AIPB Feedback on the European Commission's Proposal on Financial Data Access (FIDA)

Milan, 1 November 2023

The Italian Private Baking Association (*Associazione Italiana Private Banking*) ("**AIPB**") extends its gratitude to the European Commission for the opportunity to present its position on the proposal (the "**Proposal**") for a Regulation of the European Parliament and of the Council establishing a framework for Financial Data Access ("**FIDA**") and amending Regulations (EU) No. 1093/2010, (EU) No. 1094/2010, (EU) No. 1095/2010, and (EU) 2022/2554 (the "**FIDA Regulation**") published on 28 June 2023.

The Proposal forms part of an ambitious series of legislative measures aiming to stimulate innovation and digital advancement in the financial services industry by fostering data-driven business models. While the Proposal largely builds upon the principles enshrined in the "open banking" framework under Directive (EU) 2015/2366 (the "**PSD2**"), it pursues a much more challenging goal consisting in the sharing of financial data beyond payment accounts' information.

The creation of an "open finance" environment in the EU is a demanding task which requires a thorough evaluation of the legislative tools employed to this end and the overarching policy goals. We recognize the potential of FIDA to facilitate the provision of investment and financial services that are more tailored to the needs of the client, and we appreciate how FIDA can enhance the quality and increase the amount of the data that are employed by investment firms and financial institutions for the provision of their services.

The Proposal's attempt to strike a balance between potentially conflicting interests is also noteworthy. Some of these interests, such as data security and confidentiality, the need to protect trade secrets and intellectual property rights, and the avoidance of financial exclusion, are of paramount importance for the success of the initiative.

While recognizing the merits of the Proposal, we note that there are several legal and technical aspects concerning the scope of application of the FIDA Regulation and the obligations undertaken by data users and data holders which should still be clarified. These aspects must be defined directly in the text of the FIDA Regulation or, if this is not possible, by way of regulatory technical standards (RTS), implementing technical standards (ITS), or guidelines issued by European Supervisory Authorities (ESAs).

The lack of standardized templates or procedures could also lead to a significant fragmentation in the approaches taken by market players while implementing the FIDA obligations. The FIDA Regulation should set a clear framework for the definition of uniform standards applicable to the transmission of financial data,

and should avoid that different or multiple standards and procedures are followed by data holders and data users.

In addition to the general comments outlined above, we find it necessary to outline our proposals regarding certain aspects which could potentially have negative consequences for market players and ultimately undermine FIDA's goal to establish an "open finance" environment which is efficient, transparent and equitable for all participants, as per the following summary:

- **Need to clarify the role of FISPs** – The Proposal should limit the role of FISPs to avoid that they can use the access to financial data to perform regulated services, such as investment advice, portfolio management or distribution of financial services or products. FISPs should be allowed to collect financial data and share them only with financial institutions that are authorized to provide the relevant regulated services. FISPs should also be subject to the same rules that apply to data holders and should be under an obligation to share the data that they collect with other financial institutions and FISPs.
- **Need to review the regime applicable to third country FISPs** – Third country FISPs must also be subject to data sharing obligations under a condition of reciprocity. In addition, third country firms should be allowed to be authorized as FISPs only if they are subject to regulatory supervision and if the competent authority of their own jurisdiction entered into a cooperation agreement with EU competent authorities.
- **Need to avoid opportunistic, manipulative or fraudulent behaviours** – The Proposal does not contain sufficient measures to prevent opportunistic or manipulative behaviours by market players who wish to access financial data to gather information on the products and business operations of their competitors. There must be a list of purposes for which financial data cannot be used by data users, which must include for instance the offer of services or products mirroring those provided by the data holder. The Proposal should also avoid deceptive or manipulative behaviours to gather customer's permission and impose specific information duties on data users *vis-à-vis* the customers regarding the treatment of their non-personal data. To avoid possible frauds and identity thefts, permission can be given only with strong authentication measures in line with the PSD2 framework.
- **Need to further clarify the key terms of the FIDA Regulation** – The Proposal contains some wide-ranging terms and definitions (such as in particular the definition and list of customer data) which must be further defined and limited to avoid possible regulatory uncertainties. Data sharing obligations should not apply to data that are autonomously elaborated by financial institutions – *e.g.* to conduct market analysis, identify possible business strategies, etc. Only raw data generated from the customer interaction with the financial institution should be subject to data sharing obligations.
- **Limitations to the data sharing obligations** – Financial institutions should be entitled to refuse the transmission of certain data that are particularly sensitive for their business in exceptional circumstances which must be identified in the FIDA Regulation. The duty to grant continuous and real-time access by data users should not entail any obligation to ensure that all financial data are also updated real-time. The FIDA Regulation should set specific limitations on the number of accesses that can be made by data users in line with the EU open banking framework.

- **Need to achieve a standard set of procedures and methods to share financial data** – To avoid the multiplication of operational rules and standards – which could increase compliance costs of market players – the FIDA Regulation should provide for the establishment of a single set of protocols and technical procedures for the sharing of data. This aim should be pursued by way of EU delegated acts and/or handbooks prepared by a single EU self-regulatory body. The establishment of these common standards and procedures should require at least 36 months, after which financial institutions and FISPs should have at least 12 months to comply with the FIDA obligations.
- **Strict liability regime for data users –** The liability regime applicable to data holders and data users should be harmonised at EU level under the FIDA Regulation. Data users should be subject to a strict liability regime in case of data breach, misuse of personal data or failure to comply with the FIDA rules.

The paragraphs below provide a more detailed explanation of the position highlighted in the above summary. They also include some supplementary considerations on other aspects of the Proposal which would require additional clarifications or could be further improved. A table providing an overview of our position and proposals is attached as Annex A hereto.

