Data Mobility and the Financial Sector

Discussion Paper

DeNederlandscheBank
EUROSYSTEEM

AFM

Authors: Mirèl ter Braak (AFM), Coen ter Wal (DNB)

With thanks to Wilko Bolt, Evert Fekkes, Nicole Jonker, Wouter Vinken
for their contributions, and to the many interviewed stakeholders.

Contents

Executive Summary

Data and data mobility - i.e. the ability to share and access data - have a growing impact on the financial sector and the wider economy: they are important to the development of financial innovation and new financial business models, and can yield significant economic benefits. However, obstacles to data mobility persist, and the sharing of data can have negative (side) effects for data holders and consumers. For these reasons, policymakers have increasingly taken action to establish regulated data sharing and enhanced data mobility. These actions affect the financial sector and the mandates of financial policymakers and supervisors such as AFM and DNB. Through this Discussion Paper, AFM and DNB aim to start a dialogue with stakeholders. To that end, in this Discussion Paper AFM and DNB set out a preliminary policy vision and policy priorities on data mobility, and propose policy actions to achieve this vision.

Context of this Discussion Paper

Discussions around data and data mobility are part of broader policy debates relating to the new digital economy. The digital economy creates new opportunities - including innovation and greater efficiency - but also challenges - including around fair competition, market contestability and protection of privacy. These opportunities and challenges have led the European Commission to publish the EU Digital Strategy, as well as various regulatory initiatives aimed at ensuring fundamental rights (Digital Services Act, AI Act) and fair competition (Digital Markets Act) in the digital economy. In February 2020, and as part of these broader discussions, the Commission also published the EU Data Strategy, which sets the aim of establishing a single market for data in the EU by 2030.

This Discussion Paper should be read against the backdrop of these broader policy discussions. This Discussion Paper does not seek to present an all-encompassing approach to tackling all the challenges presented by the digital economy. Instead, its more narrow focus is aimed at laying down a preliminary vision on the regulation of data mobility in the context of the financial sector, and to contribute to a constructive debate on how to foster the benefits of data mobility while preventing possible negative externalities and risks for data holders and users.

Data mobility and the rationales for policy intervention

Greater mobility and use of data can yield substantial benefits. In the financial sector, increased use of data has contributed to the development of new, open business models, and enables the development of new and more personalized financial products. Data can also help overcome information asymmetries. Increasingly, not just traditional financial data (e.g. payments or credit data) but also data controlled by large online platforms (BigTechs), data generated by connected products (wearables, cars) or utilities data are used in financial services. At the macroeconomic level, research indicates that enabling broader data sharing throughout the economy creates economic benefits and growth.

Mitigating market failures related to data mobility is a prerequisite for welfare-enhancing data mobility, and are grounds for policy action. First, entities that control data often lack incentives to enable the sharing of that data with third parties. As a result, data tends to become concentrated with a relatively small number of entities. Since a single data asset can be used in many different processes without a reduction in the ability to consume the data - i.e. data is 'non-rivalrous' - the benefits of data sharing can be more fully reaped when data can be shared broadly. Data concentration can also stifle competition and contribute to market concentration. Concentration of data can thus provide a rationale for data-sharing rights for data holders, or for public provision of data.

In addition, although (broader) data sharing can yield economic benefits, it can also leave data holders worse off: first, if data holders are unable to control access to their data - including because they are unable to weigh the impact of granting such access - they are likely to suffer a privacy loss for which they are not adequately compensated (negative privacy externality). Moreover, if data shared by one data holder provides the data user with information on other data holders who have not shared their data, the privacy loss can extend to data holders that did not share their data (negative information externalities). Moreover, companies with pricing power can use data they have received to implement price differentiation. This can make consumers worse off, whether or not they have shared data with the user. In financial services, such differentiation could cause financial exclusion. This justifies a policy focus on consent, as well as on promoting standards that ensure ethical outcomes related to data sharing.

To realize the potential benefits of data mobility and mitigate related market failures, policymakers have proposed data-sharing regulations. In the EU, the European Commission's 2020 Data Strategy established the ambition to create a single market for data by 2030. Subsequently, a number of data-sharing regulations have been proposed -or are expected. These include data-sharing rights for data controlled by BigTechs (Digital Markets Act), and for data generated by connected products (IoT-data, Data Act). Legislation expanding the ability to share financial data (Open Finance) is also expected.

Data-market failures and policy initiatives focused on data mobility also affect the financial sector and the mandates of financial policy-makers and supervisors, including AFM and DNB:

- Fair financial markets: the sharing and use of data as part of a financial service can yield financial innovation. The suitability of these data-driven innovations and how the interests of financial consumers are protected touch on AFM's mandate to promote fair and efficient financial markets.
- Structure and stability of the financial system: both financial and non-financial data are an increasingly-important competitive asset in the financial sector; access to data will more and more affect the ability to compete in, and enter, the financial sector. Data-sharing regulations can thus affect the structure and the level of concentration and competition in the financial

sector, and therefore impact on DNB's mandate to maintain financial stability. This is especially true as non-financial firms (e.g. BigTechs) play a growing role in the financial sector[1]. Finally, the way in which data is (mis)used can affect trust in the financial system.

- Impact on wider economic structure: data-sharing regulation impacts on the structure, innovative capacity and efficiency of not just the financial sector, but of the wider economy. This impacts on DNB's role as an economic advisor to the Dutch government.

In light of the importance of data-mobility policies for the financial sector and AFM and DNB's mandates, in this Discussion Paper AFM and DNB outline a preliminary policy vision and policy priorities.

Preliminary policy vision and priorities

AFM and DNB's preliminary policy vision for data mobility is one where policy enables trusted, innovation-enhancing and equitable data mobility; and as such helps mitigate market failures and enhance the proper functioning of data markets. This policy vision applies to data-mobility policy initiatives that have a significant impact on financial services and on the mandates of AFM and DNB. This includes sharing of financial data (Open Finance), and of relevant non-financial data, such BigTech- or IoT-data.

To enable the three elements outlined in the policy vision to be achieved, AFM and DNB identify three core policy priorities for financial policymakers: safeguarding the interests of data holders, enabling data-related innovation, and creating a level data playing field:

1. Ensuring that the interests and trust of data holders are safeguarded: to build and maintain trust in data sharing, it is vital that data can only be accessed with the consent of the data holder, and that safeguards ensure that data use results in reasonable outcomes for data holders.

2. Enhancing the potential for data-based financial innovation requires that sufficient volumes and varieties of data – both financial and non-financial - *can* be shared and accessed.

3. Establishing a level data playing field entails that different types of financial entities – traditional, FinTech, BigTech, etcetera – would have equitable access to data types that are relevant for enhancing innovation and efficiency. This means different types of financial entities are subject to similar rights, rules and requirements with respect to accessing data. Access restrictions can, however, be imposed on certain entities if access for them would cause harmful data concentration.

1 See p.43-44 DNB (2021) Changing Landscape, Changing Supervision

Policy Actions

To deliver on the policy priorities, AFM and DNB propose three key policy actions for policymakers to deliver on with respect to data mobility. These actions focus on how the preliminary policy vision and priorities can be achieved in the context of EU data-mobility policy initiatives:

1. **Design Open Finance in a way that safeguards data holders' interests, enables financial innovation and enhances the level data playing field across financial entities.**

To ensure the interests of data holders, especially given the sensitivity of financial data, AFM and DNB believe the receipt of financial data in an automated and ongoing manner from a data provider under Open Finance should be made a regulated financial activity, subject to supervision. Data sharing under Open Finance should be based on Strong Customer Authentication (SCA), as it is under PSD2. Unlike PSD2, an Open Finance initiative should allow data providers to be compensated for making data available. Compensation can create incentives for data providers to make it easier to share data, and to invest in information security. Finally, data ethics should be integrated into an Open Finance initiatives, for instance by encouraging the development of ethics standards by data users that outline what are considered reasonable and ethical outcomes of data use, for instance in terms of levels of price differentiation.

Open Finance should enable the innovative potential of financial-data sharing, by making data sharing possible for a broad scope of financial (customer) data, rather than a number of predefined use cases. In implementing Open Finance, however, priority should be given to financial datasets most likely to contribute to innovation. For datasets that raise particular privacy concerns - e.g. health insurance data – automated sharing should not be implemented, at least for the time being. In addition to customer data, OFR should also include standardized data on features of financial products ('product data'). This can help enhance product comparability and efficiency in financial markets.

Thirdly, it is important that Open Finance ensures a level playing field for financial entities. To this end, AFM and DNB propose that all *receipt* of financial data be regulated by a single regulation – the Open Finance Regulation (OFR). This includes payment-account access currently regulated under PSD2. The use of data for specific financial services – e.g. payment initiation, financial advice, credit provision – can (continue to) be regulated by relevant financial regulations. OFR should be complemented by a financial-data sharing framework containing technical, operational, and business agreements that can help avoid divergent implementations of OFR. Such a framework can be developed through public-private collaboration. Moreover, in addition to streamlining rules for financial-data sharing, the OFR can also help level the playing field between access to financial and non-financial data: OFR can make access to financial data for large platforms (BigTechs) and manufacturers of connected products conditional upon implementation of pending EU regulations enabling access to BigTech- and IoT-data.

2. **In the medium- to long-term, financial policymakers should contribute to the development of horizontal (cross-sectoral) data mobility and data sharing.**

In the shorter term, data-sharing regulations in the EU are likely to focus on individual economic sectors (financial sector), types of entities (BigTechs) or datatypes (IoT-data). However, given the increasing relevance of all types of data to financial services, in the longer-term a more horizontal approach to data sharing is needed in order to achieve the preliminary policy vision. Horizontal data sharing would help ensure that data holders enjoy similar safeguards regardless of the datatype; enhance the potential for data-related financial innovation by enabling sharing of different types of data; and level the data playing field by applying the same rules to data providers and data users, irrespective of datatype. Horizontal data mobility can be enhanced through a legislative, horizontal right to share data in an automated and ongoing way. Such a right would build on the horizontal data-portability right already enshrined in GDPR and operationalize automated, ongoing sharing of data and apply to corporates and individuals.

To ensure a level playing field for financial entities, a horizontal data-sharing right should be based on a horizontal data-sharing framework. Such a framework would establish a set of rules, standards and agreements – e.g. on contracting, compensation – as a basis for data sharing for all datatypes. As part of this framework, enhanced safeguards for data holders can be introduced as well. These could include novel techniques that can help enhance privacy of data holders. However, given the inherent complexity for data holders to fully comprehend the possible consequences of sharing data, a greater responsibility for data users should also be considered. This could be achieved by requiring data users to implement measures that help ensure reasonable (ethical) outcomes of data use.

The horizontal framework can best be developed through public-private collaboration. The EU Data Governance Act establishes the European Data Innovation Board (EDIB), which is to be chaired by the European Commission and will among others consist of competent authorities and private-sector stakeholders. Its task is to advice on how interoperability and horizontal data sharing can be implemented. Given the increasing importance of non-financial data in the financial sector, financial supervisors should consider playing an active role in EDIB and in the development of a horizontal framework.

3. **Financial policymakers can consider making datasets they control available to financial entities**

Data-sharing regulations regulate the sharing of an individual data holder's data. However, access to larger datasets – i.e. containing data referring to multiple data holders – are relevant as well for financial innovation, and a level playing field between different (types of) financial entities. Datasets are often concentrated with particular entities, which generally lack incentives to share them. Such concentration, as well as the attainment of public-policy goals in areas such as availability of credit or climate-related objectives, can provide a

rationale for policy intervention, including financial supervisors and central banks providing data(sets) they control to (certain) financial entities. The challenges and responsibilities associated with such provision should be carefully considered - in particular the privacy interests of data holders and the commercial interests of those entities that have reported the data for supervisory purposes. Provision must be fully in line with legal requirements and safeguards. In making determinations on providing data, AFM and DNB will also carefully consider our respective mandates, as well as the needs, costs and benefits of providing data.

Having weighed up these elements, AFM and DNB support the proposals for the creation of a Credit Register for corporates in the Netherlands. Such a Register can help facilitate innovation, entry and competition in the market for corporate credit. It is currently under consideration and would likely have as its main source corporate loan-level data from the AnaCredit database, which is managed by DNB. AFM and DNB will also consider other areas in which provision of data could in the future be possible, taking into account our mandates and weighing up the rationales, risks and challenges, as well as the needs, costs and benefits associated with such provision.

Chapter 1 – Introduction

Data is of increasing importance to the provision of financial services and the financial sector, and data mobility can yield substantial benefits. Increasing amounts and varieties of data are being generated at increasing velocity, and new technologies have emerged enabling mass data storage and analysis. As a result, data is an increasingly important factor of production. The financial sector is no exception to this trend: as consumers consume financial services across a variety of financial entities, the ability to access financial data becomes increasingly important in offering suitable financial products, services and advice. In addition, non-financial behavioral data – e.g. data generated by connected products (Internet-of-Things or IoT-data), data on online purchases, data related to use of utilities, social-media data - is increasingly used in the financial sector to estimate consumer preferences, innovate products, and inform processes such as pricing, and risk or claims management.

Data markets are, however, prone to market failures that provide grounds for policy action. Entities that control data often lack the incentives to enable data holders to share itwith third parties. As a result, data can become concentrated with a relatively small number of entities negating the benefits of data mobility and potentially contributing to reduced competition. In addition, the actual sharing of data is associated with negative (side)effects that can adversely affect the privacy and welfare of (some) data holders and consumers. In financial services, data-induced price differentiation could improve risk assessments, but also lead to higher costs or rejection rates for some groups of (higher-risk) consumers, and potentially harm financial inclusion.

The increasing importance of data and the potential for data-market failure has led to new policy initiatives establishing data-sharing rights. In the EU, too, data sharing has moved up the policy agenda: following the implementation of sharing of payment data under the PSD2 Directive, the European Commission published its Data Strategy, which included the ambition to complete a single market for data by 2030, with the aim of realizing the potential benefits of data mobility and mitigating market failures[2]. This strategy is in part implemented through (legislative) initiatives that expand possibilities for data holders to share their financial data ('Open Finance') and non-financial data, including consumer data held by gatekeeping platforms (Digital Markets Act) and data related to connected products (Data Act)[3].

Policy initiatives on data sharing also touch on the respective mandates of AFM and DNB and supervisory tasks. AFM and DNB's supervisory mandates focus on the promotion of efficient and fair financial markets, ensuring sound and ethical financial entities, and a stable financial system. All these components of the mandates are affected by data mobility, and by data-mobility policy initiatives:

2 European Commission (2021) Data Act & amended rules on the legal protection of databases (europa.eu)
3 European Commission (2021) Data Act & amended rules on the legal protection of databases (europa.eu)

Fair and efficient markets: broadening data sharing to not just a wider variety of financial, but also of non-financial data can provide a basis for innovations in the financial services value chain. These innovations can yield benefits for consumers, including the creation of new and more personalized financial products and services, as well as more user-friendly and efficient access to financial services. However, the expansion of data sharing can also come with new risks for consumers if their data were used in ways that lead to unreasonable, unsuitable or harmful outcomes. The way in which data sharing regulations – both for financial and non-financial data - are drafted thus impacts on AFM's mandate to maintain the fair operation of financial markets.

