23.02.28

Nordic Financial Unions

NFU Analysis – Open Finance and PSD3

This document is an analysis by the NFU secretariat before the upcoming legislation on Open Finance framework including the revision of PSD2 and a new 'Open Finance' framework, which may extend the scope of data provided by APIs[1] to third parties. The aim of the paper is to give an analysis of what can be expected from the legislation and a basis to form a NFU position when the proposal is released. The legislative proposal is expected to arrive in Q2 of 2023.

Background

Open banking is not a technology-based concept. Open banking is a term being used frequently now in the financial services context, especially since regulators, policymakers and the industry started to talk about fintech. Hence, there is no technical definition of what open banking means, but there is clearly a growing consensus among the industry and regulators ‐ not only financial regulators ‐ that the growing adoption of the open banking model present opportunities for financial institutions and Fintech players to gain insights from the shared data and potentially transform traditional banking.[2]

The basis for this development was founded through the European Union (EU) Payment Services Directive 2015/2366/EU (PSD 2). Open banking permits third parties to access the account information of bank customers or initiate payments. This data sharing mechanism requires bank customers' consent and adequate technology to streamline communication between banks and third parties, namely application programming interfaces. In practice, banks open their application programming interfaces to third parties, thus providing them with account and payment related information. This enables third parties to develop new products or make payments on

[1] APIs being mechanisms that enable two software components to communicate with each other using a set of definitions and protocols.

[2] According to Google Trends, the term "open banking" started to be searched much more commonly after October 2016. See Google Trends, open banking, available at: https://trends.google.com/trends/explore?date=all&q=open%20banking

behalf of the bank customers directly from their accounts based on data collected the financial sector.

Open finance - The need to develop the concept further;

Open Finance is intended to further broaden the open banking spectrum by extending beyond the area of payment accounts to mortgages, insurance, pension, and investment services. All participants in the open finance ecosystem are supposed to benefit, and at a larger scale than in open banking. Nevertheless, open finance is still an ongoing project where the ecosystem is unbalanced as customer related information is a "one way only" giving third party actors a clear benefit of the IT-investments made in the financial sector. Charting a path for its "Digital Finance Strategy", the European Commission aims to develop an open finance regulation proposal by mid-2023, leading to a final regulation draft to enter into force by 2025.

The next decade appears to be focused on questions of data and its role in finance, the economy and society more generally. The discussion is expanding to ideas of 'Open Finance' and 'open data' more broadly, in support of 'open innovation'. The development can be compared with a battle of visions of the future, from one where data are controlled by a small number of giant firms and political players which use their control for profit and suppression, to one where data are under the control of individuals – the 'democratisation' of data – supporting a more open and innovative economy and society. In the evolution of these futures, legal and regulatory systems will play a key role in determining the paths taken by different societies.[3]

The European Union has taken the leading role in this democratisation of data process by being the first to implement mandatory open banking, with its implementation in 2015 of the Second Payment Services Directive. It was the first jurisdiction to make data sharing by banks mandatory, from 2018.

However, any discussion of EU's open banking cannot avoid looking at the broader context. In particular, the EU was also the first jurisdiction to pursue a comprehensive approach to individual data sovereignty, also on a mandatory basis, with the General Data Protection Regulation of 2016. Thus, GDPR provides for individual control over personal data, thereby relating to 'open banking' provisions under PSD2.

---

[33] Douglas W. Arner, Ross P. Buckley and Dirk A. Zetzsche, *Open Banking, Open Data and Open Finance: Lessons from the European Union* in University of New South Wales Law Research Series, page 3

Other open banking initiatives flourished on the heels of the European financial data sharing strategy, so much so that open banking is now a global movement, comprised of distinct approaches that borrow discretely elements from pioneering jurisdictions. Jurisdictions around the world are currently in the process of discussing, developing, or implementing their own frameworks for open banking regimes; distinguishing between voluntary versus mandatory regimes helps map the open banking world.

Open Finance and PSD3 – why two legislations?

The Basel Committee on Banking Supervision interprets open banking as a data sharing process, implying that banks will share their customers' data with third parties to exploit for the development of new applications, products, and services. Financial services customers' consent is the primary requirement for setting in motion such a process. The label 'customer-permissioned data' is indeed used to emphasise the centrality of customers in the whole process. Open finance draws on the dynamics of open banking.

In the EU, the General Data Protection Regulation (GDPR) and the revised Payment Services directive (PSD2) are the catalysts of open banking. The GDPR establishes a framework that empowers consumers to the portability, security, and control of their data through consent mechanisms. Meanwhile, the PSD2 traces back to a joint project between the European Commission, the European Central Bank, and the Euro system to standardize payments in Europe to reduce fragmentation across Member States, promote competition, and continue toward a pan-European digital payment system. The PSD2 sets open banking in stone through the 'access to account rule' that grants third parties' access via customer consent, access to account data and bank infrastructures. These two legislative steppingstones are the basis for the upcoming Open Finance Package.