* * * *

1. Subject matter of the Proposal and regulation of financial information service providers (FISPs)

1.1 *Regulation of FISPs* – The purpose of the Proposal is to establish rules on the access, sharing and use of certain categories of customer data in financial services, as well as on the authorisation and operation of financial information service providers ("**FISPs**").[1]

FISPs are essentially the equivalent of account information service providers ("**AISPs**") for the access to financial data. They will be eligible to access customer data if they are authorised to operate as FISPs by the competent authority of their home Member State.[2] The Proposal outlines the requirements that must be met in order to obtain a license to operate as a FISP.[3]

Financial institutions seeking access to customer data do not require a license to operate as FISP.

1.2 *Activities that can be carried out by FISPs* – The Proposal does not clearly specify the purposes for which a FISP can use the financial data collected by the customers. Considering the nature and amount of data that FISPs can collect under the FIDA, there is a risk that these data are used to offer advisory, consultancy, portfolio management or similar services, or referral and distribution activities, in the absence of the licenses that are required under the EU and national regulatory framework for the performance of such services.

The Proposal must clearly specify that FISPs are prevented to use financial data to provide any service that would require a license to operate as financial institution in accordance with the applicable EU or national regulatory framework. Particular attention should also be paid by competent authorities in

[1] Article 1 of the Proposal.

[2] Article 12(1) of the Proposal.

[3] Article 12 of the Proposal.

verifying the compliance with this restriction to avoid that the FISP license can be used as a way to circumvent the applicable licensing obligations.

FISPs should be allowed to collect financial data and share them only with financial institutions that are authorized to provide the relevant regulated services. They should act as "data enablers" allowing financial institutions to provide better services to their customers by having access to the data shared by FISPs.

1.3 *Notification duties for certain financial institutions wishing to operate as data users* – Competent authorities should assess whether certain financial institutions are adequately organised to have access to customers' financial data before this access is granted.

Although data security obligations are covered, among others, by the common framework set out under the Regulation (EU) 2022/2554 on digital operational resilience for the financial sector ("**DORA**"), we believe that certain financial institutions wishing to operate as data users should notify this intention to their competent authorities, which should evaluate the adequacy of the IT, organisational and security measures as well as of the audit arrangements adopted to ensure that they operate in line with the FIDA Regulation (in addition to DORA).

This obligation should apply to all financial institutions that are not subject to strict governance and organizational requirements under the EU regulatory framework. Credit institutions, investment firms, payment and e-money institutions, AIFMs and UCITS management companies, as well as insurance and reinsurance undertakings should be exempt from the assessment referred to above due to the strict requirements that already apply to them under EU law.

It is also worth noting that some financial institutions included in the scope of the Proposal (such as insurance intermediaries or crowdfunding service providers) are not subject to regulatory capital requirements. Consequently, these entities should be mandated to take out a professional indemnity insurance policy covering the same risks outlined in Article 12(3) of the Proposal.

1.4 *FISPs as data holders* – The definition of "*data holder*" that is used in the Proposal makes reference to financial institutions only, while FISPs seem to be excluded from the scope of such definition.[4]

It is important though that FISPs are subject to the same data sharing obligations applicable to financial institutions as data holders: FISPs could indeed collect a significant amount of data and information concerning their customers and preventing other financial institutions (or FISPs) to have access to such data and information would distort the competition among market players. The definition of "*data holders"* should accordingly be amended to include a reference to FISPs.

2. Scope of application: definition of customer data

2.1 *Definition of customer data* – The definition of customer data encompasses both personal and non-personal data "*that is collected, stored and otherwise processed by a financial institution as part of*

[4] Article 3(5) and (8) of the Proposal.

their normal course of business with customers which covers both data provided by a customer and data generated as a result of customer interaction with the financial institution".[5]

While the definition of personal data is derived from Regulation (EU) 2016/679 (the "**GDPR**"),[6] the concept of non-personal data is new and comprises all data that do not qualify as personal data under the GDPR.[7]

Customer data that are relevant for the purpose of the Proposal are those relating to the financial services and products listed in Article 2(1) of the Proposal.

2.2 *Need to further clarify the scope of the definition* – We believe that the concept of customer data must be further defined to minimise potential regulatory uncertainties.

Specifically, the Proposal should offer a clearer definition of the types of non-personal data that fall within the scope of the FIDA Regulation. Under the current Proposal the scope of non-personal data could encompass a broad range of information and details relating to the interactions between the financial institution and the customer. This might include, for instance, the technical data associated with each transaction on financial instruments, along with information and data collected in the context of the customer due diligence process followed for AML purposes. Conversely, we believe that only raw data generated from the customer interaction with the financial institution should be subject to data sharing obligations.

In the absence of well-defined parameters to identify the data that are subject to sharing obligations under the FIDA Regulation, the volume of data that data holders could be required to store and share with data users could be very extensive. There might also be divergent interpretations between data users and data holders (or between financial data sharing schemes) as to what constitutes a financial data to be shared for the purpose of the FIDA Regulation. It is not entirely clear also whether or under which conditions the sharing of financial data would require the sharing of the supporting legal or technical documentation or of the related key terms (*e.g.* terms and conditions governing the product or service offered to the customer, other information documents, etc.).

Data holders should receive explicit guidance regarding the specific data that they are required to provide to data users, or at the very least on the minimum dataset to be shared in relation to each particular service or product listed in Article 2(1) of the Proposal.

2.3 *Data that are autonomously elaborated by financial institutions* – Financial institutions undertake independent data mining and evaluation activities concerning customer data. The integration of AI

---

5 Article 3(3) of the Proposal.

6 Article 3(11) of the Proposal. According to Article 4(1) of the GDPR, "personal data" means "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*".

7 Article 3(10) of the Proposal.

tools will likely encourage these endeavours with a view to developing appropriate business strategies and offering more customer-centric services.

Data mining efforts could result in the preparation of wide-ranging research or strategy documents on customers' behaviour or preferences, as well as in the presentation of specific proposals for individual customers.

Considering the substantial investments made by financial institutions in this domain, data that are autonomously generated or elaborated by data holders should be clearly excluded from the scope of the data sharing obligations envisaged in the FIDA Regulation.

