Proposal COM(2023) 360 of 28 June 2023 for a **Regulation on a framework for Financial Data Access** and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010, (EU) No 1095/2010 and (EU) 2022/2554

FINANCIAL DATA ACCESS

cep**PolicyBrief** 3/2024

LONG VERSION

Authors: Dr. Anastasia Kotovskaia, Philipp Eckhardt | kotovskaia@cep.eu
cep | Kaiser-Joseph-Straße 266 | D-79098 Freiburg | Telephone 0761 38693-0 | www.cep.eu

A. Key elements of the EU proposal

1 Context and objectives

- Digital technologies relying on data are increasingly transforming financial markets and giving rise to new data-driven business models, products and services [Recital 1]. However, at present, [Explanatory Memorandum, p. 1 and Recital 2]
  - customers of financial institutions regularly do not have effective control over their financial data, in the sense that they face difficulties in accessing this data and in deciding about sharing it with third parties,
  - third parties interested in the financial data of customers of financial institutions face hurdles in accessing this data, which is usually collected, stored, processed and ultimately held by the financial institutions.

  As a result, customers of financial institutions cannot benefit from data-driven financial products and services developed and provided by third parties based on data being shared by customers [Recital 3].
- According to the Commission, there are three main reasons for limited data access and sharing [Explanatory Memorandum, p. 1]:
  - a lack of trust among customers when it comes to sharing their financial data due to an absence of tools to manage data sharing permissions,
  - a lack of rules governing data sharing, i.e. the financial institutions holding the data are not always required to enable data access for third parties, and
  - a lack of standardization of the data and the technical infrastructure for data sharing, which drives up the costs of data sharing.
- Thus, in 2021, the Commission announced in a Communication on a "Digital Finance Strategy for the EU" [COM(2020) 591] that it wanted to put in place a regulatory financial data access framework in order to achieve advancements in data-driven finance and overcome the said limitations [Explanatory Memorandum, p. 1 and Recital 3].
- With the proposed Regulation on a framework for financial data access (FIDAR), the Commission wants to establish rules on the access, sharing and use of specific categories of customer-related financial data in order to establish a so called "Open Finance" ecosystem [Explanatory Memorandum, p. 5, Recital 4, Art. 1].
- The aim of the proposed Regulation is to [Explanatory Memorandum, p. 2, Recitals 6–9]
  - improve the economic outcomes of customers of financial products and services and of companies from the financial sector by enhanced adoption of data-driven business models,
  - empower customers of financial institutions to decide how and by whom their financial data can be used, also in order to enhance customer trust in data sharing,
  - facilitate access to customers' financial data by third parties enabling them to offer new innovative products and services.

  Thereby, the Commission wants to strike a balance between the seamless use of customers' data and preserving high level of privacy, security, safety, and ethical standards [Explanatory Memorandum, p. 1].

2 Scope

2.1 Included actors

- The Regulation applies to three different groups of actors: data holders, customers, and data users.
  - "Data holders" are financial institutions that gather, store and process the data of their customers ("customer data") [Art. 3 (5)]. "Financial institutions" (FIs) are, in particular [Art. 2(2)],
    - banks,
    - payment institutions (PIs),
    - electronic money institutions (EMIs),
    - investment firms (IFs),
    - crypto-asset service providers (CASPs),
    - managers of alternative investment funds (AIFM) and management companies of undertakings for collective investment in transferable securities (UCITSs)
    - (re-)insurance undertakings and insurance intermediaries, and
    - institutions for occupational retirement provision (IORPs).
  - "Customers" are the users of financial products and services provided by FIs. They can be natural or legal persons [Art. 3 (2)].
  - "Data users" are both FIs as well as "financial information service providers" (FISPs) who have lawful access to "customer data" having received the customer's permission [Art. 3 (6)]. FISPs are entities that,

when authorized under this Regulation, are allowed to provide "financial information services" based on customer data [Art 3 (7)].

- FIs may act as data holders, data users or both, while FISPs may only act as data users [Recital 17, Art. 3 (6) and (8)].
- This Regulation does not apply to, inter alia [Art. 2 (3)],
  - certain AIFMs with only a few assets under management alternative investment funds,
  - certain small insurance and reinsurance undertakings,
  - IORPs with pension schemes with no more than 15 members, and
  - (re-)insurance intermediaries that are micro, small or medium-sized enterprises.

2.2 Included data

- In general, the Regulation applies to "customer data". This data [Art. 3 (3)]
  - is collected, stored and processed by FIs as part of their business with customers,
  - includes data provided by customers as well as data generated through interactions between a customer and a FI, and
  - includes both personal and non-personal data.
- However, the Regulation only applies to certain categories of "customer data", including [Art. 2 (1)]
  - bank-related data, such as on mortgage credit agreements, loans, and savings accounts,
  - investment-related data, such as on investments in financial instruments, insurance-based investment products (IBIP), crypto-assets as well as in real estate,
  - insurance and pensions-related data, such as on pension rights under occupational pension schemes or on non-life insurance products,
  - creditworthiness assessment-related data with respect to loan application processes or credit rating requests by companies.

  This encompasses also [Recital 11, 13 and 14, Art. 2 (1) (b) and (e)]
  - sustainability-related information,
  - data collected for the purpose of carrying out suitability and appropriateness assessments of retail customers, and
  - data collected for the purpose of assessing the demands and needs of retail customers.
- The Regulation does not apply to the following categories of "customer data" [Recital 9, Art. 2(1)]:
  - data on payment accounts,
  - data on life insurance products,
  - data on sickness and health insurance products,
  - data on public pension products, and
  - data on creditworthiness assessments with respect to the loan application processes of consumers.

3 Obligations for data holders

- Data holders must make customer data available to customers upon their request. This must be done without undue delay, free of charge, continuously and in real-time. [Art. 4]
- Data holders must make the customer data of their customers available to data users without undue delay, continuously and in real-time. They must do so only [Art. 5 (1)]
  - upon request from a customer, and
  - for the purposes for which the customer has granted permission to the data user.
- Data holders must [Art 5 (3)]
  - ensure – before making customer data available to a data user – the latter has demonstrated that the data holder's customer has given permission for such data access,
  - make customer data available to data users in formats based on recognized standards,
  - ensure secure communication of the customer data to data users, and
  - respect the confidentiality of trade secrets and intellectual property rights.
- Data holders are responsible for the availability of an "interface" for the sharing of customer data. However, such an interface may also be provided by [Recital 24]
  - other FIs or a group thereof,
  - external IT providers,
  - industry associations or

  - public bodies of a Member State.

  Such an interface may, in case of IORPs, also be integrated into pension dashboards covering a broader range of information [Recital 24].

- Data holders have a right to get compensation from data users for making customer data available. This applies in case the data sharing takes place as part of a "financial data sharing scheme" (FDSS) (more on these FDSSs below). [Art. 5 (2)]

4 Obligations for data users

- Data users may access customer data only when authorized [Art. 6 (1)]
  - as an FI under other EU legislation, or
  - as an FISP under this Regulation.
- Data users may access customer data only for the purposes specified in the permission granted by the data holder's customer [Art. 6 (2)].
- Data users must ensure that [Art. 6 (2) and (4)]
  - they do not process customer data for purposes other than for performing a service requested by a customer,
  - trade secrets and intellectual property rights are preserved,
  - the storage, processing and transmission of non-personal customer data is secure,
  - mechanisms are in place to prevent any unlawful access or transfer of non-personal customer data,
  - customer data is not accessible by other group entities, if the data user is part of such a group, and
  - customer data is deleted once it is no longer required for the originally permitted purposes.
- Customers have a right to revoke any permission granted to a data user. Such revocation must be performed according to contractual obligations when processing of the customer data is necessary for the performance of a contract. [Art 6 (3)]

5 Permission dashboards

- Data holders must provide their customers with financial data access permission dashboards. These dashboards must, in particular [Recital 22, Art. 8 (1–3)],
  - be easy to reach and user-friendly,
  - enable customers to manage and monitor data access permissions granted to data users,
  - indicate the customer data categories being shared,
  - indicate the specified purpose of the permission,
  - indicate the duration of the permission's validity,
  - allow customers to withdraw a permission that has been given or re-establish one that has been withdrawn,
  - warn customers about potential contractual consequences of permission withdrawals,
  - provide for a record of withdrawn or expired permissions for two years.
- Data holders should [Recital 21]
  - not design their permission dashboards in a way that encourages or unduly influences customers to grant or withdraw permissions,
  - when providing their permission dashboards, refer to electronic identification services, such as European Digital Identity Wallets (see cep**PolicyBrief** on the revised eIDAS Regulation), and
  - rely on "data intermediation service providers" – as established in the Data Governance Act [DGA, Regulation (EU) 2022/868, see cep**PolicyBrief**] – for the provision of the dashboards.
- A data holder must notify a data user about any changes to a permission concerning that data user. For their part, a data user must notify a data holder of any new permission granted by a data holder's customer. [Art. 8 (4)]

6 Requirements for responsible data use

- Where customer data constitutes personal data, its processing must be restricted to the level that is necessary in relation to the purposes for which it is processed [Recital 18, Art. 7 (1)].
- Both the European Banking Authority (EBA) and the European Insurance and Occupational Pensions Authority (EIOPA) must develop guidelines on responsible data processing. This applies to products and services, where [Art. 7 (2) and (3)]

  - the credit score of a consumer is of relevance, and
  - in the case of life, health and sickness insurance products, risk assessment and pricing of a consumer is of relevance.

