POSITION PAPER

ESBG response to the EC call for feedback on the proposed Regulation on the Financial Data Access Framework

ESBG (European Savings and Retail Banking Group)

Rue Marie-Thérèse, 11 - B-1000 Brussels

ESBG Transparency Register ID 8765978796-80

October 2023

ESBG

INTRODUCTION

The European Savings and Retail Banking Group (ESBG) took note of the European Commission's proposed Regulation on the Financial Data Access Framework and its commitment to establish clear rights and obligations to manage customer data sharing in the financial sector beyond payment accounts, and to promote innovative financial products and services for users and stimulate competition in the financial sector. ESBG welcomes the possibility to provide feedback on this proposed Regulation.

ESBG members appreciate that FIDA is built around some key principles important to ensure the level playing field, to secure data sharing and to build trust in the data sharing ecosystem: a contractual approach between the stakeholders for a sharing of responsibilities and cost, the development of tools to give customers meaningful and effective control over their financial data, and eligibility rules to make sure that all data users are subject to authorization and supervision.

However, they have some initial concerns regarding the level of ambition of some provisions, the vagueness of some others and the cumulative impact for retail banks of various regulatory packages, including, PSD3 / PSR, the Retail Investment Strategy, and the Digital Euro proposals.

Please find our members' feedback on the proposed Regulation as comments on the pararagraths below.

TITLE I: SUBJECT MATTER, SCOPE, AND DEFINITIONS

• **Data economy**: The Commission's intended objective with the EU Data Strategy and a Framework for Financial Data Access to seize the opportunities of the data economy for European consumers, companies, and the EU economy as a whole is supported. The intention of savings and retail banks is to take an active role here, both as data holders enabling third-party providers to access customer data, and as users of external data, to provide more tailored offers to customers. Our priority is therefore to ensure that the Regulation for Access to Financial Data (FIDA), in addition to creating a secure infrastructure for sharing customer data, also takes into account customer and market needs and promotes fair competition for open finance. Otherwise, there is the risk of lack of acceptance by various market players. In this respect, we support the fact that the FIDA draft assigns a central role to schemes, as these represent a central component of fair competition, yet ask for clarification on how financial data sharing schemes will be developed and under which rules. More in general, we believe that it is vital to ensure the opening of data at the cross-sectoral level in order to avoid asymmetries to the detriment of the financial sector.

• **Compensation model**: The proposal's compensation structure, limited to "reasonable compensation directly related to making data available" (art 10.1(h)(i)) and geared toward "the lowest prevailing levels in the market" (art 10.1(h) (v)) will not allow to cover all the cost incurred by data holders.
FIDA is not aligned with art. 9.1 of the Data Act, which states that "any compensation agreed upon between a data holder and a data recipient […] shall be non - discriminatory and reasonable and may include a margin". To succeed in a data-driven economy, it is essential to ensure a compensation model in favour of the data holder that allows for adequate incentives at industry level. As cost of making data available are not limited to the cost of building and maintaining the technical infrastructure required, the compensation's structure should be wider to also cover investments linked to the data itself (collection, structuration, preparation, etc.) in order to adequately remunerate the data holder. FIDA should be clearer on the nature of the costs that can be compensated (fixed/variable costs).
An alignment with the Data Act art. 9 is needed as it is crucial to ensure proper incentives for data holders to continue investing in high-quality data.

• **Step-by-step implementation**: To ensure a successful and solid implementation of the FIDA provisions, a step-by-step approach with sufficient implementation timelines and a progressive application of the scope of FIDA will be essential and should be subject to evaluation and possible adjustment before each further expansion stage. We recommend the gradual application of the text, data category by data category based on customers' needs assessment on anticipated use cases. This would be a good way to gain the necessary experience and prevent regulatory errors that would stand in the way of the legislator's intentions in the long term.