Including these types of data in the scope of the FIDA Regulation would lead to possible opportunistic behaviours by other market players, who might gain from the investments made by other data holders. This could in turn diminish the incentive for financial institutions to analyse customer behaviour data, thus undermining the quality of the services offered to the customers.

The definition of customer data as presented in the Proposal refers to data collected in the "*normal course of business with customers"* by financial institutions and includes "*data provided by a customer"* and data "*generated as a result of customer interaction with the financial institution*". Consequently, it is our interpretation that data related to a customer (or a group of customers) that are automatically processed or elaborated by financial institutions do not fall within the scope of the definition of customer data. However, we would propose that this interpretation is explicitly confirmed in the FIDA Regulation.[8]

3. Scope of application: customer data and financial institutions acting as data holder and data users

3.1 *List of customer data* – The Proposal lays down an extensive list of customer data that must be shared by financial institutions.[9] Some of the concepts that are used in the list – such as the reference to "*other related financial assets*" or the "*economic benefits derived from such assets*" – as well as the key terms used in the Proposal (*e.g.* the notion of "*savings*" or "*loans*", etc.) should be further clarified, as they are still wide-reaching and too broad.

We also suggest excluding from the scope of the FIDA Regulation any information on real estate assets, or at least to specify that data holders should only share the information (if any) that they have concerning the real estate investment(s) made by their clients, without providing any further information on the real estate asset, including as regards its value (considering also that the information on the value of the real estate asset is developed by third parties and not by the financial institution itself).

---

8 For instance, the definition could specify that customer data are included in the scope of the FIDA rules "*provided that they are either provided by a customer or generated as a result of customer interaction with the financial institution or the financial information service provider, with the exclusion of those data that are autonomously developed, generated or elaborated by the financial institution or the financial information service provider on the basis of such interaction or otherwise".*

9 Article 2(1) of the Proposal.

Generally speaking, there should be no obligation for data holders to share the information concerning any other assets that are not subject to specific regulation under the existing EU financial services regulatory framework. In the absence of a common set of rules at EU level regarding this type of investments, it would be difficult to develop common standards for the sharing of financial data. Any detailed information regarding investments in non-regulated assets could be voluntarily supplied by the customer to the relevant data user.

3.2 *Information collected for AML purposes* – While recognizing that AML matters are outside the scope of the Proposal, it is worth pointing out that streamlining the access to, and the sharing of, the data provided by customers in the context of the customer due diligence process conducted by financial institutions could significantly help simplifying the KYC activities carried out for AML purposes.

The implementation of a common framework for the sharing of financial data might serve as an initial step towards such simplification. The FIDA Regulation and the EU AML legislation should clarify whether customers' data that can be shared among financial institutions and FISPs should include also the data collected for AML purposes, and whether these data can be used by financial institutions or FISPs – *i.e.* to rely on the customer due diligence conducted by third parties or create a common database of KYC data collected with respect to each customer.

4. Allocation of the data sharing obligations in case of multiple financial holders involved in the distribution or intermediation of financial products

4.1 *Multiple data holders* – The Proposal does not address the scenario where multiple data holders are involved in the distribution or intermediation of a financial product. For instance:

(a) an investment firm or a bank might act as distributor on behalf of a UCITS management company or an alternative investment fund manager, or could invest in units or shares of a UCITS or AIF as part of the portfolio management services carried out on behalf of the customer;

(b) an insurance policy could be distributed by an insurance undertaking through an insurance intermediary (*e.g.* a bank), which in turn might operate through one or more sub-distributors.

In these cases, the customer data related to the relevant products or services are held by multiple financial institutions. Each financial institution could have different sets of data concerning the financial product purchased by the customer.

4.2 *Proposal to clarify the allocation of responsibilities* – To avoid the duplication of financial sharing obligations and clarify their allocation, the Proposal should in our view specify that:

(a) financial institutions that ultimately issue or provide the relevant financial product or service listed in Article 2(1) (*e.g.* insurance undertakings, AIFMs, UCITS management companies, lenders, etc.) are responsible for providing all customer data concerning the specific product or service that they issued or provided to the customer (in addition to any other data that they may have); and

(b) other financial institutions that are involved in the distribution or intermediation of the product or service are responsible only for the transmission of the data that they hold, considering the nature of their relationship with the customer and of the service offered to them.

5. Obligation to provide access to the customer data continuously and in real-time

5.1 *Obligations of data holders* – Under the Proposal data holders are required to make the financial data listed in Article 2(1) available to customers "*without undue delay, free of charge, continuously and in real-time*".[10]

Similarly, the financial data must be made available to data users "*without undue delay, continuously and in real time*",[11] while the data holder can claim compensation for the access to such data only if the data is made available in the context of a financial data sharing scheme or in accordance with the delegated acts adopted by the European Commission.[12]

5.2 *Need to simplify the duties to be discharged by data holders* – The requirement for data holders to make the data available "*continuously and in real-time*" could potentially burden market operators with excessive costs, while not necessarily delivering significant added value to customers and data users.

While we are aware that this provision is aligned to the approach followed under the Data Act Proposal (the "**Data Act**"),[13] we note that the elaboration of certain customer-related data could require some time. Moreover, maintaining a perpetually up-to-date record of a customer's financial portfolio might not always be feasible and could lead to substantial costs for data holders.

To address this concern, we recommend amending the Proposal to clarify that data holders must grant access to the most recent data available with respect to their customers, while there should be no duty to ensure that such data are also updated continuously and in real-time.

We also note that the obligation to make data available continuously and in real-time creates a discrepancy between the open banking and open finance framework, considering that under the PSD2 AISPs are able to access to payment service user's information "*no more than four times in a 24-hour period*", unless a higher frequency is agreed with the payment service user's consent.[14] The rationale of this limitation is also to avoid that the PSP is overflooded by access requests made by AISPs – but the same consideration could apply to access requests made by data users under the FIDA.

Finally, the Proposal should specify that access to the data can be suspended in case of maintenance activities and that data users are under no obligation to provide any assistance to data users on how the data should be accessed and processed.

