Get your infrastructure ready for open finance

Navigating the challenges and seizing the opportunities in new EU and UK finance laws

TELEHOUSE

New EU and UK laws to mandate finance sector data-sharing, presenting significant challenges and lucrative opportunities if organisations have the right digital infrastructure

Open finance is the successor to open banking, which was step one. It's a movement that aims to give consumers and businesses more control over their financial data and to enable innovation in financial products and services. Fundamentally it will make life easier for both personal and corporate customers.

It is based on the idea that financial institutions should share their data with third-party providers through open APIs (application programming interfaces). This allows consumers and businesses to choose the financial products and services that are best for them, regardless of which provider they are with.

The **Framework for Financial Data Access (FFDA)** is the proposed European Union regulation that would implement open finance across the EU. It is based on the idea that financial institutions must share their data with third-party financial entities (where customers have explicitly consented to the sharing) through open APIs. The aim is for consumers and businesses to be targeted with more appropriate tailored financial products at more competitive prices. It will also likely lead to the creation of a new swathe of innovative financial products and services for consumers to benefit from and businesses to take advantage of.

The implementation of open finance is still in its early stages, but **it has the potential to revolutionise the finance industry**. By giving consumers and businesses more control over their financial data, open finance can enable innovation and competition, and lead to better finance products and services for everyone and increased competition. The challenge for the financial institutions is that it will inevitably put a strain on underlying digital infrastructure.

Wojciech Wiewiórowski, **European Data Protection Supervisor** notes that,

> *"Without clear boundaries, one could see higher prices for important financial services or the exclusion of customers with an unfavourable risk profile. Financial authorities and data protection authorities will need to cooperate closely to ensure that individuals and their fundamental rights are protected."*

UK regulators may also extend open finance to cover energy, utilities and telecoms once the current proposals are implemented and tested.

So, what will organisations need to do to prepare for its introduction?

Acceleration of digital transformation plans will be needed, and the spotlight will fall on potential improvements to current infrastructures, connectivity, data storage, security and management as a result.

What is the FFDA and how is the UK responding?

The FFDA proposal was published by the EU Commission in June 2023, and **it could be in force by the end of 2024/early 2025** with an 18-month grace period before compliance with the rules relating to financial data sharing schemes is required. Under the proposals, customers will be able to grant and withdraw permissions for their data to be accessed by eligible third parties.

The FFDA defines several key terms that organisations need to be aware of. A "data holder" is a party with an obligation to grant access to and share data. A "data user" is a licensed party with lawful access to customer data. The regulation differentiates between a "financial information service provider," which is authorised to access data in order to provide financial information services, and a "financial institution," which can be both a data holder and a data user.

Under the FFDA, data sharing is mandated. Upon request by a customer submitted electronically, the data holder must make the data available to the data user for the purposes for which the customer has granted permission.

> As long as the data user is authorised by competent authorities to access data held by data holders, this must be done without undue delay and in real-time.

Cross-border access to data is also addressed in the regulation. In practice, data will be shared through "financial data sharing schemes". **Data holders and data users must be members of one or more of these schemes** and abide by their rules.

Data holders will also be able to levy charges on data sharing, where applicable. Relevant schemes will determine the maximum charges that can be applied for making data available through a technical interface.

The other key proposals, as covered by global law firm Linklaters, are as follows:

- Customers of financial institutions must be able to use data access permission dashboards
- Common standards for sharing access to specific data categories must be developed by financial institutions
- Financial institutions must join schemes that govern financial data sharing
- Members of such schemes must agree contractual liability
- Financial institutions can charge for making data available
- Eligibility only extends to financial institutions (FISPs) and financial information service providers to access and process customer data
- FISPs must comply with the EU's digital operational resilience act (DORA), the EU's rules around digital operational resilience, requiring an ICT risk management framework and testing against disruption

The regulation applies to the following types of data: **mortgages, credit agreements, loans, accounts, savings, investments in financial instruments, insurance-based investment products, crypto-assets, real estate, and other related financial assets**. It also includes pension rights in occupational pension schemes and European personal pension products, as well as the provision of non-life products. Data that is part of the creditworthiness assessment of a firm is also included.

