EBF_046342

11 December 2023

EBF position on the European Commission's proposal for a Framework for Financial Data Access (FIDA)

Executive Summary

We recognize efforts by the European Commission to develop a strong European data economy through initiatives such as the Data Act and Data Governance Act. Under this horizontal framework is the proposed sectoral Regulation on Financial Data Access (FIDA). The proposal aims at promoting data-driven innovation in the financial sector, possibly opening new opportunities for customers while also increasing their control of how and with whom they share data, including through tools such as permissions dashboards.

We welcome that the **management of the access to customer data** will be left to **market actors through the setting-up of financial data sharing schemes**, supported by **high level principles** in the Regulation – notably the **principle of compensation** (missing from the revised Payment Services Directive) which allows for a degree of flexibility in implementation.

However, we are concerned that the **scope** of the proposed mandatory customer data access rights **covers a wide range of financial services products, with a potentially large amount of data that is sensitive for the customer and the data holder without clear predictions on the benefit or an appreciation of the risks.** As stated in the Commission impact assessment report[1]: "*given the limited data availability and the nature of the open finance initiative, it is inherently difficult to make quantitative predictions about how its benefits at the whole economy level".*

A consideration of **potential impacts on financial intermediaries' business models is equally missing**, which was explicitly mentioned in the Council Conclusions on the European Commission Communication on a Retail Payment Strategy for the European Union[2].A study on Open Finance requested by the European Parliament's ECON Committee, notes that FIDA will accelerate structural change in the EU financial sector… "*this will lead to further gains in the market share of non-bank lenders at the expense of established banks, whose margins may shrink as IT investment weighs on profitability*.[3]"

The omission of this consideration is worrying in light of the scale of the FIDA initiative and the necessary, significant resources that will be required to develop and/or update systems to comply with FIDA. These will compete with other investments that can

[1] European Commission, Commission Staff Working Document: Impact Assessment Report, Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council 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, June 2023, pp. 61

[2] Council Conclusions on the Commission Communication on a Retail Payments Strategy for the European Union, March 2021

3 Lehmann, Alexander & Marcus, J. Scott, "Open Finance: What can an enabling framework look like", October 2023, p.12

contribute to increased resilience and economic competence. Therefore, if the risks of FIDA are not addressed (for example those stemming from the proposed regulation of Financial Information Service Providers (FISP), the Framework could put European financial entities at a disadvantage vis-a-vis third country players.

We also note that this initiative is still rooted on financial data held by entities acting in the financial space, while we believe that, in order to build real innovative data-driven financial products, there is a need to unlock the potential of data held by economic actors in other sectors and make this data accessible by financial actors, thus creating a real level playing field. There have been some steps in this direction – but more is needed.

Given that it was difficult to make quantitative predictions about the benefits of the initiative at the whole economic level, we strongly recommend a measured approach, one that strikes **a balance** between mandatory data sharing elements, including the risks, and market driven elements and sets the right incentives for innovation while maintaining customer trust. To this end, we recommend for the proposal to:

1. **Set out a precise scope, supported by clear definitions.**
    - Adopt a **granular approach under Art. 2(1)** as to what data falls in in scope to give certainty for data holders and aid scheme development later on.
    - Clearly exclude **derived and inferred data from the scope of access**; this should be reflected in the definition of customer data under Art. 3(3) and in the **relevant data categories** under Art. 2(1). Not excluding this data (e.g. results of internal assessments) could have a negative impact on market-driven offerings. The same holds true for collected data for suitability and appropriateness assessment and data which forms part of a creditworthiness assessment of a firm; what data is requested and in which format **is highly specific to the market and the product offering of a financial institution** and could therefore allow for reverse engineering of a financial institution's processes and offerings.
    - **Exclude third party data from the scope**. The data holder should not function merely as a conduit of second-hand information. Data should be limited to data that originated at the original source/data holder.
    - Limit, at a first stage, obligations to **retail and SME customer categories and the corresponding data.** Only after the review of FIDA, expand to data of corporate customers.
2. **Maintain a market driven approach for the negotiation and development of data sharing schemes, supported by gradual process and workable timeline that reflects the complexity of the task.**
    - Adopt an implementation approach that opens up customer data sharing in **different stages**, starting by a first customer data set and progressively opening to further data categories, after a careful assessment of the impact of market demand.
    - Introduce **a longer time frame to** reflect the process of developing a data sharing scheme: i) **scheme set up** (gathering participants, determining/designating the scheme owner, **agreeing the governance rules**, etc), ii) **scheme development** (including meeting Art. 10 requirements) and iii) scheme **implementation**. Allocating the necessary time for this process

allows market actors to **identify** potential **use cases** where there is customer demand and to begin work on a scheme accordingly. This also gives space for a pilot phase of the different use cases, which would allow to assess practical implications and potential risks. The interoperability of schemes and avoiding fragmentation also needs to be considered. An **18-month timeline is not feasible.**

- Reasonable compensation to the data holder by the data user (including FISP) **should not be limited to costs directly related to making the data available** (Art. 10(h)(i). It should take into account the **investments made by the data holder** in the collection, generation, structuring, preparing, and sharing of the data, as well as the quality of the data.
- The inclusion of **Article 11** ("Empowerment for a Delegated Act in the event of absence of a financial data sharing scheme") may serve as a disincentive to data holders to invest in scheme development, if there is a risk of work done so far being jeopardized because it does not fit in the time frame or the conditions of the Commission. We would suggest to delete it from the text or, as an alternative, reconsider the approach, focusing instead on evaluation and dialogue with data holders and data users.

3. **<u>Clearly define "Financial Information Services" and strengthen their authorization requirements</u>**

- The **Financial Information Service Provider (FISP) authorisation must not be a "shortcut" to providing financial services and products**. Yet recital 31 of the proposal indicates that FISP *"would provide financial products and service to customers in the union."* We stress that in this case, they should seek the **appropriate licence to do so** and would, as a result, participate in FIDA as one of the other entities under the scope.
- Include a definition of **"financial information services"** in the text, clearly setting out the scope of activities and therefore **safeguarding that FISP authorisation is appropriate**. The scope should confirm that the data accessed under FIDA by FISP can only be used to provide financial information services.
- Update the authorisation process to include an **evaluation of whether an entity applying for a FISP licence should also be a data holder under FIDA**. The criteria would be if the entity, upon application, holds other categories of customer data listed under Art. 2(1). This would help to ensure a level playing field between FISP and the other entities in the scope. For entities from outside the financial sector seeking a FISP authorisation, including a reciprocity clause as a requirement for their participation in data sharing schemes could be considered.
- Require third-country FISP to have a **direct legal presence – a subsidiary or a branch** - to receive the authorization. A legal representative is not sufficient. They must be subject to the same level of supervision under same conditions (compliance with GDPR, DORA, other relevant legislation).

