaction data.
- Addressees *and sectoral scope*: The midata initiative focuses on businesses in three sectors: energy supply; the mobile phone sector; and the financial sector (current accounts and credit cards).
- *Legal obligations*: Rather than legislating to introduce this data portability obligation, the government preferred to "take a power" pursuant to the Enterprise and Regulatory Reform Act 2013 (Goverment of the United Kingdom, 2013[39]). This allows the Secretary of State to introduce

regulations to make midata compulsory if the government is unsatisfied with progress in these sectors on a voluntary basis.[11]

- *Operational modality*: The midata initiative essentially allows consumers to download their current account transactions in a standardised format for easy comparison against accounts offered by other providers. Since then, the United Kingdom government has taken steps to implement midata in the energy sector (BEIS, 2018[40]). The United Kingdom has now adopted legislation mirroring the GDPR, including the right to data portability, and issued guidance to this end.

Read more: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/294798/bis-11-749-better-choices-better-deals-consumers-powering-growth.pdf

### *Private sector initiatives*

Responsible entity: Google

Description: The private sector, including online platforms, has been investing and innovating in the area of data portability. Since 2007, through its "Google Data Liberation Front" engineering team, Google has been developing data portability tools that allow its users to export a copy of their data from individual Google products. In 2011, with the launch of "Google Takeout", Google provides a single place for users to download a copy of their data and/or to send a copy of their data directly to another service (see next section on data portability 2.0 on the DTP) (Willard, 20 July 2018[41]).

Read more: https://opensource.googleblog.com/2018/07/introducing-data-transfer-project.html

Responsible entity: Facebook

Description: In 2010, as another example, Facebook began allowing its users to download their personal data (including profile information, photos, videos, wall posts, event information and a list of friends) (Tsotsis, 2010[42]).

Read more: https://techcrunch.com/2010/10/06/facebook-now-allows-you-to-download-your-information/

Responsible entity: Apple

Description: Recently, Apple announced that customers in certain jurisdictions can request to transfer a copy of their photos to other services, including Google Photos (Apple, 2022[43]).

[11] See Sections 89-91 of (Goverment of the United Kingdom, 2013[39]), dealing with "supply of consumer data".

Read more: https://support.apple.com/en-us/HT208514

## Data Portability 2.0: Ad hoc direct transfers of data to another data holder

### *Health Insurance Portability and Accountability Act (HIPPA) in the United States*

Responsible entity: United States Government

Description: HIPAA was introduced in the United States in 1996 to improve the flow and transfer of information related to health care. Among its major goals, HIPAA aimed to make it easier for patients to receive continuity in care if their health insurance coverage changed, such as when changing employer. In 2013, the HITECH Act significantly amended HIPAA to allow for better privacy protection in relation to electronic health records. More recently, the Department of Health and Human Services has proposed changes to the HIPAA privacy rule (which restricts the use and transfer of protected health information) to enable individuals to directly share their patient health information among covered entities (HSS, 2020[44]). This includes requiring electronic patient health information to be provided to individuals at no cost (HSS, 2020[44]). These changes are under consultation, but, if adopted, will enhance patients' data portability options.

- *Type of data*: The proposed amendments would allow for easier transfer for protected health information (PHI), being "individually identifiable health information maintained or transmitted by or on behalf of HIPAA covered entities (i.e. health care providers who conduct covered health care transactions electronically, health plans and health care clearinghouses)" (HSS, 2020[44]).
- *Beneficiary*: Currently, under HIPAA, patients can access and obtain a copy of their PHI and provide it to third parties. The proposed rules contemplate individuals' access right to direct copies of their electronic PHI to third parties. This right would require entities covered by HIPAA, including health care providers and health plans, "to submit an individual's access request to another health care provider and to receive back the requested electronic copies of the individual's PHI" in electronic format, thereby avoiding the need for the individual to be involved in the data porting.
- *Addressees and sectoral scope*: HIPAA is a sectoral regulation, as it only applies to certain health information and certain parties involved in providing health care and related services and thus covered by HIPAA.
- *Mandatory or voluntary*: The changes would create a mandatory data porting regime, where covered entities would be required to transfer data upon request by an individual.

- *Operational modality*: The proposed rules contemplate one-off data transfers between covered entities upon the user's request. While users are also able to request access and receive and deal with data themselves, the proposed regime allows for the user to provide the request to one entity and request the data be provided directly to another entity. The proposed rules would reduce the time in which covered entities are required to respond to an access request from 30 calendar days to 15 calendar days, with the opportunity of a further 15-day extension. The proposed rules also provide for circumstances in which the electronic PHI must be provided at no charge to the individual but allow for fees to be charged for direct transfer to another covered entity.

Read more: www.hhs.gov/sites/default/files/hhs-ocr-hipaa-nprm.pdf

### *The California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA)*

Responsible entity: State of California

Description: The 2018 CCPA, which took effect on 1 January 2020 and started to be enforced from 1 July 2020, incorporates a quasi-data portability obligation. In November 2020, Californians voted to approve the CPRA of 2020, and it came into effect on 1 January 2023. It complements the CCPA by updating and extending certain rules and stipulations to enhance the privacy rights of Californian consumers or households, including their rights to data portability.

- *Addressees and sectoral scope*: Pursuant to California Civil Code Section 1798.145(a)(6) and Section 1798.140(c)(1), all companies doing business in California have to comply with the CCPA. An exemption only applies if a company has an annual revenue of less than USD 25 million, collects data from fewer than 50 000 Californians annually and earns less than 50% of its income from its data commerce (Specht-Riemenschneider, 2021[45]). The CPRA has a slightly narrower scope: only those companies with annual buys, sells or shares of the personal information of 100 000 or more Californian consumers or households fall under the scope of the CPRA. Nevertheless, the CPRA has a more extended scope: it includes companies with annual revenues derived from sharing personal data in addition to selling it (IAPP, 2021[46]; Gross, 4 May 2021[47]).
- *Beneficiaries*: California Civil Code Section 1798.100 provides that a consumer shall have the right to request that a business that collects a consumer's personal information disclose to that consumer the categories and specific pieces of personal information the business has collected.
- *Type of data*: Until 1 January 2021, certain data, such as employee data and business communication data, were exempted from the scope of the CCPA (see Assembly Bills 25 and 1355). Assembly Bill 874 clarifies that "personal

information" includes information that reasonably identifies, relates to, describes or can reasonably be associated with a particular consumer or household, or could reasonably be associated, directly or indirectly, with a particular consumer or household. The CPRA introduces a new category of protected data: sensitive personal information (SPI), which can be compared to Article 9 of the EU GDPR. Relevant to data portability, and in particular to the transfer of data, is that the "CPRA imposes specific requirements and restrictions on SPI, giving users expanded rights to control businesses' use of their personal information" (Gross, 4 May 2021[47]) .