Soundness of financial entities and stability of the financial system: in addition to the significant role financial supervisors such as AFM and DNB will likely have in implementing and overseeing financial-data sharing ('Open Finance'), data-sharing policy initiatives touch on both AFM and DNB's mandates as they relate to financial stability:

First, as indicated, the ability to access both financial and non-financial data is increasingly important to the innovative capacity, operational efficiency and distribution opportunities of financial entities. Given the potential advantages that automated and ongoing access to different datatypes can bring to financial entities, the ability of different financial entities to access data can increasingly affect soundness and competitive capabilities of entities. This can over time have an impact on the structure and stability of the financial sector. The increasing role of platforms and non-financial groups in financial services only increases the impact of unequal access to data. For instance, currently a financial entity that is part of a non-financial group may have access to non-financial datasets (e.g. social-media, IoT-, or online-consumption data) that are not available to other financial entities. Such unequal access can affect competition and concentration in financial services, and thus the structure and stability of the system. Moreover, should BigTechs or other large, tech-based companies become more important in the distribution of financial products, lack of incentive to share data may harm risk assessment and management and thus pose prudential risks to risk carriers (banks, insurers).[4] Data mobility and access hence touches on DNB's mandate - to ensure sound and ethical financial entities, and a resilient financial system.

Data sharing can also impact on the level of trust in the financial sector. As indicated earlier, without adequate rules and agreements around the use of data, expanding data sharing can increase the risk that data is used in ways that harm (financial) consumers. Especially where harmful use involved financial entities, such outcomes could affect trust in, and the stability of, the financial sector. This hence touches on AFM's conduct supervision, focused on orderly and transparent financial market processes and appropriate treatment of consumers.

4 DNB (2021) Changing Landscape, Changing Supervision

- **Economic developments**: in support of its central-bank and supervisory tasks, DNB conducts economic research and provides economic advice to the Dutch government. The likely impact of enhanced data mobility and related regulation thus also impacts on DNB's economic advisory tasks.

The aim of this Discussion Paper is to set out (a) preliminary AFM and DNB policy vision, policy priorities and policy actions on data mobility, and to start a dialogue with stakeholders. Given the direct impact of the various EU legislative data-sharing initiatives and developments in data mobility on our mandates, AFM and DNB want to play an active role in the discussions around data mobility, without prejudicing in any way the role of other policymakers and supervisors. The Discussion Paper focuses on policy initiatives related to data mobility, in particular data-sharing regulations and the possible role of financial supervisors in making data available. It is not intended to focus on voluntary sharing of data, for instance between financial entities. The Discussion Paper aims to start a dialogue with stakeholders. AFM and DNB therefore invite a wide variety of stakeholders to read and respond (to) this Discussion Paper: consumers; corporates; financial entities including banks, insurers, pension funds, payment and electronic-money institutions; technology firms; consultants, and academics with expertise in data mobility.

All stakeholders are kindly invited to respond to this Discussion Paper. AFM and DNB plan to organize discussions with stakeholders via the iPanel, as well as publish a summary of responses received. AFM and DNB will subsequently review the vision, priorities and actions set out in this Discussion Paper, and determine AFM and DNB's input for the (implementation of) EU and international policy discussions around data sharing, including the EU's Open Finance initiative.

Reading guide to this Discussion Paper

The Discussion Paper is subdivided into 7 chapters. Following this introductory first chapter, chapter 2, explores the rationales for policy interventions in data markets. Chapter 3 will provide an overview of policy developments around data sharing and data mobility, in the EU and worldwide. In chapter 4, AFM and DNB set out a preliminary policy vision, policy priorities and policy actions regarding data mobility. The subsequent chapters will each focus on one of the proposed policy actions:; chapter 5 will focus on Open Finance; chapter 6 will address data sharing in the longer run; chapter 7 will consider the role of public authorities such as AFM and DNB as providers of datasets they control.

The chapters each contain dark-blue 'Overview & Discussion Questions' boxes, which provide a synopsis of the key points and proposed policy actions discussed in the preceding paragraph or chapter. Also contained in these boxes are questions that invite stakeholders to provide their views and insights. Reading only these boxes can serve as an alternative to reading the full Discussion Paper.

Overview & Discussion Questions – Purpose of the Discussion Paper

- Data mobility and data sharing are of increasing strategic importance for innovation and competition in the financial sector, as data can yield efficiency, competition and innovation benefits in the financial sector. This is true not just of financial data, but increasingly also of non-financial datasets.
- However, data markets are also prone to market failures, including data concentration caused by disincentives to share data, as well as negative effects (externalities) for data holders.
- These market failures provide grounds for policy action. Such data-sharing regulations also affect the mandates of AFM and DNB:
  - Unethical or harmful use of data by financial entities can undermine the AFM's mandate of promoting fair and transparent financial markets, as well as trust in the financial system.
  - Access to (both financial and non-financial) data is of increasing importance to innovation, business models, entry and competition in the financial sector. As such, access to data can in the future increasingly affect structure, concentration and the stability of the financial sector.
  - Data is also playing an increasing role in the wider economy. Data mobility and its role in the economy is as such relevant to DNB as an economic advisor to the Dutch government.
- Given the impact of data mobility and data-sharing regulations on the financial sector, and on AFM-DNB's mandates, the aim of this Discussion Paper is twofold:
  - To set out AFM-DNB's preliminary vision for how data access can be broadened in a way that aligns with our respective mandates.
  - To start a dialogue with stakeholders on the broadening of data access.

Q1: What role do you believe financial policymakers should play in the discussion on enhancing data mobility, both for financial and non-financial data?

Chapter 2 - Rationale for policy interventions in data markets

Data mobility can yield significant benefits, both in the financial sector and in the wider economy. However, data markets are also subject to market failures which, if left unaddressed, can impede data mobility or negate its benefits. On the basis of the existing research literature, this chapter provides an overview of the benefits of and obstacles to data mobility, as well as the welfare implications of data sharing. The chapter concludes with a brief summary of the rationales for policy action with respect to data mobility. These rationales will serve as the basis for the policy vision, priorities and actions set out in the subsequent chapters.

2.1 Benefits of data mobility

Greater ability to share and access data can positively contribute to efficiency and innovation financial services. Data sharing provides business opportunities for financial entities: first, the ability share data in an automated way could make it easier for financial entities to embed their services in products offered by third parties (banking/ insurance-as-a-service). In addition, data sharing can facilitate platform strategies, enabling financial entities to sell third-party products on their platform. Data sharing can also create a variety of benefits in core financial services processes. These include:

- *Offerings and personalization of products*: data can assist in product development and tailoring product offerings to characteristics and needs of individuals.
- *Financial advisory and wealth management services:* the ability to share more financial data in particular can enable a more complete overview of a client's financial situation.
- *Switching between and renewal of contracts:* greater availability of both client-data and product data can help select the most suitable products and enable automatic product selection and switching.
- *Investor due diligence*: greater access to (company) data can make it easier and cheaper for investors to perform due diligence on possible investments.
- *Pricing and risk management processes:* additional data can improve risk assessments and lead to more accurate pricing, acceptance and risk management decisions.
- *Onboarding:* additional availability of data can help enhance onboarding and digital ID services.

In all this, novel data sources and data-analytics techniques have become increasingly relevant, especially for mapping behavioral patterns that can give insight into consumer preferences and risks. Examples include IoT-data (see Box 1). Social-media data, online-consumption data, utilities consumption data

The research literature indicates that data mobility can yield economic-efficiency benefits.[5] The literature identifies two main mechanisms through which benefits occurs: first, data can be used as a factor of production that enables the

5 For a holistic compendium of the relevant literature, see: IMF (2019) Economics and Implications of Data; OECD (2019) Enhancing Access to and Sharing of Data (oecd-ilibrary.org).

Box 1- Examples of applications of data sharing in the financial sector

Enhancing transparency and efficiency of financial markets: the ability to share financial data - e.g. data on current, savings and investment accounts, loans, pension plans and insurance products - enables the creation of holistic overviews of a data holders' financial situation. This can improve the quality of financial advice and be used to optimize a data holder's financial-product mix.

Internet-of-Things (IoT) data in insurance: sharing of data generated by connected products, including cars, smart wearables (watches, etc.), home assistants or smart appliances can help create more accurate and real-time risk insights on driving style and health behaviors.

eCommerce data and credit: data from (large) online marketplaces can provide insights into consumer behavior and into revenue streams of vendors that sell via the online marketplace. This can help create a more accurate credit-risk profile for both consumers and online vendors.

creation of new innovations, including new or more personalized financial products and services. Second, data creates information and shifts it across agents, thus enabling learning-by-doing, which can help firms become more efficient. In the financial sector, information-creation materialize through the reduction of information asymmetries.[6] Indeed, in jurisdictions with less-developed financial systems, BigTechs -with greater availability of alternative data - have increasingly complemented traditional credit provision.[7] Learning-by-doing can also create 'virtuous data circles' at firm level: if data improves the quality of a firm's product or estimate, it would enable that firm to outperform others, thus attracting additional customers and data with which performance could be further improved.[8]

Recent quantitative impact analyses of data sharing confirm the impact of these mechanisms: research from 2021 by McKinsey & Company indicates that in the EU, broadening the ability to share *financial* data ('Open Finance') would result in a positive impact on GDP of circa 1-1.5% by 2030. Roughly half of these benefits would accrue to financial institutions - mainly through enhanced operational efficiency. SMEs would also be expected to gain substantially, through greater financial inclusion, and improved product options.[9] Estimates by the European Commission indicate that the total data economy - the total impact of data markets – is expected to grow by ca. 7% per year.[10]

6 Begenau, Farboodi, and Veldkamp (2018) Big data in finance and the growth of large firms - ScienceDirect
7 Cornelli et al (2020) Fintech and big tech credit: a new database (bis.org)
8 Farboodi et al (2019) Big Data and Firm Dynamics - American Economic Association (aeaweb.org)
9 McKinsey (2021), Financial data unbound: The value of open data for individuals and institutions | McKinsey
10 European Commission (2021) European Data Market Study 2021-2023

Overall, the empirical literature indicates that economic benefits of expanding data mobility for privately- and publicly-controlled data can total 1-2.5% of GDP. Data sharing can create value for data holders - although not unambiguously – but that even larger benefits accrue to data users and the wider economy.[11]

While the literature indicates significant medium-term economic gains from data sharing, debate is ongoing about the impact on long-term growth. Some research shows that efficiency gains are diminishing and finite. This is based on the concept of data as a factor or production that displays diminishing marginal returns. This dynamic is, for instance, displayed in the fact that for individual statistical models, increases in the accuracy of the model diminish as more data, and to a lesser extent more data variety, is used to train the model.[12] Such diminishing marginal benefits associated with data imply that economic gains may be temporary. Other research indicates that the same may be true for learning-by-doing gains: virtuous data circles, for example, may create benefits for individual businesses, but these benefits may not necessarily have spillovers to the wider economy. They may diminish over time, as the number of new consumers and the added value from greater volumes of (similar) data diminishes. Such loops can also lead to greater market concentration, which may reduce efficiency.[13, 14]

Other parts of the literature suggest, however, that data sharing can raise long-term economic growth. This argument is mainly based on the fact that data displays a significant degree of non-rivalry: it can be used for many different purposes simultaneously without a significant loss of value. This yields economies of scope: a single data asset - if it can be shared– can be used to help improve a wide variety of applications, products and services. These economies of scope, some research argues, help overcome diminishing marginal returns of data at the micro level (i.e. in a single application), and can cause data mobility to have non-diminishing or even increasing returns at the macroeconomic level[15].

Although broad data sharing is likely to yield efficiency benefits, coordination and concentration obstacles may impede such sharing. Lack of coordination and agreements as to how data is to be shared can impede data mobility. Moreover, while data sharing may yield benefits at the macro level, at the micro level such sharing may not develop. This is firstly because the strategic and competitive value of data reduces incentives for firms that control data to share it voluntarily, even if compensated.

11 OECD (2019) Enhancing Access to and Sharing of Data (oecd-ilibrary.org),p.60
12 Varian (2018) Artificial Intelligence, Economics, and Industrial Organization by Hal R. Varian :: SSRN; Bajari et al (2019) The Impact of Big Data on Firm Performance: An Empirical Investigation - American Economic Association (aeaweb.org)
13 Farboodi et al (2019) Big Data and Firm Dynamics - American Economic Association (aeaweb.org)
14 Goldfarb (2019) Digital Economics - American Economic Association (aeaweb.org)
15 Jones and Tonetti (2020) Nonrivalry and the Economics of Data - American Economic Association (aeaweb.org); Romer (1990) Endogenous Technological Change (jstor.org)

In addition to negating the innovation and efficiency benefits data mobility can bring, data and a lack of data sharing can also affect market structure in ways that reduce competition and economic value. This can first of all arise because storage of data is subject to increasing returns to scale: average storage cost drop as the volume stored increases, which means storage costs are lower for firms that hold large volumes of data.[16] All this can lead to data becoming concentrated, with large data holdings forming a barrier to entry and making it harder for new or smaller firms to compete. Moreover, data can create aforementioned virtuous circles and enhance network effects, which can increase the value for consumers of participating in large platforms (BigTechs), thereby making it easier and cheaper for platforms to provide value to consumers.[17] Depending on the structure of the underlying market, all these combined effects can contribute to markets becoming more concentrated or dominated by a small number of entities that control substantial amounts of data; resulting in markets becoming less contestable as a result. The substantial profits of 'data-dominant' firms such as BigTechs may indicate that large economic rents are earned as a result of data concentration.[18]

Overview & Discussion Questions - Potential benefits of data sharing

- In financial services, potential benefits of data sharing revolve around expanded and more suitable product offerings, improved pricing and risk management processes, and greater opportunities for switching products. Both financial and non-financial data can help to reap these potential advantages.
- The literature indicates that, at least for the short- to medium-term, economic benefits of data sharing in financial services and beyond can be significant, including GDP gains of approximately 1-2.5%.
- Discussions in the literature are ongoing as to whether the efficiency gains from data sharing are temporary, or lead to sustained increases in growth. The long-term effect in part depends on whether data can be used sufficiently widely across different products, services and sectors.
- Achieving broader data access may, however, run up against coordination problems. In addition, incentives to hoard data may impede economic benefits of data sharing from materializing. In addition, scope and scale advantages, as well as network effects associated with control of data may enhance market concentration.

Q2: What are the most significant potential benefits of broadening data sharing for financial services? The ability to share what data types would be most beneficial?

Q3: Do you believe the ability for cross-sectoral sharing of data affects the potential benefits?

16 Carriere-Swallow and Haksar (2019) The Economics and Implications of Data : An Integrated Perspective (imf.org)
17 Furman (2019) Unlocking digital competition
18 Furman (2019) Unlocking digital competition

2.2 Welfare implications of data mobility

Efficiency benefits of data sharing need not necessarily translate into an improvement in overall (social) welfare. Using the Pareto criterion, data mobility would (only) increase welfare unambiguously if it made at least one group of economic agents better off without making any other worse off. However, potential market failures in data markets, including monopoly power and negative spillover effects (externalities), would make some groups worse off. Below, consideration is given to these market failures and their welfare implications.

