KPMG
Law

FiDAR: Managing control & innovation in data-driven financial services

Introduction

On 28 June 2023, the European Commission published the proposal for the Third Payment Services Directive and Payment Services Regulation (**PSD3/PSR**). In parallel, the European Commission also published a proposed regulation for accessing financial data (**FiDAR**). These legislative proposals build on the existing open banking framework under the Second Payment Services Directive (Directive 2015/2366/EU) (**PSD2**), by empowering consumers to securely share their financial data with third parties and enable them to access a wider range of financial products and services. In terms of the implementation of FiDAR, all of the requirements will begin to apply after 24 months of the legislation being enacted, with some requirements applying 18 months after enactment.

Overview

The FiDAR proposal seeks to establish a framework to enable customers and firms to better control access to their financial data using tailored services based on relevant data, while mitigating the associated risks. The general objective is to promote digital transformation and encourage the adoption of data-driven business models in the EU financial sector. National competent authorities will also be empowered with investigatory and sanctioning powers, to investigate potential breaches of FiDAR and impose administrative penalties and other measures.

The proposal respects the existing data protection regime under the General Data Protection Regulation (Regulation 2016/679/EU) (**GDPR**) and fits into the European strategy for data, enabling data sharing within the financial sector. It reflects the focus of both the Data Governance Act (Regulation (EU) 2022/868) and the Digital Markets Act (Regulation (EU) 2022/1925) which seek to increase trust in data sharing by creating a framework for data intermediation providers. The FiDAR proposal also intends to support the EU retail investment strategy which has the objective of improving the functioning of the retail investor protection framework by providing safeguards in the use of retail investor data in financial services. Finally, FiDAR will promote and ensure compliance with the Digital Operational Resilience Act (Regulation (EU) 2022/2554) (**DORA**).

> it is hoped that an increase in access to high-quality financial services information will improve both the price and quality of services

Results from recent stakeholder consultations showed that the general public held concerns regarding data sharing, while professional stakeholders looked more favourably on the idea, although both groups expressed the need for proper safeguards. However, the evidence suggests that if properly designed, access to financial data could have positive economic and social impacts for both providers and recipients of financial services. In particular, it is hoped that an increase in access to high-quality financial services information will improve both the price and quality of services, for example through targeted savings and pensions based on a comprehensive overview of private and occupational pension entitlements. However, in order for these effects to be realised, there will be a need to protect against anti-competitive behaviour or collusion, as well as ensure that data holders do not unduly hamper competitors' ability to provide services through applying high fees for data access.

The FiDAR proposal also brings with it a significant potential impact on customers' fundamental rights, notably Articles 7 and 8 of the Treaty on the Functioning of the European Union concerning the right to respect for private life and the right to protection of personal data enshrined in the EU Charter on Fundamental Rights. This impact aims to be mitigated by the implementation of a high level of consumer protection and by ensuring that data sharing will only occur at the request of the customer. Customer understanding of any permission provided as well as full transparency will be critical in this regard.

In order to meet these objectives, the European Commission considered that the most favourable approach would be an EU Regulation that establishes a common EU framework for financial data access that includes the following characteristics:

- A requirement for market participants to provide customers with access to financial data permission dashboards, set eligibility rules on access to customer data and empower the European supervisory authorities (**ESAs**) to issue guidelines to protect consumers against unfair treatment or risks associated with exclusion.
- Mandate access to customer data sets across the financial sector subject to customer permission.
- A requirement that market participants develop common standards for customer data and interfaces concerning data subject to mandatory access.
- A requirement that data holders put in place application programming interfaces (**APIs**) without compensation, implementing the common standards for customer data and interfaces developed as part of schemes, and require scheme members to agree on contractual liability.

Obligations of Data Holders and Data Users under FiDAR

Article 3(5) defines a "data holder" as a financial institution which collects, stores and processes customer financial data as specified in the regulation. Customers can make a request under Article 4 to receive their financial data from the data holder "*without undue delay, free of charge, continuously and in real-time*."

Following a request from a customer the data holder will need to make the customer data available to the data user "in a format based on generally recognised standards" for the specific purposes permitted by the customer (Article 5).

Data holders will be required to provide financial data access permission dashboards to customers to enable them to monitor and manage their permissions given to data users. These permission dashboards will need to meet the requirements detailed in Article 8, including, for example, that the information on the permission dashboard is accurate, clear and easy to understand. Customers should be entitled to withdraw permission provided to a data user and re-establish this permission via the permission dashboard. It will therefore be necessary for the data holder and relevant data user to cooperate in making real-time information available to the customer on the permission dashboard.

Data users will include payment institutions, electronic money institutions, credit rating agencies and crypto-asset service providers. Data users will need to be authorised by a national competent authority as a financial institution or a financial information service provider (**FISP**) under Article 14 to access the customer financial data. Specific obligations are placed on data users when handling customer financial data, for example, customer data will need to be deleted when it is no longer necessary, cannot be processed for any purposes other than those specified by the customer, and cannot be processed for advertising purposes, except as permitted for direct marketing purposes under EU and national laws. Data holders will however be able to claim compensation for making customer data available to data users under Article 5(2).

In terms of cross-border information, FISPs and financial institutions will be allowed to have access to the data held by data holders established in the EEA, on both a freedom of services and freedom of establishment basis. A passporting-type notification is also provided for FISPs that want access to data for the first time in a Member State other than its home Member State.

For third country providers, it may be possible for these to obtain authorisation, but this will be subject to certain prerequisites and will require a designated legal representative in the EU. How the transfer of data within such third country entities will occur will also need to be considered carefully in light of international data transfer requirements under GDPR.

Breach of FiDAR

National competent authorities will have the power to investigate potential breaches of FiDAR and impose administrative penalties. The maximum administrative fine which may be imposed on a natural person will be €25,000 per infringement up to a total of €250,000 per year.

