Brussels, 22 November 2023
FINAL

EACB's Position Paper

on the Commission's proposal for a

Regulation on a framework for Financial Data Access (FIDA)

The **European Association of Co-operative Banks** (EACB) is the voice of the cooperative banks in Europe. It represents, promotes and defends the common interests of its 26 member institutions and of cooperative banks in general. Cooperative banks form decentralised networks which are subject to banking as well as cooperative legislation. Democracy, transparency and proximity are the three key characteristics of the cooperative banks' business model. With 2,700 locally operating banks and 40,000 outlets co-operative banks are widely represented throughout the enlarged European Union, playing a major role in the financial and economic system. They have a long tradition in serving 227 million customers, mainly consumers, retailers and communities. The co-operative banks in Europe represent 89 million members and 720,000 employees and have a total average market share of about 20%.

EACB AISBL – Secretariat • Rue de l'Industrie 26-38 • B-1040 Brussels
Tel: (+32 2) 230 11 24 • Enterprise 0896.081.149 • lobbying register 4172526951-19
www.eacb.coop • e-mail : secretariat@eacb.coop

1. Introduction

The European Association of Co-operative Banks (EACB) acknowledges the European Commission's proposal for a Regulation on a framework for Financial Data Access (FIDA).

We have conducted a thorough evaluation of this pivotal regulatory development within the financial landscape. In this assessment, we have identified both aspects worthy of praise and areas that raise concerns.

In this position paper, we emphasise areas of alignment with our previously articulated Recommendations[1] in the general remarks section while also addressing concerns pertaining to certain provisions in the third section of this paper.

Our intent is to contribute constructively to the discussion surrounding FIDA, charting a course that upholds the interests of customers and co-operative banks while ensuring the integrity and resilience of the broader financial ecosystem.

We also invite the co-legislators not to consider FIDA in isolation. Instead, it should be viewed in the broader context of various legislative proposals, whether they are in the implementation phase, like DORA, or in their final stages of the legislative process, such as the proposal for a Digital Identity, the Artificial Intelligence Act, or recently published ones like the Retail Investment Strategy, the proposal for a Digital Euro, the third Payment Services Directive (PSD3), and the Payment Services Regulation (PSR), among others. Therefore, it is essential to consider the implications of FIDA within this broader legislative landscape to ensure a comprehensive understanding of the challenges and opportunities that lie ahead for retail banking institutions.

Finally, special attention should be given to European sovereignty, especially concerning Big Tech firms, which may gain direct access to European customers' financial data and attract their assets outside the EU.

2. General remarks

The FIDA proposal is built upon some fundamental principles that hold significant importance in fostering a level playing field, securing data sharing, and instilling trust in the data sharing ecosystem. These principles form the bedrock of FIDA.

One key principle is the adoption of a contractual approach facilitated through schemes among stakeholders, aimed at delineating responsibilities and cost-sharing. This approach aligns with our stance on clearly defining liability arrangements in contracts, emphasising transparency and

[1] EACB's Recommendations For a Feasible Open Finance Ecosystem, 24 March 2023.

accountability. These contractual schemes, in tandem with the establishment of tools empowering customers with meaningful control over their financial data, underscore the user-centric nature of FIDA.

In this context, we welcome the overarching emphasis on schemes as a component of FIDA. We firmly believe that the key advantages of schemes is the establishment of a harmonised set of rules that are transparent and open for any interested market participant under supervision to join.

The inclusion of provisions regarding contractual liability and dispute resolution within a data sharing scheme, as outlined in Article 10.1(i) and (j), is worthy. This mirrors our emphasis on well-defined liability arrangements in contracts and the role they play in facilitating effective dispute resolution.

An important aspect relates to the provisions enhancing accountability and transparency within the financial sector, notably, the requirement for Financial Information Service Providers (FISPs) to obtain authorisation before accessing data from a data holder (Art. 6.1). This crucial step is complemented by their subsequent supervision under competent authorities, as indicated in Recitals 31, 33, 36, and Articles 17 onwards. We have persistently advocated for such authorisation and supervision for non-bank third parties involved in financial services.

This along with the establishment of a publicly available central register by the European Banking Authority (EBA), as mandated by Art. 15, listing authorised FISPs not only promotes a level playing field, but also ensures a higher degree of consumer protection. Such a register for FISPs will foster transparency by making clear that a certain FISP is authorised as data user. Furthermore, when dealing with entities from other EU nations, having a reliable public central register becomes invaluable in assessing their status accurately, mitigating uncertainty.

The inclusion of FISPs within the scope of the Digital Operational Resilience Regulation (DORA), as stated in Art. 35, is welcome. Adding FISPs into the scope of DORA ensures a comprehensive oversight and regulation of the entities involved in the digital financial ecosystem. FISPs inclusion in DORA would help address potential vulnerabilities and enhance the overall stability and security of digital financial services.

Lastly, another significant aspect is the exclusion of data related to a consumer's creditworthiness assessment, as outlined in Recitals 9 and 19. This aligns with our consistent advocacy through the European Financial Data Space Expert Group, emphasising the need to protect sensitive financial data that can reveal information about an individual and consequently have an impact on the individual's daily life.

EACB AISBL – Secretariat • Rue de l'Industrie 26-38 • B-1040 Brussels
Tel: (+32 2) 230 11 24 • Enterprise 0896.081.149 • lobbying register 4172526951-19
www.eacb.coop • e-mail: secretariat@eacb.coop

3. EACB's Critical Concerns on FIDA

With the positive aspects of FIDA mentioned in the general remarks, we also hold some concerns regarding the level of ambition of certain provisions and the vagueness of others.

