23 February 2024

FSUG Opinion on Open Finance

1. Introduction

The European Commission proposal for an Open Finance Regulation (FIDA) aims to extend the sharing of a wide range of financial customer data, which will consequently enable the delivery of financial products and services more tailored to customers' needs (both consumers and firms).

In this respect it is indeed important to note that, *inter alia*, FIDA applies to certain types of "customers data" which is a broader notion compared to that of "personal data" under the GDPR, which refers only to information relating to natural person ("data subject").

While the access of third-party providers to customer payment accounts is already regulated in the context of the of Open Banking under the Payments Services Directive (PSD2), the proposed Open Finance Regulation widens the types of consumer financial data that can be accessed and processed and the conditions thereof. This includes new data sources, such as savings accounts, insurance policies, mortgages, investments, and pensions to be accessed by financial and non-financial entities subject to the customer's permission. Although Open Finance can boost competition and be an enabler for financial markets, the proposal must be improved regarding consumer protection to reduce the risk of mis-selling, unfair commercial practices, exclusion and discrimination and in general for fundamental rights of consumers.

2. What financial data can be accessed?

The scope of the FIDA proposal covers a wide range of consumer financial data, notably accounts, payments and transactions of mortgages and loans, savings accounts and investment products, occupational and personal pension products, non-life insurance products and data related to the creditworthiness assessment of firms.

At the same time, data on the creditworthiness assessment of natural persons and data on life, health and sickness insurance products are excluded from the scope of the proposal, due to the very high risks of exclusion and discrimination their inclusion would create for consumers.

While the FSUG supports this policy choice, the data categories that are in the scope of the proposal are still quite broad including highly sensitive personal data that is financially irrelevant and might create risks of exclusion, discrimination, and in general have a severe impact on the fundamental rights of consumers. For example, as highlighted in the Opinion of the European Data Protection Supervisor (EDPS) on the Open Finance proposal[1], pension rights, which are in the scope of article 2(1), might include retirement benefits "in the form of payments on death, disability, or cessation of

[1] Opinion 38/2023 on the Proposal for a Regulation on a framework for Financial Data Access, https://edps.europa.eu/system/files/2023-08/2023-0730_d2425_opinion_en.pdf

employment or in the form of support payments or services in case of sickness, indigence or death",[2] which can be very revealing for consumers' health for instance. Therefore, the FSUG supports a more staggered approach according to whicgateh categories of data in scope of the FIDA regulation should be further circumscribed, so that only financially relevant data is covered, and narrowed down, in line with the precautionary principle. Moreover, data resulting from profiling activities should be explicitly out of scope due to its very high exclusion risk for consumers.

3. Data use perimeters

The proposal rightly acknowledges that excluding certain categories of sensitive data from the scope of the Regulation would not suffice to protect individuals' rights and interests and ensure that financial personal data is used in a proper and ethical manner.

Therefore, the concept of "data use perimeters" is introduced in article 7 of the FIDA proposal to ensure that the use of consumers' data will not lead to mis-selling, financial exclusion or discriminatory and unfair commercial practices (e.g. unfair discriminatory pricing). This is crucial as it would be the main safeguard for consumers against the misuse of their personal data.

According to article 7(2), the EBA is asked to develop guidelines on how data in the scope of the regulation will be used to assess the creditworthiness of the consumer, while EIOPA is asked to develop guidelines relating to financial data use for the risk assessment and pricing in the case of life, health and sickness insurance products, in cooperation with the European Data Protection Board (EDPB).

The introduction of data use perimeters is welcomed. However, the FSUG considers that guidelines are not the appropriate legal instrument to be used in this context considering their non-binding legal nature and the high negative impacts data misuse would have for consumers if these perimeters are not in place and duly complied with. For that purpose, FSUG proposes that data use perimeters should instead be introduced in the form of Regulatory Technical Standards (RTSs) developed by the competent European Supervisory Authorities (ESAs) and subject to a formal approval by the EDPB. In addition, and to ensure the highest level of legal certainty, the Regulation should positively define a minimum set of principles in the level 1 text that will be the starting point of the RTSs.