- *Operational modality*: Businesses that receive a verifiable consumer request from a consumer must "promptly take steps to disclose and deliver, free of charge to the consumer, the customer's personal information [...] by mail or electronically, and if provided electronically, the information shall be in a portable and, to the extent technically feasible, readily useable format that allows the consumer to transmit this information to another entity without hindrance" (California Civil Code Section 1798.100[d]). However, "a business may provide personal information to a consumer at any time but shall not be required to provide personal information to a consumer more than twice in a 12-month period." While the subject's transmission of the data to another controller was initially contemplated, there is no obligation under the CCPA for controller-to-controller data transfers. This is a major difference to the CPRA: "Now, under the CPRA, a consumer can request that a business transfer specific personal information to another entity 'to the extent technically feasible, in a structured, commonly used, machine-readable format'" (Gross, 4 May 2021[47]).

Read more:
https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

### *The "Right to Data Portability" (Art. 20) of the GDPR*

Responsible entity: Privacy enforcement authorities of the European Union member states

Description: The entry into force of the GDPR in May 2018 formalised the right of data portability within the European Union. Whereas the directive that preceded the GDPR gave data subjects the right to access their data,[12] the GDPR went a step further and granted data subjects a separate, distinct right of personal data portability. That right, in Article 20 of the GDPR, provides that the data

[12] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995), Art. 12.

subject "shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance…". The right applies where processing is based on consent or another legitimate category (Art 9[2]), is necessary for the performance of a contract, or when the processing is carried out by automated means (Art. 20[1]). Recital 68 explains that data controllers "be encouraged to develop interoperable formats that enable data portability" but that the right does not oblige controllers to adopt or maintain processing systems that are technically compatible.

- *Type of data*: The GDPR right only applies to personal data provided by the data subject with consent or under contract that is electronically processed. The (former) Article 29 Working Party indicates in accompanying guidance that the definition of personal data should encapsulate data volunteered by the individual or observed by virtue of their use of the service or device – but not personal data that is inferred or derived (OECD, 2015[17]).
- *Beneficiary*: For the purposes of the GDPR, "Data subject" only includes natural persons – corporations cannot take advantage of the right to data portability [Art. 4(1)]. The GDPR also provides that the right to data portability also includes "the right to have the personal data transmitted directly from one controller to another, where technically feasible."
- *Addressees and sectoral scope*: The right in the GDPR is "horizontal", in that it applies beyond specific sectors.
- *Mandatory or voluntary*: The GDPR provides a right to data portability; entities subject to the GDPR are obliged to respect it.
- *Operational modality*: The GDPR provides that the data controller provides "information on action taken" to the data subject "without undue delay" and in any event "within one month of receipt of the request". This one month period can be extended to a maximum of three months for complex cases, provided that the data subject has been informed about the reasons for such delay within one month of the original request" derived (OECD, 2015[17]).

Read more: https://eur-lex.europa.eu/eli/reg/2016/679/oj

### *The regulation for the free flow of non-personal data of the European Union*

Responsible entity: European Commission

Description: Shortly after the GDPR entered into force, the European Union introduced a regulation on a framework for the free flow of *non*-personal data in

the European Union.[13] The regulation provides that the European Commission shall encourage the development of Union-level codes of conduct regarding "best practices for facilitating the switching of service providers and the porting of data in a structured, commonly used and machine-readable format including open standard formats where required or requested by the service provider receiving the data" (Art. 6[1][a]). The Commission published practical guidance on the regulation in May 2019 with a particular focus on datasets comprised of personal and non-personal data.[14]

- *Type of data*: The regulation for the free flow of data specifically relates to non-personal data. Together, these regulations create a comprehensive framework for the free movement of all types of data (personal and non-personal) within the European Union.
- *Beneficiary*: The FFDRs contemplate data transfers between data holders to enable switching of service providers and the porting of data.
- *Addressees and sectoral scope*: Similar to the GDPR, the EU Free Flow of Non-Personal Data Regulation applies generally across all sectors.
- *Mandatory or voluntary*: The EU Free Flow of Non-Personal Data Regulation proposes a framework of self-regulation to be developed by businesses. It requires business to develop and implement "self-regulatory codes of conduct" to enable porting to data (Art. 6) subject to monitoring by the European Commission.
- *Operational modality*: The free flow of data regulation does not provide any guidance as to velocity and method but proposes that "the detailed information and operational requirements for data porting should be defined by market players through self-regulation, encouraged, facilitated and monitored by the Commission, in the form of Union codes of conduct which might include model contractual terms and conditions."

Read more: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018R1807

### Canada's proposed Consumer Privacy Protection Act

Responsible entity: Government of Canada

Description: Currently, Canadian law does not contain a general right to data portability. However, Canadians have the right to obtain access to their personal

[13] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (OJ L 303, 28.11.2018).

[14] Communication from the Commission to the European Parliament and the Council Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union (COM/2019/250 final).

information under both of Canada's federal privacy statutes. Under the Privacy Act, the federal public sector privacy law, Canadians have a right of access to information held by government institutions.[15] As of July 2022, this right of access was extended to any individual regardless of nationality or location. Under the Personal Information Protection and Electronic Documents Act (PIPEDA), the federal private sector privacy law, Canadians have a right of access to information held by private sector organisations covered by the law.

In May 2019, the Canadian government published "Canada's Digital Charter", which contains ten principles intended to guide the federal government's work on data and digital economy policy. One principle, "Transparency, Portability and Interoperability", promotes a right to "clear and manageable access to ... personal data and ... to share or transfer it without undue burden" (Government of Canada, 2019).[16] The Digital Charter Implementation Act, 2022, tabled in June 2022, proposes to enact a new Consumer Privacy Protection Act to replace Part 1 of the existing PIPEDA. The CPPA includes a right to data "mobility" that would be enabled through regulations.

Read more: https://ised-isde.canada.ca/site/innovation-better-canada/en/consumer-privacy-protection-act

### *Quebec Private Sector Act*

At the provincial level, Quebec has amended the Quebec Private Sector Act, including by inserting a data portability right similar to article 20 of the GDPR which will come into force in 2024.[17]

- *Type of data ported*: Once in force, the law relates to the porting of personal information only. Personal information held by the data holder would need to be provided "in the form of a written and intelligible transcript... [or for computerised personal information] in a structured, commonly used technological format".
- *Beneficiary and addressee*: The law allows for transfers of data to either the person who made the request and about whom the personal information relates. Further, the amendments would require that the business must, upon request, communicate the personal information to "any person or body authorised by law to collect such information".