7 Financial data sharing schemes (FDSSs)

- Data holders and data users must join a "financial data sharing scheme" (FDSS), which governs access to customer data [Art. 9].
- Data holders and data users may be members of multiple FDSSs at the same time [Art. 9].
- The members of an FDSS are data holders, data users, customer organizations and consumer associations [Art. 10 (1) (a)].
- A specific FDSS must [Art. 10 (1) (a–c)]
  - include as members those data holders and data users that represent a substantial share of the market of a specific financial product or service,
  - ensure fair and unbiased representation of data holders and data users in decision-making and voting procedures,
  - ensure that its rules apply uniformly to all its members, with no unjustified preferential or differentiated treatment, and
  - be open to participation by any data holder or data user on objective terms.
- FDSSs must have in place [Art. 10 (1) (e–g), (i) and (j)]:
  - mechanisms to amend its rules,
  - rules on transparency and, where deemed essential, on reporting,
  - common standards for data and technical interfaces,
  - rules on contractual liability of its members, and
  - systems for dispute resolution.
- Any FDSS must be in compliance with EU rules on consumer protection, data protection, privacy and competition [Recital 25].
- Within any FDSS, models must be established to determine the maximum compensation that a data holder is allowed to charge for making data available to data users. Any such compensation must, in particular [Art. 10 (1) (h)],
  - be reasonable,
  - relate to making the requested data available,
  - be objective, transparent, and non-discriminatory, and
  - be geared towards the lowest level in the specific market.

  The compensation must not exceed cost of making the requested data available, if the data user is a micro, small or medium-sized company.
- After joining a specific FDSS, a data holder must notify its national competent authority about its participation within one month. Also, within one month of setting up an FDSS, the national competent authority for the Member State in which the three most significant data holders are established, must be notified about the establishment of the FDSS. [Art. 10 (3–5)]
- National competent authorities must check whether the FDSS is compliant with the Regulation's requirements. On conclusion of such a check, they must inform EBA about the FDSS's establishment. The specific FDSS is then considered to be recognized in all Member States. [Art. 10 (6)]
- Data holders and data users must join an FDSS within 18 months after the Regulation has entered into force [Art. 9]. If, within a reasonable period of time, there is no FDSS for a certain category of customer data, the Commission may adopt a delegated act to lay down the modalities for how data holders are to make such customer data available to data users. This includes specifying [Art. 11]
  - common data and technical interface standards,
  - the compensation model, and
  - contractual liability of the entities involved in data sharing.

8 Authorization and operating conditions of FISPs

- FISPs may only access customer data as data users if they are authorized by the national competent authority of the Member State where their registered office is established. In their application for authorization, they must lay down, in particular [Art. 12 (1) and (2)],
  - the type of data access envisaged,
  - their business plan,
  - their governance arrangements and internal control mechanisms,
  - their internal procedures for security incident monitoring, handling, follow-up and reporting,
  - their business continuity arrangements, and
  - a security policy, describing, e.g., the security control and mitigation measures in place to protect customers against identified risks; such measures must ensure a high level of digital operational resilience in compliance with the requirements set out in the Digital Operational Resilience Act [DORA, Regulation (EU) 2022/2554, see cep**PolicyBrief**], in particular, with respect to technical security and data protection.
- FISPs must also demonstrate in their application that they have in place [Recital 32, Art. 12 (2)]
  - governance arrangements and internal control mechanisms for the use of information and communication technology (ICT) services,
  - security incident reporting mechanisms, and
  - procedures to test and review their ICT business continuity and ICT response and recovery plans,

  which are in compliance with the requirements set out in the DORA.
- FISPs may only be authorized, if, inter alia,
  - the information and evidence accompanying the application complies with the requirements mentioned above [Art. 14 (1)],
  - they have robust, comprehensive, and proportionate governance arrangements for their services, e.g., clear organisational structure and effective risk identification, monitoring, management and reporting procedures [Art. 14 (3)],
  - any possible outsourcing arrangements they conclude does not render them a letterbox entity or constitute a means to circumvent the Regulation's provisions [Art. 14 (5)].
- Any competent authority must decide upon an application for authorization within three months [Art. 14 (6)]. It may withdraw such authorization, if a FISP [Art. 14 (7)]
  - fails to make use of the authorization within twelve months,
  - ceases to operate for a period exceeding six months,
  - no longer meets the authorization requirements, or
  - poses a consumer protection or data security risk.
- FISPs must hold a professional indemnity insurance or a comparable guarantee enabling them to, in particular, cover possible liability due to non-authorized or fraudulent data access or use. Alternatively, they may hold initial capital of € 50,000. [Art. 12 (3)]
- FISPs must adhere to the following organizational requirements. They must, in particular [Art. 16],
  - establish policies and procedures enabling them to comply with the Regulation,
  - employ systems, resources and procedures enabling them to preserve the continuity of critical operations,
  - take steps to avoid undue operational risks in case they rely on third parties providing critical functions,
  - ensure that their directors, management and other responsible persons are of good repute and have sufficient expertise.
- FISPs established in a third country must designate a legal representative in a Member State, if they want access to financial data in the EU [Art. 13 (1)]. The third-country FISP must be authorised by the competent authority of the Member State, where the third-country FISP intends to access data. The authority must [Art. 14 (2)]
  - check, whether the FISP complies with the Regulation's requirements as well as whether it has designated a legal representative, and
  - set up an appropriate cooperation arrangement with the third country authority responsible for the FISP.
- EBA must set up a register with information on the [Art. 15 (1)]
  - authorized FISPs,
  - the established FDSSs, and
  - FISPs that want to access financial data in Member States other than their home Member State.

9 Supervision and enforcement

- Member States must designate the competent authorities with supervisory, investigatory, and sanctioning powers [Art. 17].
- Competent authorities may, in particular, [Art. 18 (1) and (2), Art. 20]
  - require any natural or legal persons to provide them with the information required to carry out their tasks,
  - conduct investigations of those natural or legal persons established or located in the Member State concerned,
  - in order to avoid the risk of serious harm to consumers, remove content or restrict access to an online interface, or order that such an interface display a warning, or be removed, disabled or restricted, and
  - impose administrative penalties and other administrative measures.
- Competent authorities may impose, inter alia, the following administrative penalties and measures [Art. 20 (3)]:
  - public statements on the infringement and the natural or legal person responsible for it,
  - ordering the cessation of the infringement,
  - disgorgement of profits gained or losses avoided due to the infringement, and
  - temporary suspension of the authorization as a FISP.
- Competent authorities may also impose administrative fines. In general, the maximum fines for [Art. 20 (3) (f) and (4)]
  - legal persons are
    - € 50,000 per infringement and a total of € 500,000 per year, or
    - 2% of their total annual turnover;
  - natural persons are € 25,000 per infringement or a total of € 250,000 per year.

  Competent authorities may, however, exceed these amounts up to a maximum fine of twice the amount of profits gained or losses avoided due to the infringement [Art. 20 (3) (e)].
- Competent authorities may also impose periodic penalty payments in case of ongoing non-compliance by a natural or legal person. Such payments must be made on a daily basis until compliance is restored. They must be imposed for not more than six months. A maximum payment imposed may amount to [Art. 21 (1)]
  - € 30,000 for natural persons, and
  - 3% of the average daily turnover for legal persons.
- Competent authorities must, when deciding on administrative penalties or measures, take into account, in particular, the [Art. 22]
  - seriousness and duration of the violation,
  - financial strength of the legal or natural person,
  - losses incurred by third parties due to the violation, and
  - impact of the violation on customer interests;
- Member States may establish rules to allow their competent authorities to close investigations on [Art. 19]
  - alleged breaches of the Regulation via settlement agreements to avoid having to commence with formal sanctioning proceedings,
  - established breaches of the Regulation via an expedited enforcement procedure to facilitate a swift decision on imposing an administrative sanction or measure.

10 Interlinkages with other EU law

- The Regulation "complements and specifies" the requirements of Regulation (EU) 2023/2854 on harmonized rules on fair access to and use of data [Data Act, see cep**PolicyBrief**]. Thus, the Data Act's requirements also apply to data sharing under this Regulation. [Recital 47]
- Basically, the General Data Protection Regulation [GDPR, (EU) 2016/679, see cep**PolicyBrief**] applies to personal data processing. The proposed Regulation does not alter the access and portability rights of data subjects regarding their personal data as provided for in the GDPR[1]. Even when a customer has granted a

[1] In contrast to the approach of the proposed Regulation, the GDPR's data portability right is limited to personal data, only applies, when technically feasible, and access must not be granted continuously and in real-time. Furthermore, it does not prescribe any standards for the sharing of financial data.

data user permission to access his financial data, the data user must comply with the requirements on the lawfulness of personal data processing under the GDPR (see Art. 6 GDPR). Data users may only process shared personal data where there is a valid legal basis (see Art. 6 (1) GDPR) and, if applicable, where the requirements on the processing of special categories of data (Art. 9 GDPR) are met. [Recital 48]

- The Regulation builds upon and complements the requirements on "open-bankingunder the second Payment Services Directive [PSD II, (EU) 2015/2366, see cep**PolicyBrief**] and its proposed revision [COM(2023) 366 and COM(2023) 367] that already regulates access to payment account data [Recital 49].
- FIs within the scope of this Regulation are already subject to the rules of the DORA Regulation [(EU) 2022/2554, see cep**PolicyBrief**]. With the proposed FIDA Regulation, FISPs are also now included in the DORA Regulation. Thus, all data holders and all data users will be bound by the requirements of the DORA Regulation. [Explanatory Memorandum, p. 8, Recital 32, Art. 35]
- The Regulation is, furthermore, interlinked with the [Explanatory Memorandum, p. 2 and 3]
  - Data Governance Act [DGA, Regulation (EU) 2022/868, see cep**PolicyBrief**] that provides for rules to foster trust in data sharing, ensure interoperability between data spaces and create a regime for data intermediation service provision,
  - Digital Markets Act [DMA, Regulation (EU) 2022/1925, see cep**PolicyBrief**] that, inter alia, allows FIs on behalf of their customers to access data held by gatekeepers, and
  - proposed regulations of the EU Retail Investment Strategy [RIS, see cep**Study** (in German only)].