2.2.1 Privacy externalities

Data sharing can create risks of negative privacy externalities, if data users take insufficient account of the privacy and interests of data holders. Privacy can be defined as the a-priori preference of data holders to have control over who can access their data. A negative privacy externality thus arises if data holders are unable to control access to their data, and weigh up the benefits and costs of sharing.[19] The size of (negative) privacy externalities is difficult to estimate: privacy is abstract, and the so-called 'Privacy Paradox' - a discrepancy between the stated and the observed value individuals place on their privacy[20] - adds complexity to quantifying the significance of the externality.

Nonetheless, privacy externalities can arise if property rights over data are not positively assigned to data holders. Although under standard economic theory (Coase Theorem), who holds property rights should not affect market outcomes, it is doubtful this holds in the case of data: data is non-rivalrous, which means that use of it in one process does not prevent it from being used in others. Since data users have more information about possible data uses than data holders, assigning property rights to data users makes it possible for them to use data in excess of what data holders are aware of, resulting in privacy externalities. Requiring consent from the data holder for individual uses of their data can help mitigate this.[21] This is indeed the premise of the EU's General Data Protection Regulation (GDPR) - which regulates the processing of personal data: GDPR generally requires that data holders consent to use of their data (or to a contract that requires such use), and limits use of data to the stated purpose ('purpose limitation')[22].

Nonetheless, it remains doubtful that in practice, data holders have the ability to provide informed consent: data holders may not be able to fully comprehend and fully oversee the purpose for which data is to be utilized, and the (potentially-harmful) consequences that this purpose may have for the data holder. Making an informed decision is especially difficult given the complexity of terms, conditions and contracts.[23]

19 Acquisiti et al (2016) The Economics of Privacy
20 Carriere-Swallow and Haksar (2019) The Economics and Implications of Data : An Integrated Perspective (imf.org)
21 Carriere-Swallow and Haksar (2019) The Economics and Implications of Data : An Integrated Perspective (imf.org)
22 GDPR Articles 5 and 6 EUR-Lex - 32016R0679 - EN - EUR-Lex (europa.eu)
23 Netherlands Bureau for Economic Policy Analysis (2021) Brave New Data

2.2.2 Information externalities

Data holders can, by granting access to their own data, also create externalities for other data holders. Such 'information externalities' can arise when a data holder shares their own data, and by doing so allows the data user to also gain insight into the preferences or risks of data holders that have not granted access to their data. The data user can gain such insights if the correlation between preferences or risk profiles of data holders is not zero. In that case, data holders who have not shared their data suffer a (partial) privacy loss. Given that they have already suffered a privacy loss, such data holders may be persuaded to share their data at a lower level of compensation.

2.2.3 Market power, price discrimination and financial inclusion

In markets where companies have market power, data sharing can enable price discrimination. Additional data about the preferences (or risk profiles) of consumers can enable companies to design price-discrimination strategies. These can include first-degree discrimination, where companies are able – based on data – to set individual prices for consumers based on their individual preferences. First-degree price discrimination can be applied particularly to those data holders who share their data. However, the mere fact that a data holder is unwilling to share data could also have signaling value: in financial services, for instance, not sharing one's data may signal that the data holder represents a higher financial risk. This can oblige data holders to share their data at low compensation to avoid being worse off for not doing so.[24] Data sharing can also enable third-degree price discrimination, where a company sets and designs different prices and products for which consumers with different preferences or risk profiles will subsequently self-select. Third-degree price discrimination can be applied to both data holders who have and those who have not shared their data.[25]

Data sharing can enhance, but potentially also harm, financial inclusion. In addition to product and distribution innovation, data sharing in financial services can thus reduce information asymmetries. Data sharing can, for instance, make it possible to better determine a consumer's risk profile and apply price differentiation (discrimination) in insurance premiums or in borrowing rates. This can make pricing decisions more accurate and reduce adverse selection. Some consumers will be made better off, as their ability to better reveal their low risk profile (or high client value) can result in lower cost of financial products. Access to data not traditionally used in the financial sector can also enable greater financial inclusion, by for instance making it possible to provide financial products to consumers for whom more traditional financial data is not available. This may, for example, apply to consumers an extensive credit history. Similarly, nontraditional data can enable (improved) estimation and mitigation of risks that cannot be adequately

24 He, Huang, Zhou (2020) Open Banking: Credit market competition when borrowers own their data
25 Bergemann et al (2021) [2004.03107] The Economics of Social Data (arxiv.org); Choi et al (2019) Privacy and personal data collection with information externalities

assessed using traditional data, thus for instance enabling new risks to become insurable.[26]

However, a risk also exists that enhanced data mobility results in more granular risk assessments and pricing which can ultimately reduce access to financial products for higher-risk individuals[27]; either by making them less affordable, through cherry-picking of risks, or through outright denial. AFM and industry research for the Dutch insurance sector indicates that pricing has indeed become more granular and dispersed, although no significant adverse effects on availability (through denial) can be observed.[28]

2.2.4 Trust externalities

A data breach affects not just the company at which a breach takes place, but also the data holder and other data users. Companies that control data will have some incentives to secure data, given its strategic importance and potential liabilities it can incur in the case of a breach. However, breaches also undermine confidence in overall data security and willingness to share data, thus affecting other data users.[29] Data mobility is hence subject to a trust externality, for which companies are neither charged (if a data breach occurs) nor compensated (if sufficient security investment prevents a breach). This can cause investment in data security that is suboptimal from a social-welfare perspective.

26 Carriere-Swallow and Haksar (2019) The Economics and Implications of Data : An Integrated Perspective (imf.org)
27 Carriere-Swallow and Haksar (2019) The Economics and Implications of Data : An Integrated Perspective (imf.org)
28 AFM (2021) The personalisation of pricing and conditions in the insurance sector; Verbond van Verzekeraars (2021) Solidariteitsmonitor 2021
29 Kashyap and Wetherilt (2019) Some Principles for Regulating Cyber Risk

Overview & Discussion Questions – Welfare implications of data sharing

- Data sharing can yield efficiency benefits, but these need not automatically lead to welfare increases. Using the Pareto criterion, data sharing will only enhance welfare if one group of economic agents is made better off and no others are made worse off. Market failures may lead to Pareto-suboptimal outcomes.
- One such likely market failure are privacy externalities, which can occur if data holders are insufficiently able to control who has access to their data and for what purpose.
- Companies with pricing power may also be able to use data to extract value from consumers through price discrimination. In the financial sector, this can be particularly harmful if it leads to loss of access to financial products and services (financial exclusion).
- Information externalities can also arise if a data user gains insights into a data holder's preferences or risks by analyzing data obtained from another data holder. In such instance, not only does the data holder who has not granted access to their data suffer a privacy loss, but the insights gained can also be used in a way that harms the data holder's interests.
- Data sharing can increase the risk of data breaches. Private incentives for companies to invest in data security do not take into account the negative impact of breaches on broader trust in data sharing. This can create socially-suboptimal levels of investment in data security.

Q4: How significant do you believe privacy and information externalities of data sharing to be?
Q5: How do you assess the impact of data sharing on financial inclusion?

2.3 Rationales for policy interventions

Benefits of data sharing, and failures in data markets can present rationales for policy interventions. These rationales for different policy actions are outlined below:

- *Data hoarding provides a basis for data-sharing rights and public provision of data:* data-sharing rights can serve to mitigate insufficient levels of data sharing resulting from incentives to hoard data. The fact that the benefits of data sharing increase as a greater variety of data can be accessed, provides grounds for horizontal (across sectors and datatypes) rather than sectoral data-sharing rights.
- *Impact of data concentration on market concentration and competition can provide a rationale for data-sharing rights and public provision of data:* through data-related scale advantages and contributions to network effects, data concentration can affect market structures in a way that reduces competition. This can provide a rationale for data-sharing rights.
- *Privacy and social externalities are grounds for a policy focus on data ethics*. Especially in markets with pricing power, data sharing can enhance price discrimination at the expense of consumers (data holders), both those who have shared their data and those who have not. This can be particularly harmful, including in the financial sector, if price discrimination causes loss of access to products and services. This can provide grounds for policies that focus on limiting harmful effects for data holders.
- *Trust externalities argue for allowing compensation,* to eable data holders to recoup investments in data security. Policy can ensure such compensation is fair and reasonable, in order to ensure access to data.

Overview & Discussion Questions – Rationales for Policy Interventions

- The benefits of data sharing, as well as the market failures associated with data markets and data sharing create rationales for public-policy interventions. These rationales will inform the preliminary policy vision, policy priorities and proposed policy actions set out later in this Discussion Paper.
- Negative privacy externalities provide a rationale for assigning data-property rights to data holders, so as to limit socially-excessive use of data. Moreover, granting data holders the right to share their data can help limit data hoarding, especially if the right applied across economic sectors and datatypes. Data concentration can provide grounds for public provision of key datasets to a broader array of data users.
- Overcoming potentially negative welfare effects resulting from data-enhanced use of price discrimination can provide a rationale for policies focused on avoiding undue harm for data holders (i.e. data ethics), both for data holder who have and those who have not shared their data.
- Public coordination of data-sharing implementation agreements can help overcome coordination problems that can hinder data sharing. Policy requirements aimed around data security and rules around recouping investments in data-sharing infrastructure can help internalize trust externalities.

Q6: To what extent do you believe data sharing can help mitigate market concentration?
Q7: Which externalities related to data sharing do you believe to be most important?

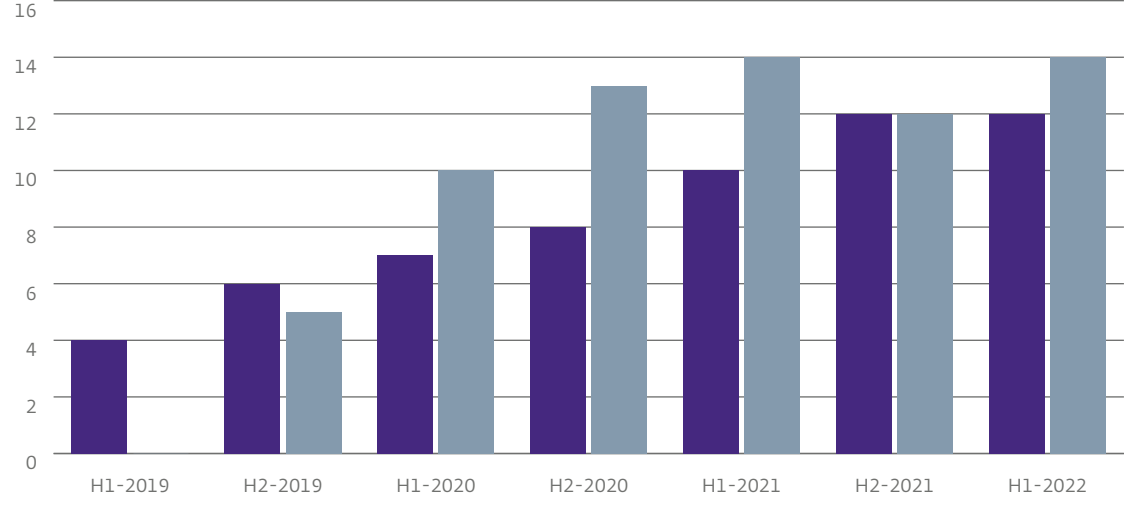
Chapter 3 - Developments in Data Mobility

Given the potential benefits of data mobility and the market failures in data markets, data mobility has become of increasing importance and interest to policymakers. This Chapter will review the impact of, and discussions around, data sharing policy initiatives. In particular, the chapter will discuss the impact of the first legislative data-sharing initiative in the EU - the sharing of payments data under the revised Payment Services Directive ("PSD2") - on financial innovation in the Dutch financial sector. It also provides an overview of current discussions and developments around legislative data-sharing initiatives, in the EU and globally.

3.1 Market developments in data sharing: the PSD2 experience in the Netherlands

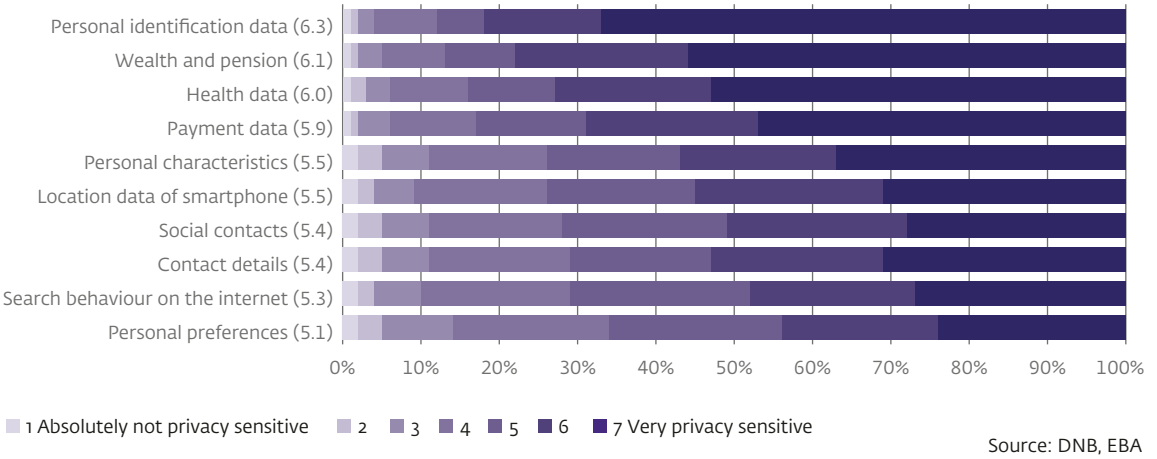
As the first EU legislative data sharing initiative, PSD2 has served as a catalyst for data sharing in financial services. The PSD2 Directive entered into force in 2019. As the first legislative data-sharing initiative in the EU, PSD2 regulates mandatory access to payment-account data for the purposes of initiating payments from a payment account (payment initiation services); or of aggregating of payment accounts data (account information services). Account information services (PSD2 service 8) make up the bulk of innovation under PSD2: in the Netherlands, a total of 29 entities have obtained a PSD2 license. Currently, 26 entities currently have a license, of which 14 solely provide

Figure 1 - Steady rise in number of PSD2 entities licensed by DNB



Source: DNB, EBA

Figure 2 -Sensitivity of datatypes



Source: DNB, EBA

account information services and 12 provide both PSD2 services (Figure 1).[30]

New services offered by PSD2-entities include, for example, online administration and accounting programs for businesses, the ability to assess commercial loan applications on the basis of payment history (incoming and outgoing payments on the payment account). For individuals, new services include aggregated financial statements, online housekeeping books, 'budget apps' intended to prevent consumers from taking on excessive amounts of debt, investment apps that automatically round up digital payments and automatically invest the rounded amount. Banks have also developed additional services, in particular in the area of account information. These services focus on offering overviews of consumers' current accounts. Three incumbent non-bank payment institutions have also obtained PSD2 licenses.

A quarter of Dutch consumers indicated that they have shared their data as part of PSD2[31], in particular with the bank with which they hold their primary bank account(s). DNB surveys indicate that consumers are particularly willing to share their data with providers they trust and where a clear (financial) benefit is linked to the sharing of data. For example, willingness to share is highest for services providing advice on maximizing interest rates on savings accounts. DNB surveys show, however, that individuals remain concerned with how their data is used. Consumers view financial data as highly sensitive (Figure 2), and therefore mainly share data with their own bank(s), in which they have relatively high levels of trust.