[15] Privacy Act, Government of Canada, 1985, https://laws-lois.justice.gc.ca/ENG/ACTS/P-21/index.html.

[16] Government of Canada, *Canada's Digital Charter: Trust in a digital world*, 2021, https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html.

[17] National Assembly of Quebec, *Project de loi nº 64*, 2020, http://m.assnat.qc.ca/en/travaux-parlementaires/projets-loi/projet-loi-64-42-1.html.

- *Sectoral or general*: The law provides a general, cross-sector data portability right.
- *Ex ante or ex post*: The law is an ex ante regulatory model.
- *Mandatory or voluntary*: The law provides a mandatory model as part of broader privacy and data protection regulation – businesses must comply.
- *Operational modality*: The law does not provide details as to the velocity of the transfer or other details about the operational modality.

Read more: https://www.legisquebec.gouv.qc.ca/en/document/cs/p-39.1

### *The Regulation of Electronic Commerce and Efforts Regarding Competition in the Republic of Türkiye*

Responsible entity: Government of the Republic of Türkiye (hereafter "Türkiye")

Description: Türkiye enacted the Law No. 6563 on the Regulation of Electronic Commerce.

- *Addressees and sectoral scope:* Law No.6563 is a sectoral regulation as it concerns electronic commerce service providers.
- *Beneficiary*: Electronic commerce service providers are allowed to transfer their sales data from electronic commerce marketplaces without any charge. They are also able to provide free and effective access to this data and any processed data obtained from it. This approach seeks to fosters a dynamic environment that promotes collaboration and a shared understanding among all parties involved. The aim is to reduce the dependency of electronic commerce service providers on electronic commerce marketplaces, thereby reducing the lock-in effect, enabling multiple access and foster data portability.
- *Data type*: Non-personal data.
- *Mandatory or voluntary:* The data portability obligation is mandatory.
- *Operational modality*: Article 2/2 (b), introduces a legal obligation for electronic commerce service providers to offer technical means for the free transfer of data obtained through their sales, as well as free and effective access to both the original and processed data. This obligation concerns data portability.

Read more: https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6563.pdf

### ***Brazil's General Data Protection Law –*** *Lei Geral de Proteção de Dados Pessoais*

Responsibly entity: Government of Brazil

Description: Brazil enacted a General Data Protection Law in 2018 (LGPD, being the Portuguese acronym for *Lei Geral de Proteção de Dados Pessoais*).

- *Beneficiary*: One of its greatest innovations is the broad right to data portability, which allows consumers to request an entire copy of their data in an interoperable format, which they can then take to competitors. According to Art. 18(2) LGPD, the data subject has a right to access his or her data, which corresponds to a right to be informed about such data. Art. 18(5) LGPD grants a right to data portability, which is imported from Article 20 of the GDPR.
- *Addressees and sectoral scope*: The LGPD is a cross-sectoral privacy protection regulation and thus applies across sectors.
- *Data type*: Art. 18(5) LGPD applies to both data provided by the data subject and observed data.
- *Operational modality*: Art. 18(5) LGPD gives the right to "portability of the data to another service or product provider, by means of an express request and subject to commercial and industrial secrecy, pursuant to the regulation of the controlling agency". One of the major differences to Art. 20 of the GDPR is that the LGPD does not establish a major threshold that requires the specific consent of the data subject. For the LGPD, the request to data portability does not have to be based on an existing contractual relation to request this right from a data controller, as long as this is technically feasible. Further, the LGPD does not establish an exemption to exercise this right when the processing of personal data is necessary to perform a task carried out in the public interest or in the exercise of an official authority vested in the controller.

Read more: https://www.gov.br/cidadania/pt-br/acesso-a-informacao/lgpd

### *Singapore's data protection obligation*

Responsible entity: Singapore's Personal Data Protection Commission ("PDPC")

Description: The PDPC introduced a new data portability obligation in the Personal Data Protection Act ("PDPA") in 2020. This obligation will only come into effect with the issuance of forthcoming regulations.

- *Addressees and sectoral scope*: The data portability obligation applies to porting organisations (i.e., data controllers) that are prescribed under regulations. At the time of the data porting request, the porting organisation must have an ongoing relationship with the data subject concerned.
- *Data type*: The data portability obligation applies to personal data: (a) in the possession or under the control of the porting organisation; (b) that is, or belongs to a class of personal data that is prescribed under regulations; (c) that is held in electronic form on the date the porting organisation receives a data porting request; and (d) that was collected or created by the porting organisation within a prescribed period before the date the porting organisation receives the data porting request. Certain types of personal

data will be excluded from the data portability obligation, including opinion data kept solely for an evaluative purpose, and derived personal data.

- *Operational modality*: Only natural persons can avail themselves of the data portability obligation. Porting organisations are not required to transmit data to the data subjects themselves and receiving organisations must have a presence in Singapore. In the future, the PDPC may extend data portability to like-minded jurisdictions with comparable protection and reciprocal arrangements.
- *Mandatory or voluntary*: The data portability obligation is mandatory, subject to certain conditions being fulfilled. The PDPC has the power to review an organisation's: (a) refusal to port data; (b) failure to port data within a reasonable time; and (c) fees for porting data.

Read more: https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act

### *Selected private sector initiatives*

#### *The Data Transfer Project (DTP) and the Data Transfer Initiative (DTI)*

Responsible entity: The Data Transfer Initiative (DTI)

Description:

In 2017, Google, Meta, Microsoft, Apple and Twitter (now X) joined forces to establish the DTP (DTP, n.d.[48]; Github, n.d.[49]; Microsoft et al., 2019[50]). The project was born from the recognition that data portability was not only a regulatory requirement but also an opportunity to improve user experience. By working together, these companies sought to build a shared set of tools for direct data transfers. This collaboration was intended to relieve users from the burdensome task of managing their data transfers, ensuring that their data portability needs were met more efficiently.

DTP was launched in 2018 as an open-source, service-to-service data portability platform so that "all individuals across the web could easily move their data between online service providers whenever they want". The DTP was motivated by the recognition that "portability and interoperability are central to innovation". In particular, the DTP aims to enhance the data portability ecosystem by reducing the infrastructure burden on both providers as well as users, with a goal to increase the number of services that provide portability.

The DTP uses services' existing APIs and authorisation mechanisms to access data. It then uses service-specific adapters to transfer those data into a common format, and then back into the new service's API. In particular, the terms of each organisation's API determine the data types that may be

transferred between the providers. Overall, this includes data stored in a specific user's account. However, depending on the organisations involved, it may not be necessarily limited to that specific type of data. Use cases for the DTP include porting data directly between services such as for "i) trying out a new service; ii) leaving a service; iii) backing up your data".