• **Reciprocity as a central principle**: In order to guarantee fair competition between financial institutions and licensed companies (FISPs) and to create incentives for investment in innovative technologies, FISPs should also be considered data holders for data that they have directly obtained from their own customers and that falls under the scope of FIDA.

The current FIDA draft obliges regulated financial institutions to open up to licensed companies (so-called Financial Services Information Providers, FISPs), but leaves open the purposes for which FISPs use the data.

Art. 3.3 defines the term "customer data" in such a way that it only refers to data held by financial institutions as defined in Art. 3.8. Art. 2.2(a)-(n) defines "financial institutions" and explicitly excludes FISPs. Companies that are not financial institutions under Art. 2.2. (a)-(n), but hold a FISP license, are thus legally only data users and not data holders. This means that companies from other sectors (e.g., energy) with a FISP license may access data from financial institutions, but financial institutions do not have legal access to data of such providers.

In its impact assessment report, the European Commission points out that reciprocity is established by the Digital Markets Act (DMA), as large platform gatekeepers are obliged to grant simplified access to their data.[1] We consider the DMA to be a milestone of fair competition of a European data economy. At the same time, however, it is not sufficient to establish fair competition. The obligation of the DMA currently applies exclusively to seven companies (Amazon, Apple, Microsoft, Samsung, Alphabet, Meta and Bytedance). Thus, no reciprocity is established with other companies that hold a FISP license. This restricts fair competition, as banks could offer their customers much more tailored products if they had access to customer data in other sectors, such as energy and mobility.

A link with the work of the European Data Innovation Board (established by the Data Governance Act -DGA-) should be provided in order to support cross-sector data use.

Contrary to the access regime on IoT data introduced in the Data Act proposal, FIDA does not prevent "gatekeepers" to access data. FIDA should take inspiration to art. 5.2 and 6.2(d) of the Data Act (final compromise text version - 7th July of 2023-) in order to prevent gatekeepers to become data users and to access to financial data.

FIDA provides an obligation for third country FISPs to designate a legal representative in EU but not to store or process data in EU (recital 33). This could represent a risk on customers' data protection and generate distrust on their side. For third country FISPs (art. 13), FIDA should condition their authorization to the verification by the competent authority (in coordination with data protection authorities) of their compliance with EU data protection rules, particularly with regard to data localization. Therefore, we call to limit the capacity of becoming a FISP to entities located in the internal market only.

We understand that the registered Account Information Service Providers (AISPs) (art. 2.2(b)) could benefit the same rights provided by FIDA as other data users. This could represent a risk of opportunistic behaviour by entities wishing to access the full scope of financial data but preferring this AISP registration regime instead of the FISP's authorisation regime. FIDA should either require AISPs, already registered as such but wishing to access financial data, to also apply for FISP's authorisation regime, or introduce a single common authorization regime for both AISPs and FISPs.

• **Critical questioning of the scope of categories of customer data:**

FIDA will apply to a broad scope of customers' data categories. This level of ambition on the scope appears unrealistic regarding the heterogeneity of data between the products, under each category and between countries for the same category. Under each category,

[1] EU Commission (2023): Impact Assessment Report on FIDA, p. 51, link: EUR-Lex - 52023SC0224 - EN - EUR-Lex (europa.eu)

data in scope of the regulation are not clearly defined with no precise distinction of data covered by trade secret.

We would recommend adding to Article 2 that personal data which is sensitive (article 9 GDPR) should be scoped out.
We believe that data that are not in-scope should be clearly listed in article 2 or in another article rather than merely being mentioned in the recitals. Calculations or suitability appropriate assessments made by a financial institution in the interaction with customer, and data analysis provided by the customer might be included as well in this list of data categories that are not in the scope of FIDA.