30 In July and August 2021 three companies had their PSD2 license withdrawn.
31 DNB (2020) https://www.dnb.nl/en/actueel/dnb/dnbulletin-2020/a-quarter-of-dutch-consumers-shared-payment-data-in-exchange-for-services

In addition to trust, consumers indicate the perceived benefit of data sharing, the way data is used (anonymously, linked to the data holder),[32] and the services linked to the data all play an important role in data-sharing decisions.[33] This can help explain the Privacy Paradox: while data holders indicate they greatly value their privacy, other factors can in practice persuade them to divulge privacy-sensitive data.[34]

Markets participants and stakeholder perceive PSD2 as having had a more significant impact in corporate payments markets, but not as a game changer so far. Compared to payment services for consumers (individuals), PSD2 is perceived to have had a greater impact on the corporate market segmen: the number of payment service providers that corporates can choose from has increased, including new providers that have entered the Dutch market. In addition, PSD2 has made it possible for smaller companies to deploy business administration and accounting software packages that are directly linked to payment accounts.[35] On the whole, however, PSD2 is not perceived as having thus far been a game changer. While the entry of new providers has had a positive effect on competition and has unlocked new services, these advances are perceived to be limited. The likely reasons for this includes the relatively high level of efficiency of the Dutch payment system pre-PSD2, which created limited room for new providers; and the limited scope of data that can be shared under PSD2, or difficulties in PSD2 implementation.[36]

The PSD2 implementation also provides a number of lessons, in particular on the importance of a sufficiently-standardized implementation. Although some technical requirements were laid down in PSD2's Regulatory Technical Standard, and while standardization efforts were made by industry subsequent, the diversity in application programming interfaces (APIs, interfaces that are used for exchanging data between applications) complicated implementation, increased the need for so-called API aggregators to interpose themselves between data users and data providers, and increased implementation cost.

Beyond PSD2, there has been an increasing focus on data mobility. Financial institutions increasingly consider building business models around data mobility, both by utilizing data but also as part of platformization strategies. In the Netherlands, the public-private Dutch Data-Sharing Coalition (DSC), in which the insurance industry is a participant, is working on creating a framework for cross-sectoral data sharing.[37] Internationally, private-sector initiatives to enable data sharing include the RAM framework developed by the International Data Spaces Association, My Data Principles, and the GAIA-X framework. European financial entities are

32 Bijlsma et al. (2021), Not All Data are Created Equal - Data Sharing and Privacy by Michiel Bijlsma, Carin van der Cruijsen, Nicole Jonker : SSRN
33 Van der Cruijsen (2020). Payments data: do consumers want banks to keep them in a safe or turn them into gold?, Applied Economics 52(6), 609-622.
34 Barth & De Jong (2017) The privacy paradox â€" Investigating discrepancies between expressed privacy concerns and actual online behavior â€" A systematic literature review | Elsevier Enhanced Reader
35 SEO Economisch Onderzoek (2022) PSD2 Evaluatie
36 SEO Economisch Onderzoek (2022) PSD2 Evaluatie
37 Home - Data Sharing Coalition

Overview & Discussion Questions – Market developments in data sharing

- The introduction of data sharing rights for payment account-related data under PSD2 has stimulated FinTech innovation in the Dutch financial sector, in particular in the area of account information services.
- Data holders have also shown a substantial willingness to share their payments data, but this willingness mainly extends to sharing of data with the data holder's own bank in instances where they perceive a financial benefit. Data holders also indicate they perceive financial data as more sensitive than other consumer datatypes, including social-contact, preferences and location data.

Q8: Should other important market developments around data sharing be considered?

also working on the SEPA API initiative, which aims to standardize data sharing in the financial sector. The SEPA Payment Account Access (SPAA) Scheme is the first concrete deliverable SPAA aims to set common agreements on sharing payment account related data. In the future, it can serve as a basis for sharing of other financial data, and potentially for non-financial data.

3.2 Regulatory developments: enhancing data mobility

3.2.1 European Union

The 2020 European Commission's Data Strategy has refocused attention on the importance of data sharing. In the Data Strategy, published in 2020, the European Commission sets out its ambition for the establishment, by 2030, of a single market for data. To achieve this, various pieces of EU legislation have been proposed, or are expected, that relate to expanding and regulating data sharing (see Table 1). These include the Data Governance Act - which creates a first regulatory framework for providers of data intermediation services - the Digital Markets Act – which enables sharing of customer data controlled by gatekeeping platforms (BigTechs). Proposals for an EU Data Act would make it possible to share data generated by connected products (IoT-data), and would set common requirements for all data-sharing regulations, for instance on compensation, consent and dispute resolution.

The Digital Finance Strategy (DFS) provides more detail on the creation of a financial data space. In particular, the DFS, which was published in September 2020, lays out the Commission's priority to expand the right to share data to both private and public data in the financial sector and establish a 'common financial data space'. In November 2021, the Commission released a proposal for a European Single Access Point (ESAP); a register operated by ESMA providing investors access to all financial reporting data that has to be made public under EU

Table 1 - Overview EU legislative data sharing initiatives

EU initiative	Substance of initiative	Status
Data Governance Act	Proposals include a notification regime for data-sharing service providers, which provide consent and data-sharing management to consumers.	Agreement reached
Digital Markets Act	The proposals include mandatory automated data-sharing by large, gatekeeping platforms (e.g. browsers, market places, social media platforms). APIs, SCA, etc. not mandated.	Agreement reached
Data Act	Provides data holders with a right to share data generated by their connected products (Internet of Things or IoT-data) with third parties. It also lays down horizontal requirements that will underpin all legislative data-sharing initiatives.	Proposals published March 2022
European Health Data Space Regulation	Gives data holders the right to share health data, and regulates access rights for health professionals. It also introduces a labelling scheme for certain wellness apps.	Proposals published May 2022
Open Finance legislation	Expands mandatory data-sharing from payments data to the rest of financial services (actual scope unclear)	Proposal expected end-2022
Payment Services Directive (PSD2)	Review includes user-experience and compensation for data sharing. It may lead to amendments ("PSD3").	Review expected end-2022
European Single Access Point (ESAP)	CMU Action Plan announced the setting up of a Financial Data Space consisting of regulatory reporting data (NFRD, ESG, financial reporting).	Proposal published November 2021
Open Data Directive	Requires high-value public datasets to be made available in an automated manner.	Implementation by end-2021

financial regulation.[38] The DFS also foreshadowed legislative Open Finance proposals to expand the data-sharing rights from payments data to other financial datasets. Recently, the Commission launched a Call for Evidence and target consultation on Open Finance[39].

3.2.2 International

In a number of non-EU jurisdictions, proposals are under consideration to implement or expand data mobility. In these jurisdictions – the UK, US, Australia (see Box 2) – data sharing in the financial sector has been a first step towards implementing horizontal (i.e. across sectors) sharing of data.

38 European Commission (2021) resource.html (europa.eu)
39 European Commission (2022) Call for Evidence Open Finance

Box 2 – Overview Horizontal Data Access Initiatives

In 2020, the **United Kingdom** Government published its National Data Strategy (NDS), which defines keys missions for policymakers. The first of these is the unlocking of the value of data, including through Smart Data Initiatives, of which Open Finance is the most mature. The Financial Conduct Authority (FCA) has published a Call for Input[40] and Feedback Statement on Open Finance[41]

In the **United States**, debates on data portability have quickly risen to the top of the political agenda. In 2021, the SAFE Data Act was tabled in the U.S. Senate, aimed at allowing consumer to access and port their data. In addition, proposals were tabled for an ACCESS Act, which would require Big Tech platforms to ensure their interfaces are interoperable with other business so as to enable user data portability. Both bills are currently being considered by the U.S. Congress.[42] [43] In financial services, rulemaking is expected on operationalization of data sharing. Section 1033 of the Dodd-Frank Act provides for consumer rights to access to financial records. In October 2020, the Consumer Financial Protection Bureau (CFPB) published an advance notice of rulemaking, soliciting input on how risks related to data sharing can be mitigated, as well as on the costs and benefits of data-sharing frameworks.[44]

Australia has introduced comprehensive regulations to enable cross- sectoral data sharing. The Consumer Data Right (CDR) regulation provides a cross-sectoral framework for data sharing. The framework is implemented on a sector-by-sector basis, starting with banking and energy. Open Banking constitutes the first tranche of CDR. As of July 2020, four major banks are required to share product data as well as, when directed to do so by the data holder, consumer data.[45]

40 FCA (2019) https://www.fca.org.uk/publications/calls-input/call-input-open-finance
41 FCA (2021) FCA publishes feedback to Call for Input on open finance | FC
42 White & Case (2021) House Bill Mandating User Data Portability and Platform Interoperability
43 Brookings Institution (2021) One year after Schrems II, the world is still waiting for U.S. privacy legislation (brookings.edu)
44 Consumer Financial Protection Board (2020) Consumer Financial Protection Bureau Releases Advance Notice of Proposed Rulemaking on Consumer Access to Financial Records | Consumer Financial Protection Bureau (consumerfinance.gov)
45 Australian Competition and Consumer Protection Commission (2020) Commencement of CDR Rules | ACCC

Box 3 – Open Finance and Open Banking initiatives

The **Hong Kong** Monetary Authority has introduced a four-stage approach to implementing Open Banking, starting with APIs providing access to product information and to data needed for new credit-card and loan products. In late 2021, guidance was provided on the implementation of the third phase, which focused on sharing of account balances. The fourth stage will require that payments and transfers information be made available for automated sharing.[46]

India has implemented data-sharing in the payments sphere through its Unified Payments Interface (UPI) and is based on a publicly-developed open API and standardized payment instructions. Regulated FinTechs and banks can use the UPI-infrastructure to send and receive payments..[47]

The Monetary Authority of **Singapore** (MAS) has thus far supported the implementation of Open Banking through non-binding means, including an API exchange (APIX) and, together with the banking industry, an API Playbook containing standards and a list of recommended APIs.[48]

In addition, a significant number of jurisdictions have implemented or are considering implementing Open Banking and Open Finance initiatives. In most cases, these initiatives are centered around the development and implementation of open and standardized Application Programming Interfaces (APIs), which enable third parties to obtain access to relevant financial data. Some jurisdictions - such as India, Singapore - have opted to faciltate the development of data sharing.[49] Others –Colombia, Chile and South Africa[50] – are exploring Open Banking/Open Finance regulation (see Box 3).

46 Hong Kong Monetary Authority (2021) Hong Kong Monetary Authority - Phased Approach (hkma.gov.hk)
47 Carriere-Swallow et al (2021) India's Approach to Open Banking: Some Implications for Financial Inclusion (imf.org)
48 ABS, MAS (2018) abs-api-playbook.pdf
49 Deloitte (2019) Open Banking around the world | Deloitte | FSI
50 South Africa Financial Sector Conduct Authority (2020) Regulating Open Finance – Consultation and Research Paper

Overview & Discussion Questions – Policy developments in data sharing

- The EU's Data Strategy expresses the ambition to create a single market for data by 2030. This is being implemented through legislative proposals, including the Data Governance Act, Digital Markets Act (enables sharing of BigTech data), Data Act (enables sharing of IoT-data) and Open Finance (financial-data sharing).
- Internationally, many countries are focused on enabling sharing of financial data (Open Finance). However, in the UK, US and particularly Australia, policy initiatives are being considered or implemented that would make possible data sharing across various important economic sectors.

Q9: What policy developments are of particular importance to financial regulators and supervisors?

Chapter 4 – Policy Vision for Enhancing Data Mobility

This chapter outlines a preliminary AFM and DNB's policy vision for data mobility, and also set out more concrete preliminary policy priorities and policy actions that stem from the vision. The vision, priorities and actions are informed by the potential benefits of data mobility and possible market failures in data markets, which offer a rationale for policy intervention in data markets. The policy actions proposed in this chapter will each be discussed in the subsequent chapters.

4.1 Policy vision and policy priorities

In setting out the preliminary policy vision, AFM-DNB take account of the rationales for policy interventions in data markets. As set out in chapter 2, data mobility can create substantial benefits in financial services and beyond. However, market failures can impede data sharing or negate its benefits. Both benefits and market failures can offer rationales for policy intervention.

Therefore, AFM-DNB's preliminary policy vision for data mobility is one where policy enables trusted, innovation-enhancing and equitable data mobility, and as such contribute to the mitigation of market failures and to the efficient functioning of data markets that are relevant for financial services.

Trusted data mobility means data holders feel confident in engaging in data transactions because they trust that they control how their data is accessed, and that their interests are taken into account in the way their data is used. This can help mitigate privacy and information externalities. Data mobility can be innovation-enhancing when financial entities can access sufficient and sufficiently-varied datatypes and datasets. Finally, equitable data mobility is achieved when financial entities of all types face a level data playing field, which means they have equitable opportunity to access relevant data following the same rules in a way that does not lead to suboptimal concentration of data with certain (types of) entities.

The preliminary policy vision aligns with the AFM and DNB's mandates, which are centered around promoting efficient fair and efficient financial markets, ensuring the soundness of financial entities and the stability of the financial system (see Chapter 1). Moreover, the policy vision aligns with the rationales for policy intervention as set out in Chapter 2, as it focuses on mitigating the market failures set out there.

The policy vision is meant to apply to all data mobility policy that has a significant impact on financial services, the financial sector and the respective mandates of AFM and DNB. This includes legislative initiatives for the sharing of financial data - known as Open Finance - but also applies to the sharing of non-financial datasets that are relevant to the financial sector and AFM-DNB's mandates. These include policies for automated sharing of BigTech- and IoT-data.

4.2 Policy priorities

To put the policy vision into practice, (financial) policymakers should prioritize policies aimed at establishing meaningful data sovereignty for data holders, ensuring sufficient availability of data,

and implementing streamlined and reciprocal rules for access to data. Below, each of the main policy priorities to be pursued will be outlined in greater detail:

- **Safeguarding data holders' interests:** in order for data mobility to be successfully enhanced, it is vital that a data holder trusts that they can control who accesses their data, and that data sharing will not cause outcomes detrimental to their interests. Where financial entities are involved in data transactions – be it as a data provider or data user – this trust also affects confidence in financial entities and the financial system. Maintaining trust in data sharing should therefore be a key policy priority. This can best be achieved through the principle of meaningful data sovereignty, which entails that data holders should have control over what entities can access their data; i.e. that data can only be shared with the consent of the data holder. However, as it may not always be straightforward for data holders to consider every way in which a data transaction could affect their interests, a responsibility should also fall on data users to ensure their use of data results in reasonable outcomes for data holders.

- **Sufficient data available for sharing:** to achieve the full potential of data-related innovation for financial products, services, processes or business-models, it is key that data holders have the ability to share relevant data. While this policy objective could be established through voluntary data-sharing initiatives, entities where relevant data is concentrated face incentives not to provide that data to third parties (see Chapter 3). Therefore, legislative data-sharing initiatives that create an obligation for data providers to share data they control with third parties – subject to the approval of the data holder – are likely needed. Moreover, it is important that the scope of these initiatives be sufficiently wide and not restricted to designated use cases.

