# FiDA: is the EU prepared to move from Open Banking to Open Finance?

Explainer

*Judith Arnal and Fredrik Andersson*

## Introduction

The digital transformation is an unstoppable process and data is at its core. Data-driven innovation can bring enormous benefits to the public sector, companies and citizens. Still, the right conditions in terms of connectivity, processing and data storage, computing power, cybersecurity and adequate governance structures for handling the data need to be in place to grasp the full potential of the digital economy. Significant progress has been made in the EU. At cross-sectoral level, the General Data Protection Regulation (GDPR) in 2016 was followed by the Regulation on the Free Flow of Non-Personal data (FFD) in 2018, the Cybersecurity Act (CSA) and the Open Data Directive in 2019. In 2020, the European Commission tabled a European Strategy for Data, building on recently passed cross-sectoral regulations like the Data Governance Act and the Data Act.

But on top of trying to put in place the conditions at cross-sectoral level to unleash the power of data, the EU has also adopted a sector-specific dimension – and finance is a case in point here. One of the first steps was the Payment Services Directive 2 (PSD2), approved in 2015, which established Open Banking, giving third party providers (TPPs) access to payment accounts and leading to the creation of Account Information Service Providers (AISPs) and Payment Initiation Service Providers (PISPs).

Moreover, data-driven finance was identified as one of the priorities of the 2020 Digital Finance Package and as a follow up, on 28 June 2023, the European Commission tabled the Financial Data Access and Payments Package, comprising an amendment to PSD2 (which would become PSD3), a Payment Services Regulation (PSR), as well as a legislative proposal for financial data access (known as the FiDA Regulation).

With PSD3/PSR, the Commission intends to improve some of the shortcomings that have not allowed Open Banking to take off in the EU (according to the Commission, Open Banking was only used by 5 % of customers in 2021) and to move further by introducing Open Finance with FiDA. This would imply the possibility of sharing much more data, like data on loans, savings, investments, pensions, and non-life insurance products, in real time and continuously, of course with consumer consent. If the set-up proposed by the Commission goes forward as proposed, Open Banking would be regulated under PSD3/PSR and Open Finance under FiDA but under very different conditions.

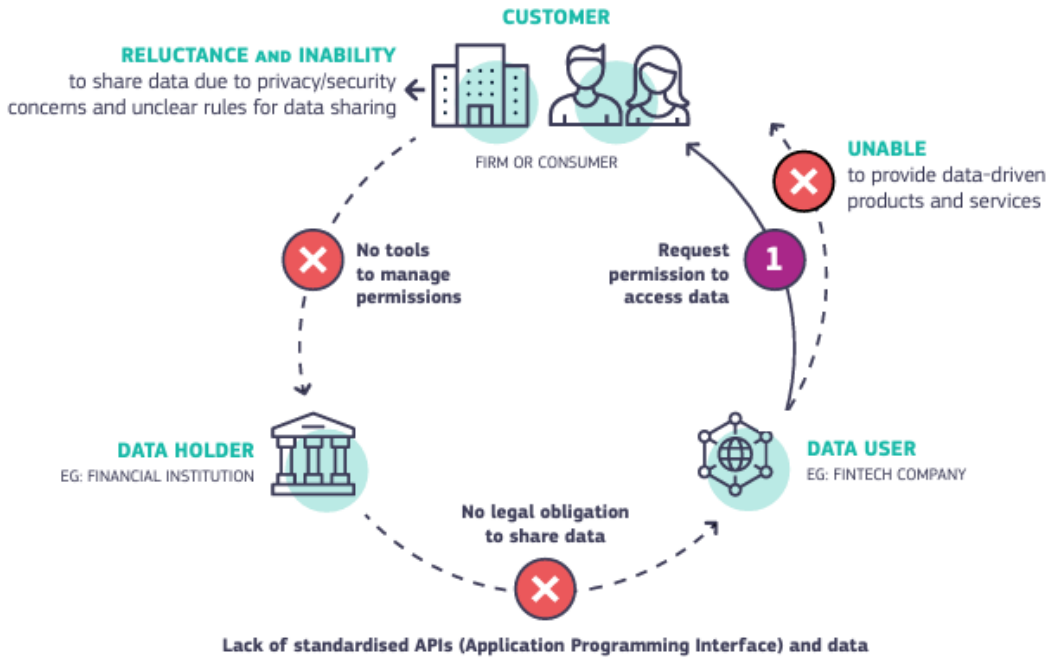
This ECRI Explainer aims to understand the rationale behind the FiDA proposal and its main features, as well as assessing the Commission's original proposal and its expected interaction with other pieces of legislation. In short, is the EU really and finally prepared to move from Open Banking to Open Finance?

