Financial data access

Position Paper DNB and AFM

DeNederlandscheBank
EUROSYSTEEM

AFM

Contents

This Position Paper sets out AFM and DNB's policy vision and priorities for data access

Policy action is needed to reap the benefits of data access, as well as to mitigate the potential drawbacks

Policymakers should prioritize actions that enable trusted, innovation-enabling and equitable data access

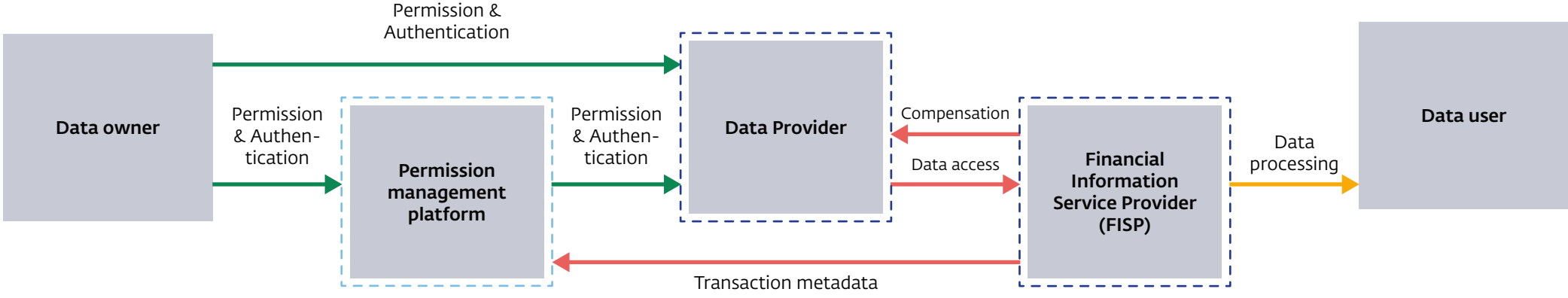
A balance should be struck between elements of data access that should be regulated cross-sectorally and those that can best be set on a sector-by-sector basis

Open Finance Regulation should promote innovation and a level data playing field, while it should also protect data owners through data ethics requirements for financial-data users

Additional requirements are needed to ensure that the use of data is in the interest of the data owner (customer)

Trusted, innovation-enabling and equitable access to (financial) data

Outline of the proposed roles, transactions and applicable regulations/frameworks



Entity regulated by Data Governance Act (DGA)

Entity regulated by Open Finance Regulation (OFR)

Transaction subject to GDPR and data ethics requirement

Transaction subject to horizontal guidelines

Transaction subject to SIF

Note: This diagram is only a first sketch.

This Position Paper sets out AFM and DNB's policy vision and priorities for data access

In recent years, various market and policy initiatives around data access have been proposed or implemented; in the Netherlands, in Europe and around the world. Some EU examples are: GDPR which enables data portability and PSD2 that introduced regulated automated and ongoing sharing of payment and account balance data after permission of the data owner. In the Netherlands, (market-led) initiatives around both sectoral and cross-sectoral data mobility have also been developed in recent years, for instance the Data Sharing Coalition.

Access to data is increasingly relevant for financial services: this is true not just of traditional financial data – e.g. payments, credit, insurance loss data – but also increasingly of non-financial data, such as energy, BigTech or IoT data. Such increased availability of data can provide benefits for consumers (data owners), as well as for providers of financial services (data users), but it can also present risks.

Data access initiatives, as currently being developed at EU-level, touch on AFM and DNB mandates. Data are used increasingly for the purposes of offering, pricing and administering of financial services. The way in which data are used impacts the interests of financial consumers and touches AFM's mandate to promote fair and efficient financial markets. As data is increasingly becoming a competitive asset, the ability to access data can also have implications for the (competitive) structure of the financial sector and DNB's mandate to maintain prudential stability of financial entities and ultimately the stability of the financial system.

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. The position paper should be read against the backdrop of the broader policy discussions relating to the new digital economy.

This Position Paper sets out AFM and DNB's policy vision and priorities for data access, in the context of the financial services value chain, with the aim of contributing to ongoing and future legislative discussions and initiatives related to data access. In September 2022 AFM and DNB published a Discussion Paper on this topic, containing a preliminary policy vision. Consultation responses were received from a diverse group of stakeholders, for which AFM and DNB are thankful. A summary of the consultation responses and AFM and DNB's reaction can be found in the Feedback Statement. Following the responses from and discussion with stakeholders, AFM and DNB now publish this Position Paper.

