Mastercard's recommendations on FIDA for trilogue negotiations

Mastercard supports the creation of a framework that drives innovation, empowers customers to access their financial data and fosters competition in the financial sector. These elements are key to the future of the EU's financial landscape.

Please find below our recommendations to achieve a successful framework which are in line with the objectives to speed up, simplify and improve EU laws to drive better results. We encourage co-legislators to include these provisions as they work to finalize its text.

Executive Summary

1. **Refine the definition of 'customer data'. 'Customer data' should be limited to raw data and explicitly exclude derived or enriched data**, aligning with the proposals from the Council and the Parliament. We also strongly endorse the Council's proposed amendments to protect against reverse engineering practices that would stifle innovation.

2. **Enable responsible data use through GDPR alignment.** The text should **clarify that all legal grounds provided under GDPR can be relied on** and that **data can be used for purposes such as fraud prevention** in accordance with the GDPR. In addition, the text should allow greater flexibility for data users in terms of **intra-group and third-party data sharing**. Such transfers are necessary to offer secure and safe digital services and should be permitted, provided they align with the protections outlined in the GDPR.

3. **Clarify the roles of data users and data holders.** We **support clarifying the roles of data users and data holders** to ensure legal certainty. The final text should reflect the Parliament's position that data users do not automatically become data holders upon receiving customer data. In addition, we suggest that AIS data (not just AISPs) is excluded from the data holder definition to ensure consistency.

4. **Ensure that FIDA and PSR terminology is consistent.** We welcome proposals to **align the legal basis** ('permission' instead of 'explicit consent') **and dashboard requirements between FIDA and PSR.**

5. **Standardize the development of Financial Data Sharing Schemes to facilitate data sharing in the market.** We support proposals that favor a market-driven approach to developing the schemes and their compensation mechanism. Schemes should not be limited to specific data types, industries of geographies. Finally, we also suggest a clear distinction between scheme and technical standards, to maximize interoperability and efficiency.

1. Refine the definition of 'customer data'

We support the Council and Parliament's amendments to the definition of customer data in Recital 9, which clarify that FIDA's scope is limited to 'raw data' and derived and enriched data are out of scope. We propose clarifying Recital 9 as follows:

> Recital 9: The data included in the scope of this Regulation ***only refers to raw data that occurs as a result of normal course of business between data holders and their customers. It should not include confidential business data or trade secrets, nor data derived, inferred or enriched by the data holder or other intermediaries in the data flow. It*** should demonstrate high value added for financial innovation as well as low financial exclusion risk for consumers."

These clarifications are essential to ensure a level playing field and encourage organizations to continue to invest in innovation.

We also welcome the Council's amendment to this recital to protect organizations against reverse engineering practices and help prevent organizations from replicating and profiting from another organization's unique, innovative solutions. Without such safeguards, organizations may be discouraged from participating in FIDA due to the risk of their proprietary technology or processes being easily replicated and their investments undermined.

To ensure consistency and legal certainty, we recommend this definition is also replicated in Article 3 (3) as follows:

> "Article 3 (3): 'customer data' means ***raw*** personal and non-personal data ***in digital form*** that is collected, stored and otherwise processed by a financial institution as part of their normal course of business with customers which covers both data provided by a customer and data generated as a result of customer interaction with the financial institution. ***It does not include confidential business data or trade secrets, nor data derived, inferred or enriched by the data holder.***"

2. Enable responsible data use through GDPR alignment

The new FIDA framework must function seamlessly alongside the GDPR (Regulation (EU) 2016/679), which already set a high standard for data protection while encouraging effective data use. This means leaving the GDPR to regulate the use of personal data unless there is a clear policy reason for including additional or more restrictive language. Ensuring this alignment with GDPR will help ensure a coherent legal framework for data sharing, drive the innovation agenda and will also help reduce regulatory burden, in line with the objectives of the Commission's simplification agenda.

We support the Council's proposed amendments to Recital 48 that clarify that all legal grounds provided in the GDPR remain available. This protects personal data to accepted EU standards, while also not unduly hindering the use of the data. To ensure the key objectives of this legislation are met in practice, we strongly recommend the co-legislators to also incorporate this clarification in Article 6 FIDA as follows:

> "Article 6 (2): A data user shall only access customer data made available under Article 5(1) for the purposes and under the conditions for which the customer has granted its permission ***and where it has a valid legal basis under Regulation (EU) 2016/679***. A data

user shall delete customer data when it is no longer necessary for the purposes for which the permission has been granted by a customer."