## The rationale behind FiDA

Data is all over finance – they are present in payments, loans, investments and insurance services, among others, impacting many essential areas of daily life. But as showcased by the Commission when presenting their FiDA proposal in June 2023, customers (either an individual consumer or a firm) currently face two challenges. First, they are reluctant to share their data, because of a lack in understanding on how secure the data is and for who will be getting access. According to the Commission, customers do not have access to tools that would allow them to control or view the personal (but financially relevant) data they have shared. The second challenge lies squarely with the financial institution holding the data. The data sharing obligations are currently vague, giving them a degree of flexibility in how the data is shared. Uneven data sharing creates a unlevel playing field. The repercussion of unevenly sharing data falls on data users, such as fintech companies. Under the current circumstances, they might not always be given the necessary access for them to offer new, innovative solutions to customers.

A Commission public consultation on financial data access highlighted a lack of trust over privacy, data protection and digital security as consumers' main concerns. Nevertheless, the Bank for International Settlements conducted a US study in 2021 to understand consumers' trust in data holders, giving grades to different types of data holders. What the study showed was that while important to further increase trust, traditional financial institutions were the most trusted data holders, more so than government agencies.

***Figure 1. Issues in financial data flows***




Source: European Commission

The proposal's objective is to tackle these challenges. It would do so by giving customers more control over their data, namely to manage, view and grant access to data. Secondly, it would standardise how data is shared. Finally, it would make it easier for data users to request access from data holders, allowing users to offer new products and services to their customers.

Multiple reasons are behind the limited access to data. There is currently a lack of tools and rules defining how users can manage the financial data that they share. Unclear procedures on how data is collected, stored and shared have numerous consequences on how consumers approach digital financial services. Without widespread trust in how data is managed by financial players, the uptake of different services struggles to gain traction and the quality of services is hampered by customers' reluctance to share data. Existing regulatory frameworks are not clear on when customers are required or should share their financial data to get access to relevant services.

Furthermore, the interests of data holders and users can sometimes diverge. There is currently no standardised technical infrastructure. This is a costly challenge for data users as they have to adapt their data extraction to each data base.

## What is in the proposal?

The Financial Data Access framework is a proposal to define the rights and obligations so as to manage how customer data - other than payment accounts data – is shared in the financial sector. Under PSD2, sharing payment account data was regulated. With FiDA, the Commission is going one step further by regulating how all types of financial data are shared – and how they are controlled.

Six building blocks, as explained in more detail below, make up the FiDA proposal, namely: (1) types of data, (2) data holders, (3) data users, (4) permission dashboards, (5) compensation and (6) financial data sharing schemes.

### Types of data

The Commission proposes that FiDA would apply to the following categories of customer data: (1) mortgage credit agreements, loans and accounts, with the exception of payment accounts including data on balance, conditions and transactions; (2) savings, investments in financial instruments, insurance-based investment products, crypto-assets, real estate and other related financial assets; (3) pension rights in occupational pension schemes and on the provision of pan-European personal pension products; (4) non-life insurance products, with the exception of sickness and health insurance products; and (5) data which forms part of a firm's creditworthiness assessment collected as part of a loan application process or a request for a credit rating. Aligned with the increase in control, the regulation also specifically states in Recitals 9 and 19 that it would exclude health-related data and consumers' creditworthiness data (but business data is included in the regulation).

### Data holders

Data holders are (1) credit institutions, (2) electronic money institutions, (3) investment firms, (4) crypto-asset service providers, (5) issuers of asset-referenced tokens, (6) managers of alternative investment funds, (7) management companies of undertakings for collective investment in transferable securities, (8) insurance and reinsurance undertakings, (9) insurance intermediaries and ancillary insurance intermediaries, (10) institutions for occupational retirement provision, (11) credit rating agencies, (12) crowdfunding service providers and (13) pan-European Personal Pension Product (PEPP) providers.

Upon request, financial institutions will be obliged to make customers' data available to data users requesting access to data based on customers' consent. The customer data would be made available to the data user without undue delay, continuously and in real time. Data holders will be allowed to claim compensation from a data user for making customer data available only if the customer data is made available in accordance with the rules and modalities of a financial data sharing scheme.

