Finance Watch

Making finance serve society

Ensuring Consumer Protection in the Financial Data Access (FIDA) Regulation

Robust regulatory safeguards for responsible data use and governance

A Finance Watch Position Paper

December 2024

Finance Watch

Introduction

The open finance framework in the EU, also known as the Financial Data Access (FIDA) Regulation, is approaching the final stage in the ordinary legislative process. As the co-legislators negotiate the final legislative text, it is imperative that the right safeguards are embedded in the Regulation to protect consumers from the considerable risks that open finance brings, such as financial exclusion, mis-selling and data protection/privacy risks.

Both the European Parliament and Council positions adopted at the end of 2024 provide important improvements to the European Commission proposal from June 2023 in key areas, such as the data perimeter rules and safeguards for gatekeepers. This position paper provides recommendations on which positions the co-legislators should adopt in the final legislative text to make sure that FIDA is safe and beneficial for consumers.

Key Takeaways

1. **Legally-binding data use perimeter rules (Article 7) that cover all essential financial services are needed**
   To prevent data misuse that can result in financial exclusion, mis-selling, and data protection/privacy risks, legally-binding data use perimeter rules are needed that cover loans, mortgages, life and non-life insurance, and retail investment products.

2. **There is a need for strong supervisory scrutiny of gatekeepers and their subsidiaries acting as data users, with a legally-binding role for the ESAs**
   The rules must make clear that gatekeepers and their subsidiaries can only access FIDA data if they can demonstrate an ability to comply with the special rules for gatekeepers. In addition, the European Supervisory Authorities (ESAs) should have a binding role in the assessment of these entities' eligibility to access FIDA data.

3. **Governance of data sharing schemes should include comprehensive supervisory reviews and a strong role for the ESAs**
   To ensure consumer protection, competent authorities need to be tasked with carrying out comprehensive reviews of the schemes' arrangements. In addition, the ESAs need a strong supervisory role to ensure an equal level of protection for consumers across the EU.

4. **Strong rules are needed to protect consumers from undue influence when granting data access**
   Strong rules are needed to prevent the use of dark patterns to influence consumers' decisions to grant or withdraw data sharing access.

5. **Strong penalties rules are needed to dissuade infringements**
   Given the considerable negative implications of FIDA rules infringements for consumers, strong penalties provisions are needed to dissuade data users and holders from breaching the rules. These rules should be aligned with the open banking penalties provisions.

I. Legally-binding data use perimeter rules (Article 7) that cover all essential financial services are needed

The Financial Data Access (FIDA) Regulation will enable financial services providers to access large amounts of consumer data. This creates a risk of the wrong types of personal data being used for different possible use cases, such as creditworthiness assessments or risk assessments and pricing of insurance products. This risk of misuse of retail consumer data can lead to the mis-selling of financial services, resulting in financial detriment for consumers, such as over-indebtedness. Conversely, it can result in consumers being either unfairly excluded from certain products or services, or exposed to unfair and discriminatory commercial practices.

Therefore, it is crucial that there are strong and legally-binding data use perimeter rules for all essential retail financial services in the final legislative text of FIDA. Essential financial services include personal loans and mortgages, all types of insurance products as well as retail investment products (including pensions).

Finance Watch welcomes that the co-legislators have recognised the need for the data use perimeter rules to cover all of these essential financial services in their respective proposals. However, to ensure that the data use perimeter rules are adhered to, instead of mandating the European Supervisory Authorities (ESAs) to draw up guidelines for their implementation, it is crucial that the ESAs are mandated to draw up legally-binding Regulatory Technical Standards (RTS) for this. The ineffectiveness of guidelines alone in this context is backed by evidence in two Finance Watch studies on malpractices in the EU consumer credit market.[1] These studies show that the already existing EBA Guidelines on Loan Origination and Monitoring, which include guidelines on creditworthiness assessments (CWAs), have not been effective in preventing the misuse of data irrelevant for CWAs.