AFM and DNB's main message is – as in the Discussion Paper – that policymakers should prioritize actions that enable trusted, innovation-enabling and equitable data access. To ensure trust, it is vital that data can only be accessed with the consent of the data owner, and that safeguards ensure that data use results in outcomes that are in the interest of data owners. Enhancing the potential for data-based financial innovation requires that sufficient volumes and varieties of data – both financial and nonfinancial – can be shared and accessed. Ensuring equitable data access means subjecting different types of financial entities to similar rights, rules and requirements with respect to accessing data, while having the possibility to impose access restrictions on certain entities if access for them would cause harmful data concentration.

The main changes compared to the Discussion Paper revolve around the use of privacy-enhancing technologies, used definitions, and the balance between and implementation of horizontal and vertical measures. This Position Paper explicitly includes the use of privacy-enhancing technologies, particularly as discussions with stakeholders taught us that these technologies can help avoid sharing of data and help manage access to data, thus mitigating privacy and trust externalities. Furthermore, definitions used in this Position Paper (see also Annex I) have in places been altered to bring them in line with (final versions) of EU legislation and/or with definitions as used more broadly in policy discussions around data access. This is also why this position paper uses the term "data access" instead of "data mobility". And while the Discussion Paper stated that financial policymakers should contribute to the development of horizontal (cross-sectoral) measures in the medium- to long-term, while vertical (sector-specific) measures are more likely in the short term, this Position Paper aims to find a balance between horizontal and vertical measures that should be taken, as recommended by stakeholders, without distinguishing in time. Lastly, this Position Paper further details how such measures could be implemented.

The Position Paper starts by reviewing the potential benefits and drawbacks of data access. It then outlines AFM and DNB's policy vision and priorities. Finally, the Position Paper discusses the implementation of data access, both at the horizontal (across sectors) levels as specifically for financial-data sharing (Open Finance).

Policy action is needed to reap the benefits of data access…

Data access can generate substantial benefits for data users and data owners (Box 1), through the offering and consumption of innovative, personalized or competitive financial products and services, including embedded financial services. Data access also leads to better insight into behavioral patterns, and therefore to better risk assessments and a reduction in information asymmetries. For financial entities, data intermediation services can also be a new way to generate value for consumers as data mobility becomes more widespread.

Policy action is likely needed to maximize potential benefits of data access. Data is non-rivalrous - meaning a data point can be used in many different processes simultaneously without it being depleted. This means that enabling (broader) access to data can generate significant economic benefits (see also Box 1). However, given the competitive value of data, entities that safeguard data on behalf of their customers may be inclined to exert too much control, thereby obstructing other parties right to access this data. Therefore, to ensure maximum benefits of data access – and a level playing field – a regulatory right to access data in an automated and ongoing manner should be established.

Box 1 Potentional advantages of data access

Product innovation
- New data-related services
- New products or enhancing the value of current products

Competition
- New entrants have access to more data that enables them to compete
- Greater choice for consumers
- Greater opportunities for switching

Better Assessments & Inclusion
- Better assessment of risk and behavioral patterns of data owners
- Inclusion of groups that were previously excluded, by for instance making it possible to provide financial products to consumers for whom more traditional financial data is not available

Personalization
- More personalized advice, products and services

...and to mitigate potential drawbacks of data access

Public policy also has a role to play in mitigating potential negative (side) effects of enabling (broader) data access. These effects can significantly reduce the benefits of broader data access (see also Box 2).

Lack of meaningful data sovereignty can negatively affect data owners. Even if the data owner has to provide permission for the use of their data, a lack of understanding of the impact of sharing can cause negative externalities. In such a case, data owners are likely to suffer a privacy loss for which they are not adequately compensated.

Also data owners that have not provided access to their data could be affected. As long as correlations exist between data owners, insights gained through data access can be applied to data owners who have not shared their data. This enables greater price differentiation and discrimination, which can in turn lead to exclusion. Moreover, willingness to share data or not can itself become an input in pricing decisions.

Data access could enhance market concentration and undermine competition. The data starting point matters: entities that start off with large amounts of data can provide superior (personalized) services and attract customers and more data. Network effects can create winner-take-all outcomes.