This is something that the European Data Protection Board (EDPB) has also recognized as an issue.[1] Not including the above would overlook the reality that processing activities involve multiple operations relying on different lawful bases, such as legitimate interest. Introducing restrictions that go beyond GDPR would significantly limit FIDA accomplishing its objectives to give consumers more control and provide innovative products and services. **Importantly, the accumulation of different (and sometimes contradictory) rules at different levels would increase complexity and challenges in the implementation of the file.**

We see some of these restrictions in Article 6 (4)(a), where data users can process customer data only for the service explicitly requested by the customer. This restriction would impede processing for important purposes, such as product improvement (e.g. state of the art fraud technologies), even when such processing takes place in accordance with GDPR. Introducing such restrictions beyond those established by GDPR could stifle innovation, ultimately limiting benefits to consumers and the European market. Therefore, we recommend the following:

> **"**Article 6 (4a): Obligations on a data user receiving customer data.
>
> (4a) not process any customer data for purposes other than for performing the service ~~explicitly~~ requested by the customer ***or as permitted by Regulation 2016/679***"

In addition, the proposal restricts data users from sharing customer data within the same group of companies. Restricting intra-group data access as proposed in Article 6 (4)(f) conflicts with the technological and operational reality of data flows and data security needs of today and could lead to vulnerabilities in fraud detection activities.

In practice, different financial entities within the same group are involved in the same processing activities or provide complementary services, including for essential purposes, such as fraud prevention and threat intelligence.

Prohibiting such data sharing would disrupt customer experience (as data users would not be able to leverage the best tools/solutions regardless of location) and the development of services that benefit consumers (e.g., fraud prevention, troubleshooting, 24/7 customer support). If the intention of Article 6 (4)(f) is to appropriately protect personal data, this is already achieved via the robust transfer safeguards under the GDPR. We propose amending Article 6 (4)(f) to clarify that intra-group data sharing should be governed by the existing controls under GDPR:

> **"**Article 6 (4) (f): Where the data user is part of a group of companies, customer data listed in Article 2(1) shall only be ~~accessed and~~ processed by ~~the entity~~ ***other entities*** of the group ~~that acts as a data user~~ ***in line with the protections provided under Regulation 2016/679***."

We are also concerned about the proposed Parliament text (Recital 10 and Article 4 (aa)) and Council text (Article 6 (4) (h)) that would prohibit transfers to 'any third party'. Digital services often need to rely on expert third party providers to function (e.g., to ensure cybersecurity), who already are in compliance with the high standards of the GDPR and other legislation, such as the Digital Operational Resilience Act. This prohibition would hinder the development and functioning of

[1] Statement 2/2024 on the financial data access and payments package, May 2024 edpb_statement_20230523_financialdatapaymentpackage_en.pdf (europa.eu)

competitive, effective and consumer friendly financial services. We recommend deleting Article 6 (4) (h), or amending it as follows:

> "Article 6 (4) (h): ~~not~~ transfer customer data to any third party ***in accordance with Regulation (EU) 2016/679.***"

Achieving FIDA's objectives to promote customer choice and enable responsible innovation will be challenging when fraud prevention activities may be restricted by the data use obligations mentioned above.

3. Clarify the roles of data holders and data users

By definition, all data users will access customer data. If the trigger to becoming a data holder was accessing customer data as such, every data user would also need to take on the responsibilities of a data holder (e.g., dashboard requirements). This would cause confusion and would impede the effectiveness of FIDA.

Therefore, we support the Parliament's language in Recital 17 to specify that a data user that is a FISP should not become a data holder by virtue of accessing or receiving data from a data holder. However, we recommend that the final text should not only refer to 'FISPs', but to 'data users' in general, so that all financial institutions would equally benefit from this provision.

We also recommend this to be explicitly recognised in Article 3 (6) in the definition of 'data user', to avoid confusion and ensure a level playing field.