Investment data: We believe that the scope of investment data defined in Art. 2.1(b) is to be critically questioned. A starting point when defining investment data should be that a distinction must be made between data that naturally exist with a financial institution on a customer without interviewing the customer and data captured throw questionnaires and data that has been processed i.e., artefacts created from internal processes. Data that naturally exist without interviewing a customer should not be excluded whereas data that has been processed must fall outside the scope of FIDA. Such distinction is in line with Article 29 Working Party (replaced by EDPB) guidelines on the right to data portability (see below). A distinction between data that a financial institution holds naturally and processed data would also entail that the data collected for the purpose of suitability and appropriateness tests within the meaning of Art. 25(2) and Art. 25(3) of MiFID II should not be included. This data is mainly internal and tailored to the respective in-house processes and cannot be used by a third party due to the individuality of the internal process. On the contrary, if this data had to be provided automatically, third parties would be tempted to simply apply it to their own processes. This would create an enormous risk of incorrect advice or incorrect investment decisions for customers ("miss selling"). Moreover, the ability of each distributor to determine its own approach to clients drives competition and innovation within the industry. Thus, the specific details of valuation are a quality attribute, a differentiator of each institution's investment advice. Complete standardization of these processes could potentially lead to a loss of quality in the valuation process and could hinder or even eliminate institutions' efforts to continuously improve the quality of these processes. The transfer of this data would therefore run counter to the Regulation's objective of enhancing the utility and fit of financial services for individual customers. On the other hand, the list of data derived from investment accounts should be limited and should not include the part of the proposed article 2(9) which refers to "other data points relating to lifecycle events of that instrument" which is disproportionately broad, as its implications.

Data from a creditworthiness assessment: The scope of the data pursuant to Art. 2(f) is unclear when checking the creditworthiness of a company for a loan application or for a rating. While the associated customer benefit is at most in the form of operational facilitation in the provision of data to multiple, potential lenders or rating agencies, here too the data used is likely to vary in detail from institution to institution, which can be explained by provider-specific rating systems and input variables. The risk assessment of credit exposures is a core competence of lenders and an important competitive factor that must be maintained in order to ensure a broad credit supply and diversity of offerings. Standardizing this data for data access is a misguided policy goal and undermines competition. Therefore, as previously stated, we would recommend the gradual application of the text, data category by data category based on customers' needs assessment on anticipated use cases. Recital 9 states that this Regulation should also not cover data collected as part of a creditworthiness assessment of a consumer, however recital 20 establishes that EBA and EIOPA should closely cooperate with the European Data Protection Board when drafting the guidelines, which should build on existing

recommendations on the use of consumer information in the area of consumer and mortgage credit, notably the rules on use of creditworthiness assessment and on credit agreements for consumers. The Regulation should make clear that credit worthiness data of natural persons are excluded from the FIDA framework.

Suitability and appropriateness assessments: Suitability and appropriateness assessments data should not fall within the scope of FIDA, since it constitutes part of the internal processes of the entities. The application of this data to other entities with other procedures may lead to inappropriate investment or advisory decisions. Furthermore, the evaluation processes of each entity are part of its strategy, and standardization of them would result in a decrease in the quality of services. Likewise, it should be clarified that the results of the suitability and appropriateness assessments, as well as the demands and needs assessment under the Directive on insurance distribution (IDD), should not be within the scope of customer data, only the data that is provided by the customer as part of this process should be included. We are concerned that FIDA framework may increase the current IDD obligations regarding information gathering in respect of the clients' demands and needs assessment.

The definition of customer data under art. 3.3 may give rise to interpretation. This definition is not aligned with the categorization of data provided by the Article 29 Working Party (replaced by EDPB) guidelines on the right to data portability (WP 242 rev.01- April 2017) and seems to include "processed data" in the scope whereas recital 9 of FIDA clearly states that "the sharing of customer data in the scope of this regulation should respect the protection of confidential business data and trade secrets". The Art. 29 WP guidelines make a clear distinction between "data provided by the data subject" ("actively and knowingly" or "by virtue of the use of the service or the device") and "inferred data and derived data […] created by the data controller on the basis of the data "provided by the data subject"".
Processed data by the financial institutions should be out of scope as they represent an asset for the company falling in the scope of trade secret. An alignment with the Art.29 WP guidelines categorization should be done, clearly excluding from the scope of FIDA "inferred data and derived data".