11 Date of application of the Regulation

- The Regulation applies [Art. 36]
  - 18 months after the date of its entry into force with respect to the requirements on FDSSs and the authorization of FISPs, and
  - 24 months after the date of its entry into force for all the other requirements.

B. Legal and political context

1 Status of legislative procedure

28.06.2023	Adoption by the Commission
Open	Adoption by the European Parliament and the Council, publication in the Official Journal of the European Union, entry into force

2 Options for exerting political influence

Directorates General:	DG Financial Stability, Financial Services and Capital Markets Union
Committees of the European Parliament:	Economic and Monetary Affairs, Rapporteur: Michiel Hoogeveen (ECR, NL)
Federal Ministries:	Finance (leading)
Committees of the German Bundestag:	Finance (leading)
Decision-making mode in the Council:	Qualified majority (acceptance by 55% of Member States which make up 65% of the EU population)

3 Formalities

Basis for legislative competence:	Art. 114 TFEU
Form of legislative competence:	Shared competence [Art. 4 (2] TFEU)
Procedure:	Art. 294 TFEU (ordinary legislative procedure)

C. Assessment

1 Economic Impact Assessment

1.1 General assessment

In our everyday lives, consumers, companies, and organizations constantly feed incumbent FIs – be it banks, insurance companies, asset managers or others – with an enormous amount of personal and non-personal information. This can happen at any time: during the contract initiation process, on conclusion of a contract, while onboarding or during the lifetime of the contract. In a digitized economy, access to and control of such information plays an ever-increasing and decisive role for those institutions in being able to offer competitive products and services. This is especially true of financial products and services as, according to the Commission, among the various sectors their providers use data the most.[2] Having said that, the availability of data and the control of it by only a few actors – here: incumbent FIs – may come at a cost. It may, for instance, inhibit market entry, limit competition, result in less customer choice, lack of innovation, too few products and services tailored to the needs of corporate or private customers, and may act as a factor driving market concentration.

The Commission's proposals on a Financial Data Access Regulation (FIDAR) is, in essence, a means to reduce such costs since it envisages the breakup of those "data bottlenecks" and opens up the data trove for wider use by both FIs customers as well as interested third-parties, such as other (non-incumbent) FIs or financial information service providers (FISPs). It rests on the assumption that the "value of secondary data reuse [by customers and eligible third parties] for the society as a whole [is] larger than the private value of primary data use [solely by incumbent financial institutions]".[3] Or, in other words, the data trove should not stay with incumbent FIs alone but should be exchanged, shared and reused more widely in order to reap their full potential for the whole economy.

Such an approach has some valid reasoning from an economic point of view. First, the wide use of customer information may be associated with economies of scale as data gathering and processing often involves high (initial) fixed costs but low (subsequent) marginal costs. Furthermore, the value and quality of a data-based good regularly increases with the availability of such data. Economies of scale can therefore justify and support the increased utilization of data, hereby counteracting market concentration tendencies and lowering market entry barriers. Second, data controlled by one market participant may be used by several other participants without losing its value (also for the initial holder of the data). In that sense, it may be regarded as a non-rivalrous good that can serve as the input for multiple use cases, as consumption of the data by one party does not restrict another party's ability to consume the same good. If informational goods incorporate such characteristics, it may be welfare-enhancing not to restrict their use but to actively promote their exchange and further use as they may be considered a public good.

However, there may be other, equally valid economic reasons for not using financial data. Not all such data can be regarded as a public good calling for widespread data reuse. Data may, in fact, obtain the characteristic of a club good as with the number of (potential) users, its value – for the incumbent financial institution, but also for third parties – may decrease (at some point). Although financial data cannot be "overused", each additional user of a certain dataset reduces its value for other users, as one must generally assume a limited number of possible new products and services offerings build upon a certain data set(s) – even with a high level of innovation. Limiting the amount of (potential) data users can therefore make sense in order to retain its value. This is particularly true as incumbent financial institutions are often regarded as both club owners and club members. The character of data as a club good may thus make it worthwhile to limit financial data exchange and reuse in order to maintain the incentives for the data holders – here: incumbent FIs – to invest in its production. Enhanced exchange and reuse would mean having to share the benefits of data production with third parties risking the loss of a competitive edge vis-à-vis those parties.

As a consequence, any political or regulatory measures to promote open finance must try to strike the right balance between, on the one hand, opening up data bottlenecks to overcome inefficient underusage of finance related information and, on the other hand, restricting widespread usage to ensure sufficient investment in data production in the first place. In the battle between on the one hand a strictly proprietary and, on the other, a rigorously open access approach, the FIDAR proposal tends to advocate in favour of the latter. Seemingly, the Commission believes the incentives for incumbent financial institutions to be strong enough that (a) they won't

[2] Impact assessment, p. 7.
[3] Impact assessment, p. 6.

refrain or reduce data gathering activities even though they must fear having to share the value of those activities with others and (b) that measures created by incumbent FIs to "unlock informational vaults"[4] are necessary.

In the following, we want to dive into the Commission's regulatory approach more concretely to judge whether or not it can be regarded as economically sound:

In future, the Commission wants to oblige a multitude of FIs, as holders of various customer-related data ("data holders"), to make such data available to their respective customers, upon their specific request. Furthermore, for their part, the customers may give permission to the data holders to share the said customer-related data with third parties ("data users"), i.e. other FIs and/or financial information service providers ("FISPs"). The Commission justifies these requirements in particular by arguing that they give FI customers "effective control over their financial data"[5] and allow them to reap the benefits of the "development and provision of data-driven financial products and financial services"[6] by data users due to customer financial data being shared with them.

In general, in markets driven by effective competition, it could be expected that different (incumbent) FIs, who were able to create informational vaults, would need to provide financial products or services with various attractive models for data access, sharing and reuse in order to attract the interest of potential customers. This should at least be the case if the said customers have an inherent interest in utilizing the locked-in financial data themselves or in entrusting them to further data users for the provision of any added-value products or services. FIs deciding against offering such a model would have had to fear losing customers and, ultimately, would have risked a market exit. In such a scenario, there would be no need for any regulatory intervention like that being envisaged.

Nonetheless, with the proposed Regulation, the Commission now seems to conclude that there is no such effective competition for the best data access, sharing and reuse model(s). Firstly, it suggests that there exist market failures across the whole range of FIs, regardless of their respective products or services offerings. And, secondly, it suggests that such failure also applies to any type of (potential) customer, be it a company or a consumer. Such universal, undifferentiated judgement, however, seems unconvincing. Not in any case one may observe an unassailable market power on the part of data holders that would prevent customers from gaining data access or data transfer rights. There is no indication of any irreconcilable information asymmetries between data holder and customer that would impede the latter's ability to make an informed financial product or service purchase decision compatible with his data usage-related preferences. And also, there is no indication of any such strong negotiation position on the part of a data holder that would allow him to force potential customers to conclude data-related contractual agreements that are unfavourable to the latter.

As a consequence, the envisaged overarching and indiscriminate regulatory concept seems flawed:

First, while one may agree that data access and sharing rights are justifiable with respect to customers that are consumers, this is not the case with respect to business customers. Whereas the former may lack sufficient information, fail to pay enough attention or fully grasp the full implications of deciding for or against a financial product or service and their incorporated data access and sharing possibilities and, furthermore, may not be in a position to "dictate" contract terms, this is not true of professional costumers. It may be assumed that they are able to reduce alleged information asymmetries, decide upon "fair" contract conditions and be in a more favourable negotiation position. It may even be the case that an FI as data holder has to follow the demands of its professional customer rather than the other way around. Thus, the proposed Regulation should differentiate between B2C and B2B scenarios, leaving the latter out of the scope since no comprehensive market failures are observable.

Second, obliging a multitude of FIs – as data holders – to provide for data access and transfer options for all of their financial products and services, irrespective of any identified market failure for their respective offerings, is disproportionate. Such a general duty encroaches unjustifiably upon their entrepreneurial freedoms, gives rise to costs and ties up resources for the development and maintenance of data access/transfer infrastructures and interfaces and may, ultimately, lead to increases in prices of the data holder's products or services. If, at the same time, no demand materializes for access to specific customer data from either customers or potential data users, the build-up of such data sharing ecosystems is simply redundant. Ultimately, such a general and overarching duty may in fact incentivize FIs to design less (customer-)data driven financial products or services. This, however, would go against the spirit of the proposed Regulation. Consequently, to be justified, the proposed Regulation should, at least, be much more tailored to those financial products or services that have a realistic chance of attracting interest, both from customers as well as third parties, to make (innovative) use of accessed customer

[4] Awrey, D., & Macey, J. (2023). The Promise & Perils of Open Finance. Yale J. on Reg., 40, 1.
[5] Recital 2.
[6] Recital 3.

data. Only with such a more focused approach – looking at promising use cases[7] –, can the FIDA Regulation be a success. Otherwise, disproportionate regulation could result in a waste of resources creating unused and costly data sharing ecosystems. This scenario should be avoided.

