

AMICE Position paper on the proposed Regulation for financial data access (FIDA)

1.	General remarks	1
2.	Enhance customer trust in data sharing.....	3
2.1.	Clarify, categorise and narrow “customer data”	3
2.2.	Clarify the scope of the guidelines on data use perimeter	4
2.3.	Clarify the concept of customer’s permission	4
2.4.	Provide strong authentication mechanisms and encryption standards	5
3.	Ensure fair competition	6
3.1.	Reaffirming the need for reciprocity	6
3.2.	Strengthening the protection of trade secrets	8
4.	Enable an effective implementation of the regulation.....	9
4.1.	Extending the deadline for establishing the financial data sharing schemes	9
4.2.	Dispelling interpretative uncertainties	10
4.3.	Ensuring fair compensation	10
5.	Conclusions	13

1. General remarks

AMICE, the Association of Mutual Insurers and Insurance Cooperatives in Europe, welcomes the opportunity to provide feedback on the European Commission’s initiative to establish a framework for using and accessing customer data in finance through the proposed Regulation on Financial Data Access (FIDA). Removing barriers to effective and secure control and sharing of financial data is critical for fostering data-driven solutions and competition in the financial sector, ultimately benefiting consumers and businesses alike.

AMICE members are characterised by their central focus on their policyholders, who are generally the owners of their insurers rather than the external shareholders. The products, services and benefits derived from our members’ activities are conceived and applied for the best interests of their policyholders, with a long-term perspective at the core of the relationship between the mutual/cooperative insurer and the policyholder. It is therefore not a purely commercial relationship but rather based on the principle of solidarity between its members. Therefore, we are of the view that the FIDA should ensure that the fundamental principles of mutual insurance, such as the principle of solidarity and the customer-centric approach are preserved.

AMICE appreciates the Commission's initiatives to promote the uptake of a more digital and data-driven economy, in view of the positive spill overs toward the insurance industry. Digital technologies are reshaping insurers' business models, leading to better customer experiences, more personalised and innovative services, as well as improved risk assessment and underwriting.

However, creating European data spaces introduces challenges, including new potential vulnerabilities and a higher risk of data loss and abuse due to increased accessibility and involvement of multiple parties. Hence, for this model to succeed, cautious rules for accessing customer data are essential to balance data access with minimising risks for customers. Striking this right balance is challenging and, in this perspective, we commend the Commission for developing a framework on financial data access that, while retaining a **customer-centric approach**, goes beyond the "open banking" model established by the Payment Services Directive (PSD2), without merely replicating it. In particular, AMICE welcomes that **financial institutions are given the autonomy to define through financial data sharing schemes the terms, conditions, and important aspects governing access to customer data**. This approach offers greater flexibility compared to that adopted by the PSD2, where most implementation aspects were rigidly defined by regulations and standards set by policymakers. Furthermore, we appreciate the fact that, unlike the PSD2, the Commission introduced in the FIDA the principle of the **necessary compensation** for accessing the data.

Having said that, we identified several critical issues in the Commission's proposal, which risk hindering the uptake and potential benefits of the new Open Finance framework. Below is presented a brief overview of the proposed amendments to the FIDA's provisions, which will be elaborated further in the subsequent sections. Overall, our requests to the co-legislators aim to:

1. **Enhance customer trust in data-sharing** – AMICE suggests the adoption of a narrower scope of data to be shared, excluding special categories of data of highly sensitive nature (such as health-related data), as well as proprietary data and enriched or inferred data that goes beyond mere raw data. In addition, to increase legal certainty and consistency with GDPR principles, AMICE recommends clarifying the categories of customer data suitable for sharing and the rules on permission dashboards. Enforcing strengthened customers' authentication methods and protocols would also effectively mitigate risks for customers.
2. **Ensure fair competition** – To establish a level playing field with gatekeepers, we advocate for the introduction of a reciprocity clause allowing effective customers data portability from gatekeepers to financial entities, subject to customers' consent.

It is crucial that co-legislators give earnest consideration to the preservation of fair competition. Presently, the framework of obligations outlined by FIDA appears skewed, resulting in a significant imbalance that adversely affect financial entities, placing them at a **competitive disadvantage against third parties such as gatekeepers or extra-EU Fintech firms**.