When making customers' data available, data holders must: (1) request data users to demonstrate that they have obtained the customer's permission to access their data held by the data holder; (2) make customer data available to the data user in a format based on generally recognised standards and at least to the same quality that they have; (3) ensuring an appropriate level of security for the processing and transmission of customer data to the data user; (4) provide the customer with a permission dashboard to monitor and manage permissions; and (5) respect the confidentiality of trade secrets and intellectual property rights when accessing customer data.

**Data users - the creation of FISPs**

Only financial institutions and Financial Information Service Providers (FISPs) can be data users, i.e. can have access to customers' data. FISPs are a new type of regulated entity introduced by FiDA and they will have to comply with a number of requirements to be authorised. On substance, FISPs need to be incorporated in the EU or designated, in writing, to a legal or natural person as their legal representative in one of the EU Member States where the FISP intends to access financial data. From an operational viewpoint, proper governance and internal control mechanisms must be established, complying with business continuity, digital operational resilience, outsourcing and incident reporting requirements.

Financially, FISPs need to hold professional indemnity insurance covering the territories where they access data or some other comparable guarantee, covering their liability resulting from fraudulent/non-authorised data access. Alternatively, FISPs can hold initial capital of EUR 50 000 that can be replaced by professional indemnity insurance or another comparable guarantee after it begins its operations. FISPs will benefit from the so-called EU Passport, having access to customers' data from other Member States, following a simple notification procedure. The European Banking Authority will create and maintain a registry of all authorised FISPs, including information on those that are operating based on the EU Passport.

Data users would only be allowed to access customer data for the purpose and under the conditions that they were initially granted permission. Customers can withdraw their permission at any point. The processing of personal data would be limited to what is strictly necessary to provide the financial service. When the data user is part of a group of companies, customer data would only be accessed and processed by the entity within the group that acts as a data user.

Data users would need to adopt a number of safeguards, namely: (1) putting in place adequate technical, legal and organisational measures to prevent the transfer of or access to non-personal customer data that is unlawful under EU law or a Member State's national law; (2) taking the necessary measures to ensure an appropriate security level for the storage, processing and transmission of customer data; (3) deleting customer data when it is no longer relevant to the original permission granted by the customer; and (4) preventing the transfer of customer data to third parties where no legal basis exists.

**Permission dashboards**

Data holders would be required to provide customers with a dashboard to monitor and manage the permissions a customer has provided to data users. The permission dashboards would: (1) provide the

customer with an overview of each ongoing permission given to data users; (2) allow the customer to withdraw their permission previously given to a data user; (3) allow the customer to re-establish any withdrawn permission; and (4) include a record of permissions that have been withdrawn or have expired for a duration of two years. Moreover, the data holder would ensure that the permission dashboard is easy to find on its user interface and that the information displayed on the dashboard is clear, accurate and easily understandable. The data holder and the data user given permission by a customer would cooperate with each other to make information available to the customer via the dashboard in real-time. A data user would then inform the data holder of any new permission granted by a customer regarding their data held by that data holder.

### Compensation

An important point for industry that is being introduced by the Commission under Article 5 of FiDA is the possibility for data holders to seek compensation for making customer data available in a standardised form. For Open Banking under PSD2, this is not possible. Allowing for appropriate compensation would provide the incentives to develop and maintain high quality application programming interfaces (APIs). This supports a level playing field, opens up new avenues for innovation and helps to cover data holders' data management costs.

### Financial data sharing schemes

Within 18 months from the entry into force, data holders and data users would become members of a financial data sharing scheme governing access to the customer data. It would work as a sort of industry self-governing body, whose main aim would be to bring data holders, data users and consumer organisations together to foster the development of common data sharing and industry recognised interface standards, as well as a joint standardised contractual framework governing access to specific datasets.

Financial data sharing schemes would, among other things: (1) define the common standards for the data and the technical interfaces to allow customers to request data sharing; (2) establish a model to determine the maximum compensation that a data holder is entitled to charge for making data available through an appropriate technical interface; (3) determine the contractual liability of its members, including if the data is inaccurate or of inadequate quality; and (4) provide an independent, impartial, transparent and effective dispute resolution system to resolve membership issues and disputes among scheme members.

If a financial data sharing scheme is not developed for one or more categories of customer data and there is no realistic prospect of such a scheme being set up within a reasonable time period, the Commission would be empowered to adopt a delegated act to supplement the regulation by specifying the modalities through which a data holder would make customer data available.

### Implementation period

The proposal will become applicable 24 months after the entry into force while articles referring to financial data sharing schemes, authorising FISPs and legal representatives will apply 18 months after the entry into force.