Box 2 Potentional drawbacks of data access

Privacy

- Consumers are unlikely to be able to oversee the full impact of granting access, undermining privacy, even with permission

Data Security

- Data breaches affect not just the data owner involved, but overall trust
- When private companies do not take this broader negative impact into account, socially sub-optimal levels of investment in data security may result

Market Concentration

- Enabling access to more data could benefit large incumbents and cause too much market concentration

Financial Exclusion

- Data access could lead to greater price differentiation due to personalized pricing, and exclusion of certain high-risk individuals
- Data owners who have not shared data can thus be affected by others doing so

Policymakers should prioritize actions that enable trusted, innovation-enabling and equitable data access

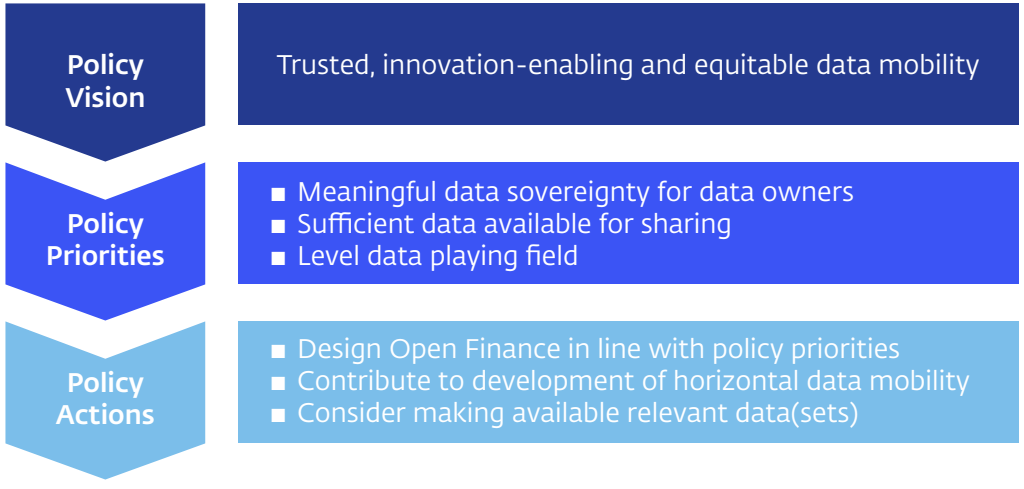
This Position Paper sets out AFM and DNB's policy vision and priorities on data access. The policy priorities are based on the vision and are considerations that should guide policymakers. Both the vision and priorities cover 3 key areas:

Trusted data access requires that data owners have confidence that they can control who has access to their data. It also means that data owners must be able to trust that the analyzes and outcomes resulting from data access are in their best interest. In order to ensure that the interests and trust of data owners are safeguarded it is vital that data can only be accessed with the consent of the data owner, and that additional safeguards are in place to ensure that data-use results in outcomes that are in the interest of data owners. The latter is also crucial for protecting the interests of data owners who have not shared their data, and to counter financial exclusionary impacts of data access. Additional safeguards refer to ethical frameworks on the use of data in combination with existing regulations such as the GDPR and the Duty of Care in financial legislation. Furthermore, 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. Privacy-enhancing technologies can also be of valuable use, particularly as these technologies can help avoid sharing of data and help manage access to data, thus mitigating privacy and trust externalities. An example of such a technology is Zero-Knowledge Proof (ZKP) functionality, which enables data users to validate information needed without receiving data that would provide them with additional (unintended) information.

Sufficient data should be accessible to enhance innovation. Legislative initiatives that create an obligation for data providers to share data they control with third parties – subject to approval of the data owner – are needed to enable the sharing of sufficient and sufficiently varied data.

A level data playing field implies equitable, but not necessarily equal, access to data. It would be desirable that any type of financial entity were able to access any type of data relevant for the provision of financial services, while avoiding negative impacts on market concentration. Hence, in AFM and DNB's view equitable access means that undue barriers to data access like a lack of standardization should be removed, while restricting access should be possible if there is a risk of data concentration.

Figure 1 Policy Vision, Policy Priorities, Policy Actions



Some elements of data access should be regulated cross-sectorally…

A horizontal basis that harmonizes requirements for various elements of data access across sectors is needed to ensure commonality in data access. These elements include permission management, identification & authentication, compensation principles (fair, reasonable, non-discriminatory and non-duplicative), data security, liability and conflict resolution (see figure 2).