According to FIDA, financial entities are obliged to share customers' data with other financial entities and with third parties qualifying as Financial Information Service Providers (FISPs). Conversely, FISPs are subject to relatively lenient requirements for authorisation, without a similar obligation to make customers' data available to financial entities. This asymmetry in obligations creates a unilateral flow of information from financial entities to third parties, devoid of essential reciprocal obligations.

The **lack of reciprocity in the data flow** not only hampers fair competition but also limits customers' empowerment over their personal data. Furthermore, there is a tangible risk that FIDA could pave the way for (non-EU) Big Techs' entry into the EU financial markets. These

corporations could exploit the FISPs' authorisations as a tool for amassing users' financial data, which in the future could be utilised for the provision of various financial or intermediation services. The described scenario should be firmly avoided, considering that gatekeepers, wielding their market dominance and powerful lock-in effects, could easily influence customers to obtain their consent to access data. The consequent data monopolisation threatens the competitive landscape and bears ominous implications for the stability of the financial markets.

Furthermore, the protection of trade secrets needs to be strengthened, considering that it now relies on a provision that is insufficiently defined and lacks clarity.

3. **Enable an effective implementation of the regulation** by extending the implementation timeline of the FIDA (36 months) and financial data sharing schemes (24 months), while also introducing fairer compensation mechanisms and ensuring the accuracy of the shared customer data.

In light of the above, AMICE advocates for targeted amendments to the FIDA proposal that would unlock the full potential of the new Regulation, while mitigating the major risks for customers, financial institutions and the overall soundness of financial markets, as described below.

2. Enhance customer trust in data sharing

AMICE welcomes the Commission's objective to establish a secure data sharing framework, which empowers customers with effective control over their data and allows firms to leverage the potential of data-driven innovation.

In this context, FIDA also aims at enhancing consumer trust in data sharing, providing additional safeguards in terms of data protection and digital operational resilience requirements. Indeed, without consumers' trust, the whole Open Finance framework would inevitably fail its policy objectives.

To share their data and grasp the opportunities offered by FIDA, consumers should have unwavering confidence in the security of their data, full control over the shared data, with the right to determine the purpose and the conditions under which their personal data will be used. To this end, consumers should have ready access to relevant information and data management tools, ensuring their ability to exercise their GDPR rights effectively.

However, establishing an effective Open Finance framework while ensuring customers' trust is challenging for both policymakers and financial entities considering:

- i) the large volume and variety of data sets that will be shared;
- ii) customers simultaneously managing multiple contractual relationships with various data holders and users.

Insurers have a longstanding commitment to data privacy and consumer protection. To maintain this commitment in an Open Finance framework, AMICE believes that implementing appropriate safeguards is essential. At the same time, **a well-defined scope would facilitate compliance with the GDPR principle of data minimization**, clarify liability allocation in data processing, and enhance consumer awareness about data sharing and its implications.

To this end, AMICE would like to raise the attention of the co-legislators on the following shortcomings in the Commission's proposal and share its recommendations.

2.1. Clarify, categorise and narrow "customer data"

The scope and definitions set the foundations for the implementation of the FIDA Regulation.

Article 2 sets the scope of the Regulation but the definition of “customer data” that it provides is very broad and does not properly identify which (personal/non-personal) data is suitable for sharing, opting instead to refer to an exhaustive list of financial products/services to which customer data relate (e.g. mortgage credit agreements, investments, loans, pension rights, non-life insurance products).

Thus, AMICE calls on the co-legislators to clarify and categorise “customer data” under Article 2 to better understand which data is suitable for sharing.

In addition, the scope of the proposed regulation should be restricted to insurance products where data sharing represents a real benefit in terms of financial innovation, and therefore exclude provident, statutory and medical liability insurance products.

The data exchanges that currently exist in public/private partnerships (fight against the unclaimed life insurance contracts, files of insured vehicles, etc.) should be excluded from the scope of FIDA.

Considering potential risks to customers, AMICE recommends explicitly excluding from the scope of FIDA special categories of personal data related to the customer, due to their highly sensitive nature, such as health-related data (Article 9 of GDPR) and provident, statutory and medical liability insurance products from the scope of FIDA.