---

10 Article 4 of the Proposal.

11 Article 5(1) of the Proposal.

12 Article 5(2) of the Proposal.

13 Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data.

14 See Article 36(5)(b) of the Commission Delegated Regulation (EU) 2018/389.

6. Customer's permission to the sharing of customer data and purpose of the data treatment

6.1 *Customer's permission as a condition for the sharing of financial data* – The Proposal clarifies that the data holder must make available to the data user the customer data listed in Article 2(1) of the Proposal "*upon request from a customer submitted by electronic means*" and "*for the purposes for which the customer has granted permission to the data user*".[15]

The data user must access the customer data only "*for the purposes and under the conditions for which the customer has granted its permission*"[16] and must "*not process any customer data for purposes other than for performing the service explicitly requested by the customer*".[17] The data user must also "*respect the confidentiality of trade secrets and intellectual property rights when customer data is accessed*".[18] It must "*delete customer data when it is no longer necessary for the purposes for which the permission has been granted by a customer*".[19]

6.2 *Competition concerns and risks of opportunistic behaviours* – According to the approach followed under the Proposal, the customer's permission is the central factor to determine the purpose for which customer data can be used.

Although the customer's consent is undoubtedly essential for grating access to customer data, it cannot be sufficient in our view to define the range of purposes for which customer data can be used.

The Proposal should at least specify those cases where the use of customer data is considered illegitimate, at the same time leaving room for financial institutions and customers to determine the legitimate purposes for which the data can be used.

In this respect, it is crucial to recognize an essential difference between the sharing of data in an open banking and an open finance environment.

Transactions on payment accounts reflect the spending patterns and choices of payment service users. Sharing data on payment transactions provides limited access to proprietary information concerning the business of other PSPs.

On the contrary, sharing data on transactions in the financial products considered under the FIDA Regulation permits competitors to gather business information on the services and products offered by data holders to their customers.

The offer of financial services or other products is the result of multiple efforts and investments made in market research and modelling, data gathering and elaboration, and financial engineering. Each financial institution's competitive advantage is grounded on its capacity to understand and anticipate market trends and manufacture financial products that are best suited to meet the clients' needs.

---

15 Article 5(1) of the Proposal.

16 Article 6(2) of the Proposal.

17 Article 6(4)(a) of the Proposal.

18 Article 6(4)(b) of the Proposal.

19 Article 6(2) of the Proposal.

In an "open finance" environment there is a notable risk that market players can exploit the access to financial data held by other financial institutions to reverse-engineer the financial models or algorithms used, or replicate the financial products offered, by their competitors. These opportunistic behaviours could lead to unequitable competition and other market distortions. For instance, data sharing mechanisms could enable other players to emulate the competitors' products at lower costs, leveraging also AI tools.

These opportunistic behaviours could discourage investments in the development of proprietary trading or asset allocation models, stifle innovation and ultimately lower the quality of financial services available to the customers.

6.3 *The Proposal should identify those uses of customer data that are not legitimate* – To address the concerns mentioned above the Proposal specifies that the financial data must be used in compliance with the purpose authorised by the user, and provided that the confidentiality of trade secrets and intellectual property rights is safeguarded.

However, it is important to acknowledge that financial research, models and algorithms that are used by financial institutions are not necessarily protected as trade secrets or intellectual property rights under applicable laws. Additionally, relying solely on the obligation to safeguard the confidentiality of these data might not be sufficient to prevent opportunistic uses by market competitors.

We recommend that the Proposal includes a comprehensive list of illegitimate purposes for which the use of customer data is strictly prohibited, irrespective of the customer consent. Specifically, data users should be explicitly barred from utilising customer data acquired from data holders to:

(a) offer services or products mirroring those provided by the data holder;

(b) engage in reverse-engineering or similar activities in respect of the services or products of the data holder;

(c) probe into the data holder's business model with the intent, for instance, to identify its partners, the economic terms applied to its services and products, etc.

In this respect, we note that a similar approach is already followed under the Data Act, which specifies for instance that the third party receiving the data upon request of the user must not "*use the data it receives to develop a product that competes with the product from which the accessed data originate*" and further details the purposes for which the data cannot be used.[20]

More generally, the use of the financial data gathered from other data holders should be strictly limited to the purpose of improving the service offered to the customer. The compliance with the prohibitions provided for in the list should be subject to strict oversight by the supervisory authorities and any use going beyond this purpose should be considered a misuse a financial data subject to severe sanctions in accordance with the FIDA Regulation.

[20] Article 6(2) of the Data Act.

6.4 *Forms for the expression of the customer's permission and information duties* – The risks highlighted above are even more relevant considering that the Proposal does not specify how the customer's permission should be expressed.

By stating that the request can be submitted "*by electronic means*", the Proposal does not exclude the possibility that the customer's permission collected through manipulative tools, devices or procedures. Furthermore, the Proposal does not impose any specific information duties to data users wishing to collect the customer's permission – other than those that are generally provided for under the GDPR for personal data.

In this respect, we would propose to:

- further specify the procedure that must be followed by data users to gather the customer's permission in order to exclude the risks of opportunistic behaviours;
- introduce a general principle whereby the customer cannot be deceived or manipulated by data users for the purpose of getting its permission to the sharing of data;[21]
- standardise as much as possible the forms to be used for the purpose of collecting the customer's consent and ensure that these forms have the same structure and granularity of the permission dashboards used in accordance with the FIDA Regulation (in order to avoid that the information included in the forms do not match with the information requested in the dashboard, *e.g.* with respect to the types of products for which the consent is given, etc.);
- introduce reliable anti-fraud mechanisms to ensure that the consent is given by the user; these mechanisms could consist in the adoption of strong customer authentication (SCA) tools similar to those regulated under the PSD2;
- impose information duties on data users regarding the purpose of the treatment of non-personal data under the FIDA in line with the GDPR rules on the treatment of personal data.