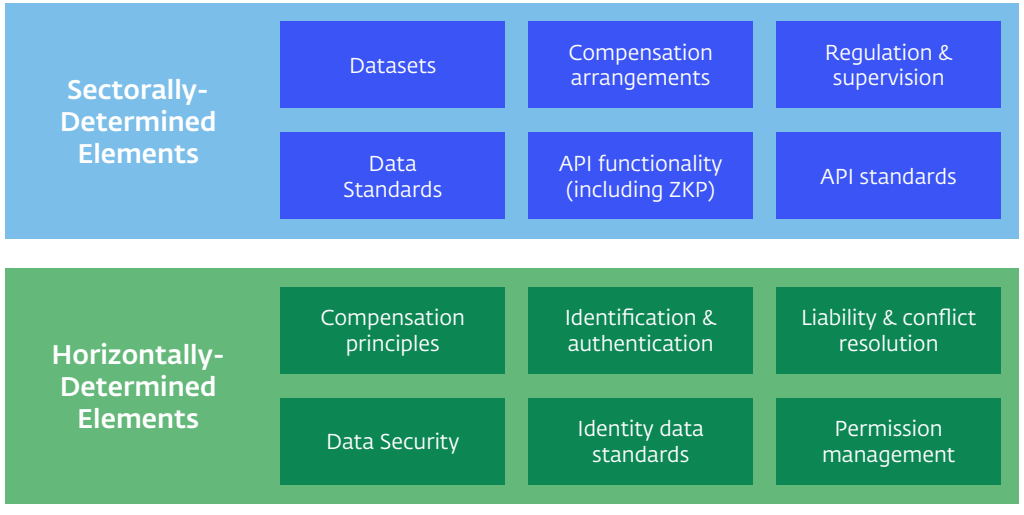
Strong Customer Authentication should be applied for the initial data transaction, with periodical reauthorization performed by the data user. Permission by the data owner must remain the basis for data access. The data user should be made responsible (and liable) for performing periodic (180 days) reauthorization.

Horizontal agreements on integration of eID schemes would help to enhance user experience. Enabling the use of external eIDs that provide a high level of assurance in data transactions should be made possible. Such eIDs would not only enable more efficient onboarding of new clients, but would make it possible for data owners to authenticate data transactions with different entities using a single set of credentials. Horizontal guidelines on user experience and integration ensure a level data playing field.

To enable permission management tools ('consent dashboards'), horizontal agreements should be made regarding reporting of data-transaction metadata. Cross-sectoral overviews of data access permissions empower meaningful data sovereignty. This requires that for each data transaction, metadata (e.g. identity data user, data owner, data provider) is made available to the consent dashboard provider, either directly by the data user or through a centrally logging of transaction data.

In addition to horizontal regulations such as Data Act and DGA, horizontal guidelines under the Data Act should be drafted by public and private stakeholders through the European Data Innovation Board (EDIB) and adopted by the European Commission. Sectoral (financial) supervisors should apply the guidelines. A horizontal Soft Infrastructure Framework (SIF) could also be created by EDIB to set standards on horizontal datasets, e.g. data-owner identifiers (name, address, data of birth, LEI codes), which are relevant across sectors.