1.2 Scope of the Regulation

Furthermore, with regard to the broad scope of both the FIs and data categories included, there is a need for several clarifications, specifications as well as adaptions to the concepts chosen. This includes:

- clarifying the term "customer". This seems necessary because for some financial products and services the party "making use" of them is not necessarily the party that has a contract with the FI. This may apply for instance to insurance or pension products, where there are policy holders or beneficiaries. Ultimately, the FIDA Regulation should make clear that only natural persons, with whom FIs have a contract, will be considered as "customers";
- specifying the customer data categories falling within the scope of the FIDA Regulation to provide for legal certainty. Currently, the proposed Regulation includes some data categories, which (a) may not be deemed financial data – like real estate related data –, and which are not generally held by FIs themselves[8] and (b) are ambiguous, e.g. when referring to customer data on any "other related financial assets". Thus, FIs covered by the Regulation may, in their capacity as data holder, regularly be confused or in doubt about whether, and if so, how, they have to provide data access;
- making sure that "customer data" within the scope of the Regulation does not go beyond "raw data", thereby excluding data that is generated or processed by FIs and thus objectively qualifies as "derived or inferred information".[9] The legislature must ensure that where raw data has been somewhat enriched by an FI, it is voluntary rather than obligatory to share this data. Such a restriction is fundamental. Otherwise, investment incentives on the part of incumbent FIs with respect to data-driven financial products or services would be jeopardized and their innovation potentials unduly diminished. Clearly, data users may often be interested in such enriched data and sharing them may incentivize competition on secondary markets. However, it would be an invitation to engage in free-rider behaviour by building innovative data-driven financial information services on efforts undertaken by the initial data holder(s). The exclusion of derived or inferred data would, thus, ensure that data users who receive data based on customer permission still endeavour to generate innovations on the basis of the data received;
- finding a more suitable and coherent approach concerning the handling of "sensitive" financial data. In general, many consumers are reluctant to share specific categories of private financial data at all due to their sensitivity, e.g., data on their health status or creditworthiness. This is understandable not only from a privacy perspective but also with respect to the potential risk of exclusion or discrimination.[10] Exclusion of such sensitive financial data – as envisaged for data related for life insurance, sickness and health insurance products and creditworthiness assessments with respect to consumer loans – from the scope, is therefore welcome. Only then, can sufficient trust be built up, especially on the part of consumers, in the appropriateness of the FIDA framework. Nonetheless, limiting the exclusion to these specific insurance products and creditworthiness assessments seems incomplete as there are many other financial products and services where sensitive data play an equally decisive role (e.g. accident insurance). As a result, it would be advisable not to concentrate on the exclusion of specific products or services deemed "sensitive" a priori, but to provide for a non-exhaustive list of sensitive customer data categories to be excluded from the scope of the Regulation. Such a list would be established directly in the Regulation by the legislature, while the three European Financial Supervisory Authorities – EBA, ESMA and EIOPA – could be tasked with (a) specifying the list in a more granular manner, and (b) adapting the list, in case new sensitive data types arise or others become less sensitive, via delegated acts;
- adding a definition of "financial information services". Currently, the Regulation leaves open, what kind of services this term encompasses. As a result, there is much room for interpretation of the kind of offerings

---

7 To identify such use cases, the Commission should consult all involved actors – financial institutions, customers and fintech companies – interested in becoming a FISP.

8 As a result, they are not the holder of such data and thus, their inclusion is unnecessary.

9 Concretely, "customer data" should, first, be restricted to data provided by the customer intentionally. Second, it should encompass data directly arising out of interactions between the data holder and the customer, when the latter makes use of the financial product or service. However, such "interaction data" should not encompass data that is actively created or enriched by the FI. In this sense, legislature must clarify what is meant by "data generated as result of customer interaction", which forms part of the "customer data" definition.

10 Increased exchange of particularly sensitive financial data may, for instance, result in a higher potential for differential pricing of financial products and services, often detrimental to vulnerable and/or low-income customer groups. Furthermore, some customer (groups) may be squeezed out of markets, when their risk status is unsatisfying or when they decide against sharing their data.

FISPs may provide. However, this must be made clear in order to align the regulatory requirements – i.e. authorization or organisational requirements – which FISPs need to fulfil, with the specific risks that their services could pose. In any case, if such financial information services also consist of services that are currently only provided by regulated FIs under sector-specific EU financial law, FISPs should, when providing those services, need to be subject to such a law;

- limiting data sharing duties for customer data relating to suitability and appropriateness tests, as well as demands and needs assessments, which are an integral part of advisory processes on financial and insurance products, to the customer data that has been collected but not enriched by FIs during such processes, and only to data categories deemed non-sensitive;
- reconsidering the strategy to exempt certain smaller FIs from the scope of the proposed Regulation. Clearly, such measures are meant to avoid overburdening them with costly regulation. However, firstly, such exemptions may create distortions of competition between large and small FIs, which are not justifiable. Second, they are, built to a certain extent on the assumption that it is harder for customers and potential data users to gain access to the customer data held by large FIs than that held by small FIs. This interpretation assumes that big FIs are more sophisticated when it comes to conditioning data-utilization options for themselves. However, such an assumption is too simplistic. For example, small FIs can also provide specialized financial products or services and have a dominant position in a specific market segment. Thus, the distinct regulatory treatment of small and large FIs is not, in any case, appropriate. Furthermore, it may even be in the vital interests of (some) small FIs to be covered by the Regulation. This could be the case, inter alia, where potential customers develop a strong preference for offerings that provide the most suitable data access and sharing possibilities. In such a case, they may be driven out of the market if they are unable to provide this in the data exchange ecosystem created by the proposed Regulation. As a result, if the legislator is not including small FIs in the scope of the Regulation from the outset, it should at least allow these FIs to opt-in, i.e. allow them to voluntarily abide by the Regulation's requirements and, thus, for instance, to become members of FDSSs as well;
- clarifying, whether a data user, if it is an FI and has received customer data based on a customer's permission, will "automatically" become a data holder itself, when it collects, stores, and otherwise processes the data obtained. As such interpretation may have grave repercussions and legal certainty is at stake, the legislature should come up with a more unambiguous legal provision.

1.3 Obligations for data holders

Data access right for customers

As elaborated in section 1.1 of the Economic Assessment, we reject the Commission's approach of introducing a broad data access right for customers of FIs. Only where such customers are consumers, could this be justifiable. Irrespective of these general reservations regarding the obligation for FIs to make data available to their customers upon request, we also question the envisaged requirement for them to do so "without undue delay, free of charge, continuously and in real-time". Although such data access may strengthen the customer's legal position vis-à-vis incumbent FIs and increase customer trust and confidence in subsequent data sharing activities, it is nevertheless ill-suited.

First, there is no justification for a "free of charge" data access right for customers, particularly but not solely with respect to business customers. The making available of data by FIs and the related establishment of data access interfaces and infrastructure does generate costs for FIs. Thus, if FIs are unable to recover those costs by charging any fees for making data available, they may either need to raise the price of their products or services or reduce data collection in the first place. Such a "free of charge" approach may be particularly problematic where a large number of customers refrain from making use of their access rights at all.

And second, "continuous and real-time" data access does not make sense for each and every financial product or service within the scope of the FIDA Regulation. This is because, for many such products or services – think of insurance or pension products – the generation of customer data does not occur constantly, but only occasionally. Thus, continuous and real-time access should only be compulsory where it is plausible and of relevance. Otherwise, there may also be the risk of customers being permanently confronted with potentially less valuable data deliveries by data holders after they requested data access.

Data access right for data users

As also stated above (section 1.1.), we also have doubts about the requirements for FIs to pass on customer data to interested data users, upon their customer's request. Clearly, such sharing of customer data may serve several tangible purposes – e.g., foster competition, stimulate innovation, facilitate financial product/ service switching, lower market entry barriers, potentials for more tailored and personalized product/service offerings, or an easier management of the customer's personal finances. Nonetheless, such an "obligatory" transfer requirement can

only be warranted when specific customer data that raises the interest of certain data users can be classified as a "significant input factor" deemed “essential” for the provision of a specific downstream product or service. Such essentiality can only, however, be taken for granted when the input factor – here: customer data – is indispensable for the production of the downstream good. This requires that the potential data user is unable to resort to other actual or potential inputs; i.e., any kind of substitute data. In addition, the potential data user must be effectively unable to develop the input factor itself; i.e., the technical, legal or economic obstacles to build up a data trove comparable to that of the data holder must be so strong that the potential data user is not in a position to do so. Furthermore, any potential denial by the data holder of access to customer data must de facto lead to an eradication of competition on downstream markets. However, if those criteria are not fulfilled, the duty for data holders to share customer data, goes too far, may result in simple free-rider behaviour by potential data users, reduces the value of investments made in data utilization by data holders and, ultimately, could prove counterproductive as data holders incentives for developing data driven financial products or services may diminish. Consequently, the regulatory approach taken by the Commission to bolster customer data exchange is too far-reaching and not sufficiently targeted.

On a positive note, the Commission allows data holders to obtain compensation, not only from their customers, but also from data users, for making customer data available to them (no “free of charge” delivery requirement). This takes account of the investments made and costs incurred by the data holders for providing data access facilities and ensures a fair distribution of the many expenses involved in creating the financial data sharing ecosystem.[11] On a negative note, again, the obligation to transfer customer data to data users on a “continuous and real-time” basis is flawed and should be adapted in line with data access by customers (see above). Furthermore, it must be made clear that data holders may also claim compensation from data users where data sharing takes place outside of FDSS.[12]

1.4 Obligations for data users

The requirement for data users only to be allowed to access customer data when authorized by competent authorities should be warmly welcomed. Such an obligation is straightforward for several reasons. First, it increases trust among the customers of data holders, and especially consumers, that their data are only being used by entities subject to a proper supervisory framework. Second, the fact that both types of data user – FIs under their respective sector specific EU regulatory frameworks and FISPs under the proposed FIDA Regulation – need an authorization, ensures, in principle, that they act on an equal footing and that there is, in this regard, a level-playing field. And third, it is decisive for ensuring the integrity of financial markets as it helps to avoid potentially sensitive financial data being (mis-)used and exploited by market participants that are outside the financial market’s regulatory radar. Moreover, it is welcome that the proposed Regulation foresees an authorisation regime for third-country FISPs that have to comply with the same requirements as EU FISPs, and therefore aims to ensure the same standard of treatment for data in the EU regardless of the FISP’s country of origin. However, the current proposal does not fully consider the risks stemming from third-country FISPs (see section 1.8).