- **Level data playing field**: policymakers should set it as their objective to create a level 'data playing field', by giving different types of financial entities an equitable opportunity to have relevant datasets – financial and non-financial – shared with them by data holders. This objective includes the removal of undue barriers to obtaining access to data. Such barriers can stem from a lack of technical standardization, for instance of APIs or data vocabularies. Unequal access terms and conditions can also lead to an unlevel playing field; for instance when financial entities face different rules for different datatypes, with respect to authentication of data transactions, contracting or compensation arrangements, or safeguards for data holders. A level playing field, however, does not necessarily imply that all types of financial entities should always have *equal* access to all datatypes; if giving certain entities access to certain datasets would cause risk of data concentration that could in turn cause future data and market concentration, the option of restricting such access should be available.

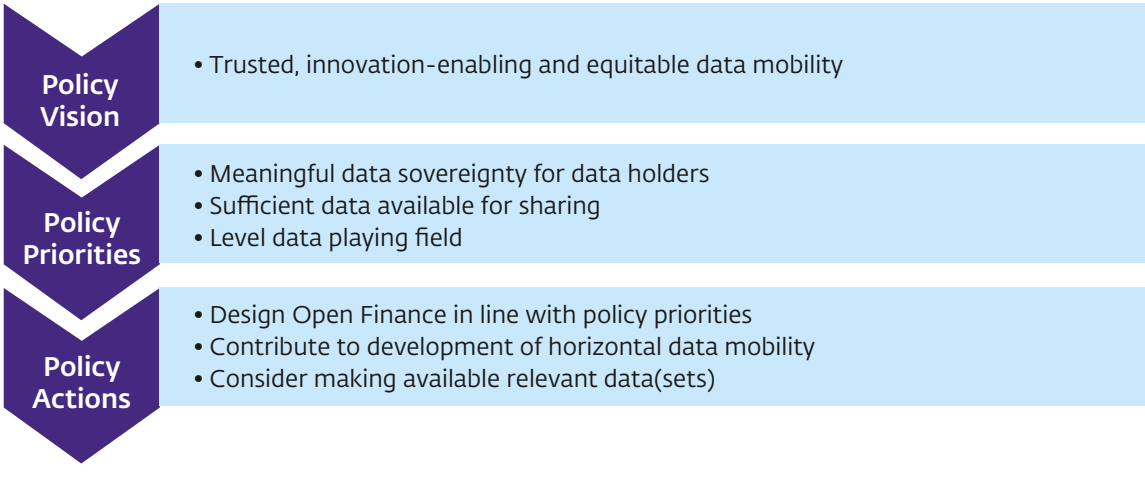
4.3 Policy Actions

Financial policymakers can achieve the policy objectives through both short-term and more medium-term policy actions. Broadly speaking, AFM-DNB propose the following main policy actions for financial policymakers to pursue:

- **Develop an Open Finance framework with sufficient safeguards for data holders and a sufficiently broad scope.** The European Commission is expected to put forward (legislative) proposals for an Open Finance framework in the EU, aimed at expanding financial-data sharing beyond payments data. To establish Open finance in a way that aligns with the policy priorities set out in paragraph 4.2, AFM and DNB believe policymakers should ensure sufficient safeguards for data holders, including through public supervision of financial-data users and a greater focus on reasonable use of data. A broad scope would also enable financial innovation. Finally, priority should be given to ensuring a level (and reciprocal) playing field with other data-sharing regulations. Chapter 5 will elaborate on Open Finance.

- **Over the longer-term, financial policymakers should actively contribute to the development of a horizonal framework for data mobility:** while in the short- to medium-term broadening of data sharing will be implemented through sectoral legislative initiatives, to achieve the policy vision, a longer-term effort should be pursued to achieve a horizontal data-sharing framework, to establish an undergirding structure for sharing of different relevant data types. Such a framework would enable streamlined safeguards for data holders, enhance the potential for data-related financial innovation, and create a level playing field for all

Figure 3 – Overview of Policy Vision, Policy Priorities and Policy Actions



types of entities active in the financial sector. Chapter 6 will discuss the design of a horizontal data-sharing framework and the role of financial policymakers.

- **Consider making available datasets controlled by public (financial) authorities to financial entities:** financial supervisors and other public authorities control datasets that, if made available, could facilitate innovation and a level data playing field. Public authorities – including financial supervisors and central banks – can consider the rationales, benefits, challenges and risks associated with making publicly-controlled data available to (certain) financial entities, as well as how such provision aligns with their mandates. Chapter 7 will further reflect on this.

Overview & Discussion Questions –Policy Vision, Policy Objectives and Policy Actions

- AFM-DNB's preliminary policy vision for data mobility is one where policy enables trusted, innovation-enhancing and equitable data mobility
- To realize this (preliminary) policy vision, policymakers should pursue the following policy objectives:
  - *Safeguarding the interests of data holder*: data sharing should be based on the consent of data holders, but data users also have a responsibility to avoid reasonable outcomes for data holders.
  - *Sufficient data availability:* legislative data-sharing initiatives (e.g. Open Finance) should enable the sharing of sufficient and sufficiently-varied datasets so as to enable (financial) innovation.
  - *Level data playing field:* this objective consists of creating streamlined access . It does not preclude restrictions on access to certain datasets for certain (financial) entities.
- Key policy actions for financial policymakers include:
  - Develop an Open Finance framework with sufficient scope and safeguards (Chapter 5)
  - In the longer run, actively contribute to the development of horizontal data sharing (Chapter 6).
  - Consider making available data controlled by (financial) public authorities (see Chapter 7)

Q10: What are your views on the policy vision and policy objectives as outlined?

Chapter 5 – Data mobility in the financial sector: Open Finance

In its 2020 Digital Finance Strategy, the European Commission announced a legislative Open Finance initiative to expand the possibilities for data sharing in the financial sector. This chapter outlines AFM and DNB's preliminary proposals for policy actions with respect to Open Finance; in particular, how an Open Finance can safeguard the interests of data holders (paragraph 5.2), enables financial innovation (5.3) and level the data playing field for financial entities (5.4).

5.1 Introduction

Open Finance relates to an expansion of data-sharing right from payments data – as enabled under PSD2 - to, among others, data related to credit, savings, investments, insurance and pensions. The European Commission has launched a consultation, call for evidence and expert group to inform the development of an Open Finance legislative initiative. This chapter will set out proposals for the development of Open Finance in a way that ensures data holders' safeguards (paragraph 5.2), enables innovation (5.3) and helps level the data playing field for all financial entities (5.4).

5.2 Safeguarding the interests of data holders

5.2.1 Supervision

Statutory safeguards and ongoing supervision should remain in place as prerequisites for the ability to obtain access to financial data. Survey data indicates that data holders consider financial data among the most sensitive of datatypes. Security breaches or misuse of financial data could thus have major negative implications for trust in financial-data sharing, and in the financial system more generally. Hence, for the time being, data users that receive financial data under Open Finance should be made subject to regulation and supervision. For incumbent financial entities, this can be integrated into existing supervision. A proportionate regime can be created, based on the number of data transactions conducted by a provider. This is analogous to current proportionality under PSD2, which is based on payment volumes.

5.2.2 Consent management & transaction authentication

As set out in chapter 4, AFM and DNB consider consent from data holders to be an important prerequisite to data sharing. Below, considerations around consent management and authentication will be set out:

Strong Customer Authentication (SCA) should be required for financial-data transactions. To ensure (data) transactions have been authorized by the actual data holder, the PD2 Directive that be applied; i.e. that at least two out of three factors - knowledge, possession and inherence - should be used to authenticate a data transaction. In recent years, innovation has taken place in authentication factors, including the development of geolocation and biometric factors, used to identify an individual's unique behavioral patterns. It has therefore been suggested to move towards a more 'factor-neutral', outcomes-based authentication requirement. AFM and DNB believe, however, that maintaining SCA is

necessary for data transactions under Open Finance, both because it may be difficult to detect unauthorized data transactions that are not related to payment initiation; and because - once data has been (illicitly) processed - it is difficult for its adverse effects - privacy loss - to be undone.

Enabling use of eIDs can enhance user experience. In the previous paragraph the importance of SCA was emphasized. However, as part of an Open Finance framework, consideration should be given to the way in which such SCA can be provided. Different from PSD2, Open Finance would involve many different datatypes, to be provided by many different financial entities. Authenticating data transactions with each individual financial data provider using identity credentials issued by that provider (which differ from those issued by others) is unlikely to be optimal from a user-experience perspective. Indeed, these concerns already materialize under PSD2 where data holders have to authenticate transactions with multiple banks; this issues are likely to be greater still in the context of Open Finance. A potential solution for a loss of user experience may lie in enabling the use of external eIDs that provide a high level of assurance in data transactions. Such eIDs would not only enable more efficient onboarding of new clients,[51] but would make it possible for data holders to authenticate data transactions with different entities using a single set of credentials. The proposed EU's Digital Identity Wallet (EDIW) initiative[52], for instance, would require all EU Member States to nominate at least one (public or private) eID product for use throughout the EU, including for instance in onboarding. This could lay a basis for use of national or private-sector eID in authenticating data transactions. To ensure trust, it is important that concerns related to privacy and security of EDIW be addressed. Similarly, sufficient corporate eID schemes must be available. Corporate eIDs require additional functionality that identifies individuals who can authenticate transactions on the company's behalf.

The way in which (re-)consent is managed can also be reconsidered. To make it easier and more intuitive to manage the consents for the sharing of data they provided, data holders should have the ability to revoke their consent not just through the data user, but through the data provider as well. In addition - and in line with recent EBA proposals for some data transactions under PSD2 – an Open Finance framework could include a 180-day re-authentication requirement. Over the longer term, consideration should be given to the role of data intermediaries in the management of consent and authentication.

5.2.3 Compensation for use of data-sharing infrastructure

Under Open Finance, (renewed) consideration will have to be given to whether the prohibition on compensation for data providers for making data available - that currently exists under PSD2 - should also be included in Open Finance. Below, arguments

51 DNB (forthcoming), 'Van Herstel naar Balans'
52 European Commission (2021) Commission proposes a trusted and secure Digital Identity (europa.eu)

for and against allowing compensation will be weighed up:

Enabling compensation can improve incentives for data providers to invest in data security and user-experience. Investing in secure data-sharing infrastructure can enhance trust in data sharing. Such investments hence carry externalities which could (partially) be priced in by allowing providers to be compensated for successfully-completed API requests. Such arrangements could also create incentives for data providers to optimize user experience, and to achieve greater standardization. This could ultimately enhance data sharing more than detailed regulation around (obstacles to) access.

The PSD2 implementation has shown that not allowing compensation can also create costs. An important argument against compensation for data providers under PSD2 was that such compensation would raise the cost of sharing data, thus reducing the positive impact of data sharing on innovation and competition. Requiring a zero access fee was also meant to minimize regulatory costs by avoiding the costs that come with establishing the optimal level of an access fee. However, the PSD2 implementation has shown that a zero access fee may create regulatory costs of its own. These are related to disincentives for data providers when it comes to achieving standardization and a good user experience. Such disincentives require more extensive supervision aimed at establishing proper access. Similarly, lack of incentives to achieve standardization has contributed to the divergence in data-sharing infrastructure (APIs) under PSD2. This divergence has, in turn, led to the rise of API aggregators. These are service providers that 'translate' a data-access request from a third-party provider to the various bank APIs, thus removing the need for the third party to be able to link to a wide variety of bank APIs. However, such aggregators themselves increase data-transaction costs. As data sharing is expanded under Open Finance, all these costs are likely to increase, in addition to the additional investments required in infrastructure.

Regulatory and market developments also point to wider acceptance of compensation. The proposals for an EU Data Act establish for all legislative data-sharing initiatives the (fair and reasonable) compensation for data providers, and at-cost compensation where the data user is a micro-enterprise or an SME.[53] Although the Data Act proposals allow sector data-sharing regulations to set a lower- or zero-level compensation, the introduction of compensation for making available IoT-data raises the prospect of an unlevel playing field for financial-sector data providers. Compensation is also part of the industry-led SEPA Payment Account Access (SPAA)Scheme, which is under development by a multi-stakeholder group within the EPC, as part of the wider SEPA API Access initiative. The SPAA scheme includes fees for the use of APIs, except for data covered by the PSD2 prohibition. These fees could vary depending on differences in the cost, risks and value created by the specific datatype. Such baseline access fees reduce

53 Article 9 Proposals EU Data Act https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0068

negotiation and contracting costs for data providers and data users, as well as market fragmentation.[54]

Weighing up the arguments for and against compensation for making data available, AFM and DNB believe that regulated compensation arrangements are on the whole beneficial. It is important to emphasize that data providers should only receive compensation for *access* to the data (which through APIs), not for the data itself. One method for determining the level of compensation in the case of mandatory data access is the Long-Run Incremental Cost method; a method often used to determine the level of acceptable pricing for use of infrastructure.[55] This method was applied for instance with respect to telecom and utilities infrastructure, and limits the compensation an entity can charge to the amount required to cover its cost plus investments required to upgrade and update the infrastructure.

5.2.4 Ethics standards

Ethics standards with respect to data use should be integrated into Open Finance. Data transactions under Open Finance, as is the case for other EU legislative data-sharing initiatives, will be based on consent by data holders. While it is important that data holders have control over what data is accessed by what parties, it may be difficult for them to take full account of all the ways in which the data they have agreed to share could be used, and what consequences this may have for them. Therefore, data users should carefully consider what data types they wish to use in what processes, and determine measures to mitigate unduly-harmful effects of data use. This can, for instance, involve determining what (maximum) level of price differentiation is ethically acceptable. Similarly, data users should consider how they will ensure reasonable outcomes for data holders that do not wish to share data. Policymakers should encourage the development and application of ethics standards, and consideration should be given to including such standards (or requirement to develop them) in a data-sharing framework (paragraph 5.4), or in an Open Finance legislative initiative. This would be without prejudice to comparable requirements already included in financial regulation (see paragraph 6.2).

54 Scheme members can bilaterally negotiate lower fees.
55 The LRIC method sets fees in a way that allows the network owner to cover the costs that it has to incur to maintain the network, but also to enable the network owner to make the necessary investments to innovate or become more efficient.

Overview & Discussion Questions – Safeguarding interests of data holders

- Given the sensitivity of financial data and the impact of unauthorized or unethical use of data on financial stability, statutory regulation and supervision are considered desirable for the moment.
- In light of limited detection and recourse options in case of unauthorized data transactions, Strong Customer Authentication (SCA) should be required for financial-data transactions.
- Under Open Finance, compensation to data providers for the use of their data-sharing infrastructure -although not for the shared data itself – should be permitted. Such compensation can yield aligned incentives for data providers to improve user experience.
- To safeguard data holders' interests, ethics standards should be applied. These address what data types will be used for what processes, and how unreasonable impacts of data use are mitigated.

Q11: Should Open Finance be subject to statutory regulation and public supervision?
Q12: How can strong customer authentication be maintained in a way that ensures acceptable user experience? What, if any, role do you see for eIDs?
Q13: Do you believe compensation for use of data-sharing infrastructure should be permitted as part of the OFR? If so, how should fee levels be determined?
Q14: How can data ethics be incorporated as part of Open Finance?

5.3 Enabling financial innovation

This paragraph will focus on the desired scope of the Open Finance initiative, with respect to the datasets that are to be made subject to data-sharing rights, the types of data holders to whom data-sharing rights should at least be granted, and the types of data users that should be allowed to access financial data.