2.2. Clarify the scope of the guidelines on data use perimeter

Under Article 7, FIDA provides that EBA and EIOPA, in close cooperation with EDPB, shall develop guidelines on the processing of customer data in the context of products and services related to the credit score of the consumer and to risk assessment and pricing of a consumer in the case of life, health and sickness insurance products (which should be coherent with the said FIDA scope of application). In particular, the guidelines developed by EIOPA should set out how data in the scope of FIDA can be used in products and services related to risk assessment and pricing in the case of life, health, and sickness insurance products (Recital 19, FIDA).

These provisions raise concerns to the extent that they lack clarity regarding the precise scope of application, use cases and implications of the abovementioned guidelines are unclear.

AMICE recommends that co-legislators further **clarify in the legislative text the scope of the future guidelines on data use perimeter**. This clarification should ensure that the forthcoming guidelines provide for a flexible framework¹ without adversely impacting innovation and competition in the market. In this context, AMICE highlights the importance of broadly involving stakeholders’ representatives in the process for issuing the guidelines.

2.3. Clarify the concept of customer’s permission

According to the FIDA proposal, customer financial data can only be shared at the customer’s request, and the customers can withdraw their permission to share the data at any time. To this end, **FIDA requires data holders to provide customers with “permission dashboards”**, which give customers a holistic overview of permissions granted, facilitating real-time modification of these permissions, and warning users to the potential contractual consequences linked to the withdrawal of such permissions. FIDA provides that the data holder and the data user for which permission has been granted by a customer shall cooperate to make information available to the customer via the dashboard in real-time. While AMICE supports the introduction of “permission dashboards” as pivotal

¹ Please see the European Commission’s Impact Assessment Report, page 49.

tools for data control, we recommend targeted amendments to reinforce transparency in the data chain and improve customers awareness on the consequences of their decisions.

As highlighted by the EDPS in its Opinion², the term “permission” in FIDA is not defined and this oversight breeds legal uncertainty for data holders, users, and customers alike. Indeed, **the use of the term “permission” in the proposed regulation is ambiguous, potentially being mistaken for similar terms** such as “consent” and “performance of a contract”, which represent the legal bases according to which personal data are usually processed by the financial sector (GDPR, Article 6(1)(a) and (b))³.

The current ambiguity about the meaning of “permission” within FIDA might also unduly or inadvertently distort the contractual obligations binding the customer or data subject. Reference is to the case where a customer intends withdrawing a permission which is necessary for the data holder/user to perform the contract. In that circumstance, withdrawing the consent would imply the termination of the contract, which is often subject to conditions according to the contractual terms.

Considering the above, AMICE suggests the explicit and careful definition of the term “**permission**” **within FIDA**. Such definition, in line with EDPS Opinion, should unequivocally distinguish “permission” from other terms, such as “consent”, “(explicit) consent” or “necessity for the performance of a contract” within the meaning of the GDPR. For instance, in situations where a customer alters permissions through the dashboard, **such changes should not precipitate automatic contract termination with the data user**.

2.4. Provide strong authentication mechanisms and encryption standards

Given the multitude of participants in the data sharing ecosystem, ensuring data security is key. Data security is the cornerstone of consumer trust, which is the fuel needed to propel the Open Finance framework forward. In this regard, AMICE would like to emphasise that **FIDA must enforce uniform standards among all market participants within the data chain**, aligning with GDPR and DORA, thus ensuring a consistent and secure experience for all users.

To ensure a high standard of data protection and foster customers’ trust, AMICE advocates for the introduction of technical rules aimed at supporting data holders in online customer identification and in authenticating consent for granting or withdrawing permissions. To this end, implementing secure customer identification mechanisms, such as the use of two-factor authentication (drawing upon the Strong Customer Authentication model of the PSD2), or the eIDAS protocol is crucial⁴.

AMICE advocates for the provision of reinforced and secure customer identification mechanisms (such as SCA or eIDAS) to mitigate the risks of privacy infringements and potential fraudulent activities. AMICE also recommends the embracement of advanced encryption standards, enhancing security in the data sharing mechanism and providing additional layer of protection to all stakeholders involved.

² Please see EDPS Opinion n. 38/2023 on the Proposal for a Regulation on a framework for Financial Data Access, published on August 22, 2023.