To advance the work of the DTP, the Data Transfer Initiative (DTI) was established as a nonprofit organisation with the support of three of the five DTP's contributors — Apple, Meta, and Google. Today, DTP is a project within DTI and no longer a standalone initiative and DTI works in collaboration with its partner companies with the mission of "empowering technology users by enabling them to transfer their data from one service to another"[18] thanks the development and deployment of open source data transfer tools. Since evolving into the independent DTI organisation, the work has grown to include projects on trust building, mapping the portability landscape, collaborating with a broader set of stakeholders, and serving in various capacities as an expert resource to regulators.

Read more: https://dtinit.org/

### *MyData Global*

Responsible entity: MyData Global

Description: MyData Global is a non-profit organisation with over 90 organisational members and over 600 individual members from over 40 countries on 6 continents that aims "to empower individuals by improving their right to self-determination regarding their personal data" (MyData Global, n.d.[51]). It promotes a model in which a "human-centric paradigm is aimed at a fair, sustainable and prosperous digital society, where the sharing of personal data is based on trust as well as balanced and fair relationship between individuals and organisations". The "Declaration of MyData Principles" includes a set of voluntary principles for data portability. Two points can be highlighted here:

- *Type of data*: The primary goal of MyData Global is to empower individuals to use their personal data to their own ends, and to securely share them under their own terms. Therefore, MyData Global focuses on "all personal data regardless of the legal basis (contract, consent, legitimate interest, etc.) of data collection, with possible exceptions for enriched data".
- *Operational modality*: MyData Global aims to "empower individuals to effectively port their personal data, both by downloading it to their personal devices, and by transmitting it to other services [...] securely and easily, in a structured, commonly used and machine-readable format".

[18] See https://dtinit.org/

Read more: https://mydata.org/about/organisation/

## Data Portability 3.0: Real-time continuous data transfers enabling interoperability

### *Early sectoral developments in the United States: From data portability 1.0 to 3.0*

Responsible entity: United States Government

Description: The Obama Administration launched a series of "My Data" initiatives from 2010 to give consumers more control over their personal health, energy,[19] finance or education data.[20] These started as data portability 1.0 initiatives as they were limited to enabling users to access and download or print their personal data with a "click of a simple button". One such initiative was "Blue Button", which was launched in the context of the health care system.

- *Beneficiaries and the type of data*: The objective of "Blue Button" was to allow patients to better access their medical records on line so they can track their health, correct errors and transfer information between health care providers.[21] Americans can access their health data for free in a comprehensible form, in part due to financial incentives available from the federal government to encourage providers to adopt electronic health records.[22]
- *Addressees and sectoral scope*: "Blue Button" supported the coming together of public and private sector organisations on the health care system in the United States, including federal agencies (the Departments

[19] Another My Data initiative, "Green Button", allows utility customers to download their energy usage information in a consumer- and machine-friendly format. Launched in January 2012, the initiative is designed to promote competition and innovation among industry players. Over 50 utilities and electricity providers have signed onto the initiative (with more having pledged to join in time), allowing some 60 million homes and businesses to be able to download their usage data (see www.energy.gov/data/green-button). Both the Blue Button and Green Button initiatives focus more on providing data subjects with the right to access their data, rather than on their ability to request a data controller to share it with another controller. Both initiatives are voluntary for organisations to join, which is a significant difference from enforceable regulations like the GDPR.

[20] See further, The White House, President Barack Obama, *My Data: Empowering All Americans with Personal Data Access* (15 March 2016), https://obamawhitehouse.archives.gov/blog/2016/03/15/my-data-empowering-all-americans-personal-data-access (accessed 3 October 2019).

[21] See further Health IT, *Blue Button* (8 April 2019), https://www.healthit.gov/topic/health-it-initiatives/blue-button (accessed 3 October 2019).

[22] https://www.healthit.gov/topic/health-it-initiatives/blue-button/frequently-asked-questions and https://www.healthit.gov/topic/health-it-initiatives/blue-button/logo-and-usage

of Defense, Health and Human Services, and Veterans Affairs). Over roughly five years, approximately 16 000 health care organisations and providers (a majority of those in the United States) signed up to the voluntary Blue Button programme.[23]

- *Operational modality*: Blue Button was initially implemented to give veterans the ability to download or print their personal health records with a click of "a simple blue button". The Department of Veterans Affairs and the Center for Medicare and Medicaid Services under the Department of Health and Human Services were the first to offer Blue Button downloads to veterans and to Medicare beneficiaries. Two years later, in 2012, the Automate Blue Button Initiative (which provided the basis for Blue Button+) was introduced to standardise data formats and automate data transfer mechanism to enable data transfers between health data-holding organisations, patients and authorised third parties, effectively making Blue Button a data portability 2.0 initiative (Graham-Jones and Panchadsaram, 5 February 2013[52]). In 2018, the Blue Button 2.0 Implementation Guide was introduced. It defines an API standard for the transfer of "a variety of information about a beneficiary's health, including type of Medicare coverage, drug prescriptions, primary care treatment and cost" (Center for Medicare and Medicaid Services, 2018[53]). This new standard enables developers to register a beneficiary-facing application, a beneficiary to grant an application access to four years of their data and effectively makes Blue Button 2.0 a data portability 3.0 as defined in this note.

Read more: https://obamawhitehouse.archives.gov/blog/2016/03/15/my-data-empowering-all-americans-personal-data-access

### *Japan's Banking Act*

Responsible entity: Financial Services Agency of Japan

Description: An amendment of the Banking Act in 2017 in Japan, which takes a voluntary approach, requires that banks disclose their terms and conditions to Electronic Payment Service Providers (EPSPs) and do not discriminate against certain EPSPs. The Act also requires that third-party service providers that receive customers' banking data should have relevant measures to protect such sensitive data. On the other hand, the amendment requires EPSPs to register with the regulatory authority and to make only relevant use and management of depositors' banking information. It also sets up an amicable dispute resolution

[23] See further, The White House, President Barack Obama, *My Data: Empowering All Americans with Personal Data Access* (15 March 2016), https://obamawhitehouse.archives.gov/blog/2016/03/15/my-data-empowering-all-americans-personal-data-access (accessed 3 October 2019).

system for disputes between EPSPs and their customers. A co-regulatory approach was used to develop technical standards for the open banking APIs and the model contract between a bank and EPSPs.