5.3.1 Scope of Open Finance

To enable innovation, the Open Finance scope should be broad and not limited to specific use cases or services. The Open Finance scope would pertain to financial data, which in this Discussion Paper is defined as (unprocessed) data provided by, or generated by or on behalf of a data holder in the course of a regulated financial service. Achieving the full potential benefits offered by data sharing is based on the *ability* to share sufficient types of data for sufficient purposes. The ultimate scope of Open Finance should therefore not be limited to particular datasets, or aimed at particular use cases. Rather, it should enable data holders to share a wide range of financial data, and enable it to be used for a variety of purposes. (see Table 2). Such a broad scope is without prejudice to legal requirements on data minimization.

In addition to customer data, an Open Finance initiative could also include automated access to standardized high-level product information. This Discussion Paper has thus far focused on *customer* data -i.e. data that is provided by and can be linked to customers. However, standardized *product* data - information on key characteristics of financial

products (see Table 2) - can also be highly valuable: product data can for instance help the development of comparison services, which enable consumers to identify optimal financial product mix and thus contribute to comparability and efficiency in financial markets. Standardized product data can also be used by supervisors for monitoring pricing and product developments in financial markets. Given these advantages, AFM and DNB believe standardized financial-product should also be included in the scope of an Open Finance initiative. Product-data standardization is, however, complex: terms and conditions of financial products contain nuances and are structured differently. Implementation could first focus on higher-level and more objective product information.

A broad data scope should be combined with a sequenced implementation, based on a pre-set rollout, with clear timelines for completion of each phase. AFM and DNB consider that priority can best be given to implementation of datasets for use case which yield substantial benefits for data holders (consumers), and to data that support policy objectives, e.g. the Capital Markets Union initiative. Finally, privacy sensitivity of datasets should be

Table 2 – Overview possible Open Finance datasets

Financial Product	Relevant product data	Relevant customer data
Mortgage credit	Interest rate, term of repayment, type of mortgage, embedded insurances, mortgage provider.	Principal amount, payment history, payment transactions, account balances, property value.
Consumer credit	Interest rate, term of repayment, principal amount of loan or credit, name credit institution, home NCA, etc.	Payment transactions, credit amounts, credit limits, account balances.
Savings	Name saving product, interest rate, account terms, DGS information.	Account balances, payment transactions.
Non-life insurance	Name insurance company, home NCA, coverage limits.	Payment history (delinquency), claims history (non-health related).
Life insurance	Tax status, surrender options, conditions, home NCA, etc.	Relevant risk data categories, including income or wealth information.
Pension	Type of pension plan, name pension funds, name employer, home NCA, tax status.	Projected pension benefit, pension contribution rate, default retirement age.
Investment	Historical performance, cost and fees, machine-readable versions of mandatory disclosure documents (e.g. KID, KIID), home NCA.	Balance and transaction information, investment history (exposure, risk profile, suitability assessments).
Payments	Cost of payment accounts, services included in the payment account package.	Account balance, transaction history, overview of recurring payments.

considered in setting priorities: although processing of shared data should in all events have to comply with GDPR requirements. Open Finance could deprioritize or exclude sensitive data from automated sharing. Such sensitive financial data would ,for instance, include data related to health insurance claims. Taking account of these considerations, the following datatypes could be given implementing priority:

- *Wealth management data, include data on savings, investment and retirement-savings accounts.* Investment data can also include data on insurance-related investment products. The ability to share these data types can yield benefits in terms of providing financial information services. It also enables more holistic and accurate financial advice. Similarly, standardized product data on savings, investment account products could be made available in this category.
- *Credit data:* the ability to share data around outstanding loans and credit can enhance the efficiency and lower the cost of due diligence processes with respect to credit provision. In the Netherlands, a credit register for natural persons has long-since enabled credit providers to perform due diligence on applicants. A similar register for corporates is currently under discussion. In enabling sharing of credit and loans data, (existing) pooled solutions where data is centrally aggregated should also be considered as a viable alternative to bilateral sharing between data providers and data users.
- *Non-life insurance data:* the ability to share claim-history data can enhance due diligence processes. Data on insured objects or events can

Box 4 - Potential data intermediation services

- *Technical services:* banks have gained substantial experience in the development of API catalogues and may be able to offer this expertise to new data providers as data mobility is expanded.
- *Consent management:* some financial entities offer – sometimes as a complementary service - consent dashboards and other tools that enable data holders to manage data-sharing consents.
- *Managing compensation:* compensation paid to data holders or data providers can be administered and processed through data intermediaries.
- *Data portfolio management:* if, in the future, intermediaries were to receive 'writing rights' -i.e. the ability to conduct data transactions on behalf of a data holder- management of data access consents on behalf of data holders could emerge as an important service. This, however, will require regulation in addition to the proposed DGA or existing GDPR.
- *Collective agreements:* under the DGA, data cooperatives could be established which would negotiate terms and conditions for data access with data users on behalf of groups of data holders.
- *De-correlation services:* intermediaries can play a role in enabling de-correlation data of data holders to mitigate social externalities of data mobility.

enable better advice; standardized information on insurance products (coverage, premiums) can help select optimal insurance products.

5.3.2 New business models based on data sharing

Financial policymakers and supervisors should contemplate financial entities becoming not just data providers and users, but data intermediaries. The rise of data intermediation services will also enable data-related business model innovation for financial entities. Such innovation includes helping consumers manage consent for data transactions, negotiating with data users and on behalf of groups of data holders about the term and conditions of data utilization (see Box 4 below). Consumer surveys indicate that financial institutions enjoy a strong trust position with data holders. In addition, banks have gained experience with regulated data sharing through PSD2, and some are already providing eID services. Some financial entities appear to be well-positioned to become data intermediation service providers. Financial policymakers should monitor shifts in business models and new prudential risks that may stem therefrom.

A growing focus on data intermediation by financial entities may require more cooperation between financial and data-intermediation supervisors. The new Data Governance Act (DGA) creates a regulatory basis for the provision of data intermediation services, which would impact financial entities offering intermediation services. DGA requires a legal split between data intermediation services] and other business operations; data obtained through intermediation service provisions may not be used in other parts of a business.[56] This can create new operational risks which may require greater collaboration between financial and DGA supervisors.

Overview & Discussion Questions – Enabling financial innovation

- An Open Finance Regulation should enable sharing for a broad set of financial data. Priority should be given to implementing sharing for data with greatest innovative potential, including wealth-management, credit, non-life insurance data.
- Financial entities may become more involved as providers of data intermediation services, such as providers of APIs, eIDs, or consent management, as well as data cooperatives. This may be enhanced by regulatory certainty provided by the EU DGA.
- Such a shift in financial entities' activities may lead to new operational risks, which may require closer cooperation between financial and non-financial supervisors to address.

Q15: Should scope of Open Finance be broad or focused on specific use cases?
Q16: How should implementation (priorities, sequencing) be organized?
Q17: How do you see the role of financial entities in data intermediation evolve?

56 Article 11 Data Governance Act.

5.4 Creating a level data playing field

5.4.1 Open Finance Regulation

Expansion of financial-data sharing should be regulated through an Open Finance Regulation. Industry-led initiatives – including the SEPA API initiative and its SPAA scheme - can play an important role in the *implementation* of Open Finance. However, in order to overcome incentives not to share data, ensure equal and sufficient safeguards for data holders, and a level data playing field for data users, an Open Finance Regulation (OFR) should be adopted. OFR should enact a data-sharing right with respect to designated financial data. As such, it would require relevant financial entities to make data available to licensed data users (see below); with the exception of small and micro-sized entities to ensure proportionality. OFR should lay down requirements for authentication, consent, operational resilience and compensation arrangements. It should also enable the Commission to designate what financial data is to be made subject to the OFR data-sharing right.

OFR should cover receipt of financial data ('read access') - including of account information - but leave use of financial data ('write access') in financial service to existing regulation. The current PSD2 legislation provides an appropriate mechanism for implementing the sharing of payments data. Given its focus on payments, it is, however, less suited as a framework for organizing Open Finance. Continuing to regulate sharing of payments data under PSD2 while introducing OFR to cover the sharing of other financial data would, however, create the risk of divergent requirements for financial-data sharing. A straightforward way of streamlining financial-data sharing would therefore be to consolidate regulation of 'read access' to data under an Open Finance Regulation (OFR). Read access refers to the ability to receive, aggregate and analyze data received, and to provide, for instance, consolidated financial overviews to data holders. Indeed, AFM and DNB propose that the OFR be based on a new category of financial services: financial information service (FIS). FIS could be defined as the receipt and aggregation of financial data covered by data-sharing rights established by OFR. FIS would include receipt of account information; access to which would be removed from PSD2 as a separate payment service. As such, OFR would be the singular regulation covering reading access to all designated financial data; and it would be 'activity-agnostic' by containing general requirements on the right to share and the conditions for financial-data transactions. This is in line with enabling innovation as set out in paragraph 5.3.

Use of data ('write access') in financial services can be regulated under existing financial regulation. Write access refers to the ability by financial entities to take action on the basis of received data. This includes initiating transactions (as included in PSD2), opening bank accounts or switching from one financial services provider to another. It is conceivable that under an OFR, new 'write-access' services will emerge, for instance automated switching services. Services based on write access can be covered by existing, relevant regulations, such as regulations for payment initiation financial advice, intermediation and

distribution. Providers of services based on write access would still have to comply with OFR to obtain automated access to financial data.

Access to financial data can be linked to effective implementation of the Digital Markets Act (DMA) and Data Act. A degree of reciprocity would be built into OFR: it would treat receipt of financial data as a regulated financial service, thus ensuring that all financial-data recipients would be considered financial entities and required to provide access to financial data they may control. However, entities whose primary activities are outside of financial services may not in practice control significant volumes of financial data, and could hence receive financial data without substantially reciprocating.

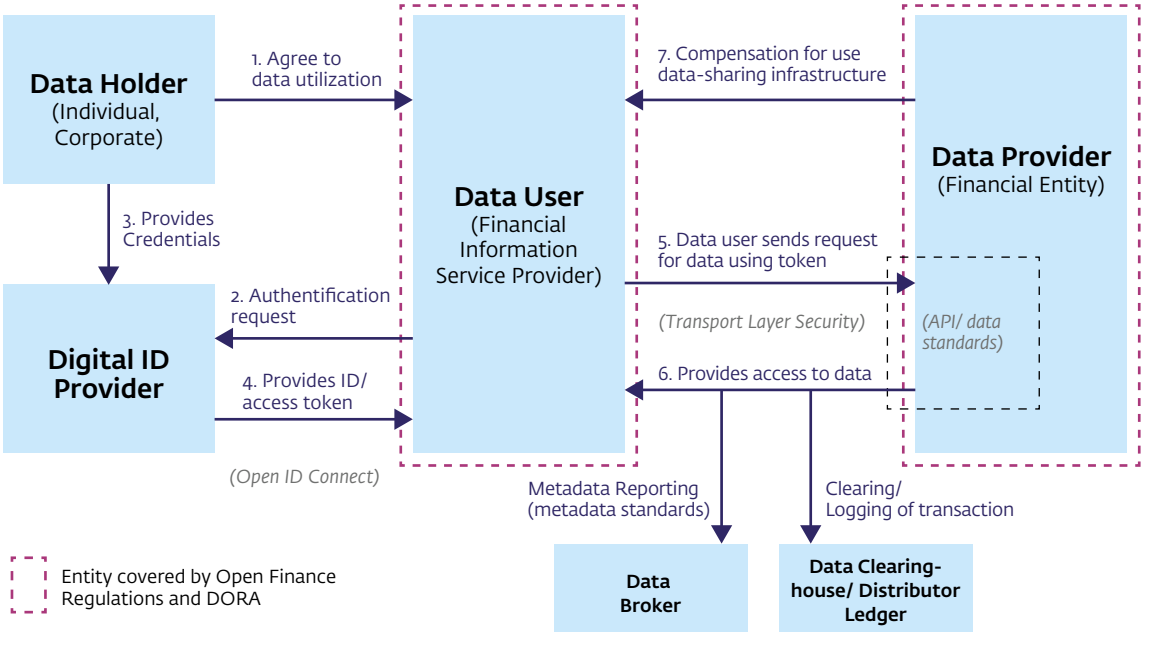
A horizontal approach to data-sharing – i.e. requiring all corporates to enable automated sharing of customer data - could ultimately resolve reciprocity concerns. Such an approach would be possible over the longer-term (see chapter 6), but is unlikely in the short-term given its complexity. Nonetheless, the DMA - which enables access to customer data controlled by BigTech platforms - and the proposed Data Act – which enables access to IoT-data - can help mitigate some of the risk of data becoming concentrated with large technology-native entities, by requiring such entities to make valuable customer data they control available for data sharing. A reciprocity provision in OFR linked to the DMA and Data Act could help overcome some concerns around a level data playing field: such a provision in the OFR would enable entities that have to provide data under the DMA and Data Act to access financial data under OFR only if and when the DMA and Data Act were fully implemented and effectively enabled all financial entities to access BigTech- and IoT-data. The European Commission could be tasked with periodically assessing whether such 'effective reciprocity' has been established. The Commission could also be given powers to block access to financial data for certain data users more permanently if such access would cause data concentration and an unlevel data playing field with an impact on the structure and stability of the financial sector. Such a prohibition would be analogous to the one in the EU Data Act, which bans gatekeeping platforms' from accessing IoT-data.

5.4.2 Technical implementation of financial-data sharing

Greater standardization in implementation of Open Finance should be pursued. Insufficient standardization has hindered the implementation of the PSD2 Directive; for Open Finance to succeed, further work it is important that greater standardization be pursued in key areas. These include:

- APIs: standardization of API architecture, functionality, and discoverability, as well as data fields.
- Information security: standards regarding the confidentiality, integrity and authenticity of data;
- Data standards, including standardization of data message formats, data structures, and data semantics standards, that lay down a common understanding of the meaning of data assets. Data-quality standards and standards for latency should also be developed.

Figure 4 – Stylized representation framework for financial-data sharing



- User experience standards: authentication requirements and rules on undue obstacles to access.
- Meta-data standards: common descriptions of data.
- Compensation: ensuring that compensation levels are fair, reasonable and non-discriminatory. The introduction of compensation enhances the need for automated logging of data transactions, via a central party or through decentralized infrastructure.

OFR should make it possible to endorse frameworks developed through (public-)private collaborations. The SPAA scheme developed through the SPAA Multi-Stakeholder Group (MSG) and managed by the EPC is an example of such a framework. The aim is to expand the scheme over time to cover other financial assets as well.[57] The OFR could empower this industry-led work by delegating the development of standards and requirements to the SPAA MSG and endorsing a framework or scheme produced by it, provided it meets the criteria set out in OFR.

57 See EPC (2022) https://www.europeanpaymentscouncil.eu/news-insights/insight/sepa-payment-account-access-spaa-developing-new-scheme-through-multi

In addition to the development of an architectural framework, the potential of applying new technologies to data sharing should be further explored, in particular the use of shared ledgers. Shared ledgers (or Distributed Ledger Technology, DLT) can enable automated data sharing, and transaction traceability which can help detect unauthorized transactions. Moreover, through smart-contract functionality, shared ledgers can be used to manage access to data assets and settle compensation.

A framework should also include a standardized contract to avoid a need for bilateral negotiations. Under PSD2, data sharing is not dependent upon a contract being in place between data provider and data user.[58] The proposed EU Data Act, however, does. Such bilateral negotiations can, in practice, create undue barriers to data sharing, particularly for smaller data providers and data users. A framework should therefore give consideration to developing a standardized contract.