TITLE II: DATA ACCESS

• **Obligation to make available data to the customer**: Art. 4 states that a data holder shall, upon request of the customer, provide the data listed in Art. 2.1 without undue delay, free of charge, continuously and in real-time. However, legislators should take in mind that "real-time access" can lead to security risks, high costs and legal problems (privacy, intellectual property).

In our opinion, such a claim can currently only be realized via online banking as an established electronic customer interface. We believe that it should also be considered that other data holders concerned may not yet offer digital access in this form. This might particularly be the case for smaller institutions. If customers do not (want to) participate in online banking, there should be no entitlement to use another electronic channel for lack of viable alternatives. This should be clarified in the Regulation. This is without prejudice to the provisions of the GDPR, which already stipulate extensive data access rights and a right to data portability and create uniform conditions horizontally, i.e., across sectors. The data access claim under the FIDA can, from our point of view, not be considered as a framework for the sector-specific fulfillment of requirements under the GDPR, since different goals are pursued by this. This should be clarified in the FIDA.

For some members, the B2C model, as proposed in art. 4, could place the customer as an intermediary between a data holder and a potential data user. Not only this model could run against the interest of the customer who would assume full responsibility of any data transfer he would initiate to data users, but it could also represent a risk to the functioning and balance of the entire data sharing ecosystem. An uninformed customer could transfer his financial data to an entity that does not comply with European regulations on data protection. With opportunistic behavior, some data users could prefer to go through this free model instead of the B2B model that could include a compensation through a scheme. One may wonder whether this model is completely justified. If the right to data portability of GDPR art. 20 needs to be improved, this should be done via a GDPR revision.
Data driven innovation should be at the benefits of customers but not under their responsibility. In that way the B2B data sharing model, with the central role given to customers, is better able to maximize innovation while protecting customers.

• **Obligation on a data holder to make customer data available to a data user:**

Trade secrets and intellectual property rights: Art. 5.3.(e) and Art. 6.4.(b) foresee an obligation for both data holders and data users to maintain the confidentiality of trade secrets and intellectual property rights when accessing customer data pursuant to Art. 5.1. However, neither the data holder nor the data user could provide a guarantee for the protection of business secrets in relation to the customer data, since only the (company) customer knows whether access to certain data affects its business secrets or intellectual property rights. In addition, such an obligation could involve a great potential liability for the data holders and data users concerned to a completely unclear extent. Moreover, a need for protection of trade secrets should rather exist for the data holder. After all, the collection and processing of customer data to an extent individually specified by the data owner or according to a provider-specific system can be a differentiating feature in competition and thus affect its trade secrets or IP rights. We therefore recommend that it should be clarified that the aforementioned paragraphs in Articles 5 and 6 serve to protect the data holder.

"The sharing of customer data in the scope of this Regulation should respect the protection of confidential business data and trade secrets." is mentioned in recital 9. Given the importance of this concept, we consider the wording in Recital 9 not be enough. We would suggest including it in an article.

TITLE III: RESPONSIBLE DATA USE AND PERMISSION DASHBOARDS

• **Data protection**: FIDA introduces a permission mechanism, in addition to the need for a valid legal basis under GDPR art. 6.1, but lacks clarity on the way those 2 mechanisms will concretely work in practice.
The withdrawal of permission does not necessarily lead to the end of validity of a legal basis and of the processing. Thus, making customers responsible of possible contractual consequences of the withdrawal of a permission by warning them (recital 22) could not be enough to avoid legal inconsistencies and customers unsatisfaction. FIDA should provide better clarity on the interaction of the permission mechanism with the GDPR legal basis and explicitly specify which GDPR legal basis a data user may or may not use.

• **Permission Dashboard**: We believe that FIDA's requirements for configuring the dashboard should be high-level, establishing general principles while leaving flexibility to data holder in configuring the details.