Figure 2 Sectorally and horizontally determined elements

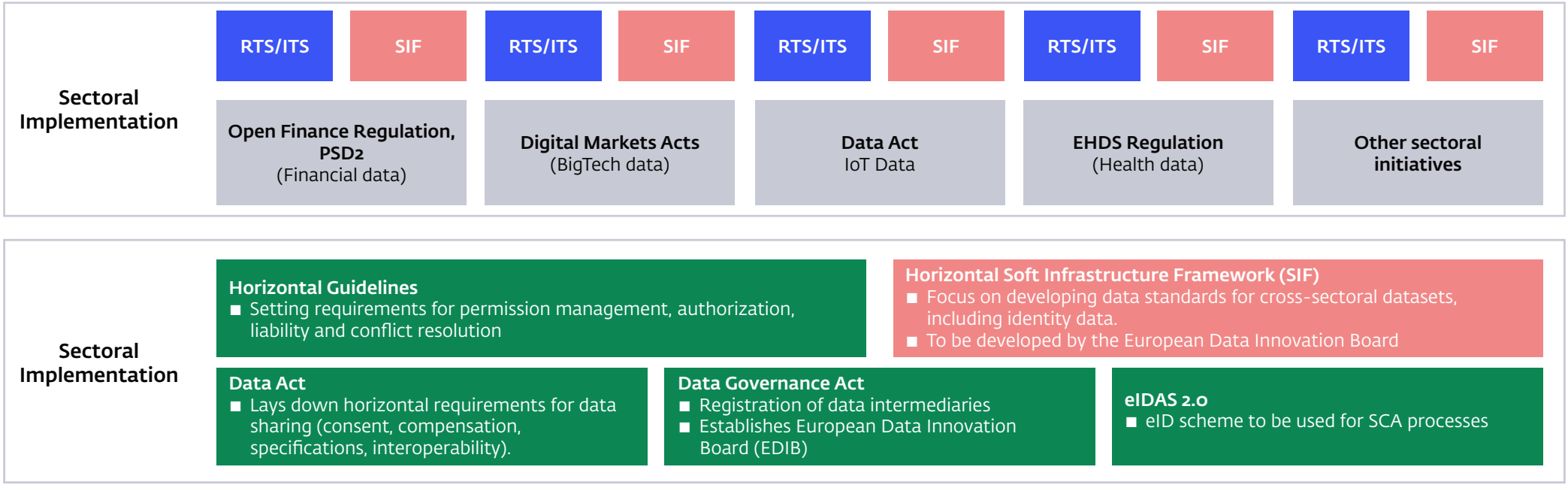


...while certain implementation elements can best be regulated on a per-sector basis...

Certain sector-specific parameters for data access for individual sectors – including financial services – can be set in sectoral regulation or frameworks. In particular, sectoral regulation can establish the basic right to data access for that particular sector and determine the precise datasets to be shared.

In addition, sectoral regulation can determine how technical standardization and compensation arrangements should be organized, e.g. through implementing legislation or through soft infrastructure frameworks that are drafted by public and private stakeholders (see figure 3).

Figure 3 A horizontal basis and sectoral implementation



Open Finance Regulation should promote innovation and a level data playing field…

Open Finance legislation should take the form of a binding Regulation: the Open Finance Regulation (OFR), which should regulate read access to financial data, including to payment-account information. Write access (providing financial services with the use of data) should be regulated in sectoral financial legislation, including payment initiation under PSD2.

OFR should not limit the purposes for which data can be used but open up datasets for sharing based on market demand and innovative potential. Via ITS and in consultation with stakeholders, relevant datasets provided by the data owner or generated in the course of a financial service consumed by the data owner as well as product datasets should be included in OFR. Highly-sensitive data – e.g. health insurance data – should be excluded. OFR should not limit the purposes for which data can be used, e.g. to specific use cases. However, use cases could be useful in identifying datasets that are to be prioritized in the implementation of Open Finance.

Financial-data users are to be regulated as Financial Information Service Providers (FISPs) and made subject to horizontal guidelines on data use and financial licensing and supervision. These firms should also comply with the DORA requirements and put in place the required cyber-security standards. FISPs would have to provide access to relevant financial datasets they may control. This ensures financial-data reciprocity.

Open Finance should regulate for an equitable data playing field relating to all datatypes relevant for financial services. To also ensure an equitable data playing field across all datatypes relevant for financial services, Open Finance should only permit entities covered by data-sharing provisions of the DMA and Data Act access to financial data if financial entities have obtained effective access to BigTech data under DMA and IoT data under the Data Act. In addition, the Commission should be able to reject access to entities if such access would create undue market power in the financial sector.

Box 3 Operationalizing OFR

Detailed implementation of OFR should occur in collaboration with stakeholders through multilateral Soft Infrastructure Frameworks (SIFs). Such implementation allows for greater flexibility and can improve incentives and functioning of Open Finance. These SIFs can be made responsible for working out specific specifications, particularly with respect to business (e.g. compensation arrangements) and technical agreements (data and API standards).

OFR should regulate for the parameters within which SIFs can operate. OFR should for instance enable compensation based on FRAND principles to create incentives for data providers to make it easier to share data and to invest in information security. To avoid undue proliferation of SIFs, OFR should set requirements for SIFs. They should:

- Represent a majority of Member States;
- Represent a majority of financial entities covered by a specific sharing requirement (i.e. for (a) particular dataset(s);
- Be in line with horizontal and sectoral requirements and interoperable with relevant other SIFs (e.g. horizontal SIFs)
- Where national-level SIFs are more appropriate – e.g. for IORPs, where markets are organized primarily at national level - OFR should apply the above requirements at national level, although sufficient interoperability with other schemes should be required.