The European Parliament (EP) text recognises this, and therefore rightly proposes the introduction of RTSs for the data use perimeter rules for all insurance products and credit products, which should be adopted in the final legislative text.

In addition, the final legislative text should also introduce RTSs for suitability and appropriateness assessments for retail investment products, even though disappointingly, only guidelines are foreseen in both the EP and Council texts for these products. Retail investment products can be very risky and therefore the absence of data use perimeter rules to prevent the mis-selling of these instruments can result in huge financial detriment for the consumer. This can diminish trust in capital markets among retail investors. In turn, it may also undermine retail participation in capital markets, which is essential for advancing the Savings and Investment Union (SIU) – a top priority of the mandate 2024-2029.

[1] Finance Watch, *Consumer credit market malpractices uncovered*, 2021, see pages 18-19 and Finance Watch, *Tackling causes of over-indebtedness in the EU consumer credit market*, 2022, see pages 20-22.

The EP proposal under Article 7(3a), which stipulates that the RTSs for the data use perimeter rules for insurance should address the 'right to be forgotten' of survivors of cancer or other chronic diseases and mental conditions, should also be included in the final legislative text. Studies show that many cancer survivors face exclusion with regards to insurance because of their medical histories, although they have been cured for many years, even decades.[2] Despite this, only eight EU Member States have currently implemented a 'right to be forgotten' for cancer survivors in legislation, and the number of years survivors must wait to enjoy this right varies. A rule introducing the right to be forgotten has been introduced for credit-related insurance policies in the new Consumer Credit Directive (CCD)[3] and similar rules are needed in other EU consumer financial services legislation.

Moreover, it is imperative that the proposal under Article 7(4c) of the EP text is adopted in the final legislative text. This proposal would ensure enforcement of the data use perimeter rules by mandating the ESAs to undertake regular comprehensive reviews of data users' compliance with the rules, including thorough and documented assessments of the data processed in the provision of financial services.

II. There is a need for strong supervisory scrutiny of gatekeepers and their subsidiaries acting as data users, with a legally-binding role for the ESAs

Large BigTechs (firms such as Meta, Alphabet or Amazon), also known as 'gatekeepers' under the Digital Markets Act (DMA),[4] accessing and processing FIDA data, either directly or through subsidiaries, poses considerable consumer risks. Through their commercial activities, gatekeepers have collected huge amounts of financially irrelevant data on consumers, such as social media data. There is a risk that these entities could combine FIDA data with the financially irrelevant data they have accumulated from other sources. In turn, this can lead not only to financial exclusion risks but also to an uneven-level playing field between gatekeepers and traditional providers of financial services.

Therefore, Finance Watch welcomes that both co-legislators have included in their respective proposals regulatory safeguards to mitigate the risks stemming from gatekeepers and their subsidiaries accessing FIDA data. However, to be effective, the final legislative text must ensure that these measures are sufficiently robust and watertight.

For one, adequate regulatory measures must be in place to address the risks stemming from gatekeepers or their subsidiaries that are financial services providers and therefore data users. In this area, the EP position has a number of gaps in comparison to the Council position. Unlike the Council position, the regulatory safeguards in the EP position in Article

[2] Journal of Cancer Policy, *A right to be forgotten for cancer survivors: A legal development expected to reflect the medical progress in the fight against cancer*, Volume 25, September 2020.
[3] Official Journal of the EU, *Directive (EU) 2023/2225 on credit agreements for consumers*, 2023.
[4] Official Journal of the EU, *Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector*, 2022.

18a only apply to entities which are owned or controlled by a gatekeeper, and not directly to gatekeepers acting as data users themselves. While gatekeepers currently mostly use subsidiaries to provide financial services, rules are needed that are future proof in case gatekeepers become direct providers of financial services.[5] Therefore the Council position that introduces restrictions and special supervisory scrutiny measures for both gatekeepers and their subsidiaries acting as data users should be adopted in the final legislative text.