Permissions by data holders’ customers

The restriction that data users can only access customer data when customers have granted their permission and that they can only use accessed data for the purposes specified in the permission, is crucial for the success of the FIDA Regulation. Currently, there is often a strong reluctance among FI customers to share their (financial) data at all. This has to do with fears regarding privacy and (personal) data breaches, a perceived lack of control over when and to what extent their (financial) data is used and by whom, concerns with respect to data and cyber security as well as risks related to financial exclusion. Thus, putting customers in the driving seat and allowing them to decide on the utilization options of third parties is appropriate as it may increase customer confidence in the fact that data sharing possibilities are being used for their benefit.

Trade secrets and intellectual property rights

The obligation for data users to respect the confidentiality of trade secrets and intellectual property rights when customer data is accessed is appropriate as it preserves the willingness of data holders to invest in and innovate data-driven financial products and services, and maintains the incentive for business customers to participate in data sharing ecosystems. Nonetheless, a more straightforward measure would be – as in the Data Act[13]

[11] The “compensation” topic is dealt with in greater detail in section 1.7.

[12] Art. 5 (2) is unclear in this respect. It could be understood to mean that the right to get compensation only applies to data sharing within FDSS.

[13] See Art. 4 of Regulation (EU) 2023/2854.

(see cep**PolicyBrief**) – to allow data holders to withhold or suspend access to specific data that involves trade secrets, if they can demonstrate that a data user's measures to preserve data confidentiality are insufficient and that the data holder could suffer serious economic damage from disclosure of the data. In addition, a data holder may often lack possibilities for monitoring whether a data user is maintaining the confidentiality of accessed data as well as for enforcement measures in the event of non-compliance. Thus, there should be requirements applicable to data users specifying the kind of safeguards they must put in place to preserve trade secrets, and provisions enabling data holders to take action against data users if they handle the data negligently.

Restriction on transferring customer data to other group entities

The proposed prohibition, preventing data users from making customer data available to other entities within the data user's group, increases customer confidence in data sharing in the sense that their data is not simply and unknowingly distributed to other market actors. It also prevents circumvention of the regulatory framework as customer data cannot be easily transferred to unregulated non-FI or non-FISP market participants outside the FIDA Regulation. However, the envisaged prohibition should not be incontrovertible. If a customer voluntarily agrees that its data can be shared with other group entities, is able to make an informed decision in this regard, and the said entities are authorized and supervised either as FIs or FISPs, such a transfer should be possible.

1.5 Reciprocity

According to the proposed Regulation, any FI falling within its scope may be a data holder, a data user or both. Thus, within an FDSS, FIs have to make data available and may also be able to access data from other FIs. On the other hand, FISPs are only data users by definition. They can never become a data holder and are not obliged to reveal their data troves vis-à-vis FIs. Thus, a mismatch exists which needs to be resolved, as illustrated by the following example: A certain company applies for authorization as a FISP which, when granted allows the company to request customer data from a certain FI, based on the permission of the FI's customer. Having received the customer data, the company may combine it with other inhouse data – stemming from its core business – to provide a certain financial information service. By contrast, an FI acting in its capacity as a potential data user, is unable to receive customer data from such a company and, as a result of this lack of data, may not be able to provide a similar financial information service. To overcome such a scenario, FISPs must also be obliged to make their respective customer data available to FIs. Such a step is necessary to avoid competitive distortions to the detriment of FIs and to ensure a level-playing field.

1.6 Permission dashboards

The obligation for data holders to provide their customers with permission dashboards empowering them to effectively manage and monitor for whom, when and for what purpose data users can access and use their financial data is crucial for upholding and fostering trust among customers when it comes to the sharing of their data. Permission dashboards can be an effective means to ensure confidence and can provide customers with much-needed reassurance that they can retain control over their data. Irrespective of this generally positive assessment, the legislature should give further thought to two aspects. First, if each and every data holder were to provide for their own permission dashboards, consumers and companies that are customers of multiple FIs would be confronted with numerous different dashboards on a daily basis. The more FIs they have a contract with, the harder it would be for them to keep an overview of the permissions that have been granted, withdrawn or re-established. Thus, user experience with such a plethora of dashboards may suffer and could, ultimately, undermine the willingness of customers to participate in open finance. Second, with the existence of, potentially, multiple different dashboards, based on different standards and using different interfaces, the exchange of permission-related information between the three actors involved – data holders, customers and data users –is likely to be overly complex, costly and prone to failure. As a consequence, the legislator should advocate for solutions allowing FIs that offer similar financial products and services, and that deal with comparable types of customer data, to collaborate on developing such dashboards and agreeing on common standards in order to find joint or at least similar dashboard solutions. Such cooperation may at least be advisable within the evolving distinct FDSSs, where different data holders and data users come together for the exchange of specific types of customer data.

Role of electronic identification services

Recourse to electronic identification services[14], including European Digital Identity Wallets (EDIWs, see cep**PolicyBrief**), by data holders when providing permission dashboards may serve as an effective means for all

[14] Electronic identification services enable users to identify themselves digitally to a third party, make use of services which require identification and/or submit credentials digitally.

actors involved in a customer data sharing process to ensure that the identity of the person granting a permission actually matches that of the data holders' customer. This increases (legal) certainty and reduces potential liability risks for both data holders and data users. To ensure effective competition between providers of any digital identification solution, the legislature should, however, abstain from promoting public solutions – EDIWs – over potentially more straightforward private solutions. Data holders should be free to decide, whether to use an identification service at all, and if so, whether to use an EDIW or a private service. This seems warranted to uphold incentives for private digital identity providers to stay within the market and search for innovative solutions.

Design of permission dashboards

With the provision specifying that data holders are not allowed to design their permission dashboards in a way that would encourage or unduly influence customers to grant or withdraw permissions, the Commission wants to avoid them being nudged towards decisions that may not be in their own best interests, but actually (only) in those of the data holders. Such a restriction on data holders' ability to rely on so called "dark patterns" is appropriate. Due to the high sensitivity of a lot of financial data, restricting dark patterns that try to manipulate customers, is of major importance when it comes to increasing customer confidence and giving them control over their data. However, to increase legal certainty regarding the involvement of data holders in dark-pattern behaviour, it would seem advisable for the legislature to transform the provision from a non-binding recital into a binding article.

1.7 Financial data sharing schemes (FDSSs)

Promoting the development of financial data sharing schemes (FDSSs) is a welcome step towards removing some of the existing barriers to data sharing in the financial sector. This is because such FDSSs can bring together all relevant market actors allowing knowledge and expertise to be pooled, the development of common technical standards and data formats to be facilitated, and the agreement on joint contractual terms and conditions to be eased. Consequently, FDSSs may bring about a reduction in transaction costs for data holders and data users compared to data sharing based on bilateral agreements.

Obligation to participate in FDSSs

Thus, the promotion of FDSSs as pursued by the Commission, and the aim that the default solution should be for the sharing of customer data as specified under the proposed Regulation to take place within FDSSs, is laudable. Nonetheless, there may be cases, where the forced participation of both data holders and data users in such schemes is not worthwhile. This can occur, inter alia, where there are only a few potential users of specific customer data, i.e., a lack of demand, in case of niche markets or highly specialized financial products or services. Then, the resources needed to establish a specific FDSS would not usually justify the potential return on its creation for both data holders and data users. In such defined cases, there should remain room for agreements outside FDSSs. In order to ensure consistency and to avoid creating misaligned incentives, however, data exchange outside of FDSSs must follow similar requirements as that within FDSSs. In this regard, the legislature must clarify two important aspects. It should specify that the exchange of customer data will still be allowed outside such schemes, e.g., via bilateral contractual agreements, and clarify in which cases this should be permitted.[15] Second, it should specify more concretely the requirements governing non-FDSS data sharing. This relates, especially, to the question of whether data holders may claim compensation from data users in such a case. If not, data users would lack the incentive to join an FDSS as they could receive the data outside the schemes for free. In order to avoid such a situation, data holders should be allowed to claim compensation from data users in non-FDSS scenarios.[16]

Market- vs. state-driven approach with respect to FDSSs

The proposed Regulation envisages several rather high-level guiding requirements and principles with regard to the establishment, design and structure of FDSSs. It gives involved market actors a high degree of freedom to decide upon transparency and reporting rules, data and interface standards and on determining liability issues. Thus, it advocates a bottom-up rather than a top-down approach. The Commission seems to trust in the wisdom

[15] According to Art. 9, both data holders and data users are obliged to join an FDSS and only such FDSSs would govern the access to customer data. Thus, data users may only gain access to customer data when they are a member of a FDSS. On the other hand, according to Recital 50, access, sharing and using data may also take place on a contractual basis, not referring to the Regulation's requirements.

[16] According to Art. 5 (2), data holders may claim compensation from data users "only" if the customer data is made available to a data user within an FDSS. Furthermore, Recital 50 states that the model for determining the level of compensation should be defined as part of the FDSSs. Thus, this could be read that data holders are not allowed to claim compensation from data users in case data sharing takes place outside of FDSSs (if still allowed).

of the market instead of presuming that the state knows best when it comes to finding the most suitable data sharing ecosystems. This is to be welcomed. Due to both data holders and data users being equally represented in such a scheme and having a say in its creation and about its governance, the risk for biased solutions to the detriment of one side of the market will also remain relatively low. Consequently, the Commission's approach allows, in principle, for the evolution of suitable solutions, a high degree of adaptability and market neutrality, and avoids any politically driven distortion of competition. Clearly, there may also be risks to such a – mainly – market-driven approach. First, it could result in the establishment of various FDSSs within the EU with a highly diverse universe of governance rules, inconsistent technical standards and data formats and disparate compensation agreements. Second, different FDSSs may lack interoperability inhibiting data exchange between customers. And third, data holders and users required or desiring to participate in several FDSSs will have to abide by different requirements and agreed conditions, thereby increasing their data-sharing-related expenses. To dampen such – not to be underestimated – risks, while not completely abandoning the envisaged market-oriented regulatory approach, it may be advisable to establish one or several high-level forums. Such forums should be established prior to the adoption of the FIDA Regulation and consist, inter alia, of affected and involved FIs, FISPs, standardization bodies and the EU Commission in order to develop some guidance, common principles and minimum standards on the governance of FDSSs. Preferably, such guidance, principles and standards should be spelled out in advance to allow for the swift evolution of FDSSs thereafter, taking account of the fora's recommendations.