4. **<u>Clarify roles and responsibilities in the operationalisation of permissions</u>**

dashboard and ensure strong security and fraud protection

- Clearly set out the **responsibilities** of the **data holder** and the **data user** in the provision and update of the dashboard and specify that permission focuses on the 'access' versus the legal basis for processing. The latter is **defined between the data user and the customer and, therefore, it cannot be managed via the data holder**.
- Avoid overly prescriptive requirements for the dashboard to allow for data holders to develop and adapt them for user needs. It must also be aligned with the requirement under the Payment Service Regulation (PSR) in order to facilitate customer's experience and allow data holders to leverage on the investments made.
- Security must be at the foundation of any data sharing- without it there is no trust from customers. Therefore, there should not be a **different level/standard of security** applied by data holders and data users on **the same type of data and on the same type of services.** This is particularly important in view of the broad scope of data and the number of actors in the FIDA ecosystem. Compliance with the **Digital Operational Resilience Act (DORA)** by all entities participating in FIDA (including FISP) is an important step forward yet there still may be differences between data holders and data users in terms of the level of requirements.

5. **Take lessons learned from PSD2, specify the interplay with relevant regulation, and work towards real cross sectoral data sharing**

   - Build on the **lessons learned, the implementation and the investments made** (e.g., API infrastructure, standards, etc) **under PSD2**.
   - Develop the interplay with horizontal legislation including the GDPR, Digital Markets Act (DMA), the Data Governance Act and the Data Act in the text. Further on the DMA, we stress the need for an **operationalised implementation of the data related obligations by designated gatekeepers**.
   - The goal of cross-sectoral data sharing should not be lost in FIDA, thereby jeopardising the full opportunities of the data economy.

Considering the elements above would, in our view, help create a framework that provides legal certainty as well as conceivable opportunities for data holders, data users, and customers when sharing their data, while also helping to address the risks.

FIDA RECOMMENDATIONS

1. Clarify definitions under Article 3

A well-defined scope is supported by clear definitions. For the moment, instead of providing a good foundation for the proposal, several of the definitions under Article 3 raise more questions than answers. This could lead to different implementations and multiple Q&As from the European Supervisory Authorities (ESAs) (as it happened under PSD2), challenging scheme establishment, and as a consequence of this, an increase in continuous developments and costs.

To help address these risks, we recommend to:

- Update the definition of "customer" under Art. 3(2) to include **only retail and SME customers**. **Wholesale customers should be excluded**, at this stage, from the scope.
- Introduce a **clear exclusion of derived and inferred data under Art. 3(3),** which may fall into the current unclear wording of "*data generated as a result of user interaction with the financial institution."* We propose the following definition:

  Proposed update: Article 3(3): Customer data means personal and non-personal data, provided by the customer (directly or observed) that is collected, stored by a financial institution ***in connection with an existing agreement between the customer and the financial institutions as the primary data holder for the provision of such financial products and services; data generated by financial institutions, by processing data provided directly by the customer shall not, in any case, be considered as customer data****".*

- **Exclude data acquired from a third party** (e.g., purchased from a third party, accessed from a public registry), as the data holder may not be the **'original' data holder**, which could have consequences for **data accuracy and liability if this data is shared**. An exclusion of data received from third parties will also provide clarification for those cases in which the data is subject to that third party's rights and the data holder may legally or contractually be prevented from sharing it.
- Include the clarification that protection for the **confidential business information and trade secrets** of the **data holder** as well as the customer under recital 9.

<u>Please see the annex for detailed comments on the definitions under Article 3.</u>

2. A clear scope under Article 2

Scope is governed by what is proportionate and necessary for a well-defined purpose. It is therefore essential to clearly **define and distinguish between different categories of data under Article 2** and therefore, which data is suitable for sharing. This requires a more **granular approach**. A clear scope also facilitates compliance with the GDPR

principle of data minimization and fosters trust so more data is not shared than needed.

As a foundation, we therefore recommend the following:

1. Only data that is shared by the data holder with the customer **in a secure online environment** (e.g., via a customer's online banking services) should be covered by the Regulation and shared with a licenced data user.
2. The categories in scope must reflect the definition of customer data (based on the above recommendation):
    i. Any **derived and inferred data under Art. 2(1)(a)-(f) should be excluded**,
    ii. **Only data** connected to the **provision of the specific service is concerned** and;
    iii. That **data which is not from retail or SME customers** is **excluded.**
3. For legal certainty, the text should refer to **existing European legislation defining and governing the financial product**, where available.
4. Any data provided by **third parties** should be excluded. As mentioned above, a data holder may not be the "primary" data holder; for example, when granting a mortgage, data relating to the loan is coming from notaries or the public cadastre, or data from the tax administration, etc. This data is not primarily attributable to the lender and should not be included in the definition of customer data. There may also be a confidentiality aspect.
5. As a granular approach to the scope is missing, there is a risk that other financial institutions active in the same field may get hold of **internal pricing strategy in** relation to the **products of the data holder.** This could have a negative impact on market competition and is already considered as a risk under legislation such as the Data Act. Therefore, **any data related to the internal pricing strategy should be excluded.** We would recommend that the access right is limited to **key conditions of the product or service instead.**
6. Include a clarification on the geographical scope: FIDA should only be applicable on data that are available following the offering of financial services in the EU.