## Our assessment of the proposal

### The scope of 'customer data'

As Commissioner McGuinness put it, 'what FiDA is proposing is to oblige data holders to share and make customer data available to data user'. While this sounds like a good idea on paper, it is also a statement that raises questions. The term 'customer data' is broad, and it creates uncertainty about what data will be used and how safe data access is guaranteed. The Commission's possible intention is for the private sector to spell out in their data sharing schemes what the term 'customer data' specifically means. Nevertheless, leaving such a definition to the private sector could take self-regulation too far in a very sensitive issue and, ultimately, if the private sector is not able to agree, it would still be up to the Commission to define them.

### Should debtors decide what information to share?

The current credit eco system is based on a three party collaboration. The banks acting as creditor, the debtor (i.e. the customer in need of credit) and the credit data base in-between. Under current legislation, creditors are allowed to access relevant financial customer data upon request on a basis of legitimacy. It implies that if the creditor has a legitimate reason to perform a verification of the debtor, then they are able to receive the data necessary for a creditworthiness assessment.

The current FiDA proposal introduces a new type of data sharing philosophy, which even if it puts the consumer in control of their data, could also jeopardise the current credit system. First, allowing individuals with a limited understanding of the importance of sharing financial data between financial actors can lead to a deterioration in data quality. Second, a consumer is likely to be unwilling to share data that negatively impacts their profile, so-called *bad data*. Removing bad data from the equation would result in lower data quality, with negative impacts on the consumer and ultimately on general access to credit and financial stability. The consumer profile developed would be less accurate, thus resulting in creditors taking on more risk. The way for creditors to compensate for increased risks would be to increase their interest rates, increasing the cost for all consumers. Therefore, consumers' right to only share positive data and keep '*bad data*' for themselves should be curtailed.

### Should gatekeepers be allowed to obtain a FISP licence?

A first element to consider is whether gatekeepers (popularly known as 'Bigtechs') under the Digital Markets Act (DMA) should be able to obtain a FISP licence, allowing them to enter the European financial services market in a far more wide-ranging way. A second worrying element is the potential lack of reciprocity in data sharing with the same firms, with gatekeepers potentially accessing the data but not being required to share that data with financial entities. The FiDA proposal contains relevant safeguards here. For instance, only licenced entities would be able to access the data and they would be prohibited from sharing the data within their group. Furthermore, practical experience with Open Banking under PSD2 indicates this has not been particularly problematic.

Finally, the DMA has helped improve the level-playing field between gatekeeper platforms and financial services providers who, based on a customer's request, would be able to access the relevant customer data held by these large technology providers to offer new financial services to businesses and consumers.

### Big Bang or use-case approach?

FiDA would be a Big Bang in terms of how data is shared in the financial sector. Even if there are compensation mechanisms, in contrast to Open Banking, the private sector would still need to make

major investments. In the context where the take-up of Open Banking has been very low, it is questionable that such a Big Bang approach is warranted. It would possibly make more sense to start with a use-case approach and based on how successful that is, decide later whether further steps are warranted.

If a Big Bang approach were to be followed, the implementation deadline would likely need to be extended beyond the one currently proposed, to give the private sector enough time to adapt, particularly to develop and implement the schemes and common interfaces required.

**Compensation costs should be monitored**

As stated above, the FiDA proposal will entail high costs for the private sector. Introducing compensation models for data holders is a good step forward to split the costs of setting up data sharing infrastructure and for maintaining and securing customer data. Nevertheless, it will be essential to monitor how compensation is requested as overly high data access costs could be destructive and hamper innovation.

**Co-existence of Open Banking and Open Finance?**

Although Open Banking and Open Finance share a similar philosophy, they differ on an important point – while Open Banking is based on a non-contractual right of access at no cost, with Open Finance, the FiDA proposal requires that data-holding entities and data-using entities reach contractual agreements for sharing financial data, where the data-holding entities can demand reasonable compensation for the costs of making the data available.

Open Banking will be regulated under PSR/PSD3 and Open Finance under FiDA. So, does it make sense to rely on different mechanisms and legal texts just because of the type of data shared (payment account data versus all other data) and considering that in many 'real life' situations (e.g. taking on a mortgage or a car loan) both kinds of data are intertwined and relevant when a customer is looking for a financial service?

In short, it does not seem to make sense. It seems, from a legal and practical viewpoint, that it would be easier to build Open Finance alongside Open Banking, but in the long run, this will probably complicate financial regulation and practices unnecessarily. That is why it would make more sense to consider merging Open Banking with Open Finance.