³ In this respect, it is worth remarking that insurance companies can process personal data under other legal grounds than consent or performance of a contract. For example, in scenarios involving the proactive collection of personal data amid fraud investigation initiatives, companies frequently invoke the “legitimate interest” clause provided by GDPR.

⁴ The eIDAS protocol is currently being revised with the introduction of the so-called European ID Wallet, which is aimed at providing a safe, reliable and simple tool for identification.

3. Ensure fair competition

AMICE fully supports the Commission's objective of fostering competition and innovation within the financial sector. Nevertheless, we advise the co-legislators to consider further amendments to the proposed regulation. Our recommendations primarily seek to:

- (i) address the existing imbalance between financial entities and Big Tech firms that may secure authorisation as Financial Information Service Providers (FISPs), either directly or indirectly;
- (ii) enhance the safeguarding of trade secrets, which is currently dependent on the ambiguous and insufficient provisions stipulated in Articles 5 and 6 of FIDA.

3.1. Reaffirming the need for reciprocity

It is worth noting that FIDA's provisions on FISPs do not distinguish between Fintech startup, financial entities, or Big Tech companies qualifying as gatekeepers pursuant to the Digital Markets Act. The neutrality of the FISP definition, coupled with the absence of "financial information services" definition, creates a pathway for Big Tech firms to obtain authorisation as FISP, either directly or through affiliated entities.

While AMICE firmly believes that competition promotes innovation and consumer welfare, we cannot ignore the potential risks associated with Big Tech firms utilizing FISP authorisations to fortify their data oligopolies. There is a tangible concern that these firms might exploit the acquired financial data to offer services in direct competition with established financial firms, particularly in credit and insurance intermediation⁵. Recital 31 of the FIDA proposal is indeed worrying as it envisages the possibility for FISPs to "provide financial products and services to customers in the Union".

Given the extensive access to consumer data and superior analytics capabilities at the disposal of Big Tech firms, financial entities find themselves at a clear disadvantage⁶. This disparity, acknowledged by numerous scholars, poses a threat to competition, consumer welfare, and the overall stability of the financial sector⁷. Hence, it is crucial for legislative initiatives like FIDA, and others in the realm of Open Data and Data Economy, to not only promote competition but also ensure a level playing field and robust consumer protection.

⁵ As to the insurance sector in particular, in the research papers BIS – *From clicks to claims: emerging trends and risks of big techs' foray into insurance*, 2023, the authors point out that Big tech entities already act as insurance risk carriers or underwriters as well as insurance intermediaries in a number of jurisdictions across the globe.

⁶ For a broader analysis of this issue see, amongst others, F. DI PORTO, G. GHIDINI – *'I Access Your Data, You Access Mine'*. *Requiring Data Reciprocity in Payment Services*, published in ICC, 2020. The authors reached the conclusion that, in the payment services sector, a true level playing field between banks and BigTechs would be achieved through the introduction of a reciprocity clause, which would further empower the customers' control over their data and act as a stimulus for innovation.

⁷ In this respect see, amongst others, P. ARMSTRONG, S. BALITZKY, A. HARRIS – *BigTech – Implications for the financial sector*, in ESMA Report on Trends, Risks and Vulnerabilities, No. 1, 2020. More recently, in the research paper BIS – *From clicks to claims: emerging trends and risks of big techs' foray into insurance*, 2023, the authors argue that "As big techs' regulated insurance activities (as risk carriers or insurance intermediaries) continue to grow, a new big tech-specific regulatory approach might be warranted. Big techs' involvement in insurance and financial services more generally entails additional risks compared with traditional players. Potential risks to financial stability originate not only from the provision of financial services in combination with commercial activities but also from significant linkages with traditional financial institutions as service providers. Financial stability concerns also arise from big techs' tendency towards excessive concentration in the provision of both financial and technology services. These risks are not fully addressed by existing sectoral financial regulations and a regulatory rethink is warranted".