Building on this foundation, **please find in the annex the detailed comments on** the **specific categories of customer data under Art. 2.**

Nevertheless, we would like to highlight in particular that data under **Art. 2(1)(b), data collected for the purposes of carrying out an assessment of suitability and appropriateness** in accordance with Article 25 of Directive 2014/65/EU should be **excluded from the scope** as:

i. There are **different proprietary methodologies** among service providers for assessing appropriateness and suitability, which may include trade secrets. In other words, the questionnaires, and the interaction with the customer to draw up this assessment, can differ between banks and contain an element of expertise and bank know-how. In addition, data collected for the suitability assessment reflects the peculiarities of the service and advisory model adopted and the "catalogue" of products designed and offered to clients by each financial institution. It would therefore be counterintuitive if banks would be required to share this data as it

would mean that data holders, such as banks, would not be able to differentiate themselves, and may opt not to provide these added services anymore.

ii. Data collected in the suitability and appropriateness test is **a snapshot of the relevant data collected from the customer at a point in time**. The customer's data may change quickly after they provided it to a bank (e.g., their salary or their holdings of financial instruments may have decreased). In the case of one-off advice**, there is no legislative obligation for banks to update the data on an ongoing basis.** Therefore, there is a risk that the data which will be shared under FIDA will not be relevant anymore in terms of the customer.

iii. There are **potential liability issues** faced by service providers when using customer exploration data collected by a different provider.

iv. Data used in suitability assessments can be extremely broad and will contain **sensitive business and personal information**. For example, these may contain business plans, hedging strategies, expected future cash flows, or personal information.

v. We underline that the result of the assessment should also be excluded from the scope – we understand that is the intention but re-iterate the importance of this.

3. Maintain a market-driven approach for the development of Financial Data Sharing Schemes supported by a gradual process and reasonable timeline

We welcome that aspects of a **market driven approach** are included in the proposal, allowing the market itself to determine how the data in scope is to be shared, in a **standardized** and **contract-based way**, with **compensation.**

For this to function and given the broad scope and the time required for the data holder to prepare the data for sharing, we recommend **a gradual market-based implementation and rollout.** This includes proceeding with data sharing at different stages, starting by a first customer data set and progressively opening up to further data categories, after a careful assessment of the impact and of market demand (the potential use cases).

The Commission references the SEPA Payment Account Access Scheme (SPAA) as an example of financial data sharing schemes, the proposal should therefore also take the lesson learnt in that context in terms of the timing and the steps, and the whole process required to establish this initiative.

3.1 Important considerations

To facilitate the market driven approach for scheme development, there are several aspects to consider:

i. **Providing a workable timeline** for scheme development to account for the complexity of the **process, the different actors, as well as different product areas.**

Eighteen months to develop and implement a scheme is not feasible. Furthermore, Article 9.1. does not specify that data sharing needs to commence or that the technical infrastructure needs to be in place. It only indicates that data holders or data users shall

become members of a data sharing scheme.

Timing is also important to **meet the representative criteria** under Article 10 (a)(i). To help this, we suggest to build out further the "**significant portion" of the market criteria,** while also clarifying the role of customer organizations in data sharing schemes. For the moment, they are listed as members, but is this as an active participant and in which function or rather that of an observer.

ii. Giving the necessary time to for potential use cases to emerge

There is a risk that financial entities set up schemes that have low usage. We therefore believe that **more time is needed for potential use cases to emerge**; these can also serve as an **incentive to bring different market actors around the table**. The use case approach also seems to have been part of the Commission's thinking, as seen by the FIDA Impact Assessment[4].

Elements that could help identify potential use cases in the scheme set up phase include **pilot projects.** They can pinpoint practical and technical challenges and can be particularly beneficial for use cases in areas such as investment, where there are more sensitive considerations.

iii. Agreeing/designating scheme owners

Time is needed to agree on and designate a scheme owner or allow time for the emergence/designation of one. Agreeing the governance rules between the participants is also essential. This would include ensuring the necessary resources and staff for the running of the scheme.

iv. Undertaking the technical work to develop a rulebook on how data will be shared

This includes meeting the requirements under Art. 10 of the proposal. If we take the example, of SPAA, this was built on significantly more standardized payment-related data which is not the case in some of the datasets/products envisaged in scope. It is positive that the **development of standards will be market-driven**, allowing not only scheme members but also other parties and bodies to develop common standards and technical interfaces. This also gives the space to leverage existing international and European standards, as well as work done in other fora such as the Berlin Group and other initiatives in European countries.

The interoperability of schemes also needs to be considered during the development phase. This can be achieved in different ways and should be left to the scheme members, and the market, to decide.

Finally, technical work also involves identifying synergies with existing frameworks, where

[4] European Commission, Commission Staff Working Document: Impact Assessment Report, Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council 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,

relevant, to avoid duplication in costs in terms of implementation and maintenance.

v. Defining the contractual liability framework and dispute resolution mechanisms.

For the moment, there is very little on liability in the proposal, beyond that it should be determined in the scheme. Customers need to be sure not only about what data they are sharing and with who, but where do they turn to in case of any problem: complaints, functionality issues or simply when something goes wrong (including for permissions dashboards, who is liable for financial loss, data breaches, insufficient information security, illegal use of data, etc.).

As a first step and building on what is already in the text in terms of what the data user can and cannot do, we suggest to use the horizontal principles in the **Data Act**, **notably Art. 11 on *technical protection measures and provisions on unauthorized use or disclosure of data*** as a basis, and to directly reference it under Art. 10(1)(i). This would also help to ensure consistency in the contractual liability measures across (potentially) multiple schemes and in terms of the user experience.

vi. Relationship with existing schemes

The interoperability and relationship with existing national schemes when covering the same set of data as under FIDA should be considered. Currently, in several countries (for example Denmark) public/private collaboration based on the sharing of data have been established in areas such as pensions.

3.2 Scheme implementation

While the text already indicates that accessing the data under Art. 2 should take place through a data sharing scheme, we believe it is important to clarify that **data users** including FISPs and AISPs cannot **rely on FIDA for data access in the absence of a scheme and their membership therein.**

If FISP or any data user wishes to **access data in the absence of a scheme, they should do so through bilateral agreements.** Any other option or fallback would only create disincentives for data users in scheme negotiations and hinder fostering trust between them and data holders.

In this context, EBF would like to take the opportunity to highlight that screen scraping, mobile app API re-engineering and other ways to connect to customer data through customer channels are less secure mechanisms for a third party to obtain customer data from a data holder. These methods make it difficult for the data holder to see the nature of the data that is being accessed. Nor is the data holder informed of the reason for the data to be taken. Also, the data holder has no way to show it in a permission dashboard (not even touching controlling/changing permissions). It is therefore important that FIDA provides a data sharing framework that takes these considerations into account.