6.5 *Possibility to refuse the transmission of data or information that are particularly sensitive from a competitive or business standpoint in exceptional circumstances* – The Proposal currently lacks provisions addressing the need for data holders to protect the confidentiality of exceptionally sensitive data when fulfilling access requests from other data users. These sensitive data could pertain, for instance, to the economic or other terms agreed upon with other financial institutions for the distribution of a product or service, or data that are material for the respective business operations (*e.g.* data that can disclose information on the IT security system of the data holder).

In some cases, customers' data could embed price sensitive information or an information that is otherwise relevant according to the Market Abuse Regulation (*e.g.* a loan extened to a customer for the acquisition of qualified shareholdings in a listed company).

[21] Article 6(2)(a) of the Data Act provides, for instance, that the third party receiving the data "*shall not […] coerce, deceive or manipulate the user in any way, by subverting or impairing the autonomy, decision-making or choices of the user, including by means of a digital interface with the user*".

Other examples of data that are particularly sensitive are those data that are covered by strict confidentiality obligations agreed upon with other entities, whose disclosure could expose the data holder to liability for breach of contract.

The Proposal should allow data holders to selectively omit the transmission of particularly sensitive data, even though this possibility should be restricted to exceptional circumstances clearly identified in the FIDA Regulation. Data users should have the right to challenge this decision by lodging a complaint with the competent authority of the data holder or the applicable financial data sharing scheme, which would then determine whether the refusal of the data holder was legitimate.

7. Financial data sharing schemes

7.1 *Rules on the functioning of financial data sharing schemes* – The Proposal provides that data holders and data users must become members of financial data sharing schemes to share customer data.[22]

Financial sharing schemes must be set-up as self-regulatory arrangements by industry participants with the participation of customers' organisations and associations.[23] Each financial data sharing scheme must set out the common standards for the data and the technical interfaces to allow customers to request data sharing; these standards or technical interfaces may be developed by scheme members or by other parties or bodies.[24]

As a fall-back solution, if a financial data sharing scheme is not developed for one or more categories of customer data and there is no realistic prospect of such a scheme being set up, the Commission may adopt delegated acts to specify, among others, the common standards for the transmission of the data and, where appropriate, the technical interfaces to be used by customers to request data sharing.[25]

7.2 *Need for a common set of rules and standards for the sharing of financial data* – While we appreciate the Commission's intent to delegate the definition of the operational rules and standards for the transmission of financial data to market participants, we are afraid that the potential proliferation of multiple financial data sharing schemes could introduce complexities and raise compliance costs to be borne by market operators due to the multiplication of the operational rules and standards referred to above.

EU Institutions should ensure that a single set of operational rules and standards (including as regards the technical interfaces to be used by customers) is established at EU level in order to streamline the process to be followed by FISPs and financial institutions to share customer data.

The common set of rules and standards could be defined through a combination of delegated acts issued by the Commission in the form of RTS or ITS, on the one side, and guidelines or standards issued by EU self-regulatory bodies or market associations, on the other side.

22 Title IV of the Proposal.

23 Article 10(1)(a) of the Proposal.

24 Article 10(1)(g) of the Proposal.

25 Article 11(1) of the Proposal.

As the timing for the development of this framework will be significant, we propose to provide for the application of a 36-month period for the establishment of the common standards and procedures for the sharing of financial data, and an additional 12-month period for the full implementation of such standards and procedures by financial institutions and FISPs.

8. Compensation

8.1 *Compensation mechanisms* – Financial data sharing schemes must establish a model to determine the maximum compensation that a data holder is entitled to charge for making data available to data users.[26] The model must be based on a series of principles identified in the Proposal, according to which any such model should, among others, (i) be limited to "*reasonable compensation directly related to making the data available to the data user and which is attributable to the request*", and (ii) be "*devised to gear compensation towards the lowest levels prevalent on the market*".[27]

The Proposal also provides that if the data user is a micro, small or medium enterprise ("**SME**") any compensation must not exceed the costs directly related to making the data available to the data recipient and which are attributable to the request.[28]

8.2 *Observations regarding the compensation mechanisms* – While we recognize that imposing excessively high compensation could hinder the functioning of the data sharing mechanism envisaged under the Proposal, it remains crucial that data holders receive an appropriate compensation for sharing customer data.

Compensation should not only cover the costs incurred by data holders to ensure that financial data can be accessed by data users. The compensation should also include a margin which should remunerate also the investment made in the collection and production of the data, depending also on the format, nature and volume of such data.[29]

Furthermore, we would propose not exempting data users qualifying as SMEs from the duty to pay a reasonable compensation (exceeding costs) to the data holders. This exemption could reduce the overall compensation paid to data holders, particularly as many Fintech companies operating as FISPs or making use of the access to financial data under the FIDA Regulation would likely qualify as SMEs, at least at the initial stage of their operations. This amendment would ensure that fair compensation is maintained and data holders' interests are duly accounted for regardless of the nature of the entity requesting access to financial data.

8.3 *Non circumvention principle and nature of the information made available to the customer* – According to the FIDA Regulation, if a customer requests the data on its own, the data holder should provide them free of charge; conversely, if a customer requests that the data are made available to a data user by the data holder, the data user should pay a compensation.

---

26 Article 6(2) of the Proposal.

27 Article 11(1)(h)(i) and (v) of the Proposal.

28 Article 11(1)(h), last sub-paragraph of the Proposal.

29 This approach would be consistent with Article 9(1) of the Data Act.

This mechanism could create an incentive for data users to solicit potential customers to ask themselves to have access to the data held by the data holders, and to subsequently transfer such data to the data users. By doing so, the data users would avoid the payment of the compensation due to the data holders.

The FIDA Regulation should clearly state that data users should not use the customers' rights to ask access to their data free of charge in order to circumvent the payment of the compensation due to data holders.

In addition, we also propose specifying that customers should only be allowed to have access to the data and information contained in the mandatory documentation made available by data holders (*e.g.* periodic reports, etc.) and that any other financial data can only be shared upon a request made by a data holder. Otherwise financial institutions would need to put in place two different mechanisms for the sharing of financial data – *i.e.* a standardised mechanism for the sharing of financial data with data users, and a separate mechanism for the sharing of the same data with the customers, which could hardly be standardised.