Moreover, in line with Opinion 38/2023 of the EDPS, the legislator should require that the EBA and EIOPA, in coordination with the EDPB, introduce restrictions to combining "customer" data obtained pursuant to the Open Finance proposal with other types of "personal data". This is important since several data combinations may be unlawful and/or present heightened risks for consumers. This could be the case for personal data obtained from third-party sources, such as social media or data brokers, data obtained via tracking technologies such as cookies as well as data obtained by data users under the Data Act.

[2] Article 6(4) of the IORP II Directive

In addition, to ensure that consumers are sufficiently protected, data use perimeter rules should also cover more services. In the case of article 7(2) of the FIDA, this should be expanded to cover additional retail banking services, such as mortgage credit agreements and payment services. Excluding those services from the scope of this provision would significantly fragment and lower consumer protection. Insofar as article 7(3) is concerned, non-life insurance products such as motor and home insurance should be covered as well. As confirmed by recent findings[3] data misuse in the provision of these types of non-life insurance products can lead to discriminatory commercial practices such as unfair discriminatory pricing. In addition, without robust data use perimeter rules for non-life insurance products, Open Finance creates a high exclusion risk for vulnerable consumers. Since its establishment, the insurance business model has been built on 'solidarity' or 'risk pooling'. This business model allows potentially vulnerable consumers with higher risk profiles to still be able to afford insurance (be 'insurable') as the risk is spread out collectively between policyholders. The proliferation of access to consumer data under Open Finance, however, could endanger this business model as the easy accessibility of large amounts of personal data will allow highly granular personalised risk assessments, which can lead to certain vulnerable consumers becoming financially excluded (denied insurance coverage or being faced with prohibitively high insurance premiums).

In addition, to effectively ensure the reduction of inequalities, the data use perimeters relating to insurance should extend the "right to be forgotten" for cancer survivors under the new Consumer Credit Directive (CCD2) article 14(4)[4] to insurance policies not related to credit and cover also chronic diseases. This will be in line with Europe's Cancer Beating Plan,[5] the European Parliament's 2020/2267(INI) motion for a resolution,[6] and national legislation of multiple Member States, such as Spain and the Netherlands. Moreover, data perimeters must also touch upon the use of AI tools in those sectors and set out a minimum set of rules for their deployment.

Finally, data use perimeter rules should also cover other essential financial services products, namely personal pension products and retail investment products.

4. Interplay with data and consumer protection legislation

The proposal states in the recitals that the GDPR is applicable insofar as personal data is being processed. While FSUG very much welcomes that, the proposal should be without prejudice to the EU data and consumer protection legislative framework at large, notably the Unfair Commercial Practices Directive, the Unfair Contract Terms Directive and the Consumer Rights Directive (as it has recently incorporated the rules on distance marketing of financial services).

---

[3] https://www.fca.org.uk/publications/market-studies/ms18-1-general-insurance-pricing-practices-market-study

[4] It is therein provided that "Member States shall require that personal data concerning consumers' diagnoses of oncological diseases are not used for the purpose of an insurance policy related to a credit agreement after a period of time determined by the Member States, not exceeding 15 years following the end of the consumers' medical treatment".

[5] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/promoting-our-european-way-life/european-health-union/cancer-plan-europe_en.

[6] European Parliament 2020/2267(INI), Strengthening Europe in the fight against cancer - towards a comprehensive and coordinated strategy, article 125 accessiblehere:https://www.europarl.europa.eu/doceo/document/TA-9-2022-0038_EN.html.

This also relates to sectoral legislation on financial services, such as the Consumer Credit Directive and the Mortgage Credit Directive, which lay down specific rules on the categories of data to be processed with regards to creditworthiness assessments.

5. Permission vs. GDPR legal bases for processing personal data

The FIDA proposal provides that customer data shall be made available from a "data holder" to a "data user" only where the customer has granted their permission, and for the purposes this permission relates to.[7] To allow customers to manage their permissions and have effective control over their data, data holders shall provide customers with a permission dashboard,[8] displaying the permissions granted, including "when personal data are shared based on consent or are necessary for the performance of a contract".[9] In that sense, besides obtaining permission by a customer, data users need to comply with their obligations under article 6 of the GDPR and obtain a legal basis for processing personal data.[10]

This provision could, however, be misinterpreted and understood as any legal basis for processing under the GDPR, which is not the case. Moreover, when the processing of personal data is based on consent, customers have the right to "withdraw his or her consent at any time, as provided in the Regulation (EU) 2016/679".[11]

To ensure that there is no ambiguity as to the legal bases necessary for processing personal data under the GDPR and the word "permission", the FSUG recommends clarifying this in the final text of the Regulation.