- *Types of data ported*: At the request of users, the EPSPs transmit depositors' transactions or account inquiries to their banks through a digital platform.
- *Beneficiary and addressee*: Considering the accelerated trend overseas that innovative services emerged from the combination of financial service and digital technologies, the amendment of the Banking Act in 2017 was introduced to create a regulatory environment where financial institutions can collaborate with fintech firms for innovation, while ensuring consumer protection.
- *Sectoral scope*: The amendment applies to depositary financial institutions (banks) and fintech firms that need to be registered to the Japanese financial authorities as EPSPs.
- *Ex ante or ex post*: The regulation requires ex ante registrations and organisational and security measures for EPSPs and banks, while the authority has the regulatory power to ask for a report, impose remedial measures etc.
- *Mandatory or voluntary*: The amendment does not require banks to use the open APIs. Despite its voluntary approach, 72% of banks (100% for Japan domiciled banks) accepted the implementation.
- *Operational modality*: Despite the voluntary nature of the initiative, at the time of September 2019, 95% banks (100% for Japan domiciled banks) accepted the implementation of open API.[24]

Read more: https://www.fsa.go.jp/singi/kessai_kanmin/siryou/20191223/05.pdf

### *Payment Service Directive for Payment Businesses in the European Union (PSD2)*

Responsible entity: European Commission

Description: PSD2, established in November 2015, sets out the rules concerning strict security requirements for electronic payments and the protection of consumers' financial data, guaranteeing safe authentication and reducing the risk of fraud; the transparency of conditions and information requirements for payment services; and the rights and obligations of users and providers of payment services. It also requires payment service providers, including banks, to allow a third party (payment initiation service providers or account information

[24] https://www.fsa.go.jp/singi/kessai_kanmin/siryou/20191223/05.pdf

service providers) to access their customers' account data and data used for payment transactions subject to the explicit consent by the customers.[25] [26] Because of the nature of the EU directive, implementation depends on member countries.

- *Types of data ported*: PSD2 allows third parties to access payment service providers' account data and the data used for payment transactions. Beyond this regulatory requirement, the directive triggered the commercial-based portability via APIs of other kinds of data such as identity authentication, credit scoring, trading of foreign exchange and data on loyalty programmes.
- *Beneficiary and addressee*: PSD2 aims to put in place comprehensive rules for payments services to open up payment markets to new entrants leading to more competition, greater choices and better prices for customers.
- *Sectoral scope*: The directive applies to payment service providers.
- *Ex ante or ex post*: Requirements of the directive for data access and transfer, as well as other obligations, are ex ante, while the directive and related legal instruments require competent authorities' ex post enforcement power over payment service providers.
- *Mandatory or voluntary*: Third-party access to account data and the data used for payment transaction is mandatory.
- *Operational modality*: Real-time data transfer is enabled via open APIs.

Read more: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_19_5555

### *The Digital Markets Act of the European Union*

Responsible entity: European Commission

Description: The Digital Markets Act (DMA) is an EU regulation aimed at fostering fair and contestable digital markets. Established in September 2022, it targets large digital platforms, known as "gatekeepers," that have a significant market presence in the EU. The DMA aims to prevent these companies from abusing their market power and to allow new entrants to compete effectively. It covers a wide range of obligations, including data portability, interoperability, and prohibitions on certain business practices like combining data from different services owned by the same company.

In particular, the DMA provides for an obligation on designated gatekeepers to ensure effective portability of data (see Article 6(9) of the DMA). Recital 59 of the DMA gives further details on the rationale for this obligation and on how it should

[25] https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32015L2366

[26] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L2366

be carried out to be effective. It also specifies that this obligation complements the right to data portability under the GDPR (European Commission, 2022[16]).

- *Beneficiary*: The DMA aims to benefit consumers and businesses by ensuring a higher degree of competition in European digital markets. More specifically in terms of data portability, Art. 6 (9-11) DMA differentiates between three types of beneficiaries: (i) "end users" (individuals using core platform services) benefit from the ability to access and port data they have provided or generated through their activities on core platform services (Art. 6(9) DMA); (ii) "business users" (business entities using core platform services) gain access to both aggregated and non-aggregated data, including personal data, that is generated in the context of their use of these services (Art. 6(10) DMA); and (iii) "third-party online search engines" are granted access to ranking, query, click, and view data generated by end users on online search engines.
- *Type of data*: The type of data covered by Art. 6(9) DMA slightly varies depending on the beneficiary. For end and business users it includes data provided by the users or generated through their activities on the core platform service. In the case of business users, more specifically this can also include "continuous and real-time access to, and use of, aggregated and non-aggregated data, including personal data" that is provided for or generated in the context of their use of the core platform. (Art. 6(10) DMA). In the case of "third-party online search engines" (Art. 6(11) DMA), they are granted access to ranking, query, click, and view data generated by end users on online search engines.
- *Addressees and sectoral scope*: Similar to the GDPR, the DMA applies generally across all sectors. However, it specifically targets large digital platforms operating in the EU (gatekeepers as defined in Art 3 DMA). As of September 2023, the European Commission has identified 22 services provided by six companies - Alphabet, Amazon, Apple, ByteDance, Meta, and Microsoft - as "gatekeepers".[27] These services range from operating systems, number-independent interpersonal communication services to online social networking services and online intermediation services.
- *Mandatory or voluntary*: Art. 6(9-11) DMA provides mandatory obligation to all businesses that are designated as gatekeepers by the European Commission.
- *Operational modality*: The operational modality slightly varies depending on the beneficiary but involves in the case of end and business users the provision of "continuous and real-time access" to data free of charge. For end users more specifically Art. 6(9) DMA also mandates that "tools to facilitate the effective exercise of such data portability" be provided as

[27] https://digital-markets-act-cases.ec.europa.eu/gatekeepers

well. In the case of business users, Art. 6(10) DMA requires that "effective, high-quality, continuous and real-time access" be provided. Gatekeepers are also required to provide access to personal data to a business user but only when it is directly related to the end user's interaction with products or services offered by the business user on the platform, and the end user has explicitly consented to share this data. In contrast to end and business users, data access to third-party online search engines should be provided "on fair, reasonable and non-discriminatory terms". Where personal data is involved that data should be anonymised before access is granted.

Read more: https://digital-markets-act.ec.europa.eu/index_en

### *The Data Act of the European Union*

Responsible entity: European Commission

Description: The Data Act is an EU regulation aimed at harmonizing rules on fair access to and use of data. The Act focuses on increasing legal certainty for consumers and businesses to access data generated by products or related services they own, rent, or lease. The Act aims to unlock the potential of data by providing opportunities for its reuse and by removing barriers to the development of the European data economy. It covers various obligations, including penalties for infringements and administrative fines. It addresses key issues such as lack of clarity on data usage, barriers to data sharing, and limited ability to combine data from different sectors. The Act aims to remove these barriers while preserving incentives for data generation. It covers various obligations, including penalties for infringements and administrative fines.