9. Liability

9.1 *Absence of a comprehensive liability regime* – The Proposal does not contain any comprehensive framework regarding the liability of data holders and data users in case of data breach or improper use of the customer data shared in accordance with the FIDA Regulation. It only specifies that a financial data sharing scheme "*shall determine the contractual liability of its members, including in case the data is inaccurate, or of inadequate quality, or data security is compromised or the data are misused*".[30] For personal data the liability regime follows the relevant provisions of the GDPR.

9.2 *Harmonised rules on liability of data holders and data users* – In our view the Proposal should define the liability regime applicable to data holders and data users more clearly. The absence of harmonised rules on liability could lead to different standards and potential regulatory arbitrage in the establishment of financial data sharing schemes.

Data users must be held accountable under a strict liability regime *vis-à-vis* both data users and customers in case of any data breach or misuse of personal data, or any failure to comply with their obligations under the FIDA Regulation. Exceptions from liability should be permitted only if data users can demonstrate that the breach was caused to *force majeure* or other events beyond their reasonable control notwithstanding the adoption of any reasonable preventive measures.

Applying a strict liability regime to data users would serve as an additional incentive for them to adopt the security measures necessary to prevent any data breach or misuse of personal data. The rationale of the strict liability regime would also stem from the fact that data users are best positioned to assess these risks and take out an adequate indemnity insurance coverage against them.

9.3 *Notification duties in case of data breach* – Data users should have a duty to notify any data breaches both to the data holder that shared the relevant financial data and to the customer to which these

[30] Article 11(1)(i) of the Proposal.

data are related. The notification would allow data holders and customers to take any appropriate actions and measures to address the breach of data, including by bringing actions against the data user for breach of the obligations provided for under the FIDA Regulation in accordance with the liability regime referred to in the paragraphs above.

10. Regime applicable to third country service providers

10.1 *Third country firms' authorisation to operate as FISPs* – According to the Proposal third country firms can be authorised to operate as FISPs provided that certain requirements are met.[31]

These requirements include, among others, the designation of a legal representative in one of the Member States from where the FISP intends to access financial data. The Proposal specifies that where the third country FISP is subject to supervision, the competent authority must seek to put in place an appropriate cooperation arrangement with the third country authority to ensure an efficient exchange of information.

10.2 *Reciprocity condition* – The Proposal should stipulate that the access to the data of EU customers by third country FISPs is permitted under a precondition of reciprocity – *i.e.* provided that the third country FISP becomes member of a financial data sharing scheme and allows EU financial institutions and FISPs to access to its customers' data in accordance with the EU framework.[32]

This reciprocity requirement would avoid that the open finance environment established under the FIDA Regulation could result in a competitive disadvantage for EU firms.

10.3 *Supervision of third country firms and cooperation agreements* – Under the Proposal third country firms that are not subject to any form of regulatory supervision and are established in a jurisdiction with no cooperation agreement in place with EU competent authorities can be licensed to operate as FISP.

While it is true that these third country firms must appoint a legal representative that is liable for non-compliance with the FIDA Regulation,[33] this safeguard might not be sufficient to address the risks connected with possible data breaches or misuse of personal data by third country firms.

We would accordingly propose to limit the access to customer data to those third country firms that are subject to regulatory supervision in their own jurisdiction and to specify that the existence of a cooperation agreement between the competent authority of the FISP and the relevant competent authority of the third country is a mandatory condition to grant the authorisation to operate as FISP. The cooperation agreement should ensure that the competent authority of the third country can exercise enforcement powers towards the third country FISP in case of breach of the requirements set forth in the FIDA Regulation, and is accountable for such enforcement *vis-à-vis* the competent EU authorities.

---

31 Article 14(2) of the Proposal.

32 The above proposal is based on the assumption that FISPs will also be considered as data holders subject to sharing obligations under the FIDA – see under para 1.4 above.

33 Article 13(3) of the Proposal.

The requirement to set up a EU subsidiary or a branch of the third country firm In the EU territory could also be explored in order to strengthen the enforcement powers of EU competent authorities.

10.4 *Identification of the EU competent authority* – Finally, the Proposal should specify more clearly the criteria to be followed in order to identify the competent authority of the home Member State that is responsible for (i) authorising the third country firm wishing to operate as FISP in the EU, and (ii) allowing such third country firm to transmit the notifications necessary to exercise the cross-border rights envisaged under the Proposal.[34]

11. Cross-border access to data

11.1 *Procedure for the cross-border access to data* – According to the Proposal FISPs and financial institutions are entitled to have access to the data of Union customer held by data holders established in the Union pursuant to the freedom to provide services or freedom of establishment.[35]

FISPs wishing to have access to such data for the first time in another Member State must communicate certain information to the competent authorities of their home Member State, which must in turn transmit this information to the competent authorities of the host Member State within 1 month.[36]

11.2 *Extension of the notification duties to financial institutions* – We would propose to extend the notification duties referred to above to all financial institutions wishing to have access to customer data on a cross-border basis.

This would allow data holders to have full transparency on the permissions of the financial institutions requesting access to the financial data. It would also ensure that competent authorities are informed on the intention by the relevant financial institutions to have access to any such data on a cross-border basis.

11.3 *Starting date of the data access and other aspects concerning the cross-border notification* – The Proposal must specify that (i) the competent authorities of the home Member State must promptly notify the FISP of the transmission of the notification to the competent authorities of the home Member State, and (ii) the access to the financial data in the host Member State is permitted starting from this date.

Competent authorities of the home Member State could also be given the possibility to review the notification and raise objections if the FISP (or financial institution) does not ensure that the conditions set out under the FIDA Regulation to have access to financial data are satisfied.

11.4 *Identification of the place where the access is made* – The Proposal should specify what is the criterion to identify the Member State where the access is made. For instance, if the access pertains to a non-

[34] This can be done by introducing the notion of "Member State of reference" for the purpose of the FISP authorisation and the related regulatory responsibilities, in line with the existing EU financial services legislation (see in particular Article 37 of the AIFMD).