A review after four years will decide whether more data needs to be brought under the scope of the regulation, if any changes in contractual practices of data users and holders are needed and whether any other entities should be given data access.

The response from the UK

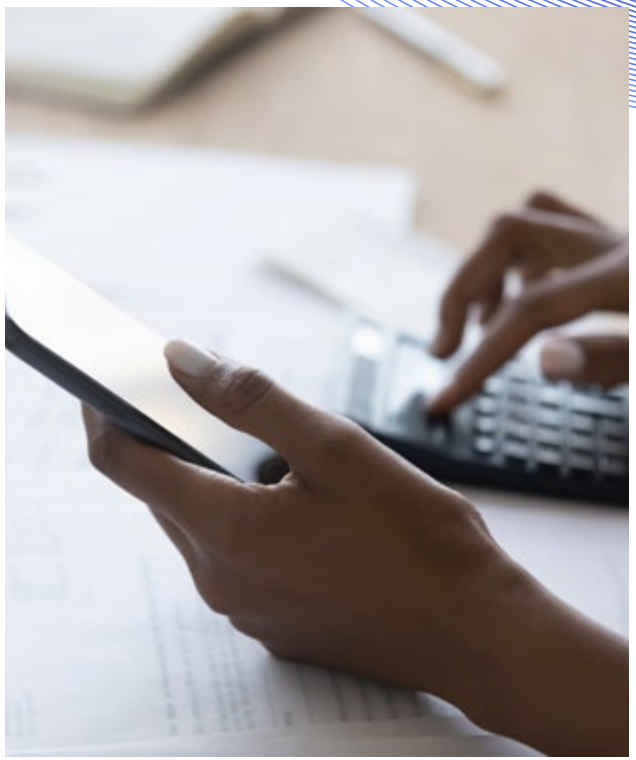
The FFDA development is being closely monitored in the UK amid efforts to build a 'smart data' framework, which is enabled by the Data Protection and Digital Information (No. 2) Bill. **This Bill** is currently making its way through parliament. In November 2023 the UK Government **tabled an amendment** to the bill, which will allow regulators to create a Smart Data Scheme for financial services and provide for the secure and consented sharing of customer data with authorised third-party providers.

> *"Design of the UK frameworks is being guided by a 'Smart Data Council', which looks to transpose the approach and success of the UK's open banking measures to other sectors, such as energy, which enables greater sharing of data to benefit customers. techUK are a member of this Council and I recently had the pleasure of joining the meeting to help shape the direction and approach with insight from the FS sector,"*
>
> Andy Thornley, Head of Financial Services, TechUK.

This body also comprises key government departments, regulators, industry bodies and consumer groups, including representatives from Citizen's Advice and Innovate Finance, which represents UK Fintechs. Innovate Finance's aim is for open finance to keep the UK competitive as other countries catch up.

Switching bank accounts has increased in the UK following the introduction of open banking, but the main feature has been the development and uptake of products and services from the data generated. This change has also helped turbo-charge the fintech sector, driven by the introduction of PSD2 and the CMA Order. The **European Fintech Association** has described the proposals as *"another step for the EU to lead the revolution towards tech-driven, fully digital financial services"*. Additionally, open finance has the potential to expand to cover energy, utilities and telecoms in the UK.

The proposed UK legislation is disruptive but not immediately imminent. There is a two-year plan for development, and the JROC (Joint Regulatory Oversight Committee of the FCA) which stresses efficient use of data, is involved. In accordance with the two-year timeframe, it's likely that work on open finance will escalate significantly in a year to 18 months' time.



Now is the time to prepare

Even though legislation may be months away, **UK organisations need to prepare now**, given the potential scale of the proposals. There are significant challenges but also the potential for major opportunities. **Open finance could lead to new products** such as smart, event-driven contracts, and these depend on having data moving quickly. Data will be passed around financial services companies in the same way as a medical record should be in the NHS, so it will require the introduction of digital IDs to track these movements.