This section focuses on:

Gradual Approach to Data Access: Safeguarding Interests of Customers and Financial Institutions

Clarifying and Narrowing Down Data Scope, Entities in FIDA, and its Territorial Application

Definitions

Considerations Surrounding Articles 4 and 5

Safeguarding Trade Secrets and Intellectual Property Rights in FIDA: Striking the Right Balance

Need for Clarification on Advertising Purposes and Direct Marketing

Reconsidering Article 7 in FIDA

Clarifying the Concept of 'Permission' in FIDA and Its Interaction with GDPR Legal Basis

Establishing a Framework for Clearer Permission Dashboards

Financial Data Sharing Schemes

- Advocating Voluntary Implementation of Schemes in Open Finance
- Challenges of Implementing FIDA Schemes and Establishing Governance within an 18-Month Timeline
- Enhancing Compensation Structures in FIDA: A Call for Fair and Comprehensive Remuneration
- Balancing the Commission's Delegated Power

Stronger Cooperation between FIDA's Competent Authorities and GDPR' Supervisory Authorities

Aligning EBA Register: FIDA with PSD2/PSD3

Rebalancing Penalties for Natural Persons

FIDA and Cross-Sector Data Access

➢ Gradual Approach to Data Access: Safeguarding Interests of Customers and Financial Institutions

Art. 2.1: We have concerns regarding the broad inclusion of various financial products and services within the scope of the categories of customer data. The proposal covers mortgage, credit, savings account, investment services, and more, encompassing a wide range of sensitive financial information. Such extensive access by various entities raises the potential for misuse or compromise.

Rather than opening up to a diverse range of products and services all at once, **we suggest adopting a methodical, prudent and gradual approach which would safeguard the interests of both customers and financial institutions**. **We propose commencing with those categories of data that would directly benefit customers based on a staggered approach guided by customers' needs and anticipated use cases**. **FIDA should exclude data categories for which there is no strong demand in the market**.

This proposed methodology holds several advantages:

- By initially concentrating on the categories of data that offer clear benefits to customers, it would enable a more focused and proportionate approach to data access. This approach ensures that data access is aligned with genuine customer needs and avoids encompassing areas with less evident benefits.

- It would alleviate the burden on financial institutions and information service providers in terms of data processing, and security. To manage and safeguard the extensive categories of data under FIDA requires significant resources and infrastructure investments. By narrowing the scope to customer-beneficial data categories, these entities can better allocate their resources on effectively managing and securing the essential data required for their specific services, resulting in improved operational efficiency and cost-effectiveness.

- It would enhance customer confidence and foster trust in financial institutions and information service providers because it would demonstrate the value of data sharing to customers, while also safeguarding their privacy and controlling costs. This, in turn, would encourage individuals to engage in digital financial services with peace of mind.

- It would better serve the interest of clients and simplify the implementation of the Regulation by reducing the complexity of data access, sharing, and compliance procedures for both data holders and users. Financial institutions can focus their efforts on specific data categories, ensuring the implementation of proper governance, security, and compliance measures. This facilitates smoother adoption of the Regulation.

Focus on

Art. 2.1 letters (a) and (e), letter (b) on the investment data collected for the purpose of carrying out suitability and appropriateness assessments, and letter (f)

We are particularly concerned about the inclusion of credit, data collected for the purpose of carrying out suitability and appropriateness assessments, non-life insurance products, and data which are part of a creditworthiness assessment of a firm.

Concerning **credit and non-life insurance products (Art. 2.1 letters (a) and (e))**, these products are based on global risk pooling among all clients. New entrants in the market, or stronger price-competition, may lead to a division in the market by focusing solely on lower-risk clients. This could potentially destabilise the risk pooling approach if traditional service providers end up catering primarily to higher-risk clients.

With regard to the scope of **investment data defined in Art. 2.1(b) we reiterate our concerns[2] and recommend excluding investment data collected for the purpose of carrying out suitability and appropriateness assessments as defined in Art. 25 of the 2014 Markets in Financial Instruments Directive (MiFID II) from the scope of FIDA.**

The risk profile of a customer relies on input and output data. With regard to the former, the risk profile is established on the basis of information provided in compliance with the regulatory framework, but more importantly from the ongoing trust relationship established with the advisor, provided voluntarily by the customer each time. Concerning output data, the risk profile depends on the timing (new source of revenues, adverse events requesting funding), the products (some products can be used to finance retirement, others studies or a mix with a different risk appetite) and the assessment performed by each financial intermediary (some financial institution will consider 5 levels of risks whereas others 3; some institutions will consider 20% of equity max whereas for a similar level of client appetite others will consider 25%).

The new Art. 25 in MiFID under the 'Omnibus Directive' proposal[3] – as part of the Retail Investment Strategy package – regulates, among other things, the standardisation of information for suitability and appropriateness assessments. ESMA is tasked to define a mandatory list of key information, which would need to be presented in a standardised way in a report. We believe that a standardised format across Europe is unlikely to meet the needs of either clients or investment firms. With a standardisation of customer-profile data it would not be possible to suit every client's specific needs. ESMA in its April 2022 letter to DG FISMA's Director-General stated in particular that '*the proposal to apply a unique and standardised retail investor assessment regime that no longer differentiates among the various investment services might raise questions of whether a 'one size fits all' approach can effectively serve all different types of retail investors and situations'*.

Moreover, the changes to Art. 25 of MiFID introduced by the Omnibus Directive, along with the FIDA proposal, give rise to additional concerns regarding the potential re-use and portability of the standardised report. This is particularly noteworthy given the cross-references made in the explanatory

[2] Page 13 of the EACB's Recommendations For a Feasible Open Finance Ecosystem, 24 March 2023.
[3] Proposal for a Directive of the European Parliament and of the Council amending Directives (EU) 2009/65/EC, 2009/138/EC, 2011/61/EU, 2014/65/EU and (EU) 2016/97 as regards the Union retail investor protection rules. COM/2023/279 final.

EACB AISBL – Secretariat • Rue de l'Industrie 26-38 • B-1040 Brussels
Tel: (+32 2) 230 11 24 • Enterprise 0896.081.149 • lobbying register 4172526951-19
www.eacb.coop • e-mail: secretariat@eacb.coop

memorandum, as well as in the impact assessments of both the Omnibus Directive and FIDA[4].