At present, the process of data portability from Big Tech firms to financial entities is ineffective. Customers intending to allow access to their data (for benefits such as insurance premium discounts) are often obstructed due to alleged violations of terms and conditions⁸. **This lack of reciprocity not only stifles competition and innovation within the financial sector but also hinders customer control and ownership over their data.**

In this regard, we acknowledge the EU legislators' awareness of the necessity to prevent excessive concentration within digital markets and ensuring a level playing field. This awareness is evident through the safeguards incorporated within the Digital Markets Act (DMA), particularly the obligation outlined in Article 6(9) of DMA, which mandates gatekeepers to facilitate data portability⁹. Even in the FIDA's impact assessment, the Commission is aware of the need to ensure a level playing field with large tech companies, when stating that *“the Digital Markets Act would ensure reciprocity in terms of data access between financial sector firms and large technology companies. To make it effective, **the data access right under this initiative would not become operational before the corresponding data access right under the Digital Markets does**”*.

Given the paramount importance of reciprocity with gatekeepers for establishing a fair level playing field, **we urge the introduction of an explicit reciprocity clause within FIDA**. Such a clause, contingent upon informed customer consent, would allow data holders to access specific customer data retained by a FISP qualifying as a gatekeeper, such as online search queries, purchase history, social media contents.

The incorporation of an effective reciprocity clause within FIDA would incentivise the financial industry to enhance their data analytics capabilities, thereby fostering effective competition with digital conglomerates. This approach would also be beneficial for smaller firms, where the net potential gain from data (information provided vs. received) is substantially larger¹⁰.

While few stakeholders have argued against introducing a reciprocity clause in Open Banking and Open Finance frameworks, citing the need to reinforce consumer control over personal data and consent rules, it is our contention that such clause would fortify consumer control over personal data. This argument is particularly relevant considering the pivotal role that financial dashboards will play in empowering consumers to control their data, coupled with the potential implementation of enhanced consent mechanisms, such as a two-factor authentication (2FA), which we strongly support.

FIDA should explicitly require open data users to be bound by the same legal framework to be able to access data. Data users from the moment they receive data from data holders must then become de facto data holders with the same regulatory and sectoral obligations to which data holders are subject.

⁸ In this respect, see the case of *Admiral vs Facebook* ([link](#)). Customers have been prevented from allowing Admiral to access their Facebook data, which would have allowed Admiral to propose lower tariffs on motor insurance, especially for new and young customers with no insurance history.

⁹ Reference is to the obligation for gatekeepers *“to provide end users and third parties authorised by an end user, at their request and free of charge with effective portability of data provided by the end user or generate through the activity of the end user in the context of the use of the relevant core platform service [...]”* (Art. 6, par. 9, Digital Markets Act).

¹⁰ Further on this topic, see IIF – *Reciprocity in customer data sharing frameworks*, 2018.

AMICE strongly advocates for the introduction of an **explicit reciprocity clause with gatekeepers** within FIDA, aligned with the provisions of the Digital Markets Act. While the Commission's impact assessment for FIDA suggests that reciprocity would be ensured through the Digital Markets Act, the critical nature of this issue warrants an explicit legislative articulation. Such a provision would not only bolster competition and innovation within the financial sector but also significantly enhance consumers' control over their data.

3.2. Strengthening the protection of trade secrets

For the successful implementation of any data sharing framework, it is crucial to clearly define the data sets to be shared. According to the Commission's proposal, 'customer data' means personal and non-personal data that is collected, stored, and otherwise processed by a financial institution as part of their normal course of business with customers. This data encompasses both information provided by a customer and data generated as a result of customer interaction with the financial institution (Article 3(3)).

AMICE believes that **the definition of "customer data" provided in the Commission's proposal should unambiguously exclude any derived and inferred data, in coherence with the policy option adopted in the Data Act.**

AMICE calls on the co-legislators to consider the important distinction between data that is directly supplied and controlled by the consumer in connection with the financial services and products listed under Article 2(1), on the one hand, and proprietary data on the other, which is created by processing/enriching consumer data in financial institutions. We argue that companies, including insurers, should not be obliged to share trade secrets, business-sensitive information or proprietary data resulting from their analytical and enrichment processes. Such data is not only integral to a company's competitive edge but also encompasses valuable expertise, know-how, and sensitive pricing information, whose disclosure could pose significant competitive risks.