In addition, it is key that the final legislative text explicitly stipulates that until a competent authority has completed an assessment and made a decision as to whether a gatekeeper, or an entity owned or controlled by a gatekeeper, has sufficient measures in place to meet the FIDA requirements for gatekeepers, it is prohibited from providing services as a data user. While such a provision is foreseen in the Council text in Article 18b(1ii), it is not in the EP text. Therefore the Council position on this point should be adopted.

Furthermore, the EP text in Article 18a(5) states that if an entity owned or controlled by a gatekeeper fails to take measures to address deficiencies identified by competent authorities in meeting the FIDA safeguards, the competent authority ***may*** determine that the entity is excluded from the scope of the Regulation. The Council text, on the other hand, is more robust in this regard and should be adopted instead as it prohibits any gatekeepers, or entities owned or controlled by a gatekeeper, that fail to take measures to fulfil the FIDA requirements for gatekeepers from accessing FIDA data in Article 18b(5)(ii):

If measures are not taken within the set deadline, or are deemed insufficient by the competent authority to fulfil the requirements under paragraph 2, the competent authority shall, within 30 working days, issue a corresponding decision to prohibit the assessed entity as referred to in paragraph 1 from providing services as a data user under this regulation [...].

Lastly, there is a need for a strong and binding role of the ESAs in the assessment of whether a gatekeeper, or an entity owned or controlled by a gatekeeper, should be granted access to FIDA data as a data user. This is crucial to prevent regulatory arbitrage and ensure that there is an equal level of protection for all consumers across the EU. Therefore, the European Parliament proposal, which foresees the ESAs providing a binding opinion on the assessment in Article 18a(4), should be adopted instead of the Council position, which only foresees a non-binding opinion of the ESAs.

III. Governance of data sharing schemes should include comprehensive supervisory reviews and a strong role for the ESAs

FIDA introduces the concept of data sharing schemes (Articles 9 and 10), which is designed to bring together data holders, data users and data subjects (customers) to facilitate the exchange of data in a transparent and properly supervised setting.

[5] For example, see Finanzwende, *MORE MONEY, MORE POWER: BIG TECHS IN FINANCE*, June 2024.

Finance Watch

Competent authorities need to be tasked with a comprehensive review of the schemes' arrangements that is not limited solely to a formalistic, "box-ticking" exercise of the criteria set out in Article 10(1). Rather, the review should also assess whether the scheme's arrangements appear appropriate and credible for the purposes of ensuring the responsible treatment of customer data. After all, the effectiveness of the proposed schemes, as well as consumer trust in FIDA, hinges on the strength and credibility of the schemes' underlying governance arrangements, including their mechanism of financial compensation to consumers for any loss of data, damage or fraud suffered.

Therefore, it is crucial that Article 10(6) of the EP proposal is incorporated into the final legislative text as it mandates regular comprehensive supervisory reviews of data access schemes' governance arrangements:

Article 10(6): ***The ESAs shall undertake regular comprehensive reviews of data access schemes' governance arrangements set out in Article 10(1). Those reviews shall include a thorough and documented assessment whether the schemes' arrangements are appropriate and credible for the purposes of ensuring the responsible treatment of customer data.***

Moreover, there is a need for the final legislative text to provide the ESAs with a strong supervisory role to ensure that there is uniform supervision of the FIDA rules across the Union. The EP text provides the ESAs with such a strong role, granting them direct supervisory powers with regards to data sharing schemes and, as mentioned in the previous section, a legally-binding role in the supervisory scrutiny of gatekeepers seeking access to FIDA data. This is important to ensure an equal level of protection of consumers across the EU, and to prevent regulatory arbitrage. In addition, many data users are likely to operate cross-border and therefore EU-level supervision of the data sharing schemes they are part of will be key.