It is a system that will work not just for individuals but also for SMEs, due to data being taken from one application and using it in another for underwriting and other beneficial purposes. A permissions dashboard for consumers and SMEs will also require a data standard that can be applied to different sub sectors of financial services. There is the question of API calls as banks require individual instances, which is hugely inefficient currently.

The current data and infrastructure challenges organisations should address

Legacy Systems

Responses to requests for personal data must be provided in a reasonable amount of time, and certain institutions will find this a difficult task due to the challenges of **legacy** systems.

> *"Banks, which hold much of this data, will struggle because of their notorious legacy systems and lack of cloud adoption, perhaps caused by a number of mergers and acquisitions. It will also be costly for institutions. Open banking was expensive for banks and open finance may have similar consequences for the broader financial services sector. However, we're starting to see more financial organisations move towards colocation services and hybrid cloud deployments so they can avoid the pitfalls of aging on-premise deployments,"*
>
> Mark White, Financial Markets & Fintech, Telehouse.

Connectivity Requirements

Financial services companies will also need to consider their **connectivity** requirements. Implementation and optimisation of open finance demands upgrading of digital infrastructure. It requires data centres with highly robust, high-volume connectivity, and organisations will have to select the right partners to avoid failing infrastructure and crashes.

> *"Fast, robust and diverse connectivity will be needed to move all this data quickly. Many will struggle if they continue to rely on their current on-premises systems, as sharing data in real time places huge pressure on networks and drives up energy use. Telehouse partners with LINX, one of the largest internet exchanges in the world to provide one-to-one connections between networks for direct exchange of traffic in a cost-effective and efficient way,"*
>
> Nick Layzell, Customer Success Director, Telehouse.

Telehouse data centres are focused on optimising their power usage efficiency (PUE) figure to help customers meet their net-zero targets. For example, energy is procured from certified renewable source generators such as wind, solar, biomass and hydro. Since 2019, we've reported our progress towards net zero targets, and our annual report shares emissions data in accordance with the Streamlined Energy and Carbon Reporting (SECR) regulations.

Security

Security will also be a key consideration for organisations. How do financial organisations keep data safe, accurate and protect against fraud and the use of fraudulent IDs?

> *"It's never been more true that as soon as protections are devised, someone out there is already thinking about how to hack them. Additionally, with the significant volume of data being generated, organisations must think how to achieve the balance between what will be created and what they need to store. The location of data (sovereignty) will become a key question, even more fraught with the risk of fines from national/EU regulators,"*
>
> Sarah Draper, General Counsel and Chief Risk Officer, Telehouse.

Telehouse data centres are designed with physical and digital security best practice in mind. They have limited entry points and physical barriers in place to prevent forced entry. Biometric scanners, CCTV and security personnel add another layer of physical security. Multifactor authentication is integrated across networks and cloud-based DDoS protections mitigate the impact of attacks for customers, while API protections can be deployed by businesses across cloud and edge sites. Encryption and strict adherence to ISO standards help protect sensitive data in transit.

Accessing the opportunities

Organisations have a great opportunity to access the benefits from the implementation of open finance, such as the introduction of new financial services to give greater choice to consumers, but they must make the right choices to ensure they can create the right products and generate a true return on investment.

Having the right infrastructure will be critical. More regulation is likely and the increased digitisation of all banking and financial services will put new strains on existing bank infrastructure. Legacy on-premises systems will not be capable of meeting these challenges or be ready for any further expansion of open finance.

Everyone in the financial services sector must make the right decisions about how they transform so they can expand and thrive in the new era of open finance. By selecting partners such as Telehouse, they can access the hyper-connectivity, security, scalability and experience to facilitate the transition and sustain future developments, enabling them to increase revenues and remain competitive.

Contact Telehouse to discover how to access the fast-evolving set of opportunities delivered by the introduction of FFDA.

TELEHOUSE

e: marketing@uk.telehouse.net
t: +44 207 512 0080

w: www.telehouse.net