> "Article 3 (6): 'Data user' means any of the entities listed in Article 2(2) who, following the permission of a customer, has lawful access to customer data listed in Article 2(1). ***A data user does not become a data holder by virtue of accessing or otherwise receiving customer data from a data holder.***"

In addition, we suggest explicitly **excluding account information service (AIS) data** from the definition of data holders in Article 3 (5). Although AIS providers (AISPs) are in principle excluded from the scope of data holders, it is unclear whether this exclusion applies to AISPs that hold additional licenses for services beyond AIS – which in turn could result in reducing competition and innovation in the market. We recommend amending the text as follows:

> "Article 3 (5): 'Data holder' means a financial institution ~~other than an account information service provider~~ that collects, stores ~~and~~ ***or*** otherwise processes the data listed in Article 2(1)***, except when that data is collected, stored, or otherwise processed as part of the provision of an account information service as referred to in Article 4(16) of Directive (EU) 2015/2366***;"

Finally, we support the Parliament's amendment in **Recital 12** to explicitly exclude payment account data regulated in PSD2 from the scope of FIDA. This will help delineate which regime applies to which data sets, providing more legal certainty to data holders and data users.

4. Ensure that FIDA and PSR terminology is consistent

We support the introduction of dashboards which can provide customers with greater control over their data sharing permissions. However, in order to achieve the most effective, user-friendly dashboards, requirements in FIDA should be fully aligned with PSR. This would also help with the objectives of the regulatory simplification agenda.

First, we would like further alignment in Article 8 of FIDA and Article 43 of PSR. The provision to allow customers to re-establish previously withdrawn permissions in article 8 (2) (c) needs to be simplified, as it could create challenges in the consumer journey if the legal conditions for access have changed. We would recommend removing this provision, in line with the Parliament's text. Making this change would also align with the Parliament's position to remove this condition in Article 43 of PSR.

"Article 8 (2) (c): ~~allow the customer to re-establish any permission withdrawn~~;"

Second, data users should remain solely and fully responsible for obtaining permissions.

Requiring data holders to prompt consumers to confirm that permission was granted to a data user, as proposed by the Council in Article 5(3)(c), would be burdensome and confusing to consumers. Only consumers can grant or revoke permissions and having data holders restrict access after a permission is granted undermines consumer control and data user accountability. This would also conflict with the current PSD2 requirements, where the ASPSP is not responsible for verifying permissions.[2]

Finally, one significant improvement in the proposal is the use of the term 'permission' to replace the notion of 'explicit consent' in PSD2, as well as of 'necessary for the performance of a contract.' The use of 'explicit consent' has been the subject of confusion resulting in the need for the EDPB to opine on it[3].[4]

The use of a contractual 'permission' will ensure that 'explicit consent' is no longer mistaken for a GDPR consent, providing more legal certainty for both businesses and consumers. For the sake of consistency, we would recommend this approach is kept in the PSR text.

5. Standardize the development of Financial Data Sharing Schemes to facilitate data sharing in the market

We support amendments by the Council and Parliament that favour a market-driven approach and give flexibility on the development of standards. In particular, we would be supportive of the Parliament's addition in Article 10 (1) (ga) and the Council's addition in Article 10 (1) (k) to clarify that schemes will include minimum technical and organisational measures, that scheme members will then implement to ensure the right levels of security for the exchanged data.

We believe that market-driven creation of standards will encourage innovation and scalability. Whilst we welcome the direction of the Council, we believe standardization should happen at two different levels: **scheme standards** (focused on ecosystem governance, roles, obligations, liabilities, problem management, performance, reporting etc.) and **technical industry standards** (focused on technical data, API and security standards and supplementary guidelines such as for User Experience). Technical industry standards should be formed through collaboration in a non-competitive manner, striving for cross-financial sector technical interoperability. Scheme standards should be formed in the commercial competitive space to

[2] See the Single Rulebook Q&A at the EBA: https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2018_4309

[3] In particular, the EDPB clarifies that *'In terms of the GDPR, the legal basis for the processing of personal data is Article 6(1)(b) of the GDPR, meaning that the processing is necessary for the performance of the contract to which the data subject is party.'*

[4] EDPB, Letter regarding the PSD2 Directive, available at: https://edpb.europa.eu/news/news/2018/letter-regarding-psd2-directive_en

encourage a fair balance of value-exchange, innovation and ecosystem protection. The current text does not differentiate between these two levels, which could constrain optimal evolution and growth of the financial data ecosystem. We would recommend making this distinction clearer, for example in Recital 28, focusing on the creating of interoperable technical standards where they do not already exist in collaboration with industry. This will help maximize the chances of global interoperability and reduce the risk of duplication – in line with the regulatory simplification agenda.