Rules on compensation for data access

The fact that data holders will be able to receive compensation from data users for making customer data available within an FDSS is, in general, appropriate. It maintains incentives for data holders to establish high quality data access infrastructures and interfaces and prevents free rider behaviour by data users. Limiting compensation to a "reasonable" level which, furthermore, must be geared towards the lowest level in the specific market[17] is, however, flawed. Clearly such a provision is intended to prevent the failure of data sharing with potential data users due to excessively high remuneration. Nonetheless, in a social market economy, it should primarily be up to the involved parties to agree on the respective data exchange conditions. A limit on compensation should only be considered an option where the data holder has unassailable market power. Furthermore, the proposed Regulation leaves open, what is meant by "reasonable" compensation, i.e. what kind of costs related to data sharing can a data holder include in calculating it. If the data holder can only claim compensation for making specific data sets available to a certain data user, this may not reflect many of the other related costs. In particular, data holders would be left with the costs related to the build-up of customer-friendly interfaces, permission dashboards and infrastructure or expenses for enabling data sharing based on dedicated data formats. Ultimately, any remuneration should reflect such efforts as well as allowing for data sharing based on fair conditions for all parties involved. In this regard, the most suitable and coherent solution would be to make reference to the compensation requirements laid down in the Data Act (see cep**PolicyBrief**) which entered into force only recently. Those requirements provide for compensation that not only includes costs related to making data available, but also with respect to investments in the collection and production of data. Furthermore, they allow for a margin that remunerates the data holder for its efforts in collecting the data in the first place.[18]

Where a data user is a micro, small or medium-sized company, the proposed Regulation stipulates that data holders must restrict compensation to a level not exceeding the costs incurred in making the requested data available. The "reasonability" is no longer the guiding criterion. The alleviations for such potential users aim to reflect the inferior negotiating power of those companies. Such favourable treatment should be rejected. First, it undermines data holders' incentive to share data in a sophisticated and value-enhancing manner. Second, it leaves them stuck with losses that increase the more smaller data users they have. Third, it distorts competition between larger and smaller data users, privileging the latter unjustifiably. Fourth, such an approach is a biased one. It rests on the postulated assumption that data users that are micro, small or medium-sized companies are always weaker in data sharing negotiations than data holders. Yet, data holders that are members of an FDSS may also be small, and many small data users could work together to build a strong negotiating position vis-à-vis the data holder. Thus, the Commission's approach lacks consistency and reciprocity in this regard. It is, furthermore, particularly jarring because the group of data users in line for this "special" treatment, which also includes medium-sized companies, is very large, thus transforming the general rule – "reasonable compensation"

[17] In this regard, it is also highly questionable, who determines and how to determine such lowest level. Both are highly ambiguous and create legal uncertainties.

[18] See also Recital 47 and Art. 9 of the Data Act [Regulation (EU) 2023/2854].

– into a special rule. As a result, the envisaged special compensation-related provisions for micro, small or medium-sized companies should be dropped altogether.

Timeframe for joining an FDSS

The obligation for data holders and data users to join an FDSS within 18 months of entry into force of the proposed Regulation is, to put it mildly, challenging. The limited timeframe is unrealistic since it has to include the whole process of agreeing on establishing a certain FDSS, clarifying its member structure and its overall governance, the subsequent development of the FDSS in practical terms and, finally, its introduction. Data holders or data users who want or are required to be a member of several FDSSs may find it particularly hard to comply as they will be forced to deal with several, potentially quite diverse "joining" processes in parallel. Furthermore, right after entry into force of the proposed Regulation, there could be a high level of uncertainty among the market actors about which FDSSs are ultimately going to emerge. There will initially be a trial run, which will also delay any decision. The timeframe should, thus, definitely be extended, to account for these obstacles. In addition, the Commission's right to establish an FDSS by itself via delegated acts, where there is no FDSS for a certain category of customer data within a reasonable period of time, must reflect such an extended timeframe for the market-led implementation of FDSSs. Also, there must be, at least, three clarifications. First, the legislature must make clear what is meant by a "reasonable period of time". This is necessary to provide legal certainty for data holders and data users as to when they have to expect such a top-down public solution. And second, before adopting such a top-down solution, there should, at first, be a deeper assessment regarding the reasons for the "failure" of a market-led implementation. Only where such a failure is well-founded and there is no reasonable expectation of finding a market solution in due time, should the Commission be allowed to act itself by adopting delegated acts to provide for an FDSS.

1.8 Authorization and operating conditions of FISPs

The different types of FIs – i.e., banks or insurance companies – are entities that are heavily regulated and supervised within the EU. They must abide by numerous pieces of horizontal and sectoral EU legislation to be allowed to provide their various financial products and services. Only allowing FISPs to provide financial information services based on customer data delivered by FIs, if they fulfil specific authorization, organization and operation requirements, is thus pivotal for ensuring that irrespective of who is undertaking a certain business, the same rules apply to the respective market actors. The requirements are crucial for enabling business to be conducted based on a level playing field for all market actors. Furthermore, only allowing market actors that are properly regulated and supervised to access – potentially sensitive – financial data is crucial to build and maintain trust among FI customers in relation to data-sharing. Also, it is crucial to uphold other paramount targets of European financial market regulation, like safeguarding financial stability and market integrity. Thus, establishing authorization and operating conditions for FISPs is absolutely appropriate. Yet, the legislature must clarify one crucial issue. The scope of the FISPs' business must be spelled out more clearly in advance. Right now, both the possibilities as well as the boundaries of their potential activities are unclear as we lack an unequivocal definition of "financial information services". However, in order to design the authorization and operating conditions in a sufficiently adequate manner, proper knowledge is required about the kind of services they are (not) allowed to offer. In the end, if "financial information services" simply mirror existing financial service offerings, provided by already regulated FIs, a separate authorization and supervisory regime would not be necessary and FISPs should be required to comply with the respective FIs' regulatory regime.

Compliance with the Digital Operational Resilience Act (DORA)

Forcing any FISP applying for authorization under the proposed Regulation to demonstrate compliance with the requirements of the Digital Operational Resilience Act (DORA, see cep**PolicyBrief**), e.g., with regard to ICT-related governance, internal control, security incident reporting as well as business continuity mechanisms and procedures, is appropriate. Naturally, FISPs should have an interest in safeguarding the digital operational resilience of their respective business as any loopholes in such resilience may damage their reputation and pose the risk of losses. However, such loopholes may often have wider negative repercussions that a single FISP alone may not sufficiently factor into its decisions. This includes potential risks of financial stability in case of a failure of ICT systems or a more general erosion of customer confidence in data sharing in case of data breaches. Thus, the requirement on DORA compliance ensures that FISPs take into account those considerable external benefits it provides. In addition to that, it preserves a level playing field between FIs, who already have to comply with DORA, and FISPs.

Treatment of FISPs from third countries

The proposed Regulation allows both authorized FISPs that are established in the EU as well as authorized FISPs that are established in a third country, and that have designated a legal representative in a Member State, to access customer data (subject to the customer's permission). This approach should be reconsidered for several reasons. First, there is a risk of distortions of competition. While third country FISPs may get access to data from customers of FIs in the EU, FISPs in the EU may not get equivalent access to data from customers of FIs in the third country. Thus, third country FISPs may be able to offer competitive financial information services in the EU, while EU FISPs may not be able to do so in the third country. However, only where reciprocity between the jurisdictions is guaranteed, and EU FISPs are, in general, allowed to access data from the customers of FIs in the third-country, should the legislature allow FISPs from third-countries to access EU customer data. Second, the fact that the designation of a legal representative will be sufficient to get data access – and no establishment of the third country FISP in the EU is required – raises supervisory and customer protection questions. Although, the national competent authorities are required to authorize third-country FISPs, check whether they comply with the Regulation and set up cooperation arrangements with third countries' authorities, they may, ultimately, lack the means and powers to ensure compliance and enforce the Regulation's requirements vis-à-vis those third country FISPs. However, this further distorts competition and could in addition undermine customer trust. To get a grip on those flaws and make the regulatory framework future-proof, the legislature should consider making two tweaks. It should only allow third country FISPs to get data access if they are established in the EU. And it should consider establishing some kind of "equivalence regime" comparable to those established in other EU financial sector laws. Referring to such a regime, the Commission would, based on the adoption of delegated acts, determine whether a third country provides for an open finance regime with options and safeguards similar to the EU's framework and, equally important, similar access possibilities for EU FISPs. If this is the case, the regulatory framework of the third country could be deemed equivalent, and the FISPs of said third country would get the chance to gain access to EU customer data and to provide their services in the EU.

Treatment of large platform services ("gatekeepers")

Another issue hotly debated in the context of the FIDA Regulation is the role of "gatekeepers", i.e., large providers of core platform services as designated under the Digital Markets Act (DMA, see cep**PolicyBrief**).[19] Those gatekeepers could, if interested, apply for authorization as a FISP and, if granted, could – in a relatively easy manner[20] – obtain financial data from the FIs' customers.[21] As a consequence, they may utilize and combine the received data with the data troves they have built up with their core businesses, which could reinforce their dominant market positions even further. In contrast to the recently adopted Data Act (see cep**PolicyBrief**)[22], the proposed Regulation does not provide for any restriction of gatekeepers with respect to access to customer data. Such a comparatively relaxed approach towards gatekeepers should, however, be welcomed, even if the opposite approach might be expected from a political perspective. This is because a differentiated treatment between gatekeepers and other potential data users would give rise to distortions of competition. Furthermore, if gatekeepers have to stay on the outside, customers would be confronted with less choice with respect to new and innovative financial information services. In addition to that, it limits the customers' ability to decide with whom they want to share their financial data. Finally, it must be kept in mind that a gatekeeper's entity that acts in its role as an authorized FISP as data user but is part of a group of companies may not share accessed customer data with other group entities. Data may only be accessed by the entity of the group that acts as a data user.[23] Thus, the legislature should stick to the Commission's stance on allowing gatekeepers to access finance-related customer data via a FISP license. In case serious competition issues arise after the adoption of the Regulation, those matters should be tackled primarily by competition law or within the realm of the Digital Markets and not within a specific law on financial data access.