Information about the exact purpose of use usually results from data use provisions agreed between the customer and the data user, some of which are extensive and of

which the data holder is not aware. Data holders can and should therefore not be subject to any further obligations than to indicate to the customer the intended use communicated by the data user.

Permission Control Dashboard is a fundamental concept and therefore a detailed definition should be provided. We ask to include such definition in Article 3.

• **Data Holder Responsibility**: The data holder must be expressly exempt from any responsibility for the inappropriate use of data and application of adequate security measures by the data user. Moreover, the proposal should also clarify that it is the data user's responsibility to provide the customer with the terms and conditions that govern the contractual relationship between the data user and the customer. This is specifically important in consumer relationships in order to safeguard consumer protection. Furthermore, the division of responsibilities and liabilities between the data holder and the data user should be aligned with the data controller's responsibilities under GDPR.

In addition, when the customer withdraws the permission through which a data user accessed their data, the data holder no longer has control over the treatment carried out by that data user on the data already accessed. Therefore, when the customer withdraws permission, the data holder will ensure that access by that data user to the data is cut off as soon as technically possible but will not be responsible for the use that the data user makes of the customer's data, even when it occurs after the withdrawal of permission.

On a general note, we believe the configuration of the dashboards must be flexible. We are therefore vigilant to ensure that FIDA and Payment Services Regulation (PSR) remain consistent on the topic of Dashboards, so that data holders are free to develop a single Dashboard for both mechanisms.

Data User Rights: Data users must have the option to establish by contract the possibility of sharing the data to which they have access through different companies in the same group. A restriction similar to that established in the DMA is not appropriate since that case regulates competition in an environment of excess data control, which is not transferable to FIDA.

TITLE IV: FINANCIAL DATA SHARING SCHEMES

We believe that financial data sharing schemes promise fair opportunities for all players in the value chain to participate and shape the process. Schemes bring data holders and data users together and reconcile the different interests. However, there are still many unanswered questions regarding the exact role, mode of operation and construction of the schemes. Therefore, to have clear guidelines, we deem it necessary to develop a definition and include it in article 3.

In this context ESBG 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 unsecure mechanisms for a third party to obtain customer data from a data holder. These methods are unreliable as they do not allow for the data holder to see the nature of the data that is being scraped. 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). In addition, screen scraping also results in processing of personal data that often is not in line with the requirements in GDPR. It is therefore important that FIDA provides a data sharing framework that takes these considerations into account. One way to address it could be giving the option to financial entities to block these accesses through screen scraping and

reverse engineering and redirect them to dedicated data access interfaces developed in compliance with FIDA.

• **Development of the schemes**: It should be clarified how financial data sharing schemes will be developed and under which rules. Schemes shouldn't be mandatory.
The advantages of a scheme (sharing of cost and responsibilities) should lead the market to move naturally towards this option and take the necessary time to conduct the negotiations of the financial and technical aspects. These last are complex and impactful for the parties and the whole EU data single market as there is a cross-sectorial connection regarding standards. Moreover, the first scheme created under a category of data, even if it only involves players from a single member state, will have a strong influence on the EU market (a form of incentive to join) as the Commission will no longer be empowered for a delegated act for this category of data. The meaning of "significant portion of the market" and the reference level (EU or national) should be clarified (art. 10.1.(a)(i)).

In addition to the governance rules detailed in art. 10, it should be clarified how the development of a scheme could start in practice and how the market could be informed at the earliest stage of the negotiations.

• **Financial data sharing scheme membership**: There are uncertainties in connection with the right of data access formulated in Art. 5. The draft stipulates that data access is to be based on schemes.

We believe that Art. 5.2 should be reformulated as follows "A data holder may claim compensation from a data user for making customer data available pursuant to paragraph 1 ~~only if the customer data is made available to a data user~~ in accordance with the rules and modalities of a financial data sharing scheme, as provided in Articles 9 and 10, or if it is made available pursuant to Article 11." Moreover, we ask for clearer clarifications on the intended use of the article, taking into consideration that scheme participation is, as for now, mandatory, while we advocate for a voluntary approach.