> Recital 28: "Data holders and data users should be allowed to use existing market - ***driven*** standards when developing common ***technical*** standards for mandatory data sharing. ***Common technical standards are a set of specifications that apply to both customer data and technical interfaces to enable access to data in scope by electronic means, to be created in collaboration with industry, to ensure interoperability for financial data access and leveraging existing standards where possible."***

We would also recommend making this distinction clearer in Recital 25. Whilst we do agree with the Council's addition that '*scheme members are allowed to use existing market standards'*, we think the language proposed in this Recital could inadvertently introduce technical interoperability issues between schemes. This is because the text does not separate technical industry standards. We recommend making this distinction in Recital 25 to ensure efficient data sharing.

In order to facilitate the establishment and development of appropriate industry standards, we would be supportive of creating a market-driven consultative forum to share best practice.

Regarding scope, we think the schemes should **not be limited to specific data types, industries or geographies.** Doing so would limit participation and therefore innovation, and would diminish scale and the overall value in areas such as fraud prevention, performance, etc. An example of these limitations can be seen in the Council's Recital 26, where *'it is expected that the number of schemes will be limited'*; and guidelines will be developed to determine the '*significant proportion of the market',* which should *'aim to represent at least 25% of customers for the given product in the given geographical market'*. In our view, the composition of the schemes should be determined by the scheme participants and their own approach to governance.

The focus of the schemes should be on enabling cross-border, cross-sectoral use cases that would work in a commercially viable manner and can expand in scope over time. This would also help build interoperability across financial sub-sectors and would enable the delivery of seamless experiences and enablement of innovative cross sectoral use cases, encouraging and reinforcing consumer adoption.

Regarding **compensation**, we support the direction of the European Parliament's text, recognising there should be sufficient incentives to foster market adoption and effective competition.

We believe the best way to create the right incentives is to create a baseline, minimum compensation model for data access that will allow value-based business models to emerge. As it stands, the cost-based approach under FIDA could lead to disparities in the market due to differing cost bases among data holders and would risk discriminating against smaller providers.

Instead, we would recommend leaving the development of scheme compensation models to market participants, in a way that can create opportunities for further investment and growth.

We suggest making the following amendments to Recital 29 and Article 10 (1) (h):

> Recital 29: "To ensure that data holders have an interest in providing high quality interfaces for making data available to data users, data holders should be able to request reasonable compensation from data users for putting in place ***those interfaces*** ~~application programming interfaces~~. Facilitating data access against compensation would ensure a fair distribution of the related costs between data holders and data users in the data value chain. In cases where the data user is an SME, proportionality for smaller market participants should be ensured ~~by limiting compensation strictly to the costs incurred for facilitating data access~~. The model for determining the level of ***baseline*** compensation should be ***left to the financial data sharing schemes. Where additional value-adding services emerge, fees above the minimum can be agreed.*** ~~defined as part of the financial data sharing schemes as provided in this Regulation."~~
>
> "Article 10 (1) (h): a financial data sharing scheme shall establish a model to determine ~~the maximum~~ ***appropriate*** compensation that a data holder is entitled to charge for making data available through an appropriate technical interface for data sharing with data users in line with the common standards developed under point (g). The model shall be based on ~~the following p~~principles ***such as*** ~~including~~ (…)"

Finally, Article 10(1)(e) cites a requirement that the scheme should "*include a mechanism through which its rules can be amended, following an impact analysis and the agreement of the majority of each community of data holders and data users respectively*". We also note that Recital 26 requires that the Schemes "*should not afford its members the possibility of preventing, restricting or distorting competition*".

We recommend that policymakers review point (e) to consider if this construct would amount to an association of undertakings within the meaning of Article 101(1) of the TFEU, as any decision of an association of undertakings in that context may be subject to scrutiny under **competition law**. Such concerns – if not addressed in the regulation – could potentially be seen by financial institutions as obstacles for setting up and participating in schemes under FIDA. **Further, we recommend that rules amendment mechanisms should be determined by the Schemes as part of a formal Scheme governance process.**