In line with this perspective, the compromise text on the Data Act proposal¹¹ clarifies that *"information derived from this data, which is the **outcome of additional investments into assigning values or insights from the data, in particular, by means of proprietary, complex algorithms, including those that are a part of proprietary software, should not be considered to fall within the scope of this Regulation and consequently not be subject to the obligation for a data holder to make it available to a user or data recipient, unless agreed otherwise between the user and the data holder (Recital 14a)**".* In addition, during the final negotiations on the text, the co-legislators have decided to include strengthened measures to protect trade secrets. For instance, the Data Act now includes safeguards against possible abusive behaviour of data holders, as well as an actual exemption to data-sharing, which allows manufacturers to refuse certain requests for access to data, if they can substantiate that such access would lead to disclosures of trade secrets with "serious and irreparable economic losses" as a result hereof. Similar safeguards should also be provided or cross-referenced within the FIDA.

AMICE recommends the following:

- i. The legislative text should clearly specify the categories of "customer data" eligible for sharing, **limited only to raw data and excluding enriched or inferred data that goes beyond mere raw data.** In addition, for the sake of legal certainty, information accuracy and

¹¹ <https://data.consilium.europa.eu/doc/document/ST-11284-2023-INIT/en/pdf>

liability, **data provided by third parties** (e.g., purchased from a third party) **should also be excluded from the scope of FIDA**;

- ii. FIDA should reinforce the **protection of trade secrets**, either by providing or cross-referencing safeguards similar to those embedded by the Data Act within the FIDA.

4. Enable an effective implementation of the regulation

Moving to open finance requires large-scale investments in ICT infrastructures, technical innovations, and human capabilities. This will imply substantial costs and adaptations for the institutions under the scope, particularly for those not applying the PSD2 data-sharing obligations and the smaller enterprises. In this context, it is essential to define a **clear and proportional framework** that ensures a smooth transition to the provisions of the FIDA, providing financial institutions with the necessary resources and a suitable timeline to embrace the data-driven innovations envisioned by the legislators.

4.1. Extending the deadline for establishing the financial data sharing schemes

Regulatory consistency is paramount in relation to the **financial data sharing schemes** (FDSS) that will manage data access under the FIDA. Based on the proposal, FDSSs will be created and managed by private entities, in line with the overarching principles outlined in the regulation. However, the Commission is empowered to issue a delegated act whenever a FDSS is not developed for certain data categories.

While AMICE supports the Commission's effort to promote private-driven initiatives, it is important to stress that establishing FDSS will be a complex process that will require a significant amount of time, extensive negotiations among stakeholders and the resolution of implementation challenges. Consequently, to ensure an effective implementation of the regulation, it is necessary that the proposal provides clear guidance on the scope and the operation of the FDSS and grants sufficient time for the establishment of these platforms.

In this regard, AMICE holds the view that the suggested **roadmap for implementing the FIDA is overly ambitious**, considering the expected technical challenges and the extensive range of information subject to data-sharing obligations. Moreover, we note that an 18-month schedule for setting up and implementing FDSS is not feasible. Whilst allowing the industry to establish the FDSS governance and standards is a positive initiative, it should be acknowledged that their setting up will necessitate in-depth discussions between data users and data holders on a variety of issues.

Therefore, we invite the Commission to **extend the current timeline for implementing the FIDA to 36 months and consequently provide for a period of 24 months for the development of FDSS**. This extension would offer data users and data holders enough time to develop data sharing schemes that are both practical and secure, ultimately leading to improved outcomes for firms and customers.

Furthermore, it is worth considering that digitalising non-life insurance data sets pursuant to FIDA will require additional efforts for insurers in terms of data collection and data quality, especially when compared to credit institutions that can leverage the experience and the investments undertaken for implementation of PSD2 to make available financial data sets pursuant to FIDA.

Therefore, AMICE recommends adopting a step-by-step approach and allowing **additional time for the implementation of FIDA with reference to non-life insurance data sets**. During the initial phase of the FIDA implementation, focus should be on data related to "financial" assets (such as securities and life policies) instead of "physical" assets as homes, vehicles, and other properties.

AMICE suggests **reviewing the timeline for the implementation** of the FIDA, by extending it at least to 36 months, and consequently providing for a 24-month period for the development of the FDSS.

Furthermore, an extended timeline for implementation should be granted to allow digitalisation of data sets related to physical assets pertaining to non-life insurance policies.