The scope of the data pursuant to **Art. 2.1(f) (data which forms part of a creditworthiness assessment of a firm)** is not very clear when assessing the creditworthiness of a company for a loan or assigning it a rating. Similarly to the investment data use case, the data used in this scenario is likely to vary from one institution to another. Each institution may have distinct preferences for the information they require. This is because individual banks and rating companies have their unique methods for assessing the risk associated with a loan. The risk assessment of credit exposures is a core competence of lenders and an important competitive advantage that must be preserved to ensure a wide range of credit options. Pursuing a policy goal of standardising this data for access could be misguided and potentially detrimental to competition.

A Wide Scope will also Impact Bank Cybersecurity and IT Architecture

We strongly question the paradox to which FIDA exposes banks, particularly in terms of cybersecurity, which consists of 5 main functions: Identify, Protect, Detect, React, and Rebuild.

Banks monitor threats (Cyber Threat Intelligence). One of the tasks of this monitoring consists of identifying the fact that company data is not circulating in the usual places of exchange for cybercrime (cybercriminal blogs, marketplaces, etc., including in the darknet). When the data of an establishment has been replicated by a multitude of 'data users', in the event of the discovery of company data in poorly frequented places, banks would be unable to identify the origin of the leak and would have to launch nevertheless all analyses on their Information System. This research is costly and will multiply proportionally to the number of leaks, therefore to the number of 'data users' holding the company's data (exponentially if the 'data users' have the possibility of transmitting data to third parties).

The implementation of FIDA will imply a paradigm shift, from a model where data is explicitly entrusted to an actor who is responsible for its protection, to a model with numerous data users, making it difficult to identify who holds it and therefore to guarantee an optimal level of protection.

[4] To illustrate, the following passages are pertinent in that context: 1) Page 5 of the Explanatory Memorandum of the Omnibus Directive '*This proposal [Omnibus Directive] is also aligned with the objectives of upcoming Commission initiatives which will seek to facilitate data sharing within the financial services sector. With the standardised report on information collected by a firm on its client for the purpose of the suitability or appropriateness assessment, this initiative is expected to facilitate, if the client requests that report, more seamless and cost-effective data sharing and re-use of such information by other firms selected by the client'*; 2) Page 7 of the Impact Assessment of the Omnibus Directive '*The Open finance initiative runs in parallel with the Retail investment strategy and coordination of the two will take place especially with regards to standardisation and/or portability of customer data'*; 3) Page 25, box 2, FIDA Impact Assessment: '*Open finance would enable less cumbersome and more effective suitability and appropriateness assessments of individuals by facilitating the reuse of input data in automated processes*'.

Despite the issuance of an authorisation for FISPs, it is not clear whether the level of requirements set for operational and cyber resilience will be imposed and verified consistently by regulators.

The conditions for the approval and supervision of FISPs must be homogeneous in all European countries to ensure a true level playing field among market players. FISPs should be subject to the same requirements as banks in terms of cybersecurity to ensure that they do not become the weak link of financial data integrity in Europe. In particular, they should not be subject to the simplified ICT risk management framework in Art. 16 DORA.

An in-depth impact analysis is an essential prerequisite, in order to identify the risks on cyber-security and privacy linked to sharing a large scope of data.

➢ Clarifying and Narrowing Down Data Scope, Entities in FIDA, and its Territorial Application

Exclusion of Derived and Inferred Data from Scope: Safeguarding Financial Institutions' Competitive Assets

Art. 3.3: The definition of customer data under FIDA is overly broad and may give rise to interpretation. The definition appears to cover not only observed and raw data, but also derived and inferred data. As highlighted by the European Data Protection Supervisor (EDPS), parts of the Proposal's Impact Assessment indicate that data derived or inferred by the data holder from customer-provided data through profiling is not intended to be within the scope of the Proposal. This should be addressed not only in the Impact Assessment but also in the Regulation itself.

Derived and inferred data represent a valuable asset, crucial for maintaining a competitive edge in the market. Allowing access to this type of data can weaken a financial institution's market position and hinder its ability to innovate and differentiate itself.

We firmly believe that the ambiguity regarding the inclusion of derived and inferred data within the scope should be definitively addressed in FIDA. This can be achieved by **amending the definition to explicitly exclude derived and inferred data generated by financial institutions**.

Furthermore, second-hand data, for example data that is collected for a credit approval, data that is handed in by the customer, but also data that is acquired from other parties should not be encompassed within the scope. The data holder should not function merely as a conduit of second-hand information. In addition the data holder is not responsible of the quality of that 'second-hand information'. It would be better if that data would be collected at the (original) source.

Defining Data Scope in FIDA Schemes

FIDA provides some indications (particularly in the Recitals), but it is generally lacking clarity regarding the specific data for each category. Furthermore, it is unclear what specific information should be provided to data users.
We suggest adding an article in FIDA that explicitly states that the type of data for specific products or services should be defined within a scheme.

Safeguarding Data Access: Mitigating Opportunistic Behaviour

- **Art. 2.2(b)**: We understand that according to Art. 2.2(b) registered Account Information Service Providers (AISPs) under PSD2 could benefit the same rights provided by FIDA as other data users. This could potentially lead to opportunistic behaviour by entities wishing to access to the full array of financial data but opting for AISP's registration regime over the FISP's authorisation regime. **FIDA should require that AISPs, which are already registered under PSD2 and intend to access financial data under FIDA, must also apply for FISP's authorisation regime**.

- Unlike the access regime for IoT data outlined in the Data Act proposal, **FIDA lacks measures to prevent 'gatekeepers' from accessing data**. **Consideration could be given to adopting provisions similar to those found in Articles 5.3 and 6.2(d)[5] of the Data Act to ensure that gatekeepers do not transition into data users and gain access to financial data**.

Defining the Territorial Application of FIDA

FIDA currently does not have a geographical limitation. This is unusual compared to other European legislations, such as PSD2, the GDPR, and the Data Act. It is also considered undesirable, as it may have a negative impact on the position of EU banks operating outside the EU. **We believe FIDA should only apply to data processed by financial services providers as a consequence of financial services that are provided in the EU**.
Therefore, we intend to propose an amendment in FIDA by adding an article specifically addressing the territorial scope.