3.3 Establish a strong foundation for the compensation principle

We strongly support the inclusion of the principle of compensation in the proposal under Art. 10 (1h). This is a key lesson learned from PSD2. However, to provide more certainty for all parties, we recommend to:

i. **Reflect the full spectrum of actions behind data sharing in the compensation criteria,** including **the collection, generation, structuring, preparing, and sharing of the data** – which all come with a cost. Covering the costs for investments and amortisation of the infrastructure is crucial and the starting point, but data sharing is not only about the creation and maintenance of the required infrastructure. It should therefore not be limited, as stated under Art. 10(h)(i) to "*reasonable compensation directly related to* ***making the data available*****."**

ii. **Reflect the quality of the data**. Recital 24 mentions that "*The obligation on data holders to share data at the request of the customer should be specified by making available generally recognised standards to also ensure that the data shared is of a* ***sufficiently high quality*****."**

    Linked to the quality of the data is the **potential value generated by the use case the data is used for**[5]. This criterion (the 'follow on use of the data') was identified in the DG Justice study for developing criteria for assessing reasonable compensation in the case of statutory data access right[6]. If the schemes are focused on data sets only, without an understanding of the use case, there may be a gap in terms of compensation as the aspect of the follow-on use of the will not be reflected, and thereby could discourage data holders.

iii. **Include a reference to Article 9(1) of the Data Act**. which mentions that compensation agreed upon between a data holder and data recipient shall be reasonable and **may include a margin**. In particular, data holders and data recipients should take into account the costs incurred for making the data available and **the investment in the "collection and production of data**". The compensation may also depend on the **format, nature, and volume of the data**. All these aspects are important to take into account when data holders and data users are developing the schemes under FIDA.

iv. **Establish a level playing field**. A challenge in the sector is that many of the FinTech companies are small or medium size which would exempt them from paying compensation beyond the direct cost under Art. 10(1). This creates a risk of circumvention by larger enterprises, who may establish a company that falls under the SME definition and seek a FISP license for this. Additionally, there is no comparable exemption for **data holders that are SMEs, which creates an unjustified asymmetry.** Small and medium sized companies **can be significant players in the financial sector in terms of data**.

v. **Competition**. A discussion with DG Competition will be necessary in the scheme development process, also showing why more time is needed for it.

[5] European Commission, Study for developing criteria for assessing reasonable compensation in the case of statutory data access right," November 2022, pp. 8
[6] ibid.

3.4 Notification of schemes

On the actual process of notification, we would recommend to include a new paragraph that expands on how, in practice this should be done. Considering that the financial data sharing scheme may not have legal personality, the notification of a scheme in accordance with paragraph 4 shall be submitted to the competent authority by a person or persons authorised to represent three most significant data holders which are members of that scheme at the time of establishment of the scheme. Each financial data sharing scheme would have a scheme owner who would be entitled to take actions for and on behalf of the scheme and all its members (this goes back to setting up scheme governance).

There are also certain elements under Art. 10(4) that may cause confusion and could lead to different authorities disputing over who should be in charge for the assessment under Art. 10(6). It could also result in a fragmentation of the approach taken by different authorities.

One possible way to address this could be to notify the scheme to one of the ESAs (depending on its scope). The ESAs would then have a join committee and could consult each other when assessing different schemes. This would help bring a more uniform assessment without potentially lengthy disputes between authorities.

3.5 Regulatory intervention in the absence of a scheme

We are concerned about Art. 11 of the proposal which empowers the Commission to adopt, under certain conditions, a delegated act to specify the modalities under which a data holder shall make available customer data.

As outlined, the development of data sharing schemes is a very complex exercise. If Article 11 is included in the proposal, it risks that the market will channel significant efforts, investments, and resources into building a scheme only to have the Commission issue a delegated act mandating how that same data set will be shared because the was not developed in the set time frame. This is exacerbated by the inclusion of **vague conditions such as "realistic prospect" and "in a reasonable amount of time".**

The market led approach should be given a real chance. **If certain schemes are not developed in the allotted time frame, this may also be an indication that there is not market need there and should be accepted.** Art. 20 already proposed penalties for infringements of Art. 9 and 10 (among other points) and should be sufficient. We therefore propose to delete Art. 11 from the text.

As a second option, if it is kept in the text, we propose that a different approach is adopted, one that requires the Commission to:

- Conduct an in-depth analysis and evaluation of a scheme's development, taking into account the views of data holders, data users and customers, as well as the specificities of the product.
- That this evaluation is conducted after a certain period of time in the scheme development process.

4. Financial Information Service Providers (FISP)

We welcome that the Regulation introduces an authorization regime for third parties to access data through the creation of the Financial Information Service Providers (FISP) category and by including such requirements as compliance with DORA. In this respect, it will be important to ensure that information on these companies can be accessed digitally, centrally at EBA and made available so that it can be simply and effectively identified/verified.

Yet there are some elements of this new category which need further elaboration in order to build trust for data sharing: a **clear definition of financial information services; stronger authorization requirements, including additional requirements for third country FISP under Art. 14(2); and a possibility for FISP to be data holders if meeting certain requirements.**

We also recommend to introduce **a requirement for AISP to be authorise as FISP to participate in FIDA.** For the moment, they are only registered to access payment account data. There is also a risk of cherry-picking – entities preferring the AISP registration regime to the FISP authorisation regime. This should be addressed.

4.1 Definition & role

A definition of what constitutes a "Financial Information Service" is missing from the Regulation. The European Data Protection Supervisor (EDPS) also mentions the lack of a definition in their opinion on FIDA[7]. They compare it to an account information service (AIS) under PSD2 where, unlike under FIDA, there is a clear definition of what the AIS service entails.

The lack of a definition is particularly worrying as recital 31 states that *"FISPs **would provide financial products and service to customers in the Union** and would access data held by financial institutions…"* If FISPs were to provide financial products and services to customers in the Union, they **would need to seek the appropriate licenses to do so, not a FISP licence.**

We emphasize that a FISP authorisation **cannot be a shortcut to the provision of financial services and products.** If this gap is created in the FIDA framework, the consequences would extend beyond it. The text from recital 31 should therefore be deleted. In our view, FISP should only be able to provide 'financial information services." What these services entail should be defined in the proposal. The authorisation should be limited to providing these services.