5.4.3 Coordination with other (legislative) data-sharing initiatives

Financial policymakers should coordinate with policymakers responsible for other data-sharing regulations. For the time being, data-sharing regulations in the EU are likely to be focused on specific sectors or datatypes. Nonetheless, to ensure as level a playing field for financial entities as possible, it is important for financial policymakers to coordinate the design and implementation of OFR with those of the Data Act and DMA. Such coordination can focus on aligning the approaches to, for instance, requirements for authenticating data transactions, safeguards for data holders, technical standardization, compensation and the need for bilateral contracts, and could form the basis for a more horizontal approach; proposals for which are set out in chapter 6.

58 Article 66(5) and Article 67(4) PSD2.

Overview & Discussion Questions – Level data playing field under Open Finance

- To streamline rules for financial-data sharing, Open Finance can best be implemented through a regulation: the Open Finance Regulation (OFR). The OFR should establish a new financial service - 'financial information services' – covering automated and ongoing receipt of financial data.
- To ensure a level implementation, a data-sharing framework should be developed that includes technical standards (regarding API architecture, information security, data standards) as well as compensation and dispute-resolution arrangements. This framework can be developed through public-private initiatives such as the ERPB's SEPA API initiative.
- To also ensure a level playing field with important non-financial datatypes, access to financial data under OFR for gatekeeping platforms and manufacturers of connected products should be reciprocal and conditional upon full implementation of DMA and Data Act.

Q18: What should the relationship be between the Open Finance Regulation and the expected amendments for PSD2 ("PSD3")?
Q19: Should access to financial data be subject to reciprocity? If so, in what way?
Q20: What components of data sharing should be standardized through a framework?
Q21: Should OFR aim for a single EU-level financial-data sharing framework (e.g. SPAA) to underpin Open Finance? Or should it leave room for multiple (e.g. national-level) schemes?

Chapter 6 – Data sharing in longer run: a horizontal approach

While a sectoral approach may be more practicable in the short run, it also leads to fragmented implementation of data sharing, which makes it harder to achieve AFM and DNB's policy priorities: regulatory fragmentation can cause data-holder safeguards to diverge between datatypes. It also limits the volume and variety of data available for sharing, and thus the potential for financial innovation. Finally, fragmentated approaches of data sharing can result in divergent requirements for access to and use of data, resulting in an unlevel playing field between different financial entities. This chapter, therefore, outlines policy actions to establish a horizontal approach to data sharing in the longer term; one that takes account of the opportunities, but also the responsibilities that come with data sharing. This can be achieved through an EU "Data Act 2.0", which can enshrine (and expand) safeguards for data holders (paragraph 6.2), establish a horizontal data-sharing right to enhance innovation (6.3), and lays a further basis for a horizontal data-sharing framework (6.4).

6.1 Introduction

Chapter 5 set out how the preliminary policy vision and priorities can be implemented for financial data through OFR. However, the distinction between financial and non-financial data is becoming increasingly difficult: a variety of datatypes will be increasingly relevant in the financial sector. Financial entities' activities are increasingly likely to be both financial and non-financial. To meet the policy priorities over the longer run, therefore, a horizontal approach to data sharing is needed; one which is irrespective of the type of data shared with or accessed by data users, including financial entities. Such an approach can be built on recently-adopted or recently-proposed EU legislation – the Data Governance Act (DGA) and the Data Act -including an future "Data Act 2.0". The next paragraphs will set out components of a horizontal approach for each of the policy priorities identified in chapter 4:

6.2 Safeguarding the interests of data holders

Data sharing can have negative welfare implications for (some) data holders, in terms of their privacy and if insights from data lead to greater price differentiation and discrimination (see chapter 2). These negative implications can become more apparent as over time data sharing becomes more widespread and more datatypes become available for sharing. Hence, as part of a horizontal approach to data sharing, additional safeguards for data holders should be considered. These can be implemented through the proposed EU Data Act (or in a future review of the Data Act). Below these additional safeguards are discussed:

6.2.1 Data sovereignty

New technologies and techniques can help implement 'data-sovereignty-by-design'. As set out in chapter 4, the ability of data holders to be in control of their data can help reduce negative implications of privacy and information externalities. The ability of data holders to manage what data users have access to their data is a key part of such control, especially as data sharing over time

encompasses more datatypes and data providers. eID solutions and consent dashboards can help data holders manage data-sharing consents. Shared ledgers and smart contracts can do the same: smart contracts provide transparency and automation with respect to the terms of access and use for data, enhance security of data sharing and provide an immutable record of data-transaction authorizations. Such a record is key for managing data-sharing consents, as well as for determining compensation for the data holder.[59]

Control over data also entails that data not be used other than for purposes to which consent has been given. For individuals, the EU's GDPR privacy regulation offers protections in this respect, such as the requirement to only process data for a defined purpose ('purpose limitation'), and to minimize the amount of data processed ('data minimization'). Novel privacy-enhancing technologies can help implement such provisions, by reducing the amount of data and information that is being shared with data users. Consideration can be given to, over the longer term, integrating such technologies into frameworks that implement data sharing (see paragraph 6.4), or in data-sharing regulations.

One of these technologies is Zero Knowledge Proof (ZKF), which enables data users to validate information needed without receiving data that would provide them with additional (unintended) information. For instance, ZKF would allow a data user to validate a data holder's age (or whether they are over a certain age) without providing the data holder's date of birth. De-correlation technologies could also help reduce information externalities.: De-correlation technologies can reduce the extent to which data users can learn about other data holders in a particular group or segment.[60, 61] De-correlation consists of purging the data of those components that are correlated with other data holders, but in a way that maintains meaningful signals and informational content. This can be done by the data provider or by an intermediary.

6.2.2 Requirements for reasonable use of data

As part of a horizontal approach, consideration should be given to whether the outcomes of data sharing are unreasonable with respect to the interests of the data holder and overall welfare. Data sovereignty and consent alone are unlikely to provide sufficient protection of data holders' interests: information asymmetries and cognitive limitations, for instance, may make it inherently difficult for such data holders to comprehend how their data will be used, what impact(s) that may have, and to weigh up such considerations in their consent decision. Therefore, existing and proposed regulations - including GDPR (personal data) and the AI Act - provide important protections with respect to how data is used, including requiring legitimate grounds for data use, limiting the purposes for which data can be used, minimizing the amount of data that can reasonably be used,

59 Siris et al (2020) OAuth 2.0 meets Blockchain for Authorization in Constrained IoT Environments | IEEE Conference Publication | IEEE Xplore
60 Acemoglu et al. (2019), Too much data?
61 Privacy by design in data sharing implies that throughout the entire data processing and analyzing process safeguarding people's privacy is taken as a principal position. The proposed ISO standard (ISP/PSC 317) specifies the design process so that it meets consumers' domestic processing privacy needs as well as the personal privacy requirements of data protection.

Box 5 - Potential measures to ensure reasonable data utilization

- *Collective data agreements:* the emergence of data cooperatives as envisaged by the EU's Data Governance Act proposals could provide a means for data holders to negotiate collectively with data users about terms and conditions under which data is used.
- *Certificate of ethical use:* currently, data usage policies are normally provided to data holders, but they are lengthy and opaque. Instead, certificates can be issued, for instance by certified private parties or the European Data Innovation Board, to confirm that data users' data usage policies sufficiently safeguard reasonable outcomes for data holders.
- *Ethics frameworks:* good practices or requirements for ethical use of data, for instance with respect to what data is used in what processes and with what levels of (additional) consent, and safeguards that mitigate potentially-unreasonable outcomes for data holders.

and preventing discriminatory biases in data use. To fully address the potential negative externalities of data sharing in the future, however, a complementary focus is needed on whether the *outcomes* of data use are reasonable and ethical from the perspective of data holders and society overall.[62]

Ensuring reasonable outcomes for data holders can be operationalized through data-use processes and data policies established by the data user. These policies and processes can for instance lay down what data will be used for what processes, as well as what adjustments and limitations could be applied to outcomes that result from data use (e.g. cap insurance premiums or loan rates) to ensure an ethical distribution of benefits of data use. These policies should also address reasonable treatment of data holders who do not wish to share their data. Such processes and policies can be established in variety of ways (see Box 5), including through certificates of ethical data use issued by third parties, or through ethics frameworks. For example, following the 2019 study by AFM and DNB[63] that looked at increasing use of data (analytics) in the Dutch insurance sector, industry adopted an ethics framework for use of data.[64]

Voluntary or private initiatives are, however, likely to result in patchy application, and private initiatives may lack the bite to compel all data users to abide by reasonable-use standards. The Data Act could therefore require data users to have in place ethics frameworks or obtain a certificate of ethical use as a prerequisite for obtaining access to data in automated and ongoing manner.[65] Such a requirement could build on concepts such as Product Oversight and Governance (POG) and the

62 See also: Wachter and Mittelstadt (2019) A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI by Sandra Wachter, Brent Mittelstadt :: SSRN
63 AFM & DNB (2019) https://www.afm.nl/~/profmedia/files/rapporten/2019/afm-dnb-verkenning-ai-verzekeringssector.pdf
64 See Ethisch kader datatoepassingen (verzekeraars.nl)
65 Bijlsma et al (2014) Kiezen voor privacy: hoe de markt voor persoonsgegevens beter kan, CPB policy brief

duty of care, which are already applied in financial regulation. POG has the purpose of ensuring that products and services are designed and distributed to a suitable target group; the duty of care obliges financial enterprises to act in the best interest of the customer. They can be warranted by the harm that privacy and information externalities can cause, and by the advantages data users derive from having automated and ongoing access to data, especially under a horizontal approach.

Exclusion of specific datasets from the data-sharing framework can also be considered if other measures are insufficient. Such datasets could then not be shared or accessed in an ongoing and automated manner. This is a far-reaching option and should only be considered where large negative externalities are likely relative to efficiency gains associated with data sharing. Prohibitions on data sharing could be linked to (existing) prohibition on use of certain datatypes. For instance, proposals for the revised Consumer Credit Directive prohibit the use of social-media or health data to assess creditworthiness.[66] Similarly, as indicated in chapter 5, health-insurance data could also be excluded from automated sharing.

Overview & Discussion Questions – Safeguards

- As the possibilities for data sharing expand over time, additional safeguards for data holders should be implemented horizontally (i.e. across sectors), for instance via the Data Act.
- These will help ensure data holders' interests are protected in an adequate and in the same way, regardless of the datatype they are sharing from or with financial entities.
- Data holders' control over data (data sovereignty) can be enhanced through new technologies, including eID, shared ledgers, zero knowledge proof or de-correlation techniques.
- However, in the longer run, horizontal measures that help ensure reasonable and ethical outcomes of data sharing should also be considered, including ethics frameworks, reasonable-use requirements or exclusion of datasets from automated data sharing.

Q22: What, in your view, would be the added value of discussed novel techniques?
Q23: What is your view on the need and design of reasonable data use requirements?

66 Recital 47 EUR-Lex - 52021PC0347 - EN - EUR-Lex (europa.eu)

6.3 Enabling (financial) innovation

In the longer run, a fragmented approach to data-sharing rights will likely impede (financial) innovation. The short- to medium-term approach to data sharing in the EU has been and will likely be sectoral, based on a number of data-sharing regulations for different datatypes. Such a fragmented approach can hinder data-related innovation, including in the financial sector, by making sharing possible for only some datatypes.

It has been suggested that in the longer run, data sharing could be based on the data-portability right contained in the GDPR itself: this right enables individuals to receive their personal data – regardless of datatype - and transmit it to a third party for automated processing if they have consented to such processing, or if processing is needed for execution of a contract. This right would govern data sharing in the absence of other data-sharing rights. The GDPR, however, does not 'operationalize' the portability right: it does not enable ongoing sharing, nor does it specify technical, legal, business or functional requirements. The right also only pertains to individuals and personal data.

In the longer-run, an 'operationalized' horizontal data-sharing right could be considered. A horizontal data-sharing right could be laid down in a Data Act 2.0 and serve to overcome fragmentation inherent in sectoral data-sharing regulations, by providing data holders with a right to share a wide variety of data, including across economic sectors. Such a right can be implemented sequentially, with a focus on datatypes that yield efficiency and innovation benefits, and on economic sectors and markets in which data concentration could adversely affect competition. A horizontal data-sharing right should apply to provided data - i.e. data that a data holder has either directly provided to the data provider, or that the data provider has observed. It would be best to leave derived data – i.e. data that has been produced due to simple processing of raw data - and inferred data – which results from more advanced processing of raw data – out of scope.[67] For both derived and inferred data, questions around intellectual property rights can arise. Moreover, enabling data holders to share the results of data innovation – i.e. inferred data - with third parties may undermine the innovative and competitive aims of broadening data sharing. A horizontal data-sharing right can also best apply to individuals and corporates; research has shown that data sharing can be particularly beneficial for corporates (see chapter 2).

Finally, a horizontal right should include the possibility for restrictions. Even when fully implemented, certain data users may be prohibited from obtaining automated and ongoing access to certain data(types) under a horizontal data-sharing right, where such restrictions are merited on the basis of data-concentration risk. Such restrictions are already included in the proposals for an EU Data Act, which prohibit the sharing of IoT-data with gatekeeping platforms.

67 European Data Protection Board (2017) ARTICLE29 - Item (europa.eu)

Overview & Discussion Questions – Horizontal data-sharing right

- In the longer run, a horizontal data-sharing right should enable individuals and corporates to share data they have provide directly or indirectly (observed data) to a data provider, with a third-party data user, in an automated and ongoing manner.
- Such a horizontal right would not be restricted to specific data types, but would build on the existing the horizontal right to data portability under GDPR.
- A horizontal data-sharing right could be implemented through a "Data Act 2.0".

Q24: Is a horizontal data-sharing right a feasible and desirable alternative to sectoral rights?

6.4 Level playing field

To enable successful data sharing and equitable access under a horizontal data-sharing right, the development of a horizontal data-sharing framework should be considered. A more fragmented implementation of data sharing in the short term can create a patchwork of frameworks for different (or within) datatypes. A horizontal data-sharing framework can serve as an undergirding basis or 'interoperability layer' that 'translates' between the different frameworks for sharing of financial and non-financial data. It can also serve to create harmonization over time, and help ensure that accessing different types of data would be subject to the same rules. A horizontal framework would be of particular relevance if a horizontal data-sharing right were introduced, as such an expansion of data-sharing possibilities would also increase the need for common rules for data sharing. Below, a high-level overview is provided of important components of a horizontal framework.

6.4.1 Development and governance

A horizontal framework would include agreements on how data is to be shared. Such a framework would lay down agreements for all participants in a data transaction to commit to, including for on Roles and responsibilities of different players in a data transaction, liability and dispute resolution, Conditions under which data can be accessed, Information security standards, data standards (syntactic, semantic and policy interoperability), infrastructure (API architecture, functionality and discoverability; common standards for smart contracts used in data transactions) and Identification and authentication.

Provisions in the DGA and Data Act provide a legal basis upon which a horizontal data-sharing framework can be based. The DGA lays down requirements for providers of data intermediation services, creating a regulatory basis for their role and responsibilities. The proposed Data Act includes requirements that would apply to all data-sharing regulations, for instance on compensation for making data available, data-access terms, and

dispute resolution.[68] The Data Act proposals also enables the Commission to request the European Standardization Organizations (ESOs) to draw up harmonized standards.