1.9 Supervision and enforcement

The establishment of a supervisory and enforcement regime that consists of competent authorities checking whether the involved market actors are properly applying the Regulation's provisions, and providing the

[19] As of today, there are six gatekeepers designated under the DMA. These are Alphabet, Amazon, Apple, ByteDance, Meta and Microsoft (see here).

[20] The burdens for gatekeepers to receive an application as FISP are mostly lower than applications as FIs.

[21] A recent joint report by the three European Supervisory Authorities (ESAs) depicts, as of today, a rather limited presence of large technology companies (BigTechs) in the financial sector. Six subsidiaries of Bigtechs are authorized as e-money institutions, two as payment institutions, two as credit institutions, three as insurance intermediaries and two as insurance undertakings. [Report on 2023 stocktaking of BigTech direct financial services provision in the EU, Joint-ESA Report, JC 2024 02, 01/02/2024, p. 6]

[22] See Recital 40 and Art. 5 (3) of Regulation (EU) 2023/2854 (Data Act).

[23] See Art. 6 (4) (f).

authorities with investigatory and sanctioning powers, is a crucial element of the proposed Open Finance framework. This applies, in particular, because many new – potentially non-regulated – companies, also from the non-financial sector, may enter the still developing markets for financial information services. Furthermore, access to the financial data of FI customers could inevitably increase cybersecurity, data security and privacy-related risks as well as risks related to financial stability, e.g., due to an increased interlinkage between (non-financial) companies. Thus, providing competent authorities with the necessary supervisory and enforcement powers helps to allow financial information services markets to flourish, ensures their integrity and upholds trust in their proper and rules-based functioning. They are also essential for a voluntary participation of business and consumer customers in the sharing of their (sensitive) financial data.

Naturally, any administrative penalties, measures and fines imposed must be in proportion to the expected damage that an infringement could cause. If the potential penalties, measures and fines which those authorities are able to impose are too rigorous, they could also act as a barrier to market entry and undermine the Commission's efforts to create thriving markets for financial data. In this regard, there could be some room for improvement so as not to deter interested companies from developing innovative financial information services.

2 Legal Assessment

2.1 Competence

The proposed Regulation is based on Article 114 TFEU that enables the EU to adopt "measures for the approximation" of the establishment and functioning of the internal market that in essence serve to achieve harmonisation in certain areas. The Introduction of common rules on financial data access addresses challenges faced by the EU single market. A harmonised legal framework for financial data sharing aims, inter alia, to facilitate cross-border financial services provision and to eliminate the current fragmentation of the internal market. Therefore, the legislative proposal can be seen as a measure for "the improvement of the conditions for the functioning of the internal market"[24]. Thus, Article 114 TFEU is a proper legal basis for the proposed Regulation.

2.2 Subsidiarity

To comply with the subsidiarity principle, the EU must avoid action that is not within its exclusive jurisdiction, unless this would be more effective than any other action taken at the lowest level of governance. Adoption of an EU Regulation is appropriate only when the objectives of such action cannot be sufficiently achieved by the Member States.

As of today, there is no harmonised regulatory framework with respect to making available, sharing, and reusing customer data held by providers of financial services. Making available, sharing, and reusing such data is principally governed by bilateral contracts between the respective data holders and interested data users. Considering that both data holders and data users of customer related financial data often operate within several Member States, and data usually flows easily across borders, it cannot be assumed that financial data access can be addressed at a national level as effectively as at EU level, in particular, when considering financial stability. Furthermore, due to the high level of market integration of the EU financial sector, market participants are already largely subject to EU regulations. Without a harmonized framework, FIs and FISPs operating across borders would be confronted by varying national specificities, leading to increased costs for cross-border service provision. The proposed Regulation therefore creates more legal certainty and facilitates the free flow of financial data across the Member States. Since there are no other potential measures at national level that would be as effective as supranational legislation, there is no violation of the principle of subsidiarity.

2.3 Proportionality vis à vis Member States

In accordance with the principle of proportionality, the measure should not surpass the boundaries of what is appropriate and necessary to accomplish the desired objective. In order to ensure the smooth operation of the internal market, adoption of the EU Regulation laying down the single framework for financial data access, sharing and reuse constitutes the most appropriate measure by comparison with the alternative options. Less intrusive options would be insufficient to achieve the desired objectives to the same extent as a single EU-wide framework. Moreover, a single EU-wide framework helps to avoid unnecessary burdens and contradictions. Alternative measures could, for instance, result in divergent conditions and interpretations of how and to what

[24] See Judgment of 5 October 2000, C-376/98, Germany v European Parliament and Council, pp. 84 and 106; judgment of 8 June 2010, C-58/08, Vodafone and Others v Secretary of State, p. 32.

extent third parties may access, store and process the financial data of customers of financial institutions. Such legal uncertainties arising from varying national legal frameworks would negatively impact EU financial markets. Thus, the principle of proportionality vis-a-vis Member States remains uncompromised.

2.4 Compatibility with EU law in other respect

Data sharing and competition

By introducing an obligation for data holders to be members of FDSSs, the Commission is striving to make market entry easier for competitors who would otherwise experience obstacles in accessing customer data that could be used for innovative business models. Also, consumers may benefit from resulting enhancements and a broader array of offerings. Information sharing is therefore supposed to establish a level playing field in the financial sector, whereas cross-sectoral sharing of data is used as a solution to avoid asymmetries in the financial sector. Schemes have the capability to enhance data accessibility and tackle data bottlenecks. Additionally, they set the stage for the development of secondary markets. From this perspective, customer data may be seen as a kind of public good. This approach to data has emerged in European competition law. However, the provisions of the proposed Regulation are not fully in line with the developments of EU competition law. The discrepancies appear when taking a closer look at the TFEU and the Digital Markets Act (DMA, s. cep**PolicyBrief** 14/2021 and 15/2021).

The so-called *"essential facility doctrine*" has long been established in European enforcement practice.[25] According to this doctrine, a dominant company must make its assets and facilities available to competitors if the latter are otherwise unable to enter the market.[26] The doctrine was originally developed for physical infrastructure but was later extended to data[27] and networks. Refusal of a dominant firm to provide access to data that is deemed essential to enter a market for its competitors can be qualified as a form of misuse of a dominant position, i.e. a violation of Article 102 TFEU. Along with this, data sharing schemes are environments that enable their participants to have arrangements that may constitute anticompetitive information exchanges among rivals (Article 101 TFEU), if the data can be effectively converted into business intelligence by all members of the pool.[28] Later, the DMA introduced a novel framework that complements traditional ex-post competition law instruments with a specific ex-ante framework having direct influence on competition. According to Art. 6(10) DMA, large platforms within the scope of the Act are obliged to grant simplified access to their data by other entities. This obligation can indeed effectively address asymmetries in the market because it applies to "gatekeepers", large companies that potentially hold a dominant position in a market. Provisions of the DMA in essence allow prohibition of the misuse of a dominant position and use the same logic as the essential facility theory, at a very early stage. Otherwise, the implementation of ex-post competition law tools would take a long time and negative consequences could be significant for the whole market. However, the proposed Regulation does not contain any limitations for gatekeepers which means they may easily join an FDSS as a data user and therefore profit from accessing customer data. In turn, this can give them additional competitive advantages which is de facto against the spirit of the proposed Regulation. Access to data sharing pools could be valuable for market participants, who, unlike the dominant tech giants, currently lack access to sufficient data resources.

It is essential to mention that the biggest gatekeepers are companies established outside the EU market (like Google, Amazon, Apple or Facebook) that already offer finance-related services or are considering introducing such services.[29] At the same time, the proposed Regulation allows third-country entities to be granted authorization as FISPs simply through a legal representation in any EU Member State. This poses a risk to fair competition since third-country entities would be able to access European customer data and use it for offering more innovative products and services whereas European entities may lack access to comparable data from third-country financial institutions in those third-countries. In any case, control over the reuse of customer data in third countries can be challenging in practice due to the lack of a framework for coordination between the various supervisory authorities in the different countries.

Other considerations regarding ensuring fair competition relate to the vagueness of the provisions on FDSSs. There is a need for setting up additional, more detailed and clear minimum requirements for FDSSs in order to ensure more consistency across schemes. Unclear rules will potentially lead to a different interpretation of the

[25] European Commission (1994) Sea Containers v. Stena Sealink; European Commission (1992), B&I Line pie v. Sealink Harbours Ltd. and Sealink Stena Ltd.

[26] BKartA and Autorité de la concurrence (2016), Competition Law and Data, p. 11.

[27] German competition law goes beyond the enforcement practice and lays down a data access claim directly in the legislative act, see § Section 20 (1a) of the German Act against Restraints of Competition.

[28] Anzini M., Pierrat A.-C. (2020) Data Pools as Information Exchanges between Competitors: An Antitrust Perspective, cepInput 05/2020.

[29] For instance, Apple and Amazon have their own payment solution, Facebook has tried to introduce its own stablecoin called "Libra"(later "Diem") but the project was terminated due to regulatory hurdles.

possible design of FDSSs. Assuming that data holders and data users will be members of multiple schemes at the same time, this may create unnecessary confusion when dealing with the schemes. Interoperability between FDSSs emerges as a pivotal consideration in this context.