4.2 Authorisation requirements

For all FISPs, we would suggest to include the following additional requirements:

- Increased capital requirements. This could be €50,000 EUR and in addition to that, require the undertaking to hold capital to cover at least 6 months of operational expenses to cover legal and operational risks.
- Several of the requirements under Art. 12 are paper based products, like documents and descriptions of x, y z. A FISP may very well engage a consultant to

[7] European Data Protection Supervisor, Opinion 38/2023 on the Proposal for a Regulation on a framework for Financial Data Access, August 2023, p. 43

produce documents in conjunction with them seeking authorization. To make sure they have strong and resilient IT-systems, they should also be required to have an independent IT-audit and testing of their systems and provide the results to the supervisory authority.

In terms of **third country FISP, Article 14** already takes a step forward regarding additional elements that a competent authority has to consider before authorizing a **third country FISP**. Yet, the approach proposed is not sufficient, particularly the requirement that a FISP only needs a legal representative in one of the member states to access data under FIDA.

Third country FISP should be required **to have a direct legal presence** – a subsidiary or a branch to receive authorisation. This would help to fulfil Art. 14(5), to ensure that FISP are not just a letterbox entity. FISP should also be subject to the same level of supervision and under the same conditions (compliance with GDPR, DORA and other relevant legislation).

4.3 FISP as Data holders in certain cases

To help ensure a level playing field under FIDA, we recommend for the FISP authorisation process to include **an evaluation of whether an entity applying for the licence should also be a data holder under FIDA** or just a data user. This would be based on **certain criteria**, notably, if the entity upon application holds other categories of customer data listed under Art. 2(1).

The proposal notes that the ESAs, when developing the RTS under Art. 12(4) shall take into account whether the undertakings provide any other services; this should be an element to consider. We therefore propose the following:

a. FISP as data users

FISP should only be data users if the entity seeking the FISP authorisation is **only providing the strictly defined financial information service.** If the entity is providing a product or a service that is in the scope of the Regulation, they should seek the **appropriate licence, not a FISP licence**. In this case, they would be a data holder as well, like the other entities listed under Art. 2(2).

It is important to remember that as a FISP, **requirements under Art. 6 will apply** as well, **notably Art. 6(4)** where the data user is part of a corporate group, data accessed under FIDA shall only be access and processed by the entity of the group that acts as a data user. **This is a central provision in the text.**

We do note however that the reference to "processing" should still allow to use a data processor in the meaning of the GDPR. Under the GDPR a data processor cannot process personal data for their own purposes but offer supporting services (e.g. cloud services).

In the case of companies designated as **gatekeepers** under the Digital Markets Act (DMA), it is essential that Article 6 obligations of FIDA are seen in conjunction with the **data related obligations under Article 5 of the DMA** to ensure a level playing field for data

access[8]. If **a FISP is part of a designated gatekeeper corporate group, the authorisation process for a FISP under Art. 12 must include a check of compliance with the relevant DMA obligation.** In other words, FISP access by gatekeepers and affiliated entities should be **conditional on DMA implementation.**

In any case, it will be necessary not only to verify how the DMA will be implemented, but also to avoid that, through FIDA, the efforts made by the EU legislator in achieving greater fairness and contestability in digital markets, as well as in ensuring a level playing field among operators, are undermined.

b. FISP as data holders

We recommend to consider **two situations** in the evaluation.

- First, if an entity is seeking a FISP authorisation to provide the strictly defined financial information service, **holds one of the categories of data under Art. 2(1)**, they should be a data holder as well.

  For example, an entity seeking authorisation as a FISP is providing lending services but, in their member state, is not required to register as a lender. They do however hold some of the categories of data under Art. 2. In the evaluation for receiving a FISP licence, they would meet the criteria of being a data holder as well, not just a data user.

- Second, if there are entities from outside the financial sector which apply for a FISP license, introducing a reciprocity clause as a requirement for their participation in data sharing schemes could be considered. This approach also acknowledges that FIDA focuses on financial data sharing, while also helping to create a level playing field vis a vis other sectors as the latter would benefit from access to customer financial data through the schemes but would not be required to make their own customer data accessible.

5. A clear framework for permissions dashboards (Article 8)

In a situation with multiple entities/data users, the requirements under Art. 8, need to be clear in order for **the process to be manageable, to be certain of who is responsible for what and to deliver the best possible experience for customers** and to foster trust.

At the same time, requirements should not be too prescriptive as to allow data holders to develop permission dashboards that are easy to use and adapted to users' needs.

We therefore recommend the following:

- Clarify that the dashboard must only be **offered to customers using online interfaces**. Imposing an obligation to offer dashboards for users that do not use online banking tools would be disproportionate and challenging to develop, as the data holder would have no mechanism to verify the identity of the party using the tools.
- The permission dashboard **does not replace** the data user's responsibility to

[8] Under Art. 5(2)(b) of the DMA, designated gatekeepers cannot combine data acquired from third parties with the data they already hold and, under Article 5(2)(c) cannot cross-use personal data from the relevant core platform services in other services provided separately by the gatekeeper

provide the customer with the terms and conditions that govern their relationship.

- As the data user will be providing the information, per Art. 8(4)(b), it should be stated that **the data holder is not held responsible for the accuracy of the data provided to them by the data user**. They are not required to summarise / interpret / check the data they receive from the data user for inclusion in the dashboard.
- **It should be sufficient to build one dashboard to meet the requirements of FIDA and the PSR.** If a data holder is already offering a permissions dashboard, it should be possible to use this to meet the requirement under the Regulation.

Obligations under the permissions dashboard should complement existing obligations under the GDPR. **Please see the Annex for more detailed comments on Article 8.**

Finally, **raising customer awareness of permissions dashboards and their functioning both** on the data holder *and* data user side, must accompany their rollout.

6. Security and fraud

Security must be at the foundation of any data sharing, particularly when there are many parties in the data sharing ecosystem; without it there is no trust from customers. We therefore welcome the proposal's alignment with the **Digital Operational Resilience Act** which has increased the requirements for operational reliability and technical robustness in the financial sector. It is also positive that all **entities that wish to access data under FIDA need to be subject to it,** including FISP.