[5] Art. 5.3 of the Data Act states: '*Any undertaking designated as a gatekeeper, pursuant to Article 3 of Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector (Digital Markets Act), shall not be an eligible third party under this Article and therefore shall not: (a) solicit or commercially incentivise a user in any manner, including by providing monetary or any other compensation, to make data available to one of its services that the user has obtained pursuant to a request under Article 4(1); (b) solicit or commercially incentivise a user to request the data holder to make data available to one of its services pursuant to paragraph 1 of this Article; (c) receive data from a user that the user has obtained pursuant to a request under Article 4(1).*'
Art. 6.2(d) states that '*the third party shall not […] (d) make the data it receives available to an undertaking designated as a gatekeeper pursuant to Article 3 of Regulation (EU) 2022/1925;*'.

➢ Definitions

In addition to the remarks regarding the definition of customer data mentioned earlier in the paper and permission (for the latter, see relevant section), we also highlight the following definitions, which need to be refined.

Art. 3(2) – Definition of customer

- In its press release[6], the European Commission emphasises that objective of FIDA is to enable consumers and firms to have greater control over access to their financial data, and support SMEs in their pursuit of better access to finance. However, currently, due to the broad definition of 'customer', FIDA applies to all customer segments, encompassing various types of enterprises, including large multinational customers of a data holder. However, particularly large corporations do not require FIDA for access to their data, as they have substantial bargaining power and should therefore be considered out of scope.

  Therefore, **and with regard to legal persons, we suggest altering the definition of 'customer' to only refer to micro, small or medium enterprises**.

Art. 3(5) – Definition of data holder

- It is not evident, across all categories of data, which entity holds the actual data and who is specifically affected by obligation. Art. 2.2 identifies the financial institutions falling under FIDA but does not provide a clear distinction between data holders and data categories. We think that a **data holder is the entity that initially provides the respective product or service to the customer**. Only by defining 'data holder' in this way can we ensure that the data remains up to date, preventing redundant access claims that could result in conflicting customer data from different sources. This could have detrimental effects on data quality within the financial data framework envisioned by FIDA. Therefore, a corresponding clarification is necessary in this regard.

If the main goal of the legislator is to help firms to port their financial data easily (like data from balance sheets, profit and loss accounts), then tax advisors, auditors, accountants, and public registers should also be included in scope and regarded as data holders. They hold this data in its original form and retain information crucial to the financial status of the customer.

[6] European Commission press release '*Modernising payment services and opening financial services data: new opportunities for consumers and businesses*' of 28 June 2023, which states: *'In practice, this proposal will lead to more innovative financial products and services for users and it will stimulate competition in the financial sector. For example, consumers will benefit from improved personal finance management and advice. Previously burdensome processes such as comparison services or switching to a new product will become smoother and cheaper, including for example, automated processing of mortgage applications. SMEs would also be able to access a wider range of financial services and products, such as more competitive loans resulting from their creditworthiness data being more easily accessible.'*

Art. 3(7) – Definition of financial information service

- The text lacks a definition for 'financial information service'. We firmly believe that it is essential to establish a precise and specific definition, following the same rational as 'account information service' defined in PSD2.

  We believe that authorisation as a financial information service provider should be limited to offering information services. If a third-party provider intends to offer financial services or commercialise financial products, it must be authorised as a financial institution. Any financial data shared should be used strictly within the bounds of the authorisation granted to the third party, regardless of whether the data is received directly or indirectly.

  This limitation on data reuse is also compliant with the purpose limitation outlined by the GDPR.

➢ Considerations Surrounding Articles 4 and 5

Challenges Regarding the Continuous and Real-time Data Access in FIDA

The mandatory requirement for continuous and real-time access to customer data in Articles 4 and 5 raises questions about its alignment with the GDPR. **Articles 4 and 5 FIDA draw inspiration Art. 20 GDPR on the right to data portability, but they go further by requiring continuous and real-time access provision of customer data in scope**.
The free of charge element goes way beyond the GDPR spirit (Art. 12 GDPR allows the data controller, when requests have a repetitive character, notably to '*charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested*'). Moreover, in FIDA, the data in scope refers to both personal and non-personal data that is provided by a customer and generated as a result of the customer's interaction with the financial institution.

The data minimisation principle, a core principle of GDPR, does not seem to fit in this context. Many parties receiving data from banks and other data holders do not require continuous information. Additionally, **providing data continuously and in real-time demands significant effort from data holders, while data users often do not necessitate real-time information. This is particularly true for accounts like savings, or mortgages, where the frequency of transactions is much lower compared to payment accounts. As a result, information that is a day old can still be valuable**. By mandating real-time and continuous data provision, a proper balance between the interests of data users and data holders is not achieved. We believe it is crucial to find a balance between facilitating efficient data access and safeguarding individual privacy rights. When necessary, a single scheme can further discuss whether more detailed provisions are needed.

For the above reasons**, we suggest replacing the continuous and real-time access elements with 'in due time'**.

Furthermore, the current very broad definition of customer data and the extensive range of data categories within scope, combined with the demand for **continuous real-time access, pose substantial implementation challenges**. The volume of data to be provided continuously and in real time is exceptionally burdensome. Additionally, beyond their mere quantity, it is essential to consider that a portion of the requested data may not be readily available for online publication, as it may reside in legacy systems or even within Excel files. The process of searching for and systematising this data entails significant costs in terms of both financial resources and time, along with substantial infrastructure and development expenses. In light of these considerations, **we recommend a reduction in the required data volume, by proposing that only data accessible online, which users can already access, should be made available to both the customer and data users upon request, adopting an approach similar to that of Articles 66 and 67 PSD2 and Art. 33 PSR.**

Redefining Data Sharing Dynamics: Assessing the B2C2B Model in Art. 4

As currently drafted, Art. 4 FIDA might position the customer as an intermediary between a data holder and a potential data user, creating a B2C2B model. This model raises concerns as it might not align with the best interests of the customer. In this setup, customers would assume full responsibility for any data transfers initiated by data users to those same data users. On the other hand, parties can act as a data user without meeting the legal requirements associated with it. Furthermore, this approach could disrupt the functioning and equilibrium of the broader data sharing ecosystem. There is a risk that uninformed customers might unknowingly share their financial data with entities that are not in compliance with European data protection rules. This scenario could inadvertently promote opportunistic behaviour, where certain data users opt for this model over the traditional B2B approach, which with FIDA could include compensation through a scheme.