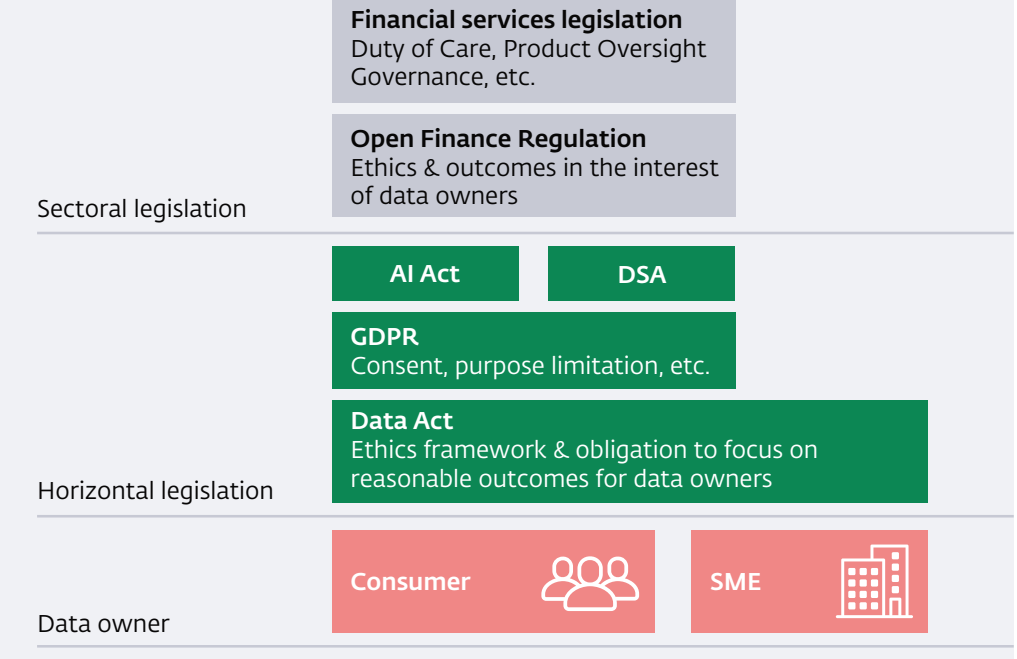
...and protect data owners through data ethics requirements for financial-data users

Data sovereignty through permission is unlikely to provide sufficient protection of data owners' interests: information asymmetries and cognitive limitations, for instance, may make it inherently difficult for data owners 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 – (see figure 4) 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, and preventing discriminatory biases in data use. But despite the aforementioned regulations plus sectoral regulations - such as the Duty of Care and Product Oversight Governance requirements for the financial sector - the risk of potential negative externalities of data sharing are not fully addressed.

A complementary focus is therefore needed in OFR on whether the outcomes of financial-data use are reasonable and ethical and in the interest of data owners and society overall. Ideally, horizontal legislation (such as the Data Act) would oblige data users to incorporate an ethics framework with a focus on ensuring outcomes that are in the interest of data owners or customers. In this way, additional protection not only applies to consumers, but also to SMEs (for which the GDPR does not offer protection). In the absence of a horizontal basis, it is important that this is still given a basis in the OFR. This can be done by requiring all financial-data users to draw up data ethics frameworks in which they set out parameters for reasonable use of data, e.g. what data is used for what processes, what impact on price differentiation and exclusion are acceptable.

It could be considered to exclude specific data sets from data access, where other measures are considered insufficient to safeguard data-owner interest.