Yet it is worth underlining that banks are required to comply with stringent rules (see, for example, BCBS239) in terms of information security, data aggregation and risk reporting. Therefore, a risk remains that data holders and data users (such as FISP) may apply different levels of security standards under a scheme. **There should not be any gaps when it comes to security, as this directly impacts the customer and could also be a reputational risk for the data holder in the event of an incident.**

An issue which deserves further attention under the proposal is the **risk of an increase in fraud based on data**. While it is mentioned under Art. 12 in the requirements which FISP providers need to meet, there is no wider consideration on the risks arising from potential access **to a broad scope of a customer's financial data/financial capacity without their knowledge**. This can be put together and used by criminals to gather information on individuals and business structures/ownership etc. leading to potential fraudulent scenarios, such as:

- Social engineering, leveraging on information usually held by a bank. Social engineering can also lead to phishing and smishing attacks to have access to the customer's credentials and carry out fraudulent transaction.
- Scams, knowledge of customers' data and financial habits could be exploited by fraudsters to convince victims, posing as industry experts, to transfer their funds to unreliable third parties, e.g., fake investments for retail customers, or BEC/CEO frauds for corporate.

To address this and to help ensure customer trust, it is important that all entities under FIDA have robust security measures in place. We would also suggest to include Secure Customer Authentication as a requirement under FIDA and leaving it to entities to decide

on the means for its implementation (including whether to leverage existing investments).

Moreover, we believe it is necessary, in the event of fraud or scams suffered by the customer due to the actions of a third party which is authorized to access data under FIDA, to provide more clarifications on the liabilities in level one. Given that there will be wider data circulation under FIDA (different schemes, entities), this is needed, together with clear obligations in terms of the liability of the data user).

7. Interaction with other relevant frameworks

7.1 Incorporating lessons learned from PSD2

Compared to PSD2, FIDA takes a different approach in relation to the possibility for a market driven approach and compensation. These are two key takeaways from the latter framework and other points, such as leveraging the investments under PSD2 (interfaces, security measures, etc) for the implementation of FIDA can also be incorporated. The level of investment that will be required by data holders for FIDA should not be underestimated and duplication in costs needs to be avoided where possible.

Departing from this, other reflections such as a lower level of adoption of services than expected under PSD2, should also be considered. There have been few evaluations of the commercial opportunities for such services, despite the significant resources required to develop and customize systems, which compete with other investments that can contribute to increased resilience and economic competence. With such a broad scope of financial data under FIDA, it also raises the question of the evaluation of expected economic benefit. As mentioned in the Executive Summary of this paper, an assessment to the impact of the business model of financial intermediaries – is lacking.

7.2 Interplay with the GDPR

A greater understanding is needed on the scope of the right of access (Art. 15 GDPR) against the right introduced under Art. 4 of the proposal. What is the difference between the data subjects' rights in the GDPR and the FIDA obligation? Clarification is needed to differentiate "permission" according to FIDA from "consent" according to the GDPR.

7.3 Interplay with the Data Governance Act (DGA)

The proposal refers to the DGA in recital 21 but only in regard to the possibility for data sharing intermediaries to provide permissions dashboards for the data holder. However, simply providing a permission dashboard as a technical provider to a data holder cannot be seen as a data intermediation service under the Data Governance Act. The reference under recital 21 therefore seems out of place.

There are also wider questions on the FIDA and DGA interaction: are schemes a form of data intermediation under the Data Governance Act? Are schemes data spaces? Including a recital in the proposal to clarify these points would be welcome.

7.4 Interplay with the Digital Markets Act

The Digital Markets Act is mentioned in the explanatory referendum as an example of a

cross-sectoral initiative that establishes "*a number of data related obligations*", also as a way, in our view, to show that the financial sector is not the only one where mandatory data sharing rights are introduced. While we do recognize this, it is important to keep in mind that only through an **effective implementation by designated gatekeepers of the data related obligations.** An operationalized implementation of the Digital Markets Act must therefore be ensured.

8. Review of the Regulation

A review 4 years after such an ambitious project means that **there will be no stability**: the review is likely to begin before the initial implementation is over. The timeline needs to take into account a gradual scheme development approach, as proposed above. It is worth noting that the Commission will be able, when reviewing the regulation, not only to add new data sets, but also to delete them (and also to delete entities in scope– see Art.31 b). The power to delete data sets which are under data sharing schemes that have been set up with considerable efforts by market actors is counterproductive.

The risk for the customer should also be considered- if their data could be used by certain providers which have been previously collected and then deleted ex-post from the scope of this Regulation. Therefore, a **clear, set scope is needed before starting implementation** the setting up of schemes in order to not make investments without any return and to risk new and continuous developments.

ENDS

ANNEX

ADDITIONAL COMMENTS ON THE FIDA PROPOSAL

Definitions

Article 3 (2):

- For the moment, all client groups are included in the **definition of a customer**– retail, SME, and wholesale. **Wholesale customers and their data should be excluded at this stage from FIDA** as i) the value of mandatory data sharing is least clear for this group and ii) wholesale customer data is hardest to standardize. Already with retail customers and SME data, data holders will have to make significant investments without clear economic benefits – adding corporate customers to the list as well is challenging.
- Instead of classifying customers as those who "make use of financial products and services", we suggest to describe them as those that are "**party to an agreement**" for the use of financial products and services referred to in Art. 2(1). It also narrows down that it can only be the customer with the contractual relationship (in the case of a consumer), not their spouse, for example or another person authorized to use the account.
- Currently, the scope is not limited to customers that live in / are established in the European Union. This should be included in the definition of "customer".

Art. 3 (3):

- The wording - "*data generated as a result of user interaction with the financial institution*" – if not clarified, could **capture derived and inferred data in the scope – data that is enriched by financial institutions.** Examples, include calculations or assessments made by a financial institution in the interaction with customer such as suitability and appropriate assessments. These processes and the data that stem from them, constitute an element of competition for the company, making use of its expertise and know-how; **it should not be subject to data sharing requirements under FIDA**. This applies to all the derived and inferred data **under the Art. 2(1) data categories**. This would also reflect the difference between provided data and inferred and derived data, which was established by the former WP29 (now EDPB) in the guidelines on the right to data portability (Art. 20 GDPR)[9].
- Customer data should only refer to data that is **listed in Art. 2(1).** The definition does is not clear on '**who' can generate such data** and, in particular, whether they can also **be third parties** (e.g., appraisers, advisors) or an electronic tool (e.g., a financial calculator, AI chatbot), or only the staff of a financial institution. We suggest that it **excludes data from a third party** (e.g., purchased from a

[9] European Data Protection Board, Guidelines on the Right to Data Portability, December 2016

third party), as the data holder (e.g., a financial institution) may not be the 'original' data holder.