Based on the above considerations, **we suggest narrowing down its scope to legal persons**.

Additionally, Art. 4 should specify that the data collected under Art. 4 can only be used for the customer's private purposes.

We also recommend removing the word 'free of charge' in Art. 4. It is neither necessary nor reasonable for business customers to receive an additional service without paying for it. If the article remains applicable to consumers, we suggest adding the words 'without extra costs for consumers'.

Clarifications Needed in Art. 5: Implications for Data Access Outside of Schemes

Although it appears clear that a data holder cannot claim compensation if it is not part of a scheme, there is ambiguity in Art. 5, paragraphs 1 and 2 regarding whether a data user not participating in a scheme would still have the right to access data from a data holder, based on the customer's agreement. This also includes a scenario where a data user seeks access to data that are not part of the scheme in which the data user participates. The paragraphs seemed to

suggest that in the absence of a scheme, the obligation for the data holder to share data without compensation would still apply. If this were the case, we believe there would be no incentive for a data user to participate in a scheme. For a data holder, the incentive would be ruled out, as the EU Commission would step in with a delegated act (Art. 11).
To adjust the ambiguity in Art. 5, **we recommend that the legal text explicitly specify that any sharing of data with a data user shall be made in accordance with the rules and modalities of a financial data sharing scheme**. **This should also imply that, according to a scheme, if a specific data field is not within the scope, a data user cannot request to receive this data field directly from the data holder through Art. 5. This should be reflected both in Articles 5 and 6**. Recital 50, concerning data sharing on a contractual basis, should remain unchanged.

In addition, Recital 10 clarifies that a request for customer data sharing can be initiated by a data user acting on behalf of the customer. However, the first sentence of paragraph 1 of Art. 5 exclusively outlines the process for a request directly from the customer (*'upon request from a customer submitted by electronic means'*). We believe Art. 5 should be aligned with Recital 10. In cases where the customer has explicitly granted 'permission' to the data user, it may prove operationally more efficient for the data user, duly authorised by the customer, to make the access request.

Finally and compared to PSD2 and PSR, FIDA lacks specific guidance on how a customer can grant 'permission' for data access, particularly in terms of confirming this authorisation to their bank. Both Articles 4 and 5 mention a customer request 'by electronic means'; however, this terminology lacks clarity. To ensure user protection, it is imperative to establish detailed technical regulations outlining the security requirements of this process.

➢ Safeguarding Trade Secrets and Intellectual Property Rights in FIDA: Striking the Right Balance

FIDA rightly acknowledges the importance of safeguarding confidential business information and trade secrets, as emphasised in Recital 9. This is further underlined in Articles 5.3(e) and 6.4(b), which places obligations on data holders and data users to respect the confidentiality of trade secrets and intellectual property rights while providing access to customer data.

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 to this consideration such an obligation to check would mean a great potential liability for the data holders and data users concerned to a completely unclear extent. Moreover, considering that Art. 5.1 requires that customer data is to be made available without undue delay, continuously and in real-time, **it is unclear how it would be possible to automatically differentiate trade secrets and confidential business**

information from the other data, if at all. Also, conducting a real-time manual evaluation would be practically unfeasible.

Additionally, we believe that due consideration should be given to safeguarding the trade secrets and intellectual property rights of the data holder. This is due to the fact that the way in which customer data is collected and processed, particularly when customised to the data holder's specifications, can represent a distinctive and competitive advantage for them. Therefore, **we propose that Articles 5 and 6 expressly limit the customer's or data user's access rights to the data in a manner that ensures no business secrets and intellectual property rights of the data holder are compromised**.

➢ Need for Clarification on Advertising Purposes and Direct Marketing

The provision in Art. 6.4(e), which states that a data user shall *'not process customer data for advertising purposes, except for direct marketing in accordance with Union and national law,'* introduces a distinction between advertising purposes and direct marketing.

While we acknowledge the need for such provisions to protect consumer interests, we believe that a comprehensive understanding of the terms 'advertising purposes' and 'direct marketing' is important. This approach will enhance clarity regarding the acceptable boundaries of data processing activities and promote legal certainty for all stakeholders engaged in such processes.

➢ Reconsidering Article 7 in FIDA

We have concerns and reservations about Art. 7, which requires the EBA and the European Insurance and Occupational Pensions Authority (EIOPA) to develop new guidelines on how personal data originating from other areas of the financial sector that are in scope of FIDA can be used to assess the credit scoring of a consumer, and in products and services related to the risk assessment and pricing in the case of life, health and sickness insurance products.
The credit scoring requirements for consumer loans are regulated in the Consumer Credit Directive (CCD). Additionally, the EBA Guidelines on loan origination and monitoring[7] have been applicable to new loans since 30 June 2021 (and to existing loans since 30 June 2022). These guidelines already encompass extensive regulations on data management, lending standards, and customer relations. Therefore, we do not see an additional necessity for mandating the EBA in this context.

Furthermore, **if detailed specifications are imposed by the legislator or regulator regarding the data to be used for credit scoring, it might potentially diminish the overall quality of credit scoring. It should be at the discretion of individual lenders to determine which data they consider relevant for the comprehensive assessment of creditworthiness**.

[7] EBA Guidelines on loan origination and monitoring, EBA/GL/2020/06, 29 May 2020.

Finally, **standardising the type of personal data required for credit scoring, risk assessment, and pricing in the case of life, health, and sickness insurance products may stifle innovation and the possibility to differentiate from competitors**.