**In spite of room for improvement, the proposal has its merits…**

Credit access could be facilitated, potentially speeding up the process for retail customers to access financial services. The proposal could also increase the personalisation of products, which would also be a benefit. Increasing data firms' access would allow for products to be developed that would be better adapted to the specific need(s) of a firm or consumer.

The framework would also allow for new tools and new market players to offer solutions that give more clarity to customers over which data is shared but would also allow for new tools making access to financial services simpler and more transparent.

**… but adequate safeguards need to be in place**

Consumers could also be exposed to increased risks under the current proposal. If safeguards are not clearly defined then consumers' data can be exposed to misuse. It is also important to highlight that data that can be accessed and included in financial credit services is limited to only the relevant data. The excessive personalisation of data and products can cause consumers to be excluded from accessing certain services. Therefore both the data and the algorithms used must be properly controlled.

## The interplay with other legislation

Starting with the Digital Operational Resilience Act (DORA), both financial institutions and FISPs will be subject to new requirements on digital operational resilience and any data sharing infrastructure will have to adhere to the requirements of the internal compliance framework on digital operational resilience (e.g. ICT risk management, business continuity, incident reporting etc.). DORA's outsourcing requirements will also be applicable.

The processing of personal data will remain regulated by the GDPR, which financial institutions and FISPs must continue to comply with. As for the sharing of non-personal data, FiDA should be seen as complimentary to the horizontal framework introduced by the Data Act.

## Conclusions

The proposal is currently being negotiated and is likely to go through many more rounds of discussions. The timeline has been extended due to the European elections, temporarily halting the negotiating process.

While measures should be adopted to help fully grasp the benefits of data – including in the financial sector – some elements of the proposal need to be further reflected upon.

To start with, the concept of 'customer data' should be further clarified, making sure that it remains clear that the data derived from assessing consumers remains out of the proposal's scope. Besides, while good to give consumers control over their data, it should be clarified when 'deleted' data has to be 'forgotten' by the data holder. The control given to the consumer should not come at the expense of data quality, consumers' access to credit and overall financial stability. Here, restricting consumers' rights to only share positive data is essential.

Allowing gatekeepers or 'Bigtechs' to have a FISP licence does not appear problematic due to safeguards, past experience with Open Banking and the level playing field measures introduced under the DMA. When comparing it nevertheless remains important to remember that data was previously only shared with third parties without any reciprocity, thus creating a few entities that were able to monopolise data knowledge. We recommend a gradual, use-case approach to data sharing over a transformative Big Bang approach, allowing for adjustments based on the level of success.

If a Big Bang approach were to be followed, extending the implementation periods for the private sector and including relevant safeguards to mitigate identified risks should be considered. Merging the Open Banking and Open Finance frameworks could streamline both regulation and practices and foster innovation but could jeopardise third parties' business models based on open banking. Despite potential improvements in credit access and product personalisation, adequate safeguards are necessary to protect consumer data and ensure fair access to financial services.

Overall, it looks like the EU is now ready to move beyond Open Banking and embrace data sharing in fields other than payment accounts – but this should be done carefully to avoid any unnecessary distortions, especially in credit markets.

# European Credit Research Institute

The European Credit Research Institute (ECRI) is an independent, non-profit research institute that develops its expertise from an interdisciplinary team and networks of academic cooperation partners. It was founded in 1999 by a consortium of European banking and financial institutions. ECRI's operations and staff are managed by the Centre for European Policy Studies. ECRI provides in-depth analysis and insight into the structure, evolution, and regulation of retail financial services markets in Europe. Through its research activities, publications and conferences, ECRI keeps its members up to date on a variety of topics in the area of retail financial services at the European level, such as consumer credit and housing loans, credit reporting, consumer protection and electronic payments. ECRI also provides a venue for its members to participate in the EU level policy discussion.

For further information, visit the website: www.ecri.eu.

# Centre for European Policy Studies

CEPS is one of Europe's leading think tanks and forums for debate on EU affairs, with an exceptionally strong in-house research capacity and an extensive network of partner institutes throughout the world. As an organisation, CEPS is committed to carrying out state-of-the-art policy research that addresses the challenges facing Europe and maintaining high standards of academic excellence and unqualified independence and impartiality. It provides a forum for discussion among all stakeholders in the European policy process and works to build collaborative networks of researchers, policymakers and business representatives across Europe.

For further information, visit the website: www.ceps.eu.