- *Type of data*: The Act covers data generated by connected products and related services owned, rented, or leased by consumers and businesses. It also includes data necessary for tasks carried out in the public interest. The type of data covered by the Data Act varies depending on the context.
- *Beneficiary*: The Data Act aims to benefit both public and private sectors by providing a framework for data sharing and usage. It aims to benefit consumers by increasing transparency on what data will be accessible and how to access them. Businesses are expected to gain from increased legal certainty and the potential for data-driven innovation.
- *Addressees and sectoral scope*: The Data Act applies generally across all sectors but has specific implications for manufacturers and designers of products that generate data, as well as for EU Member States and their public bodies in respect to public sector data.
- *Territorial Scope*: The EU Data Act applies to manufacturers of connected products placed on the market in the EU and providers of related services, irrespective of the place of establishment of those manufacturers and providers.

- *Mandatory or voluntary*: The Act provides for mandatory obligations, including penalties for infringements and administrative fines for violations of specific chapters of the regulation.
- *Operational modality*: The Data Act aims to facilitate easier data transfer between various service providers. While the Act does not explicitly mandate real-time data access in the available information, it does emphasise the need for easier and more efficient data portability. Where data is necessary to address a public emergency, the Act mandates that such data be provided to the government for free. In other situations, the data holder may request compensation.

Read more: https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_1114

### *Interoperability in Estonia – X-Road*

Responsible entity: Estonian Government

Description: E-government initiatives that aim to create data exchange platforms have also facilitated data portability. For example, in Estonia, the government has embarked on a large-scale "e-Estonia" initiative to integrate different organisational and information systems.[28] Underpinning that initiative is "X-Road" (or "X-tee"), which is a data exchange layer technology that facilitates secure transfer of data between different information systems.

- *Addressees and sectoral scope*: Organisations can join X-tee if they clear certain security thresholds and enter into an agreement with a suitable X-tee service provider.
- *Operational modality*: Joining X-tee makes an organisation part of an interoperable ecosystem with the technical ability to share data among other participants per the agreement.[29] International standards and protocols are used as much as possible under X-tee to ensure availability and standardisation.

Read more: https://e-estonia.com/solutions/interoperability-services/x-road/

### *The Australian Consumer Data Right*

Responsible Entity: The Australian Treasury, Australian Competition and Consumer Commission (ACCC) and Office of the Australian Information Commissioner (OAIC)

Description: In August 2019, the Australian Parliament passed legislation introducing a Consumer Data Right (CDR), enabling consumers in designated

[28] https://e-estonia.com/solutions/interoperability-services/x-road/

[29] https://www.ria.ee/en/state-information-system/x-tee.html

sectors of the Australian economy (a "CDR consumer") to share their data with accredited businesses.[30] In this way, the regime encourages innovation from providers seeking new clients. However, in the OECD Expert Consultation in April 2020, Andrew Stevens (Chair of Australia's CDR's Data Standards Body) stressed the importance of establishing rules and standards to facilitate interoperability (Australia's data standards were developed as open source on GitHub, with over 700 contributors from around the world), and of implementing cross-sector data portability initiatives to further innovation.

- *Types of data ported*: Data holders must share "CDR data", which includes information relating to the CDR consumer (consumer data) and information that is about goods or services in a particular sector that does not relate to any identifiable consumer (product reference data). In the banking sector, CDR data includes information about a consumer's accounts and products with a bank, such as transaction details, payee details and account balances. In the energy sector, CDR data includes information about a consumer's accounts and electricity consumption. These data sets often include personal data.
- *Beneficiaries and addressees*: The legislation defines three categories of actors: i) data holders, who are the original holders of CDR data; ii) CDR consumers, who can be either individuals or businesses that hold rights to access data held by data holders and direct that data be shared with an accredited person; and iii) ADRs, who are individuals or businesses that meet a series of criteria for accreditation to be further specified in the consumer data rules. The CDR consumer, or the ADR with the CDR consumer's consent, can request a data transfer.
- *Sectoral scope*: The CDR is sector-specific, however key datasets from multiple sectors can be considered concurrently, as is anticipated to occur for 'open finance'. The legislation confers an ongoing power to the relevant Minister to designate sectors of the economy that are subject to the CDR [s 56AC]. CDR data sharing has commenced in the banking and energy sectors (in the energy sector, sharing of Product Reference Data commenced 1 October 2022 and consumer data on 15 November 2022). The telecommunications sector has been designated as the third sector and CDR data sharing is anticipated to extend to 'open finance' which includes non-bank lending, merchant acquiring services, superannuation, and general insurance.
- *Ex ante or ex post*: The CDR is ex ante regulation.
- *Voluntary or mandatory*: Data holders must share consumer data and product reference data for designated sectors. However, the CDR is entirely optional to the consumer, and there is no value generated by the regime

[30] *Treasury Laws Amendment (Consumer Data Right) Act 2019* (Cth).

until or unless the consumer accepts a superior offer from a banking services provider.

- *Velocity and operational modality*: The data standards, empowered by the CDR Rules specify the time frames in which specific data must be provided in response to a request. Failing to disclose requested data without a valid reason (as set out in the CDR Rules) may give rise to a civil penalty order. The CDR is flexible as to the period for which data can be ported: consumers can authorise either a one-off transfer, or multiple or continuous transfers over 12 months but can withdraw their consent at any time. The CDR Rules and data standards provide detailed requirements as to what information must be provided and how data must be structured when provided via API.

Read more: https://www.cdr.gov.au/

### *Türkiye's efforts in open banking*

Responsible Entity: Central Bank of the Republic of Türkiye (CBRT)

Description: In 2019, Law No. 6493 (Article 12, Paragraph 1) on *Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions* added two basic services under the CBRT's authority and responsibility, which are referred to as Payment Services Data Sharing Services and defined to be in line with the EU's PSD2. The two services include:

- *Payment Order Initiation Service*: Payment order initiation service provided at the request of a payment service user in relation to a payment account held with another payment service provider.
- *Account Information Service*: The service of providing consolidated information on online platforms regarding one or more payment accounts of the payment service user with payment service providers, provided that the consent of the payment service user is obtained.

In 2022, these services were complemented by open banking services launched by the CBRT in the payments area as essential component of the digital economy roadmap of the monetary policy and liraization strategy for 2023. As consequence, participating banks can start providing services through the 'Open Banking Gateway' (GEÇİT) infrastructure, developed by the Interbank Card Center (ICC) that allows third parties to provide Open Banking transactions.