Based on the above considerations, **we suggest deleting Art. 7**.

➢ Clarifying the Concept of 'Permission' in FIDA and Its Interaction with GDPR Legal Basis

The term 'permission' is mentioned several times in FIDA, yet no specific definition is provided in Art. 3. Recital (22) explain that the '*permission dashboard should display the permissions given by a customer, **including** instances when personal data is shared based on consent or is necessary for the performance of a contract'*. This could imply that 'permission' encompasses consent, contractual, and potentially other aspects, indicated by the term 'including'. Although the Commission acknowledged their challenges with the wording, they also suggested that the use of 'including' is to account for the diverse entities covered by FIDA, some of which may rely on legitimate interest rather than consent or contractual performance.

Given that this combination of concepts under a single term could lead to significant confusion and legal ambiguity, it is crucial to define the concept clearly, as **it remains uncertain what the term 'permission' means and implies**.

If the text stays as is, FIDA appears to introduce a permission mechanism, in addition to the need for a valid legal basis under GDPR Art. 6.1. If this is the case, FIDA lacks clarity regarding how these two mechanisms will work in practice. Therefore, a clearer guidance on the interaction between the permission mechanism and the GDPR legal basis should be provided. The Regulation should explicitly specify, for example, that the requirements for 'permission' are not the same as the requirements for 'GDPR-consent'.

Also the EDPS in its Opinion noted an ambiguity regarding the term 'permission' and the legal basis for processing under the GDPR, namely 'consent' or 'explicit consent' or 'necessity for the performance of a contract'[8]. **We suggest taking into consideration the EDPS recommendation to clarify in Recital (48) that 'permission should not be construed as 'consent' or 'explicit consent' or 'necessity for the performance of a contract' as defined in Regulation (EU) 2016/679'**.

Furthermore, **it is not clear from the proposal how the customer grants 'permission' to the data user to access his/her data. It is considered necessary to issue specific technical regulations that clearly define the procedure for customer identification by the FISP, e.g. use of two-factor authentication on the SCA model, or use of the eIDAS protocol**. An adequate process of customer identification and collection of certified information is considered necessary as a measure to fight possible violations of banking secrecy and of the

[8] EDPS, Opinion 38/2023 on the Proposal for a Regulation on a framework for Financial Data Access, 22 August 2023, paragraphs 17 and 18.

GDPR, as well as to mitigate possible fraudulent phenomena (moreover, PSD2 requires no sensitive data to be disclosed).

➢ Establishing a Framework for Clearer Permission Dashboards

Permission dashboards or similar tools are helpful instruments for customers, since they could keep control over what type of data is being shared as well as who they have granted consent to. While recognising their potential benefits and the crucial importance of exercising GDPR rights in open finance, it is important to note that developing and implementing these tools is a complex task, even at a single entity level. It becomes even more intricate when considering that the dashboard will be provided by the data holders and the information / data will pertain to agreements a customer has with potentially multiple data users, about which the data holder has no insight.
Therefore, **we suggest that the permission dashboard be offered by data holders on a voluntary basis**.

Clarifying the liability aspects

Art. 8 on permission dashboards does not seem to define liability aspects. Recital (22) of FIDA simply states that *'the permission dashboard should warn a customer in a standard way of the risk of possible contractual consequences of the withdrawal of a permission, but the customer should remain responsible for managing such risk.'*

We believe that the **liability aspects and the consequences in case a customer decides to withdraw her/his 'permission' should be clear in the legal text**. We would like to also stress that on the relationship between two or more economic actors (data holders and data users), data holders cannot be held responsible for how data quality is assessed in the context of purposes and services provided by data users. Data users should be responsible for obtaining the data in a way that is compliant with the GDPR.

Finally, as a permission dashboard is also envisioned in the PSR, **it is important to ensure that the requirements for dashboards are harmonised between FIDA and PSR**. **Data holders should be able to offer a single dashboard to serve both the purposes of FIDA and PSR. Additionally, the data holder should have the option to integrate the FIDA/PSR dashboard with a GDPR dashboard, provided they have one**.

Providing a Permission Dashboard for Online Banking Clients only

We have noticed that **Art. 33 of the proposal for a Payment Services Regulation (PSR) outlines that the right to use account information services (AIS) and payment information services (PIS) will be limited to payment service users (PSUs) whose accounts are accessible online**. This implies that a dashboard will also be provided for those PSUs with online accessible accounts who are using PSI/AIS services. However, **there is no corresponding mention of this distinction in FIDA**, which also mandates a dashboard but without differentiation between clients who use online banking tools and those who do not. **Drawing from the provisions in the PSR proposal, we propose incorporating a similar provision within FIDA**.

➢ Financial Data Sharing Schemes

Some important points related to **Art. 9** on the financial data sharing schemes are the voluntary nature of schemes, the timeline, governance, and the compensation structure.

Advocating Voluntary Implementation of Schemes in Open Finance

The banking industry has gained significant experience with multistakeholder schemes in the area of payments and, more recently, with PSD2. Schemes represent the most efficient way to connecting around 4500 banks in Europe with approximately 1000 FinTechs, creating a clear framework of responsibilities. Despite this, we express reservations about the mandatory nature and the timeframe of financial data sharing schemes.

We have been in favour of such schemes since the beginning of the discussion around open finance. However, we have been consistently **advocating for these schemes to be implemented on a voluntary basis**. The inherent benefits of a scheme, including cost and responsibility sharing, should organically drive the market towards this option and allow the necessary time to conduct the negotiations of the financial and technical aspects. These technical considerations are complex and hold substantial implications for all parties involved as well as the EU data single market, given the interlinked nature of standards across sectors. A market-oriented approach that offers flexibility and encourages collaboration is more likely to foster innovation and meet diverse customer needs.