[35] Article 28(1) of the Proposal.

[36] Article 28(2) and (3) of the Proposal.

life insurance policy held by an Italian customer with a French insurance undertaking operating in Italy on a cross-border basis, the Proposal should clarify whether the access is considered to be made in Italy or in France (or in both countries) for the purpose of the applicable cross-border notification duties.

11.5 *Clarifications regarding the establishment of a branch* – The Proposal should state that if a financial institution establishes a branch for the sole purpose of having access to financial data of local customers, this branch must not be considered as an establishment for the purpose of the provision of the other (*e.g.* banking, investment, insurance distribution, etc.) services that the branch intends to offer in the host Member State.

12. EBA register

12.1 *Electronic central register of FISPs* – The Proposal specifies that EBA must develop, operate and maintain an electronic central register containing information on (i) the authorised FISPs, (ii) the FISPs that have notified their intention to access data in a Member State other than their home Member State, and (iii) the financial data sharing schemes agreed between data holders and data users. It further clarifies that the register must only contain anonymised data.[37]

12.2 *Proposals regarding the information available in the EBA register* – The rationale behind the anonymisation of the data included in the EBA register appears unclear.

Data holders should be allowed to verify whether the entity requiring access to the customer data is authorised to operate as FISP and has exercised its cross-border rights in accordance with the FIDA Regulation. They should also be aware of the financial data sharing schemes that can be used for the purpose of sharing the customer data with the relevant data user.

As the need for the information referred to above arises also in case the access to the customer data is requested by a financial institution, we propose to extend the information available in the register to include all financial institutions that have notified their intention to have access to customer data. These financial institutions should be enrolled in a separate section of the EBA register.

The EBA register should indicate the financial data sharing scheme(s) used by each FISP and financial institution to share customer data in compliance with the FIDA Regulation.

* * * *

We hope that the above input can offer valuable perspectives to the European Commission, the European Parliament and the Council as they continue to refine and enhance the Proposal during the subsequent stages of the legislative process.

We thank you again for the opportunity to submit this feedback and remain available to discuss its contents.

Yours faithfully,

[37] Article 15(1) and (2) of the Proposal.

ANNEX A

Summary table

No.	Issue	AIPB Position	Rationale
1.	**Subject matter and FISPs**	The Proposal should specify that FISPs are prevented to use financial data to provide regulated services. FISPs should be allowed to share financial data only to financial institutions that are authorized to provide the relevant regulated services.	FISPs cannot use the access to financial data in order to circumvent the licensing obligations applying to the provision of regulated services under the EU regulatory framework.
		Certain financial institutions (i.e. all financial institutions subject to the FIDA Regulation other than credit institutions, investment firms, AIFMs and UCITS management companies, insurance and reinsurance undertakings, payment and e-money institutions) should send a notification to their competent authorities to extend the scope of their license in order to have access to financial data as data users.	Competent authorities should assess whether these financial institutions are adequately organized to have access to financial data as data users and to treat them in accordance with the applicable regulatory framework (including FIDA, GDPR and DORA).
		FISPs should be subject to the same data sharing obligations applicable to financial institutions as data holders if they collect, store or otherwise process data.	Preventing other financial institutions (or FISPs) to have access to the financial data held by FISPs could distort the competition among market players.
2.	**Definition of customer data**	There must be a clearer definition of the non-personal data subject to the FIDA by way of RTS or guidelines issued by ESAs.	If the definition of non-personal data is too wide data holders could be required to store and share a significant volume of data. There might also be divergent interpretations and uncertainties on what constitutes a non-personal data to be shared under the FIDA.
		Data that are autonomously elaborated by financial institutions (*e.g.* as a result of data mining / data analysis activities)	The application of data sharing to this type of information could discourage data mining or data analysis activities by financial institutions and undermine the

No.	Issue	AIPB Position	Rationale
		should not be subject to data sharing obligations.	incentives to provide customer-centric services.
3.	**List of customer data and financial institutions subject to FIDA**	Further clarifications must be given with respect to certain terms used in the list of customer data subject to sharing obligations, *e.g. "financial assets"*, "*economic benefits*", etc.	The terms used in the FIDA Regulation are particularly broad and could give rise to regulatory uncertainties in the absence of clear definitions.
		Information on real estate assets should not be subject to data sharing obligations. Alternatively, the Regulation should specify that data holders should only share the information (if any) that they have concerning the real estate investments made by their clients, without providing any further information on the real estate assets (including in particular on their valuation).	Financial institutions do not always have information on real estate investments made by their customers, and should not be required in any event to share information (*e.g.* on the valuation of the asset) that is normally taken from third party sources rather than being developed by the financial institution itself.
		There should be no obligation to share information concerning any other assets that are not subject to specific regulation under the existing EU financial services regulatory framework.	It would be difficult to develop common standards to share this information in the absence of a common framework at EU level regulating the offer or distribution of this type of investments.
4.	**Distribution or intermediation activities**	The Proposal should clarify the allocation of data sharing responsibilities in case of multiple data holders distributing or intermediating a financial product.	The clarification should limit regu"ator' uncertainties and avoid imposing excessive burdens on distributors – *e.g.* regarding the features or performance of the product distributed to the customer, if they don't have access (or have limited access) to this information.
5.	**Continuous and real-time access**	The Proposal should clarify that continuous and real-time access does not mean that the available financial data must also be updated real-time.	Updating financial data real-time is not always feasible and could lead to substantial costs for data holders.