Any member of a FISP's management body or any natural person held responsible for an infringement may also be temporarily banned from exercising a management function in a FISP. The maximum administrative fine which may be imposed on a legal person is €50,000 per infringement up to a total of €500,000 per year, or up to 2% of the total annual turnover based on the most recent set of approved financial statements of the legal person, or the group of which the legal person is a member. There is also a Member State discretion for national competent authorities to impose additional administrative penalties on infringing persons. Where a person fails to remedy a breach, FiDAR also makes provision for potentially significant on-going periodic penalty payments to be imposed, with daily penalties of up to €30,000 for individuals, and up to 3% of the average daily turnover for legal persons.

EU Payment Services legislation

Currently data sharing obligations exist at an EU level in relation to payment accounts data; this is known as "open banking" and is set out in PSD2. FiDAR will greatly expand the scope of data sharing obligations to nearly all financial services data. Article 2(1) of FiDAR defines customer data as including data on mortgage credit agreements, investments in financial instruments, crypto-assets, pension rights in occupational pension schemes, savings and certain non-life insurance products.

FiDAR differs from PSD2 in that it does not provide data users with the ability to initiate transactions on behalf of customers (as is provided for payment initiation service providers (**PISPs**) under PSD2). Data users authorised as PISPs under PSD2 will however still able to initiate payments with customer consent. Another distinction is that unlike access provided by institutions to data to PISPs under open banking, under FiDAR data holders can claim compensation from data users for making the customer data available under Article 5(2) of FiDAR.

The proposed PSD3/PSR also seek to improve consumer rights, combat and reduce payment fraud by facilitating payment service providers to share information relating to fraud. These pieces of legislation will allow non-bank payment service providers access to all payment systems in the EU, along with appropriate safeguards, and aim to improve the functioning of open banking by giving customers greater control over their payment data and removing obstacles to offering open banking services, e.g. by PISPs. Together with the FiDAR proposal, these will represent a significant opening-up of customers' data, hopefully facilitating better products, services and accessibility for both customers and service providers.

Interaction with GDPR and DORA

Whilst the FiDAR proposal is generally welcome, there remains concern around the ability to share data between financial institutions and non-financial entities. It is worth noting that Article 6(4)(f) of FiDAR states that customer data must only be accessed and processed by the data user, even where the data user is part of a group. The interaction between this article and other laws, such as GDPR, is however still somewhat unclear. Where a customer requests a data holder to share their financial data with a data user, the explanatory memorandum to FiDAR still requires the request to comply with a valid legal basis for processing under GDPR where personal data is concerned. This will potentially complicated the transparency requirement under GDPR as well as making it difficult to communicate the precise scope of proposed processing to consumers.

The European Data Protection Supervisor (**EDPS**) has indicated in an Opinion on the FiDAR proposal (available here) that there is a need for clearer definitions in FiDAR, for instance, FiDAR refers to the term *"permission"*, but this is not defined in the regulation. The EDPS notes that "*permission*" should be distinguished from *"consent"* or *"explicit consent"* which is referenced in GDPR.

It is also worth emphasising that data holders and data users must comply with DORA obligations. When a FISP submits an application for authorisation to a national competent authority under Article 12 of FiDAR, a security policy document containing a detailed risk assessment of its operations will also need to be included as part of the application.

Conclusion

The introduction of FiDAR will provide customers with greater control over their financial data. The legislation focuses on transparency and aims to ensure that customers can trust open finance services, and should also facilitate the creation of tailored financial products and the ability for customers to compare financial products. FiDAR develops the data sharing protocols introduced by the PSD2 and aims to assist with progressing the digital transformation of the financial sector.

The interaction between FiDAR and GDPR will, however, still gives rise to some questions. Whilst organisations will need to have clear and workable data retention and data access policies in place, the precise nature, scope and interaction between the "permission" under FiDAR and "consent" under GDPR will need to be carefully considered. The divergence in language around "data holders", as opposed to "data controllers" or "data processors", also gives rise to additional complexity when considering and documenting legal and regulatory obligations. It will also be important to understand how FiDAR will interact with other regulatory obligations, including under PSD2 (and the upcoming PSD3) as well as under DORA. Financial institutions will therefore need to develop and incorporate a strategic and holistic approach to compliance with these various regimes.

How We Can Help

At KPMG, our deep expertise and multi-disciplinary offerings in data protection and financial services regulation positions us ideally to help you navigate these complexities. Our multi-disciplinary teams including consultants, accountants, and lawyers allow us to provide unparalleled service through a single provider.

We understand the nuances and are equipped to provide legal and strategic advice and practical solutions tailored to ensure your systems are compliant and optimised for the upcoming changes. We have an international panel of experts who are experienced in helping clients in this space. We can also assist with authorisations, as well as the implementation of policies, procedures and operational matters to ensure that firms are fully compliant with their legal and regulatory obligations.

For further discussion and to explore how we can assist your firm, please reach out to us. Let's discuss how KPMG can help you turn regulatory requirements into strategic advantages.

Queries? Get in Touch

Christopher Martin
Partner, Financial Services Regulation,
KPMG Law LLP Ireland
e:christopher.martin@kpmglaw.ie

Emma Ritchie
Director, Head of Data Protection & Privacy,
KPMG Law LLP Ireland,
e: emma.ritchie@kpmglaw.ie

Shane Carrick
Managaing Director,
Risk Consulting,
KPMG Ireland,
e: shane.carrick@kpmg.ie

Tom Hyland
Director,
Risk Consulting,
KPMG Ireland,
e: tom.hyland@kpmg.ie

kpmglaw.ie

Produced by: KPMG's Creative Services. Publication Date: November 2024. (10901)