Read more: TCMB – Open Banking Press Release (2022-48); 1. LAW (tcmb.gov.tr)

## *Private sector initiatives*

### *Solid – towards a decentralised data web*

Responsible entity: Solid

Description: In the private sector, Sir Tim Berners-Lee (inventor of the World Wide Web) launched a mid-course correction to the Web (named Solid) with an aim to bring user data securely together into a decentralised data store (Solid, n.d.[54]). Solid provides users an opportunity to bring data together into a decentralised data store, called a "Pod". The Pod acts like a personal web server for the user's data, with numerous benefits:

- Any kind of data may be stored in the Pod and the user can control that data. In particular, the user may determine who or what can access the data at a granular level using Solid's authentication and authorisation systems.
- The data are stored and accessed using open, standard and interoperable data formats and protocols.
- Any kind of information may be shared in the Pod.
- Users may share the slices of their data with people, applications and organisations that they select, and may revoke the access any time.

Since everything is interoperable, various applications may read and write the same data, instead of creating new data silos that may make the data difficult to use in their entirety. Overall, users have more opportunities with their data because their selected applications may access a wider and more diverse set of information. The technology of Solid has already been applied in a number of cases with the aim for users to control their data and extract value from it.

Read more: https://solidproject.org/about

# Bibliography


ACCC (2020), *Digital Advertising Services Inquiry Interim Report*, Australian Competition and Consumer Commission, Canberra, https://www.accc.gov.au/system/files/Digital%20Advertising%20Services%20Inquiry%20-%20Interim%20report.pdf. [3]

Apple (2022), "Transfer a Copy of Your iCloud Photos Collection to Another Service", webpage, https://support.apple.com/en-us/HT208514 (accessed on xxx xx 2021). [43]

Australian Government (2022), *Consumer Data Right - Strategic Assessment Outcomes*, https://treasury.gov.au/publication/p2022-242997. [10]

BEIS (2018), *Implementing Midata in the Domestic Energy Sector: Government Response to the Call for Evidence*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/729908/midata-energy-sector-government-response.pdf. [40]

BEUC (2022), *GIVING CONSUMERS CONTROL OF THEIR DATA: BEUC position paper on the Data Act proposal*, BEUC, https://www.beuc.eu/sites/default/files/publications/BEUC-X-2022-103%20_BEUC_Position_paper_on_the_Data_Act_proposal.pdf (accessed on 28 March 2024). [30]

BIS (2012), *midata: Government response to 2012 consultation*, Department for Business Innovation & Skills, Government of the United Kingdom, http://www.gov.uk/government/uploads/system/uploads/attachment_data/file/34700/12-1283-midata-government-response-to-2012-consultation.pdf. [38]

BIS (2012), *midata: Impact Assessment for midata*, Department for Business Innovation & Skills, Government of the United Kingdom, http://www.gov.uk/government/uploads/system/uploads/attachment_data/file/32689/12-944-midata-impact-assessment.pdf. [37]

BIS (2011), *Better Choices: Better Deals – Consumers Powering Growth*, Department for Business Innovation & Skills, Government of the United Kingdom. [36]

Center for Medicare and Medicaid Services (2018), *Blue Button 2.0 Implementation Guide*, website, https://bluebutton.cms.gov/assets/ig/index.html (accessed on 1 March 2021). [53]

CMA (2020), *Online Platforms and Digital Adverstising Market Study*, Competition & Markets Authority, London, https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study. [2]

CNIL (2020), *La réutilisation des données publiquement accessibles en ligne à des fins de démarchage commercial*, CNIL, https://www.cnil.fr/fr/la-reutilisation-des-donnees-publiquement-accessibles-en-ligne-des-fins-de-demarchage-commercial (accessed on 20 September 2023). [57]

de la Mano, M. and J. Padilla (2018), "Big tech banking", *Journal of Competition Law & Economics*, Vol. 14/4, pp. 494-526, https://doi.org/10.1093/joclec/nhz003. [12]

Di Porto, F. and G. Ghidini (2020), ""Access Your Data, You Access Mine" – Requiring Data Reciprocity in Payment Services", *International Review of Intellectual Property and Competition Law*, Vol. 307/51. [13]

DTP (n.d.), *Data Transfer Project*, website, https://datatransferproject.dev/ (accessed on 1 March 2021). [48]

European Commission (2022), "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data", *Data Act*, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0068. [16]

European Commission (2020), *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation*, SWD(2020) 115 final, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0264&from=EN#footnote44 (accessed on 28 September 2023). [33]

European Union (2018), *Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union*, European Union, Brussels, http://data.europa.eu/eli/reg/2018/1807/oj. [15]

FTC (2014), *FTC puts conditions on CoreLogic, Inc.'s proposed acquisition of DataQuick Information Systems*, 24 March, Press Release, Federal Trade Commission, Washington DC, http://www.ftc.gov/news-events/press-releases/2014/03/ftc-puts-conditions-corelogic-incs-proposed-acquisition-dataquick. [5]

Github (n.d.), *google/data-transfer-project*, website, https://github.com/google/data-transfer-project (accessed on 1 March 2021). [49]

Goverment of the United Kingdom (2013), *Enterprise and Regulatory Reform Act 2013*, legislation.goverment.uk, http://www.legislation.gov.uk/ukpga/2013/24/contents. [39]

Graham-Jones, P. and R. Panchadsaram (5 February 2013), "Introducing Blue Button+", Health IT Buzz, Consumer Engagement Blog, http://www.healthit.gov/buzz-blog/consumer/introducing-blue-button. [52]

Gross, C. (4 May 2021), "CPRA vs. CCPA: What's the difference? 6 key changes to understand", A-Lign Blog, https://a-lign.com/cpra-vs-ccpa/ (accessed on 28 June 2021). [47]

HDMC (2020), *Interim Report on Evaluation of Competition in the Digital Advertising Market Summary*, Headquarters for Digital Market Competition of the Japanese Cabinet Office, Tokyo, https://www.kantei.go.jp/jp/singi/digitalmarket/pdf_e/documents_200616-1.pdf. [8]

HDMC (2020), *Report on Medium-Term Vision on Competition in the Digital Market: Summary*, Headquarters for Digital Market Competition of the Japanese Cabinet Office, Tokyo, https://www.kantei.go.jp/jp/singi/digitalmarket/pdf_e/documents_200616-2.pdf. [4]

HSS (2020), *Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement*, 45 CFR Parts 160 and 164, Department of Health and Human Services, Office for Civil Rights, Washington, DC, http://www.hhs.gov/sites/default/files/hhs-ocr-hipaa-nprm.pdf. [44]

IAPP (2022), *Data portability in the EU: An obscure data subject right*, https://iapp.org/news/a/data-portability-in-the-eu-an-obscure-data-subject-right/ (accessed on 28 September 2023). [27]