Further regulatory provisions may be needed in the future, for instance requirements around the authentication of data transactions. The European Commission could also be given additional powers to endorse - through implementing acts - specifications of the Data Act's requirements for data sharing. Such specifications can include provisions on legal liability, or standardized contract terms – including on compensation levels - that reduce the need for bilateral contracts between data providers and data users.

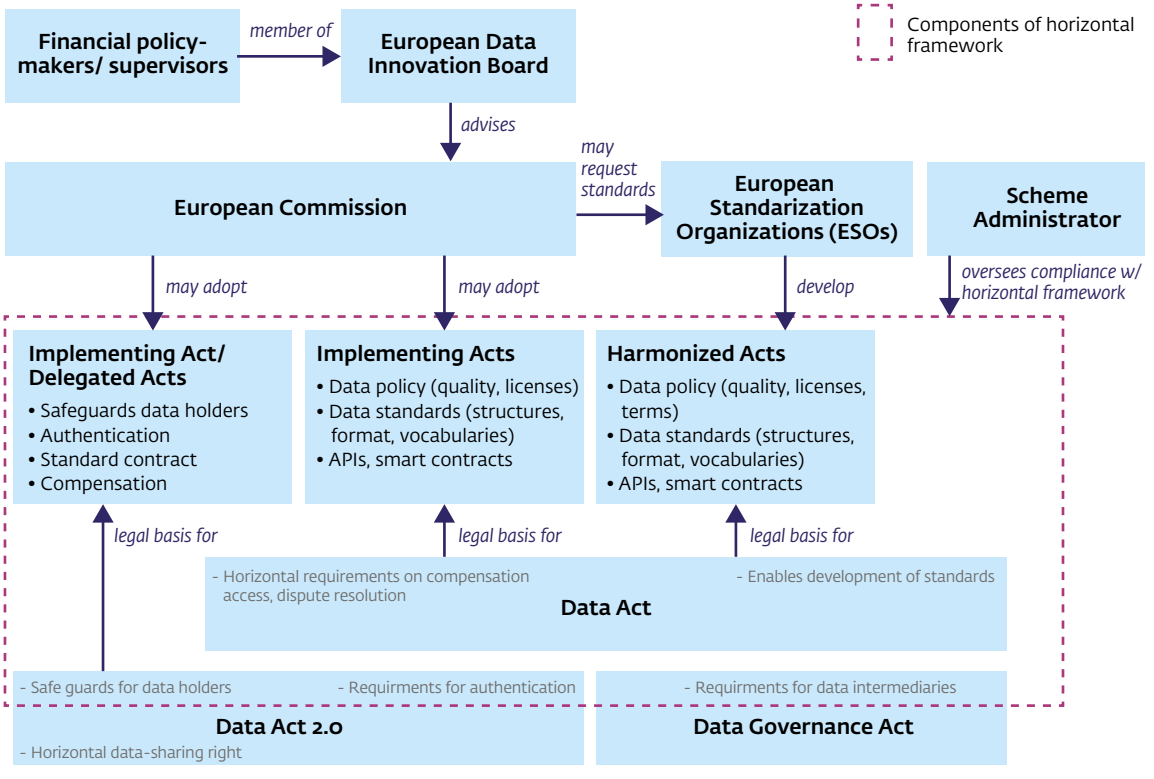
The European Data Innovation Board (EDIB) can coordinate the development of a horizontal framework. Under the DGA, EDIB is tasked with advising the European Commission on creating interoperability across data spaces and data-sharing initiatives. EDIB is to be chaired by the European Commission and will consist of relevant competent authorities from key sectors, and potentially also of private-sector stakeholders.[69] In the longer run, EDIB can be the core public-private collaborative body providing advice to the European Commission on further specifications and standards, and helping develop further specifications of the requirements laid down in the Data Act (2.0).Given this potentially pivotal role for EDIB, it is advisable that financial supervisors (e.g. ESAs) join EDIB - as is possible under the DGA.

6.4.2 Compliance with the framework

Compliance of the various participants with their respective responsibilities under the horizontal data-sharing framework can be periodically verified by external auditors in consultation with sectoral supervisors. Given that the number of participants in the horizontal data-sharing framework is likely to be high, it is unlikely that supervisors, including those for the financial sector, have sufficient capacity to certify all participants in a horizontal data-sharing framework. Moreover, many participants would not be subject to ongoing supervision. Therefore, the most practicable solution would be to require participants to have their compliance with the framework periodically certified by an external auditor, overseen by a scheme administrator. The relevant statutory supervisors - including financial supervisors - should be informed of the certification process and, where necessary, involved, for instance in the case of framework violations. It may be possible for the scheme owner to also become the dispute resolution body; this may be more practicable than creating separate bodies in each EU Member State.

68 Chapter III, EU Data Act https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0068
69 Article 26, EU Data Governance Act EUR-Lex - 52020PC0767 - EN - EUR-Lex (europa.eu)

Figure 5 – Overview Governance and components of proposed horizontal framework



Overview & Discussion Questions – Level playing field

- To underpin a horizontal data-sharing right, a horizontal data-sharing framework should be developed over time. Such a framework could serve to enhance interoperability, and ensure that financial entities (and other data users) would face the same rules, regardless of datatype.
- The framework can be based on DGA and Data Act and consist of common, horizontal agreements concerning business, functional, legal and technical elements of data sharing.
- The European Data Innovation Board could coordinate the development of the framework; and the European Commission could endorse the framework.
- Financial policymakers should actively contribute -e.g. through membership of EDIB - to ensure the framework is fit for purpose for the financial sector.

Q25: Do you believe a horizontal data-sharing framework is desirable and feasible?

Q26: How should the development of and compliance with a horizontal framework be organized?

Chapter 7 – Public provision of Data

In order to achieve the policy vision for data mobility, consideration should not only be given to the sharing of data belonging to individual data holders. The sharing of datasets, too, can be of importance to innovation and a level data playing field, including in the financial sector. Financial supervisors and central banks can consider their role in making data available.

7.1 Rationale for public provision of data

Concentration of datasets can provide a rationale for policy intervention and public provision of data. The AFM and DNB's policy vision on data mobility is aimed at mitigating market failures in data markets, to ensure that data holders' interests are safeguarded, (financial) innovation is enabled and a level data playing field is enhanced. While legislative data-sharing initiatives can play an important part in achieving this vision, they only pertain to the sharing of data of a single *individual* data holder. In general, data-sharing regulations do not mandate or regulate the sharing of data*sets* - i.e. sets that contain data of (many) different data holders. Such datasets, are, however, highly relevant to innovation and competition in the financial sector: data-related innovation often consists of reducing information asymmetries through the discovery of new insights into the preferences and risk profiles of consumers. Such innovation generally requires the use of data analytics and advanced statistical modeling. Sufficiently-large and -varied datasets are required to train such models.

As datasets are not covered by data-sharing regulations, their sharing occurs on a voluntary basis. However, as outlined in Chapter 2, entities that control these datasets will often lack the incentives to give broader access to them. This can thus result in the concentration of large datasets with a small number, or certain types of financial entities, and an unlevel playing field sector when it comes to data. In turn, this can have implications for competition in financial services, as data concentration can reinforce concentration in the financial sector, and stymie new entry and limit innovation.

Data concentration and its impact on innovation and competition could provide a rationale for public provision of data aimed at leveling the data playing field. In the context of the financial sector, this could include provision of data(sets) based on supervisory reporting data to a broader set of financial entities. The rationale for such public provision of data is strengthened data concentration negatively affects financial stability, or the attainment of important public-policy goals such as credit provision to the real economy, or climate-related objectives.

Public provision of data, however, is also associated with challenges and responsibilities that need to be carefully considered. First of all, the interests of data holders should be fully taken into account. In particular, privacy externalities have to be mitigated: any public provision must be fully in line with privacy regulations, and techniques that provide enhanced privacy assurance can be considered. In addition to protection of data holders, the (commercial) interests of the entities who have

Box 6 - Public provision of data by European financial supervisors and central banks

- *National credit registers:* in several Euro Area countries, financial supervisors or central banks are responsible for overseeing credit registers. The type(s) of financial entities required to contribute data to the register differs between countries.
- *AnaCredit:* the AnaCredit database is administered by the ESCB and contains loan-level information for bank loans to corporates. The data is reported by credit institutions on the basis of a harmonized data taxonomy. In several countries, central banks make data contained in the AnaCredit database available to financial entities.
- *Loan-Level Initiative*: under this initiative, the European Central Bank makes available granular loan-level information for asset-backed securities (ABS) that are accepted as collateral for Eurosystem monetary-policy operations. The objective is to enhance transparency of the securitization markets for the purpose of effective conduct of monetary policy. The Initiative, is operated by the European DataWarehouse (EDW).

provided the data - and any legal protections safeguarding such interests - as well as the effects on incentives to invest in data collection require careful consideration. This includes determinations regarding the type of entities to which data is provided, and at what level of granularity.

7.2 Public data provision in the financial sector

Public provision of data in the financial sector requires careful consideration. In addition to the aforementioned rationales, challenges and risks associated with provision of data, AFM and DNB also carefully weigh up the costs and benefits of such provision. Moreover, provision has to be in line with our respective mandates. DNB has a legal mandate to perform a statistics function, and to provide certain (statistical) data. This includes financial-sector data, sometimes based on supervisory reporting information.[70]

In the EU, financial supervisors and central banks have provided data, including based on supervisory reporting data. A substantial number of European financial supervisors and central banks have, over the past decade, increasingly made credit information available to financial entities. The provision is usually linked to the mandate of the relevant financial authority, such as safeguarding financial stability or the conduct of monetary policy (see Box 6).

In the Netherlands, too, public provision of data through the creation of a Credit Register for corporates is under active consideration.

70 See Mandate and collaboration (dnb.nl); Statistics (dnb.nl)

In February 2021, an analysis of the potential benefits of a Credit Register for corporates was published.[71] This analysis, which was commissioned by the Ministry of Economic Affairs, concluded that the creation of a Credit Register may have positive effects on the access to credit and can lower the costs of providing and accessing credit. Subsequently, the House of Representatives passed a motion requesting the government to start exploring the requirements to establish a Credit Register. While the exact scope and design of such a Credit Register has not yet been determined, the AnaCredit database could serve as the main data source. The AnaCredit database is managed by DNB and contains loan-level data that (if anonymized) could be returned to credit institutions that report to the Register.

By establishing a Credit Register, credit providers would be able assess the creditworthiness of firms more adequately at lower costs. Due to the provision of standardized information and by lowering information asymmetries, the Register will make it easier for credit providers to access necessary information to make an informed judgement on the creditworthiness of firms. Moreover, the Register could foster competition between credit providers by reducing information monopolies, which may induce further efficiency gains. Ultimately, this would not only lead to lower financing costs, but it also enhance financial stability and lower financial frictions that may impede the effectiveness of monetary policy transmission channels. Recently, the IMF has recommended the creation of a Credit Register for similar reasons.[72]

AFM and DNB are supportive of the proposals for a Credit Register for corporates and will continue to engage with policymakers on this subject. AFM and DNB will also consider other areas in which provision of data could in the future be possible, taking into account our mandates and weighing up the rationales, responsibilities and challenges, as well as the needs, costs and benefits associated with such provision.

71 OSIS (2021) Nut en noodzaak van een kredietregister in Nederland | Kamerstuk | Rijksoverheid.nl
72 IMF (2021) Article IV consultation Kingdom of the Netherlands

Overview & Discussion Questions – Data provision by public authorities

- Whereas data-sharing regulations like Open Finance enable the sharing of an individual data holder's information, they do not cover the sharing of (consolidated) datasets.
- Financial entities holding such datasets often lack the incentive to share. Such datasets constitute important strategic assets, as they can be used to train (powerful) statistical models.
- A lack of sharing can undermine innovation and entry, and lead to an unlevel data playing field for financial entities, which in turn can impede entry and reinforce concentration in financial markets.
- Such concentration can be a rationale for financial supervisors and central banks making data(sets) they have collected as part of their mandates available to (certain) financial entities. There are, however, significant risks and challenges that can come with such public provision, including (legal) considerations around privacy and commercial interests. These should be carefully considered and sufficiently mitigated.
- AFM and DNB will weigh up the, rationales, risks and challenges, as well as the needs, costs and benefits associated with public provision. AFM and DNB support the creation of a Credit Register for corporates, which will likely include loan-level data from the AnaCredit database.

Q27: What, if any, data should financial supervisors and central banks consider providing?

Annex - List of definitions

For the purpose of this Discussion Paper, a number of frequently-used terms will be defined as follows:

- **'Data'** as used in this Discussion Paper is an input, production factor or raw material in a particular process or task. Data is hence distinct from ideas, which can be identified as the blueprint or instruction to complete that task.[73]
- **'Personal Data'** refers to personal data as defined in the EU's General Data Protection Regulation (GDPR).
- **'Non-personal data'** as used in this Discussion Paper non-personal data means data that does not, or no longer, meets the above definition of personal data. This includes data that has been anonymized as set out under GDPR.
- **'Financial data'** refers to unprocessed data provided by, or generated by or on behalf of a data holder in the course of a regulated financial service
- **'Internet of Things (IoT) data**: data generated by a connected product. This data could be related to many different types of conent – data related to driving, to health, home activities, etc.
- **'BigTech' data**: refers to customer data (i.e. data provided by customers) that is controlled by gatekeeping platforms as regulated under the Digital Markets Act. This can pertain to social-media data, to (online) purchases on BigTech platforms, et cetera.
- **'Data sharing'** as used in this Discussion Paper, data sharing relates to the ability of data holders to grant third parties access to their data in an automated and ongoing manner.
- **'Data mobility'** refers to the ability to share data and obtain access to data in an automated and ongoing manner. This can be the result of data sharing; indeed in this instances data mobility and data sharing are used interchangeably in the Discussion Paper. However, data mobility also encompasses instances where a public authority (e.g. a financial supervisor) makes data it controls available to private-sector data users.
- **'Data holders'** refers to a legal or natural person that has the right to grant access to particular data, in line with the definition as used in the EU Data Governance Act.
- **'Data users'** refers to a legal or natural person that has the right to access particular data. This Discussion Paper follows the definition as used in the EU Data Governance Act.
- **'Data providers'** refers to a legal person that provide a data user with access to specified data under their control.
- **'Data-sharing regulations'** refer to legislative data-sharing initiatives: these are mandatory legal requirements implemented at a sectoral or potentially cross-sectoral level to enable data holders to share their data in an automated and ongoing[74] way with third parties. Examples of such framework, proposed or implemented, include data portability requirements under PSD2 or GDPR.
- **'Data-sharing right**': a legislative right for (certain types of) data holders to share their data in an automated and ongoing manner with a data user.

73 Romer (1990) Endogenous Technological Change on JSTOR
74 Normally through Application Programming Interfaces

- **'Data-sharing Framework':** a common set of agreements and rules - technical, operational, legal, business – on how data is to be shared. A data sharing framework can be specific to one data space or economic sector, or can span different data spaces and economic sectors.

DeNederlandscheBank

EUROSYSTEEM

De Nederlandsche Bank N.V.
Postbus 98, 1000 AB Amsterdam
020 524 91 11
dnb.nl