• **Financial data sharing scheme governance and content**:

Compensation: Art. 10 (h)(v) provides that the compensation for data access set in schemes should be based on the lowest market level. Such a provision would undermine the design authority of the schemes, thus undermine the incentive for their creation. Since the FIDA only covers such schemes in which data holders and data users are adequately represented, the pricing of data access should be left to the market players and regulated taking into consideration the Data Act provisions. The financial data sharing scheme should not establish a model to determine the maximum compensation that a data holder is entitled to charge for making data available, as stated in article 10(1)(h). This approach is too interventionist and will result in indirect price fixing. Establishing a price ceiling in practice will result in distorting competition and preventing innovation in financial product development.

Liability: We advocate for the establishment of a minimum on issues of responsibility of the data holder and the data user, for situations such as misuse of data, security measures, incidents, etc.

Micro, small and medium-sized enterprises: Micro, small and medium-sized enterprises acting as data users are to be granted access to customer data in return for reduced compensation limited to pure costs, in line with Art. 9.2. of the Data Act (Art. 10 (h)(vi)). However, the draft Regulation does not provide equivalent protection for corresponding data holders. This unequal treatment is detrimental to fair competition. Separate

protection with cost-based compensation should be limited, if at all, to micro-enterprises. In any case, the legislator must ensure that any size thresholds cannot be circumvented by data users, e.g., via subsidiaries, in order to obtain “discounted” data access.

Article 11 gives the Commission broad powers to adopt a delegate act with the modalities for data sharing by a data holder and the proposal should therefore clarify the concepts of “realistic prospect” and ”in a reasonable manner of time”. This can be done in cases where a financial data sharing scheme is not developed for one or more categories of customer data in scope and there is no realistic prospect of such a scheme being developed “*in a reasonable amount of time*."

TITLE V: ELIGIBILITY FOR DATA ACCESS AND ORGANISATION

No comments.

TITLE VI: COMPETENT AUTHORITIES AND SUPERVISION FRAMEWORK

No comments.

TITLE VII: CROSS BORDER ACCESS TO DATA

No comments.

TITLE VIII: FINAL PROVISIONS

We believe that the deadline in Art. 36 that states that data holders and data users must join schemes within 18 months after the Regulation enters into force is too short, given the large scope of affected data categories. This timeframe considerably underestimates the scale of the task to be accomplished for each category of data. As FIDA is built on the lessons learned from PSD2, the definition of the timing should follow the same principle. The SEPA Payment Account Access Scheme (SPAA), a private initiative in the payments sector, demonstrates that negotiation for a single category of data takes longer time.
Therefore, although we support FIDA’s scheme-based approach, we call for a voluntary approach to join them. This approach would take into account that the respective schemes have yet to be developed and would provide for a feasible and effective implementation of the provisions.

About ESBG (European Savings and Retail Banking Group)

ESBG is an association that represents the locally focused European banking sector, helping savings and retail banks in 17 European countries strengthen their unique approach that focuses on providing service to local communities and boosting SMEs. An advocate for a proportionate approach to banking rules, ESBG unites at EU level some 885 banks, which together employ 656,000 people driven to innovate at 48,900 outlets. ESBG members have total assets of €5.3 trillion, provide €1 trillion billion in corporate loans, including SMEs, and serve 163 million Europeans seeking retail banking services. ESBG members commit to further unleash the promise of sustainable, responsible 21st century banking. Learn more at www.wsbi-esbg.org.

European Savings and Retail Banking Group – aisbl
Rue Marie-Thérèse, 11 ▪ B-1000 Brussels ▪ Tel: +32 2 211 11 11 ▪ Fax : +32 2 211 11 99
Info@wsbi-esbg.org ▪ www.wsbi-esbg.org

Published by ESBG. October 2023.