4.2. Dispelling interpretative uncertainties

As to governance arrangements, Article 10(1a) of the proposal states the membership criteria for the FDSS, specifying that these schemes “shall” include customer organisations, consumer associations and “data holders and data users representing a significant portion of the market of the product or service concerned”. In relation to the latter, it would be beneficial to further specify the criteria for defining a “significant portion” of the market. Clarifications are needed so that data holders are not faced with a proliferation of schemes which would result in complexity and high implementation costs.

The proposal is unclear about who will finance the costs of setting up FDSSs, whether FDSS should be developed at EU or national level and whether they would be cross-sectoral or sector-specific ones. In this regard, the schemes should take into account the specificities of each product line (given the heterogeneity of products across Member States); the different players, the costs and time required for the centralisation of a wide range of data.

Article 9 provides that financial data sharing scheme membership is open to “data users” and not “financial information service providers”. It is unclear if data users can be part of a financial data sharing schemes even if they have not obtained an authorisation to offer services as a FISP.

In addition to the above, we ask to elaborate further on the conditions which empower the Commission to adopt delegated acts to regulate customer data sharing whenever private actors do not establish a FDSS within a “reasonable amount of time” (Article 11). **The definition of “reasonable amount of time” is not defined in the proposal and its interpretation remains unclear.** In this case, legal uncertainty may jeopardise private ventures, as schemes that have not been promptly developed may be replaced by delegated acts, leading to wasted investments and resources for companies. This is especially relevant when considering the demanding timeline for developing FDSS, as the tight schedule might deter private initiative from the very beginning.

4.3. Ensuring fair compensation

Another key aspect introduced by FIDA is the **compensation that data users should pay to data holders for making data available**. This represents an improvement compared to the PSD2, as it constitutes an incentive for entities to participate in the open finance model. However, to provide the right stimulus to the market, it is of utmost importance that the compensation system is designed with the aim to strike a balance between ensuring fair competition and guaranteeing an adequate source of income for data holders. Indeed, compensation for data holders should consider costs directly related to making the data available to the data users and the investments in the collection and production of data. Therefore, **AMICE advocates specifying that the compensation for data holders should include a reasonable margin**, in alignment with the policy approach adopted by the Data Act (Article 9). This provision, combined with the model for maximum compensation in Article 11(h), would ensure that financial institutions are adequately compensated for their investments, without inhibiting the emergence of a data economy.

AMICE expresses concern about the exemption granted to micro, small and medium enterprises, which allows them to avoid paying compensation beyond the direct costs incurred by data holders

when sharing the information with data users. Specifically, it is worth noting that larger corporations could potentially exploit this provision by setting up *ad-hoc* companies to take advantage of the exception. As a result, some institutions may be able to access customer data at a lower price through the mere establishment of a FISP, leading to an unlevel playing field in the market. For this reason, **we request that this exemption will be applied only to micro and small enterprises**, to avoid regulatory gimmicks that threaten market integrity, while at the same time promoting a competitive environment for smaller entities. In any case, given the sensitivity of pricing discussions within FDSS and their possible implications on competition rules, AMICE welcomes the possibility to advance discussions with the Commission (*i.e.*, DG COMP) to assess potential risks and ways to move forward.

AMICE urges the co-legislators to clarify that **the compensation for data holders should include a reasonable margin, beyond the mere coverage of the direct costs** associated with making the data available to data users, as well as the investments incurred in the collection and production of data. At the same time, AMICE argues that only micro and small enterprises acting as a data user should be subject to a capped compensation that is limited to the costs incurred in providing access to data.

4.4. Ensuring data accuracy

We acknowledge that the proposed FIDA regulation values an industry-led approach entitling the market participants to determine within the FDSS “the contractual liability of its members, including in case the data is inaccurate, or of inadequate quality, or data security is compromised or the data are misused”.

Nonetheless, the proposal does not clarify which entity bears the responsibility for providing erroneous financial information to customers, which may occur in case of data manipulation following a cyber incident or due to inaccurate information provided by the customers themselves.

In order to ensure legal certainty, AMICE recommends guidance on the allocation of responsibilities between data users and data holders in case of inaccurate information provided to customers by data users.