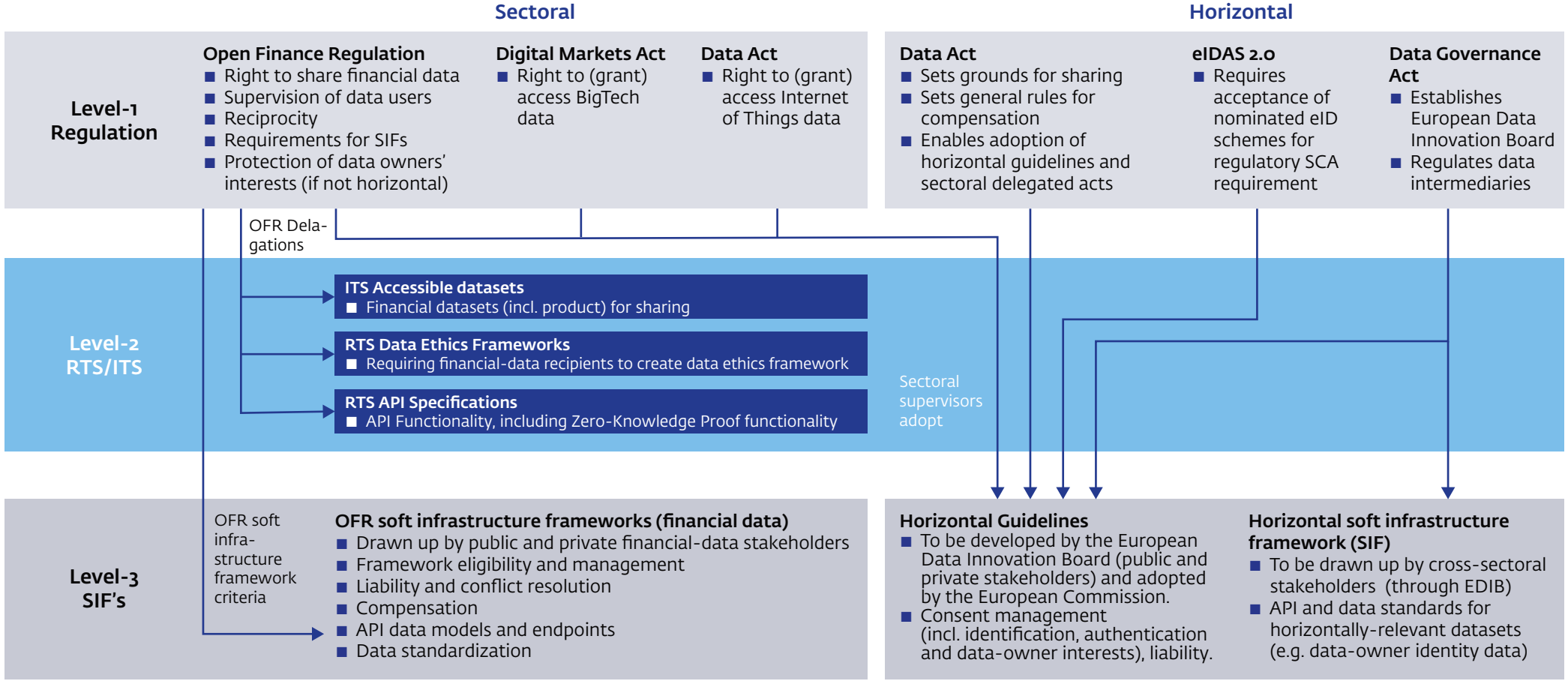
Figure 4 Applicable sectoral and horizontal legislation



Annex I – Definitions

- **Data:** as per Data Act (Art 2(1)): means any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording.
- **Data access:** means data use, in accordance with specific technical, legal or organisational requirements, without necessarily implying the transmission or downloading of data; as per Article 2(13) Data Governance Act.
- **Data owner:** a data subject or customer.
- **Data subject:** an identified or identifiable natural person, who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; as per Article 4(1) GDPR.
- **Customer:** a natural or a legal person who makes use of financial products and services.
- **Data holder:** a legal person, including public sector bodies and international organisations, or a natural person who is not a data subject with respect to the specific data in question, which, in accordance with applicable Union or national law, has the right to grant access to or to share certain personal data or non-personal data; as per Article 2(6) Data Act.
- **Data intermediary:** provider of data intermediation services as defined in Article 2(11) of Data Governance Act.
- **Data recipient or data user:** a legal or natural person, acting for purposes which are related to that person's trade, business, craft or profession, other than the user of a product or related service, to whom the data holder makes data available, including a third party following a request by the user to the data holder or in accordance with a legal obligation under Union law or national legislation implementing Union law; as per Article 2(7) Data Act.
- **Data consumer or data user:** a natural or legal person on whose behalf data is received and processed. Data consumer can be the same entity or person as the data recipient.

Annex II – Schematic Overview Legislative Proposals



De Nederlandsche Bank N.V.

PO Box 98, 1000 AB Amsterdam
+31 20 524 9111
dnb.nl

Follow us:

DeNederlandscheBank
EUROSYSTEEM