No.	Issue	AIPB Position	Rationale
		There should be limitations on the number of accesses made by data users in line with the EU rules on open banking.	Managing real-time and continuous access by data users with no limitation whatsoever could increase the IT costs to be borne by data holders.
		The Proposal must provide that the access to the data can be suspended in case of maintenance activities.	Data holder cannot be held responsible if the access to data is suspended due to the need to perform maintenance activities.
		Data holders must not be subject to any duty to assist data users regarding the access to and use of customer data.	Data holders cannot be required to invest time and resources in assisting data users on the access to and use of customer data.
6.	**Customer's permission**	The Proposal must include a list of purposes for which customer data cannot be used. The list should include, for instance, the offer of services or products mirroring those provided by the data holder.	The list could prevent opportunistic behaviours by market players who want to use access to financial data to have access to confidential information regarding their competitors.
		The Proposal must further specify the procedure to be followed by data users to gather customer's permission, and introduce a principle whereby the customer cannot be deceived or manipulated for the purpose of getting its permission to the sharing of data.	In the absence of clear procedural requirements data users could adopt deceptive or manipulative tools to get the customer's consent.
		The Proposal should standardise as much as possible the forms to be use for the purpose of collecting the customer's consent and ensure that these forms have the same structure and granularity of the permission dashboards	The standardisation should avoid that the information included in the forms do not match with the information requested in the dashboard, *e.g*. with respect to the types of products for which the consent is given, etc.
		There must be anti-fraud mechanisms in place to ensure that the consent is given by the data user, *e.g.* through the use of strong authentication (SCA) tools in line with the PSD2.	The authentication tools should avoid that the access to financial data is requested by scammers or criminals.

No.	Issue	AIPB Position	Rationale
		The Proposal should impose information duties on data users regarding the treatment of non-personal data.	The customer's consent to the treatment of non-personal data must be given on an informed basis.
		Data holders should be entitled to refuse the transmission of sensitive data from a business or competition standpoint in exceptional circumstances which must be clearly identified in the FIDA Regulation.	The transmission of certain data could negatively affect core business-related or security interests of the data holder and the confidentiality of material information.
7.	**Financial data sharing schemes**	There should be a single set of operational rules and standards regarding the access to financial data, which must be introduced by way of EU delegated acts and/or handbooks prepared by a single EU self-regulatory body.	The proliferation of multiple financial data sharing schemes could lead to a multiplication of the operational rules and standards and increase the compliance costs of market players. It could also create regulatory arbitrage opportunities by market players.
		The Proposal should provide for the application of a 36-month period for the establishment of the common standards and procedures for the sharing of financial data, and an additional 12-month period for the full implementation of such standards and procedures.	Additional timing is required considering the complexity of the standardisation process that must be undertaken in order to implement the FIDA Regulation.
8.	**Compensation**	The principles on data holders' compensation should provide that the compensation should also include a margin remunerating the economic value of the information transmitted as well as the loss of confidentiality resulting from the sharing of customer data.	Data holders should be adequately remunerated for the access granted to data holders due to the loss of confidentiality of the customers' data.
		The compensation payable by SMEs should not be capped to the costs of the data access request.	The application of this rule could significantly reduce the amount of compensation received by data holders considering that a significant number of FISPs and financial institutions having

No.	Issue	AIPB Position	Rationale
			access to the data (such as fintech companies) could qualify as SMEs.
		Data users should not use the customers' right to have access to their data free of charge in order to circumvent the payment of the compensation due to data holders.	The principle whereby customers can have access to their data free of charge could be exploited by data users to avoid the payment of the compensation.
		Customers should only be allowed to have access to the data and information contained in the mandatory documentation made available to data holders.	Should customers be entitled to request full access to all their financial data, financial institutions would need to put in place two different mechanisms for the sharing of financial data – *i.e.* a standardised mechanism for data sharing with data users, and a non-standardised mechanism for the sharing of data with their customers.
9.	**Liability**	The Proposal should introduce harmonised rules on the liability of data users and data holders.	The absence of a harmonised liability framework could lead to different standards and potential regulatory arbitrage opportunities.
		Data users should be subject to a strict liability regime in case of data breach, misuse or personal data or failure to comply with the FIDA rules.	The strict liability regime should provide further incentives to adopt strong security measures. Data users are also best positioned to insure the risks of data breaches or misuse of customer data.
		Data users should be required to notify any data breaches to data holders and customers.	The notification of data breaches would allow data holders and customers to adopt any appropriate action or measure, including bringing actions against the data user for breach of its obligations under the FIDA Regulation.
10.	**Third country FISPs**	Third country firms should be subject to reciprocity obligations when they access	In the absence of a reciprocity conditions the rules on third country

No.	Issue	AIPB Position	Rationale
		financial data of EU customers as third country FISPs.	FISPs could give rise to a competitive disadvantage for EU firms.
		Third country firms should be able to access financial data only if they are subject to regulatory supervision and if their competent authority entered into cooperation agreements with EU competent authorities.	The absence of these conditions could undermine the enforcement powers of EU competent authorities in case of breach of the FIDA rules.
11.	**Cross-border access to data**	Financial institutions wishing to have cross-border access to financial data should also follow the notification procedure envisaged under the Proposal.	Data holders and competent authorities should have full transparency on the entities that are allowed to have access to financial data on a cross-border basis.
		The Proposal should further regulate the notification procedure in line with the rules on passport rights set out in the EU financial services legislation.	The FIDA framework must be aligned to the EU provisions on passporting of financial services.
		The Proposal should clarify the criterion to identify the Member State where the financial data are accessed by the FISP or financial institution.	In case of cross-border services it is unclear whether the access is made in the Member State where the customer or the service provider is located.
		The Proposal should clarify that establishing a branch for the purpose of the FIDA rules does not trigger the application of the rules on branches under the EU financial services legislation.	The clarification should ensure that no regulatory uncertainties arise if a branch is established by a financial institution only for the purposes of the FIDA Regulation.
12.	**EBA register**	Data included in the register should not be anonymised.	The rationale of the anonymisation is unclear. The information should be made accessible by all FISPs and financial institutions.
		The register must include also the information on financial institutions that have notified the intention to access financial data (see point 1 above).	The need for transparency is not limited to FISPs.

No.	Issue	AIPB Position	Rationale
		The register must include information on the financial data sharing scheme(s) used by each FISP and financial institution.	This information is essential to understand the regime applicable to the sharing of financial data.