4.5. Ensuring consistency and avoiding fragmentation

AMICE supports FIDA’s approach opting for an industry-led standardization process. FIDA leaves indeed the FDSS members to develop common standards and to create technical interfaces to be used for the sharing of data (Article 10(1)(g)).

However, with this respect we deem important to draw the attention of co-legislators on the following aspects.

First, we suggest confirming that the standards to be defined in data sharing schemes refers to the “generally recognized standards” according to which the data holders will have to make the data available to the data user at the request of the customer (Article 5(3)(a)). The proposal indeed refers to a “format based on generally recognized standards” that the data holder should use to make the data available, without further specifying them and/or identifying any horizontal principle or value according to which they should be developed.

Furthermore, while appreciating the fact that FIDA does not mandate specific technical standards or interfaces, thus allowing to leverage existing international and European standards, we call to introduce appropriate measures to avoid fragmentation between multiple sharing schemes and to ensure consistency across the relevant contractual liability regimes. A possible solution would be

providing certain essential requirements to facilitate interoperability of data, data sharing mechanisms and services that operators should consider in the standardization processes within the different FDSSs.

AMICE asks firstly to clarify whether the common standards for customer data and interfaces concerning data that are subject to mandatory access are those to be developed by market operators within FDSS. In addition, AMICE asks to provide for key essential requirements to be taken into account during the development of such standards, in order to ensure consistency and avoid fragmentation between different financial data sharing schemes.

5. Conclusions

AMICE supports the FIDA objectives of promoting competition and innovation in the financial sector, while empowering customers' control over their data. Nevertheless, certain provisions of the proposed Regulation should be amended to not hinder the achievement of the said policy objectives.

To this end, AMICE urges the co-legislators to consider the concerns expressed above and to further amend the Commission's proposal accordingly. In particular, we strongly recommend the following:

1. Better clarify the categories of customer data that are suitable for sharing under the FIDA framework (Article 2(1)). AMICE recommends explicitly **excluding special categories of data, such as health-related data** (GDPR, Article 9) **and provident, statutory and medical liability insurance products** from the scope of the Regulation;
2. Involve stakeholders' representatives in the development of the data use perimeters' guidelines, with the aim of providing **for a flexible and proportionate framework** that shall not adversely impact innovation and competition;
3. Clarify the **concept of "permission"** according to FIDA and its interplay with "consent" under GDPR;
4. Provide for **reinforced customer identification mechanisms** (such as SCA or eIDAS) and advanced encryption standards to mitigate the risks of privacy infringements and potential fraudulent activities;
5. **Introduce an explicit reciprocity clause with gatekeepers within FIDA**, aligned with the provisions of the Digital Markets Act, with the aim not only to bolster competition and innovation within the financial sector but also to significantly enhance consumer control over their data;
6. **Prevent the risk of demutualization and excessive product standardisation.** Mutualisation protects the most at-risk populations and if these mechanisms disappear, the premiums of many policyholders may rise sharply, and some will no longer be able to get insurance.
7. Strengthen **trade secrets protection**, either providing or cross-referencing safeguards similar to those embedded by the Data Act within the FIDA. To this end, the legislative text should exclude from the FIDA's scope **enriched or inferred data that goes beyond mere raw data**. In addition, for the sake of legal certainty, data accuracy and liability, **data provided by third parties** (e.g., purchased from a third party) **should also be excluded from the scope of FIDA**;
8. Extend the proposed **timeline for the implementation of the FIDA** - which is too ambitious and challenging - up to 36 months and correspondingly postpone to 24-months the timeframe for developing FDSS. Furthermore, a longer timeline for implementation should be granted to allow digitalisation of data sets related to physical assets pertaining to non-life insurance policies.
9. Clarify that the **compensation for data holders should include a reasonable margin, beyond the mere coverage of the direct costs** associated with making the data available to data users, as well as the **investments incurred** in the collection and production of data;
10. Clarify the **allocation of responsibilities between data users and data holders** in case of inaccurate information provided to customers by data users;
11. Clarify that the **"generally recognised standards"** to be adopted for allowing data access are those to be developed by market operators within FDSS and provide for key essential requirements to be taken into account during the development of such standards, in order to ensure consistency and avoid fragmentation between different sharing schemes.