IAPP (2021), "The California Privacy Rights Act of 2020", webpage, https://iapp.org/resources/article/the-california-privacy-rights-act-of-2020/ (accessed on 21 June 2021). [46]

JFTC, METI, MIC (2019), *Options for rulemaking to address the rise of platform businesses*, 21 May, Joint Press Release, ministroy fo Economy Trade and Industry, Japan Fair Trade Commission, Ministry of Internal Affairs and Communications, https://www.meti.go.jp/english/press/2019/0521_006.html. [7]

Kerber, W. (2021), "From (horizontal and sectoral) data access solutions towards data governance systems", *Joint Discussion Paper Series in Economics*, No. 40-2020, Universities of Aachen · Gießen · Göttingen Kassel · Marburg · Siegen. [14]

Kranz, J. et al. (2023), "Data Portability", *Business and Information Systems Engineering*, pp. 1-11, https://doi.org/10.1007/S12599-023-00815-W/TABLES/3. [28]

Luzsa, R. et al. (2022), *Datenportabilität zwischen Online-Diensten: Nutzeranforderungen und Gestaltungsempfehlungen. Ergebnisse einer Bevölkerungsrepräsentativen* [34]

*Befragung*, bidt – Bayerisches Forschungsinstitut für Digitale Transformation, https://doi.org/10.35067/bv16-2z31.

Microsoft et al. (2019), *Data Transfer Project*, https://datatransferproject.dev/. [50]

MyData Global (n.d.), "About", webage, https://mydata.org/about/organisation/ (accessed on 12 March 2021). [51]

OAIC (2021), "CDR Privacy Safeguard Guidelines", webpage, http://www.oaic.gov.au/consumer-data-right/cdr-privacy-safeguard-guidelines/ (accessed on xx xx 2021). [22]

OAIC (n.d.), "CDR participants", webpage, http://www.oaic.gov.au/consumer-data-right/cdr-participants/ (accessed on 29 June 2021). [23]

OECD (2023), "Consumer vulnerability in the digital age", in OECD Publishing, P. (ed.), *OECD Digital Economy Papers*, https://doi.org/10.1787/4d013cc5-en. [31]

OECD (2023), "Data portability in open banking: Privacy and other cross-cutting issues", *OECD Digital Economy Papers*, No. 348, OECD Publishing, Paris, https://doi.org/10.1787/6c872949-en. [24]

OECD (2023), "Emerging privacy-enhancing technologies: Current regulatory and policy approaches", *OECD Digital Economy Papers*, No. 351, OECD Publishing, Paris, https://doi.org/10.1787/bf121be4-en. [32]

OECD (2023), "Shifting from open banking to open finance: Results from the 2022 OECD survey on data sharing frameworks", *OECD Business and Finance Policy Papers*, No. 24, OECD Publishing, Paris, https://doi.org/10.1787/9f881c0c-en. [35]

OECD (2022), "Data shaping firms and markets", in *OECD Digital Economy Papers*, OECD Publishing, Paris, https://doi.org/10.1787/7b1a2d70-en. [25]

OECD (2021), "Data portability, interoperability and digital platform competition", *OECD Competition Committee Discussion Paper*, http://www.oecd.org/daf/competition/data-portability-interoperability-and-digital-platform-competition-2021.pdf. [21]

OECD (2021), *Mapping data portability initiatives, opportunities and challenges*, https://www.oecd.org/publications/mapping-data-portability-initiatives-opportunities-and-challenges-a6edfab2-en.htm. [1]

OECD (2021), *Mapping Data Portability Initiatives, Opportunities and Challenges*, https://www.oecd.org/publications/mapping-data-portability-initiatives-opportunities-and-challenges-a6edfab2-en.htm. [9]

OECD (2021), *Recommendation of the Council on Enhancing Access to and Sharing of Data*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0463 (accessed on 6 March 2023). [19]

OECD (2020), *Consumer data and competition: A new balancing act for online markets?*, Directorate for Financial and Enterprise Affairs, Competition Committee, OECD, Paris, https://one.oecd.org/document/DAF/COMP(2020)18/FINAL/en/pdf. [6]

OECD (2019), *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, OECD Publishing, Paris, https://dx.doi.org/10.1787/276aaca8-en. [18]

OECD (2015), *Data-Driven Innovation: Big Data for Growth and Well-Being*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264229358-en. [17]

OECD (2015), *Drawing value from data as an infrastructure*, OECD Publishing, Paris, https://doi.org/10.1787/9789264229358-8-en. [59]

OECD (2014), *Summary of OECD Expert Roundtable Discussion on "Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking"*, Directorate for Science, Technology and Industry, OECD, Paris, http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=dsti/iccp/reg%282014%293&doclanguage=en. [20]

OECD (2013), *The OECD Privacy Framework*, https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. [58]

Solid (n.d.), "About Solid", webpage, https://solidproject.org/about (accessed on xx xx 2021). [54]

Specht-Riemenschneider, L. (2021), "Data Access Rights - A Comparative Perspective", in *Data Access as a Means to Promote Consumer Interests and Public*. [45]

Streel, A., J. Kramer and P. Senellart (2020), *Making data portability more effective for the digital economy*, https://cerre.eu/publications/report-making-data-portability-more-effective-digital-economy/. [11]

Syrmoudis, E. et al. (2021), "Data Portability between Online Services: An Empirical Analysis on the Effectiveness of GDPR Art. 20", *Proceedings on Privacy Enhancing Technologies*, Vol. 2021/3, pp. 351-372, https://doi.org/10.2478/POPETS-2021-0051. [26]

Teresa Scassa (2019), "Ownership and control over publicly accessible platform data", *Online Information Review*, Vol. 43/6. [56]

Tsotsis, A. (2010), *Facebook Now Allows You to "Download Your Information"*, https://techcrunch.com/2010/10/06/facebook-now-allows-you-to-download-your-information/?guccounter=1. [42]

Van der Auwermeulen, B. (2017), "How to attribute the right to data portability in Europe: A comparative analysis of legislations", *Computer Law & Security Review*, Vol. 33/1, pp. 57-72, https://doi.org/10.1016/J.CLSR.2016.11.012. [29]

Willard, B. (20 July 2018), "Introducing Data Transfer Project: An open source platform promoting universal data portability", Google Open Source Blog, https://opensource.googleblog.com/2018/07/introducing-data-transfer-project.html. [41]

Wong, J. and T. Henderson (2019), "The right to data portability in practice: exploring the implications of the technologically neutral GDPR", *International Data Privacy Law*, Vol. 9/3, pp. 173-191, https://doi.org/10.1093/IDPL/IPZ008. [55]