- Clarify the definition **vis-a-vis other concepts_already protected under European and national legislation** (e.g., confidential business data, **trade secrets**, intellectual property rights). **Recital 9** of the Regulation is important, as it states that "*the sharing of customer data in the scope of this Regulation should respect the protection of confidential business data and trade secrets"*. This should, in our view, apply also for the confidential **business information/trade secrets of the data holder,** not just the customer and be included directly in the definition of customer data under Art. 3(3).

  We also question whether simply "protecting" confidential business data and trade secrets is enough, especially as one of the horizontal principles under the Data Act Art. 8(6) is that "*unless otherwise provided by Union law, including Articles 4(3), 5(8) of this Regulation, or by national legislation adopted in accordance with Union law, **an obligation to make data available to a data recipient shall not oblige the disclosure of trade secrets within the meaning of Directive (EU) 2016/943".*** FIDA should be consistent with this provision.

Additional comments:

- Dashboards and schemes are two key concepts in the Regulation but are missing a definition under Article 3.

2. Scope

Art. 2(1a): mortgage credit agreements, loans, and accounts, except payment accounts as defined in the Payment Services Directive (EU) 2015/2366, including data on balance, conditions and transactions

i. Terms such as **mortgage credit agreements, loans, and accounts are not defined by FIDA**. Therefore, it is not clear how they should be understood. To illustrate: when FIDA refers to 'loans', is it a reference to any form of credit financing or to a specific legal form (e.g., 'loan' or 'credit' or 'deferred payment' or 'trade credit').

ii. The term 'account' is generally not defined in EU law. Beyond payment account there are as 'technical accounts' maintained by acquirers, but also securities 'accounts' under the national laws or FX wallets. The text needs to be clear.

iii. As **consumer mortgages are defined in Directive (EU)2014/17,** a reference should be added to this Directive to clarify that this is the intended data category.

iv. Only loans provided by a data holder (e.g., the bank) should be in scope. Loans held by a family member or loans at other banks should be excluded. This follows the logic of who is the primary data holder and customer concerned as well.

v. The term "**conditions" is very far reaching**, possibly including general terms and conditions, and **varies significantly across different types of products** such as mortgage credit agreements, loans, and accounts. The provision of real-time access to all conditions of a product contract does not seem to be intended, nor would it be justifiable from an effort vs. customer benefit point of view.

vi. The contract between a bank and a customer should be considered as confidential information.

Art. 2(1b): savings, investments in financial instruments, insurance-based investment products, crypto-assets, real estate, and other related financial assets as well as the economic benefits derived from such assets; including data collected for the purposes of carrying out an assessment of suitability and appropriateness

i. For the moment, it is unclear whether "**savings"** refers to products such as term deposits, savings accounts or rather investment products of a savings nature. We therefore recommend that the **text references the relevant existing EU legislation:**

   a. "Savings, investments in financial instruments" as specified in **Section C of Annex I to Directive 2014/65/EU (MIFID II)**.

   b. Crypto assets as referred to in article 3(1)(5) of **Regulation 2023/1114/EU (MICA).**

ii. Clarify that derivate transactions used for risk-management purposes are excluded from "investments in financial instruments".

iii. The proposal mentions financial assets such as real estate. Is this a **reference to real estate investments** (which do not seem relevant to us as they are not financial assets) **or to financial instruments that invest in this asset class**, in which case it would not be necessary to mention them (because they would fall into the category of "financial instruments"). In addition, there is **no "natural data holder" among the financial institutions listed under Art. 2(2) for this type of data**. This is due to the fact that customers' physical real estate assets are neither a product or service of a financial institution, nor are those assets managed by a financial institution on behalf of the customer. Only those data holders should be legally obliged to grant access to customer data if they are directly responsible for it in the sense of authentic source.

iv. Connected to the above, credit institutions should not be obliged to display information about the properties on which they hold mortgages. For example, in some member states this information is exhibited by the public sector, which would qualify as the authentic source ("primary source").

Art. 2 1 (c) & Art. 2 (1) (d): pension rights in occupational pension schemes; pension rights on the provision of pan-European personal pension products. Art. 2(1)(c):

i. **Art. 2(1)(d)**: Pan-European personal pension product has a distinct definition under Regulation (EU) 2019/1238 and reference should be made to it.

Art. 2 (1) (e): non-life insurance products in accordance with Directive 2009/138/EC, with the exception of sickness and health insurance products;

including data collected for the purposes of a demands and needs assessment; data collected for the purposes of an appropriateness and suitability assessment

i. Include a reference to Annex I to Directive 2009/138/EC, as it provides classes of non-life insurance products. The current wording does not explain what 'non-life insurance products' mean.

ii. Overall, is the data in scope limited to insurance policy number, type of insurance, insurer or premium and coverage. We understand that the latter is in the scope.

Art. 2(1f):data which forms part of a creditworthiness assessment of a firm which is collected as part of a loan application process or a request for a credit rating.

i. The data collected as **part of a loan application process or a request for a credit rating should not be in scope of the Regulation**. The scope of this data is very broad and includes information which may constitute trade secrets of financial institution. There are **different internal methodologies for assessing the creditworthiness of firms**; in other words, there is specific bank know-how in the processes (e.g., using information on past credit files to assess the risk). If the input data is then used by a data user (also without the further knowledge of the context/etc), this **could result in disclosing sensitive information, thereby impacting competition** (see next point).

ii. Assessing creditworthiness is a core aspect of banking and is usually related to a specific situation and credit product. By making it mandatory to share this data, subject to the pricing requirements of Art. 10(1)(h), will **allow competitors, providing similar credit products, to use this data without making the required investments, leading to a race to the bottom**. It is also a big challenge to standardize this type of data.

iii. There is the **important aspect of third-party data** where a financial institution may not be the "primary" data holder, for example, where the source is public administration (e.g., a tax declaration). If re-used it could also raise questions in terms of responsibility for data accuracy.

iv. The article should explicitly mention that the final credit score is not in the scope of data sharing.