IV. Strong rules are needed to protect consumers from undue influence when granting data access

It is crucial that strong safeguards are in place to ensure that consumers' decisions to grant data access to market participants acting as data users are not influenced by the data user. Otherwise, there is a risk that market participants may try to influence consumers to make decisions on this matter in a way that serves their commercial interests best.

Therefore, it is key that there are regulatory technical standards on the implementation of the design of data access requests to prevent dark patterns (behavioural nudges). The EP position, unlike the Council position, mandates the ESAs to draft RTSs on the design of data access requests under Article 6(2c) and this proposal should be included in the final legislative text. However, to ensure legal certainty the wording '***The ESAs may jointly***

develop draft regulatory technical standards…' should be reworded to make the mandate explicit by replacing ***may*** with ***shall***.

In addition, it is important that the financial data access permission dashboard provided to the consumer by the data holder to manage the granting and withdrawal of data access is designed in a way that does not influence the decision of the consumer to grant or withdraw any data sharing permissions. Both the EP and Council texts mandate the drafting of guidelines to ensure this, which is to be welcomed. However, the EP text is more explicit with regards to the scope of these guidelines, specifying that the dashboard should be designed in a way that does not:

- encourage or unduly influence the customer to grant or withdraw permissions, including through the use of dark patterns or pre-ticked boxes;
- deceive or manipulate the customer, or otherwise materially distort or impair the ability of the customer to make free and informed decisions;
- make the procedure to withdraw permission more difficult than the procedure to grant access.

To ensure that all of these crucial points are covered in the guidelines, the more detailed EP proposal should be adopted in the final legislative text.

Moreover, the final legislative text should include the EP proposal under Article 8(4)(iiia), which requires data users to inform data holders about i) the legal basis under Article 6(1) of the General Data Protection Regulation (GDPR) and ii), if applicable, the exception under Article 9(2) GDPR that they would rely on to access personal data contained in the customer dataset. This would help prevent data holders from granting access to personal data in the absence of an appropriate GDPR legal basis.

V. Strong penalties rules are needed to dissuade infringements

Consumers are exposed to significant risks if the rules under FIDA are breached. These implications can range from being unfairly denied a desperately needed financial service to being mis-sold an unsuitable or unaffordable financial service, which can lead to financial detriment. Therefore, it is important that strong penalties provisions are in place to deter data holders and users from breaching the rules laid down by the framework.

Given that the risks and negative implications stemming from rules breaches for consumers are the same for both open banking and open finance, the penalties provisions of the two frameworks should be aligned. The Council text foresees an alignment in Article 20 while the Commission and EP proposals include penalties provisions that are weaker than those set out in the Payment Services Regulation (PSR 1) for open banking. Therefore, the Council position on this key issue should be adopted in the final legislative text.

Conclusion

The upcoming trilogues on the Financial Data Access (FIDA) Regulation are an important milestone in the digital finance agenda of the EU. Without the right safeguards in place, FIDA can bring considerable risks to consumers such as financial exclusion, financial detriment stemming from mis-selling of financial services, and data protection/privacy risks.

It is absolutely crucial that the co-legislators introduce robust safeguards in the final legislative text. These safeguards must: prevent data misuse in the provision of all essential financial services/products; mitigate the risks posed by gatekeepers; ensure comprehensive and thorough supervision of the rules; and strengthen the role of the ESAs. As the economy, including the financial sector, becomes increasingly digitalised, increased data sharing must be used as a force for good. It must not result in consumer detriment, which would undermine trust not only in the FIDA framework but in the financial sector in general.

Author(s)

Peter Norwood, Senior Research & Advocacy Officer at Finance Watch

Contact

peter.norwood@finance-watch.org,
+32 28 99 04 35

Finance Watch has received funding from the European Union to implement its work programme. There is no implied endorsement by the EU or the European Commission of Finance Watch's work, which remains the sole responsibility of Finance Watch.

Co-funded by the European Union