Challenges of Implementing FIDA Schemes and Establishing Governance within an 18-Month Timeline

FIDA set a timeline of 18 months for joining a scheme. The long experience the industry have in creating schemes shows that, particularly when it concerns scheme between stakeholders with opposing interests, you need time to: i) set up the governance of the scheme (who can decide on what, what is the voting power of different parties, how to ensure the representation of all stakeholders in the decision making); ii) design and agree on the set of rules that everybody taking part in the scheme would have to respect.

With regard to the composition of the members of a scheme, Art. 10.1(a)(i) states that 'the members of a financial data sharing scheme shall include: (i) data holders and data users representing a significant proportion of the market of the product or service concerned […]'. **It should be clarified whether the reference market for the product/service is the EU or the national market. It is also not clear how the identification of the significant data holders and data users will be achieved, based on which assessment criteria or any relevant legislation**.

Furthermore, with the multitude of data categories under consideration in FIDA the above concerns really need sufficient time to be debated and elaborated. Not to mention the fact that the market needs to be informed at the earliest stage of the process, the development of the schemes needs to be funded, and the possibility of establishing a forum or fora to take

responsibility for the scheme(s) should be considered. **It is clear that 18 months is by far not enough to realise any of this**.

We suggest that **market participants should initially be provided with 18 months to establish schemes, along with an additional 12 months to negotiate the conditions for data exchange. Following this, all participants in a scheme should be granted at least 12 months to implement the scheme rules and set up the essential technical, organizational, and legal conditions for it**.

Enhancing Compensation Structures in FIDA: A Call for Fair and Comprehensive Remuneration

We welcome that FIDA include the principle of reasonable compensation. However, certain aspects require further attention or improvement.

Points (i) and (v) of Art.10.1(h), which cap the maximum compensation directly related to the making data available and based on the lowest prevailing levels in the market, raise concerns within the EACB. Limiting the maximum compensation can have detrimental effects on data holders' incentive to participate in a scheme.

Moreover, the wording used in Art. 10.1(h)(i), '*limited to reasonable compensation directly related to making the data available to the data user and which is attributable to the request'* is exactly the same as the one in the last subparagraph in letter (h), but related to the situation when an SME is a data user, '*not exceed the costs directly related to making the data available to the data recipient and which are attributable to the request'*. This makes the difference between the two levels of compensation non-existent.

Data holders often invest resources, time, and effort into collecting and maintaining high-quality data and they would have to further allocate resources to manage data-sharing processes, including compliance with data protection regulations. Limiting compensation may not appropriately acknowledge the investment made, in terms of both resources and compliance efforts, potentially resulting in seeing the opportunity cost of sharing data as too high when compared to potential benefits.
For the long-term sustainability of data-sharing schemes, fair compensation is essential to maintain ongoing cooperation and commitment from data holders, making it imperative to reconsider capping compensation as a policy approach.

We believe that a compensation mechanism should be established that fairly considers the costs incurred by data holders. The cost of making data available are not limited to the expenses associated with building and maintaining the necessary technical infrastructure.

The compensation structure should encompass a broader scope to also include investments related to the data itself (such as collection, structuring, preparation, etc.), ensuring a comprehensive remuneration for the data holder. This principle aligns with

Article 9.1 of the Data Act, which states that any agreed-upon compensation between a data holder and recipient should be reasonable and may include a margin.

Fair compensation is crucial for incentivising investment in new technologies, maintaining data security measures, and supporting sustainable business models in the financial sector

In addition, **the last subparagraph of Art. 10.1(h) allows SMEs, acting as data users**, to gain access to customer data in exchange for compensation limited to the direct costs associated with making the data available to the data recipient and attributable to the request. While this provision aligns with Art. 9.2(a) of the Data Act, it is crucial to note that a substantial portion of data-driven Fin-Tech firms fall under the SME category[9]. This could potentially exempt many Fin-Techs from providing compensation beyond the direct cost. We believe that this approach outlined in this subparagraph could be unfavourable to achieving a fair level playing field. Therefore, we **suggest limiting the application of the last subparagraph of Art. 10.1(h) to micro and small enterprises**.

Balancing the Commission's Delegated Power

According to Art. 11, in situations where a scheme is not established and there is no realistic prospect of such a scheme being set up, the Commission is granted the authority to adopt a delegated act. This act would define common standards for the data, and, when necessary, the technical interfaces; provide a model for determining the maximum compensation that a data holder can request; and address the allocation of liability among the entities involved in making customer data available.

We are concerned about how the assessment of the 'realistic prospect' for setting up a scheme will be conducted and what factual considerations will be taken into account. This is particularly challenging given that data holders and data users have only 18 months to join a scheme, which, as mentioned earlier in this paper, is not realistic.

Additionally, by already foreseeing in the proposal the possibility for the Commission to intervene by setting up standards, interfaces, compensation, and liability, it sends a misleading message to the entities involved in FIDA. If they know that the Commission will address the main aspects of a scheme without actually implementing one, what incentives do data holders and data users have to push for setting up schemes?
We believe that Art. 11 sets the ground for opportunistic behaviours from various entities. They may choose not to invest their staff, resources, and time in setting up a scheme and instead leave the Commission to do the heavy lifting.

[9] European Commission Staff Working Document, Impact Assessment Report acompanying the document 'Proposal for a Regulation of the European Parliament and of the Council on a framework for Financial Data Access', Page 121: 'SMEs benefit in the role as data users since a significant number of data-driven fintech firms are SMEs.' Please refer then to the Eurostat, Annual enterprise statistics by size class for special aggregates of activities. https://ec.europa.eu/eurostat/databrowser/view/SBS_SC_SCA_R2__custom_4687926/default/table?lang=en.

As a result, **we suggest moving the Commission's key actions outlined in Art. 11 to the evaluation clause, Art. 31**. This would enable the Commission, in its assessment of the various elements already specified in Art. 31, to also consider how the market has evolved in terms of setting up schemes. If not a single scheme has been established, the Commission can then contemplate intervention. This approach would provide more time for the entities within the scope of FIDA to prepare, establish, and join a scheme, while avoiding potential opportunistic behaviours.