Compatibility with data related legislation

In recent years, the EU has enacted various pieces of legislation applicable across all sectors within the framework of the European data strategy (e.g., EU Data Act, Data Governance Act). Since FIDA introduces additional sector-specific measures on data access, sharing and reuse, those provisions have to be in line with the existing legislation, especially with the data sharing requirements of the General Data Protection Regulation (GDPR).

It is necessary to ensure that the data user's access to personal data fully complies with data protection laws. At first sight, the proposed Regulation explicitly aligns its application with the GDPR, which establishes a legal basis for the sharing of personal data. The proposed Regulation mandates that the handling of customer financial data by both data holders and data users must be in line with GDPR provisions, thereby safeguarding data protection standards.

However, additional clarifications would be useful to ensure that the GDPR's principles of purpose limitation and data minimization will be respected when implementing proposed Regulation. In order to adhere to the data minimization principle, it is essential to make sure that the categories of data falling within the scope of the proposed Regulation can be clearly identified. The legal text should avoid any vague formulations allowing for different interpretations. This delineation should consider both the potential risks associated with the processing of such data for individuals and the specific characteristics inherent in the financial services to be provided.

In fact, the expansive scope of the term "customer data" could include highly sensitive personal information that may be considered disproportionate. Some types of customer data within the scope of the proposed Regulation listed in Article 2(1) may de facto be highly sensitive. Even if the data does not fall into the scope of Article 9 GDPR[30], it may still be considered as sensitive, if it is, for instance, linked to household and private activities or its usage may cause a clearly serious impact on the data subject's daily life. As a matter of illustration, financial data can be used for payment fraud and must therefore be considered as sensitive.[31]

Against this background, additional restrictions and an enhanced level of protection in regard to sensitive financial customer data are necessary to minimise potential threats to any infringements of fundamental rights to privacy and data protection. It is essential that the categories of personal data accessible under the proposed Regulation are precisely defined, considering the potential risks to individuals whose data may be accessed and utilized.

Granting permission

To start with, it is highly welcome that the proposed Regulation grants customers the power to determine the utilization of their data for purposes and under conditions explicitly agreed upon by the customer as well as to designate the entities allowed to access it with the ability to withdraw the granted permissions at any time.

Article 5(1) of the proposed Regulation lays down that customer data can be made available by a data holder to a data user solely for purposes to which the data holder's customer has expressly granted permission. To facilitate customers in managing their permissions and having effective control over their data, the proposed Regulation obliges data holders to provide permission dashboards for their customers. Recital 22 of the proposed Regulation states that dashboards have to show the permissions, including among others those where personal data is shared "based on consent or is necessary for the performance of a contract". This wording gives a hint to an interlinkage with Art. 6(1)(a) and(b) GDPR which differentiates between two different legal bases. Whereas the permission based on consent is straightforward due to signing a contract or accepting the terms of service, the second legal basis requires a necessity test to prove the lawfulness of the data processing. In that case, a fact-based assessment has to provide evidence that data processing is objectively necessary for the performance of a contract with the data subject and there are no less intrusive alternatives to reach the desired objective.[32] At the same time, the proposed Regulation allows data users to have access to customer data only upon "expressly granted permission". However, the Regulation proposal does not provide a definition for "permission"

[30] Art. 9(1) GDPR states: "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited".

[31] Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, wp248rev.01, p. 10.

[32] European Data Protection Board (2019), Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects.

which may be confusing in practice. Other data-related legislation does not contain any clarifications either. The term “permission” should not be confused with the terms "consent" or "explicit consent" used in the GDPR. Indeed, "permission" goes beyond just giving consent. When giving consent, a person, in essence, concurs with what has been proposed. Moreover, providing a service is impossible without accessing data. In that case, giving consent is necessary in order to make a counterparty legally able to provide a service. In turn, "permission" can stem from different legal grounds and includes granting the counterparty a right to perform an action. The provision of a financial service, exemplified by the issuance of insurance, remains feasible even in cases where a customer declines to grant permission for the sharing of their data with third parties. In essence, providing an initial service is not dependent on giving permission. In the case of the proposed Regulation, a customer authorises a data holder to make customer data accessible to third parties, i.e., data users. Finally, "consent" is tied to personal data, whereas "permission" can be granted with regard to various types of customer data, including non-personal data.

Nevertheless, there is a necessity for a clear definition of "permission" to be included directly within a legislative proposal alongside other terms in order to differentiate between the interrelated terminology of the data-related legal acts.

Consistency between the proposed FIDA Regulation and the proposed Regulation on payment services in the internal market (PSR)

Both the proposed FIDA Regulation and the proposed Regulation on payment services in the internal market [COM(2023) 367, PSR] envisage the establishment of permission dashboards.[33] The latter contains a requirement for account information service providers (AISPs) to put in place such dashboards allowing payment services users to manage their granted open banking access permissions.[34]

To avoid unnecessary complexities, it would be beneficial to allow data holders to build single, unified permission dashboards that enable their customers to manage permissions from both regulatory frameworks. Creating disparate dashboards would complicate customer permission management and increase operational challenges for the industry. This should be avoided.

Moreover, it is incomprehensible why the treatment of FISPs differs from that of AISPs. While any AISP must be established within the EU, for a FISP from a third country it suffices to appoint a legal representative in one of the EU Member States in order to be eligible for authorisation in the EU. We recommend following a harmonised approach regarding the treatment of FISPs and AISPs. There should be stricter requirements for third-country FISPs at least on the basis of an equivalence regime to minimise potential competitive disadvantages for EU FISPs.

D. Conclusion

Data plays an increasingly important role on financial markets and is a decisive input factor when developing new data-driven financial products and services. However, customers of financial institutions regularly lack effective control over their financial data. They face difficulties in accessing this data and in deciding whether to share it with third parties. On the other hand, third parties interested in the financial data face hurdles when accessing the data held by financial institutions which means that the customers cannot benefit from data-driven financial products and services provided by third parties based on data being shared by customers. The Commission wants to tackle these issues and establish rules on accessing, sharing and using specific categories of financial data belonging to the customers of financial institutions.

The envisaged regulatory concept is, at least partially, flawed. Data access and sharing may be justifiable with respect to consumers, but not with respect to business customers. Furthermore, obliging a multitude of financial institutions to make customer data available, irrespective of any identified market failure, is disproportionate. Such a duty encroaches unjustifiably upon their entrepreneurial freedoms. If, at the same time, there is no demand among customers and data users for the data, the build-up of data sharing ecosystems is redundant.

Furthermore, the scope of the proposed Regulation is in need of several clarifications, specifications and adaptations to the chosen concepts. The legislature must, inter alia, clarify the terms “customer” and “financial information service”, specify the customer data categories falling within the scope to provide for legal certainty, make sure that “customer data” falling within the scope does not go beyond “raw data”, find a more suitable and coherent approach to the handling of “sensitive” financial data and reconsider the strategy for exempting certain smaller financial institutions from the scope.

---

[33] Proposal for a Regulation of the European Parliament and of the Council on payment services in the internal market and amending Regulation (EU) No 1093/2010 COM/2023/367 final.

[34] Art. 43 and Recital 65, PSR proposal.

In addition to that, there is a mismatch, which must be resolved. Any financial information service provider must also be obliged to make their respective customer data available to financial institutions. Such a step is necessary to avoid competitive distortions to the detriment of FIs and to ensure a level-playing field.

We applaud the establishment of permission dashboards. Such dashboards are crucial for empowering customers to effectively manage and monitor for whom, when and for what purposes data users may access and use the customers' financial data. This upholds and fosters trust among customers in relation to the sharing of their data. Yet, the legislator should allow financial institutions offering similar financial products and services and dealing with comparable types of customer data to collaborate on developing such dashboards and to agree on common standards to find joint or at least similar dashboard solutions. Moreover, the legislator should follow a coherent approach vis-à-vis the proposed Payment Services Regulation (PSR).

The creation of financial data sharing schemes may reduce transaction costs by bringing together relevant market actors, enabling the development of common technical standards and data formats, and by facilitating the agreement of joint contractual terms. In order to reach this positive outcome, it would be better if the legislation were to ensure the interoperability of the schemes. However, in case of niche markets or highly specialized financial products or services, scope for data sharing outside financial data sharing schemes should remain possible.

The ability to claim compensation from data users for making customer data available within a financial data access scheme maintains the incentive for data holders to establish high quality data access interfaces, and avoids free rider behaviour on the part of data users. Limiting compensation to a "reasonable" level and gearing it to the lowest market standard is, however, flawed. Such a restriction is only an option where the data holder has unassailable market power. The legislature should learn from the compensation-related rules of the Data Act.

Forcing financial information service providers to abide by specific authorization, organization and operation requirements is pivotal for ensuring that irrespective of who is undertaking a certain business, the same rules apply. However, allowing third-country financial information service providers to access customer data via a legal representative may jeopardise competition if there are no equivalent possibilities for EU entities to access the customer data of third-country financial institutions.

Notwithstanding the Commission's commitment to fostering a level playing field across the financial sector, the provisions related to financial data sharing schemes are not in line with the established framework of EU competition law. Such a deviation creates legal loopholes, introducing the potential for competitive disadvantages for European companies. Additionally, it raises concerns that companies from third countries may exploit these loopholes, thereby benefiting from the reuse of the financial data of EU customers.

Moreover, there is a necessity to guarantee the alignment of the proposed Regulation with other parts of the data-related European legal frameworks, especially with regard to the General Data Protection Regulation (GDPR). It should be ensured that the principles of purpose limitation and data minimization are duly adhered to in the implementation of the proposed Regulation.

Furthermore, the legislature should harmonize its approach to permission dashboards across different legislative acts. Since both the proposed FIDA Regulation and the proposed Payment Services Regulation (PSR) require financial information services providers (FISPs) and account information service providers (AISPs) to put in place permission dashboards, both ecosystems should be based on the same principles and at least be interoperable. The best solution would be to establish a unified dashboard for convenient customer permission management.