In addition, there is a need for the regulation to explicitly prohibit the denial of financial services, from providers listed in article 2(2) of the proposed regulation, to consumers who do not avail themselves of the permission dashboard or otherwise enable data sharing under the proposal. This is important to protect, for example, consumers with lower digital literacy levels, the denial of services to whom would be unfair and discriminatory.

6. Dashboard Design

It is also important to ensure that consumers are aware of what they give their permission for and that they are made aware of how to access and use permission dashboards. Consumers must know exactly what they are giving their permission for and that their rights under the Open Finance regulation and the GDPR apply. This information should be provided to consumers in a clear and understandable manner and language.

---

[7] Open Finance Regulation Proposal, article 5(1).
[8] *Idem,* Article 8(1).
[9] *Idem,* Recital 22.
[10] *Idem,* Recital 10 & 48.
[11] *Idem,* Recital 10.

Moreover, as consumers will have to provide their permission, regardless of whether data will be shared under the "consent" or "necessity to perform a contract" legal basis, it is crucial that the minimum requirements to obtain valid consent are always applicable when obtaining permission as well.

This will ensure that the permission obtained is meaningful and not just a tick-the-box exercise, allowing consumers to effectively manage which data they want to share with whom and for what purpose. It is also essential that the dashboard design is subject to the GDPR principle of data protection by design and by default and is compliant with consumer law, notably the Unfair Commercial Practices Directive. This means, for example, that dashboards should be well-designed in an harmonised manner across providers, so as not to encourage or unduly influence the customer to grant or withdraw permissions through pre-ticked boxes or other practices such as dark patterns. Without such safeguards, there is a risk that market participants may try to influence consumers' decisions regarding this matter out of purely commercial interests.

7. Governance of Financial Data Sharing Schemes (FDSS)

The proposal foresees the creation of Financial Data Sharing Schemes (FDSS), between data holders, data users and consumers. These schemes will essentially operate as "open finance ecosystems", allowing data holders and users to voluntarily join multiple schemes, whose content and governance are decided by the members of the scheme itself "with each side having equal representation in the internal decision-making process".

Article 10(1)(e) foresees that the rules of the scheme can be amended subject to "the agreement of the majority of each community of data holders and data users respectively". This includes transparency and reporting to members' obligations, governance rules and applicable data and technical interface standards, leaving room for self-regulation, creating legal uncertainty as to the content and the governance of the schemes. Customer organisations and consumer associations, however, are excluded from participating in the amendment process while FSUG considers that instead they should have the right to participate in amending the rules of a financial data sharing scheme.

8. Enforcement of data protection legislation & cooperation between competent authorities

To ensure the effective enforcement of the EU data protection legal framework in the products covered by the Regulation, the proposal should clarify the remit and powers of competent authorities involved. For that purpose, the proposal should include explicit references to the Data Protection Authorities under the GDPR, in articles 10(6), 14(1), 18(3).

Finally, to effectively enforce the EU data protection legal framework, competent authorities under the Open Finance Proposal should be able to withdraw the authorisation granted to Financial Information Service Providers (FISPs), insofar as Data Protection Authorities have established that a FISP breached its obligations under Data Protection Law.

9. Penalties

The penalties foreseen in case of consumers' rights infringement under the Open Finance framework must be strong enough to ensure that the interests of individuals are respected and safeguarded. Given the strong negative consequences consumers face if the rules proposed under Open Finance are breached, it is important that strong penalty provisions are in place to deter data holders and users from breaching the rules laid down by the framework. Therefore, we propose to align penalties for infringing the Open Finance Regulation with those foreseen in the Payment Services Regulation Proposal for Open Banking, which are considerably higher.[12]

[12] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on payment services in the internal market and amending Regulation (EU) No 1093/2010.