We would like to reiterate that **the data user should not have access to the categories of data within the scope of FIDA unless they are a part of, and adhere to, a financial data sharing scheme**. We maintain this position because, as previously suggested, **we recommend amending Art. 5 in a way that explicitly states that the obligation to share data within the scope of FIDA is contingent upon membership in schemes**.

Interactions with Existing Schemes

A series of national approaches, limited to certain sectors and use cases, currently exist. These are also mentioned in the FIDA impact assessment, including the Berlin Group API standard and STET in France.

Although Recital (25), which states that '*such [FIDA] schemes may build upon existing market initiatives…*', and Recital (28), which states that *'Data holders and data users should be allowed to use existing market standards when developing common standards for mandatory data sharing*', seem to lightly refer to some sort of existing initiatives, we believe that **interoperability and the interaction between potential FIDA schemes and the existing national schemes should be given due consideration and explicitly reported in the proposal. FIDA should clearly allow varying governance scheme structures to coexist**.

➢ Stronger cooperation between FIDA's competent authorities and GDPR' supervisory authorities

In addition to the recommendations made by the EDPS regarding the inclusion of a provision under Art. 14(7) of FIDA[10], we propose establishing a stronger cooperation between FIDA's competent authorities and GDPR supervisory authorities, especially during the authorisation phase. This is of particular significance in the case of third-country FISPs. Therefore, **we suggest that before a FIDA competent authority grants authorisation to a third-country FISPs**

[10] EDPS, Opinion 38/2023 on the Proposal for a Regulation on a framework for Financial Data Access, 22 August 2023, paragraph 42: '*The EDPS recommends the inclusion of a possibility under Article 14(7) of the Proposal for competent authorities to withdraw the authorisation in cases where supervisory authorities under the GDPR establish that a FISP has breached its obligations under EU data protection law. This might be particularly important in what concerns FISPs' potential failures to implement appropriate technical and organisational measures to ensure that customers' personal data is adequately protected in the context of the data access and sharing mechanisms created by the Proposal. The withdrawal of an authorisation for the reason recommended by the EDPS could be facilitated by the exchange of information between supervisory authorities under the GDPR and competent authorities under the Proposal'*.

.

involving personal data, consultation with the GDPR supervisory authority should take place to verify the FISPs' compliance with EU data protection rules.

➢ Aligning EBA Register: FIDA with PSD2/PSD3

As mentioned in our general remarks, we appreciate the establishment of the EBA register. We believe that two elements in the proposal need further clarification.

The first pertains to the requirement in paragraph 2 of Art. 15, which states that '*the register referred to in paragraph 1 shall only contain anonymised data.*' This is not the case for the public register either under PSD2 or PSD3. Recital 43 in PSD3 specifies that '*the EBA should operate such a register in which it should publish a list of the names of the undertakings authorised or registered to provide payment services or electronic money services.* ***Where that entails the processing of personal data, the publication at Union level of information on natural persons acting as agents or distributors is necessary to guarantee that only authorised agents and distributors operate in the internal market and is therefore in the interest of the adequate functioning of the internal market for payment services***.'

For instance, in the case of a FISP that does not have an establishment and consequently designates a natural person as their legal representative (as per Art. 13), we propose that the name of the natural person be published on the Register. As per the PSD3 text, this is necessary to ensure that only authorised natural persons operate on behalf of the FISP in the European Union. Therefore, **we suggest the deletion of paragraph 2 of Art. 15 and the addition of a Recital similar to what Recital 43 specifies under PSD3**.

Secondly, we also observe that in **both PSD2 and the PSD3 proposal, it is stated that the EBA shall make the central register publicly available '*free of charge*'** (Art. 15.1 PSD2 and Art. 18.2 PSD3). Although this may seem like a minor clarification, **we recommend aligning the FIDA text with the current PSD2 and the new PSD3 proposal**.

➢ Rebalancing Penalties for Natural Persons

In our view, **the range of penalties stipulated in Art. 20.3(f)-(h) for natural persons** (maximum administrative fine of up to EUR 25 000 per infringement and up to a total of EUR 250 000 per year) **is disproportionate to the severity and impact of any violations of the provisions listed in Art. 20.1**.
We consider that administrative sanctions and other administrative measures for specific infringements should be scaled back to a level which is proportionate to the severity and impact of an infringement of provisions listed in Art. 20.1.

We believe that imposing a personal sanction on a director may be overly stringent, potentially deterring qualified individuals from assuming such responsibilities due to concerns about personal financial risks. Moreover, considering the nature of the regulation, we find it unnecessary. FIDA

operates in a distinctly different realm compared to regulations like DORA. The risk of identity fraud, for instance, is significantly lower when a data holder opts not to join a scheme.

➢ FIDA and Cross-Sector Data Access

FIDA does not include any cross-sectoral provision to facilitate the access of data from entities in other sectors by financial institutions. **A link with the role and tasks of the European Data Innovation Board, established by the Data Governance Act (DGA), should be made to promote the use of cross-sector data**.

4. Conclusions

Notwithstanding FIDA positive aspects also expressed in the general remarks, Cooperative banks are concerned about the potential risks associated with sharing data across such a broad scope set in FIDA, involving an extensive array of parties and purposes. The operational complexity is perceived to outweigh the anticipated benefits for the customer.

It is important that the deployment of such a system is proportionate to the creation of value for clients and remains a vector of innovation and progress, without harming the players and the security of the financial industry.

Furthermore, with the increased scope of data sharing, there is an elevated risk of cyber fraud targeting both the bank and its customers. It is reasonable to consider that in the event of a cyber failure of one of the FinTechs/FISPs accessing the data, this data could be exploited by malicious actors.

Contact:

The EACB trusts that its comments will be taken into account.

For further information or questions on this paper, please contact:

- Ms Marieke van Berkel, Head of Department Retail Banking, Payments, Financial Markets (marieke.vanberkel@eacb.coop)
- Ms Chiara Dell'Oro, Senior Adviser for Digital Policies (chiara.delloro@eacb.coop)