Additional comments on scope

i. **Recital 13:** Customer data in scope includes **"sustainability related information".** At this stage, we recommend to **exclude this category of data from the scope of FIDA** as:

- It is too early to include this type of data, given the **still developing legislative framework on sustainability** (for example, the Corporate Sustainability Reporting Directive (CSRD). FIDA should not front run this; if it does, there would be no link to existing EU legislation. Separately, alignment with CSRD is very relevant for business customers. Such alignment might increase customer demand, to facilitate their own sustainability disclosures. Yet, again, FIDA should not front-run sustainability (information/disclosure) regulations.

- The "third party data" element is very present in this type of data - often data comes from external sources in this field.
- Sustainability data is not always visible from transaction data – the assumption made in the recital is incorrect.

ii. **Interplay with PSD2:** Art. 2 and Recital 12 clearly exclude payment account as defined under Art. 4 (12) of Directive (EU) 2015/236611 (PSD2). Yet, **what is considered a payment account varies across member states.** For example, regulated saving accounts in Belgium are not considered as "payment accounts" and are out of scope of the national legislation transposing PSD2; they will therefore be subject to FIDA. In certain member states however, such as France, saving accounts are considered as payment accounts. Will they be subject to PSD2 or to FIDA?

3. Permissions dashboards

General Comments

i. A significant responsibility is imposed on the data holder for keeping up to date, real time information for the customer; the information should be accurate, the purpose of the permission should be specified, and so on. It should be clear however, that **permission dashboard does not replace the customer's agreement on data processing vis-à-vis the data user.** The proposal should therefore specify that it is the data user's responsibility to provide the customer with the terms and conditions that govern the relationship between the data user and the customer. Not the data holder. This should also include the "***possible contractual consequences of the withdrawal of a permission***", which according to recital 22 has to be part of the dashboard and something to be shown by the data holder, whereas again, it should also be clear from the start in the relationship between the data user and customer.

ii. The proper functioning of the dashboard is built around an effective cooperation between the data holder and the data user and the flow of information. As the data user will be providing the information, per art. 8 4(b), it should be stated that **the data holder is not held responsible for the accuracy of the data provided to them by the data user**. They are not required to summarise / interpret / check the data they receive from the data user for inclusion in the dashboard.

iii. Taking a wider scope, **consistency between the permissions dashboard obligation under FIDA and the Payment Services Regulation (Art. 43 PSR) is important**, particularly for data subjects to have a harmonized user experience when it comes to payment data and the data under FIDA and to also avoid duplication of investments on the part of data holders. Therefore, as the two provisions are almost identical, **we suggest that it should be sufficient to build one dashboard to meet the requirements of FIDA and the PSR.**

iv. The obligations under the permission dashboards should complement existing obligations under the GDPR. This includes the different responsibilities of the data holder and the data user, with the latter as the **data controller in the customer-data user relationship.** They are the ones who decide the **purpose of processing and need to meet the information obligations under Art. 13, for**

example. On top of this, we would like to stress that there is a responsibility of the data user, once permission is given, to comply with the GDPR, including data processing principles such as purpose limitation which FIDA also introduces through the FISP licence, that is bound to a specific purpose.

Specific comments:

i. **Art. 8(2)(a):** the paragraph should be updated to reflect that the dashboard should provide the customer "to the extent that this information was provided to the data holder by data users." This would adequately reflect that the **requirements can only be met if the information is provided by data users to data holders.**

ii. **Art. 8(2)(c)** includes a requirement that allows the customer to **re-establish any withdrawn permissions**. Yet, how would this work practically? For example, what if the purpose for processing the data by the data user has changed in the meantime? This process does not work without the involvement of the data user. In addition, it **does not comply with the principles of data minimisation or proportionality if this information would have to be stored by the data holder.** We therefore would recommend to **delete this provision.**

iii. **Article 8(4):**

- We would suggest to replace real-time with **the requirement to cooperate "immediately"** as cooperation in real time may not be possible.
- In connection with the obligation to cooperate between the data holder and the data user there should be an obligation on a data user to inform data holder about the withdrawal of permission from the customer. It may be implemented in Art. 8 (4) (c) by stating that *a data user shall immediately inform data holder of a permission withdrawal.*

4. Additional comments

Article 4

This article needs further examination in terms of the obligation to make data available to the customer. First, customers already have access to most of the data covered by the data sharing obligation **through existing channels,** such as online banking. It is our understanding that **such channels sufficiently address the requirements of Art. 4** so that no additional channels must be built.

Second, in relation to the reference of the data access "continuously and in real time", we would question if this were proportionate for all data in scope, especially where data in scope is static. We would suggest to add a qualifier such as **"where needed**". Furthermore, the wording "by electronic means" and "upon request" is vague and should be clarified by defining the security requirements of the request procedure by the client. We propose to keep the same framework as the one in the PSD2.

Article 6(2)

Article 6.2 provides for the deletion of data by the data user if it is no longer necessary to achieve the purposes for which the customer has granted his permission. However, FIDA does not contain provisions allowing for the retention of this data if it is needed for other

purposes, e.g., related to an ongoing court dispute or accounting. **The relevant GDPR provisions should apply in the case of personal data.**

Data perimeter guidelines (Art. 7)

We are concerned about the development of new guidelines on the use of personal data for creditworthiness and for assessing and pricing of life and health insurance. This may limit innovation and the possibility to differentiate from competitors. In addition, it is not clear whether the guidelines would also apply **to the use of data that is within the scope of this regulation but is already in the hands of the bank and has not been accessed from a third party.**

Article 28(1)

Article 28(1): This article would benefit from a clarification on the territorial scope of FIDA. In particular, Union customers could be clarified as customers established in the Union. Moreover article 28 should be clear that data held with non-EU branches should be considered out of scope.

ENDS

For more information:

Alexandra Maniati
Senior Director, Innovation & Cybersecurity
a.maniati@ebf.eu

Liga Semane
Policy Adviser, Data & Innovation
l.semane@ebf.eu

About the EBF

The European Banking Federation is the voice of the European banking sector, bringing together 32 national banking associations in Europe that together represent a significant majority of all banking assets in Europe, with 3,500 banks - large and small, wholesale and retail, local and international – while employing approximately two million people. EBF members represent banks that make available loans to the European economy in excess of €20 trillion and that reliably handle more than 400 million payment transactions per day. Launched in 1960, the EBF is committed to a single market for financial services in the European Union and to supporting policies that foster economic growth.

www.ebf.eu @EBFeu