NFU analysis

At this stage, before a proposal is presented we can only speculate on the exact effects the legislation might have on finance employees and the Nordic finance sector, but we find it clear that it will raise challenges and potential risks that must be addressed in the legislative process when it comes to the employee perspective, , data handling in general, and the financial system.

Implications for the financial system

When considering the potential effects that the Open Finance legislation can have on the financial system, there are scenarios where it has the potential to change the systems at its very core. One current trend in payments today, that hasn't really made its breakthrough yet, is embedded finance. Another aspect is the raise of Big Tech as actors in financial services which can erode the level playing field in the sector.

Embedded finance is when financial services are integrated into non-financial services. For example, payments traditionally are controlled by banks, the infrastructure can be handled by a fintech company, and the selling company is providing the service/product purchased. In embedded finance, due to better data sharing made possible in the existing PSD2 and open banking, the control of the customer's financial data and hence power to dictate how and when consumers and companies can use the data is taken away from banks and the opportunity is provided to smaller companies as well. The boom in online shopping and buy now - pay later (BNPL) services is accelerating this development.

It is the increased data sharing and possibility to use financial data by third parties that have made the development of embedded finance possible. With Open finance and the revision of PSD2, it is not hard to imagine that this development will blossom even more. "Fueled by customer data, embedded finance can provide access to products exactly where and when they're needed"[4].

The development raises some concerns for the financial system. On the one hand, it opens up financial services and data to more actors, but on the other hand it also possibly erodes the level playing field in the sector placing competitive advantages in the hands of companies outside the sector, for example Big Tech who already have large storage of people's data. NFU have highlighted the risks of this development in earlier analyses[5]. In Norway, for example, the PSD2 has not had the intended effect and fintech companies are struggling to get access to data. If Big Tech instead get data access, this is threatening the level playing field.

Big Tech actors are more and more entering into finance by providing a growing range of financial services[6]. Besides the risks they pose in the form of market concentration and technology dependence, the large amount of data handled by Big Tech is posing risks to finance. Big Tech companies do already manage large amounts of data, and with Open finance they will get access to financial data. That Big Tech enters into finance, with the clear motivation of gathering more information on citizens, is raising

4 *Feedzai_Whitepaper_The-Future-of-Payments-Compliance-in-Europe.pdf

5 The changing landscape in financial services | Nordic Financial Unions

6 Big Tech in Finance | Nordic Financial Unions

a lot of concerns connected to data ethics and privacy and responsibility; who owns the data?

Further, many analyses of the effects of Open banking and PSD2 shows that fraud, one of the key issues for the regulation, has not gone down but rather changed by nature[7]. Open Finance will introduce new means related to the processing and exchange of data, which may increase ICT security-risks. Sharing data with more parties, could result in increased data breaches and fraud attempts.

Consumer protection is crucial for the success of Open Finance

NFU sees the danger for consumer profiling and manipulation if finance customer data is being combined with transaction data, which can form new data in relation to predicting behavior. Especially tech and finance-illiterate consumers risk losing oversight of where their data is located and how it is being used over time. For these reasons rejects NFU a regulatory framework, which grants reciprocal data access by banks to non-financial data as an exception from EU consumer protection and data protection law. A regulatory framework however, allowing third parties to access consumers' financial data about savings accounts, insurance policies, mortgages, investments, pension, and consumer credit products based on the explicit consent by consumers, which can also hindsight be withdrawn can alleviate the aforementioned dangers and may indeed offer consumers new services and products.

NFU proposes to create a strong regulatory framework that provides customers with a right to get an overview of their own data in these new reciprocal data sharing relationships between financial institutions and third parties.

- In an increasingly data-driven world, consumers need more control over their personal data, but reciprocity would mean greater risks for consumers and ultimately less control. Therefore, companies that receive data from the financial sector should annually notify the customer of what data the customer has given the company access to and how it is used.
- Current consent rules mean to obtain consumer consent are often insufficient. Users tick a cookie box to access a website, without any idea of the consequences of this agreement. In a sensitive area such as their personal finances, consumers may be particularly unaware of the consequences of agreeing to share personal information about themselves with financial

7 *Feedzai_Whitepaper_The-Future-of-Payments-Compliance-in-Europe.pdf

institution and consequently third parties.

- Companies that receive data from the financial sector should annually notify the customer of what data the customer has given the company access to and how it is used combined with withdrawal opportunities.
- Customers of companies receiving transaction data from the financial sector shall have the right to exchange transaction data from those companies to the financial sector.

Data Protection and Governance

Open Banking in EU may have started as way to promote competition in the payments and banking industry. But it is clear now that its impact is much broader. Open Banking promises to create a new data sharing infrastructure, which will form the basis of a much extensive range of services and products across the whole of financial services, and critically, in other industries as well. This becomes even clearer with view to the EU Data Act, which completes the EU's rules governing data. NFU believes that this new EU legislative framework on data portability is potentially the most comprehensive legal framework worldwide and may successfully complement the GDPR if lowering the barriers for data sharing in the name of innovation is carefully balanced with data privacy and transparency.

Across the world, the EU GDPR has been seen to set a new gold standard for data protection. But although PSD2 and GDPR went into force the same year, they did not form a coherent data governance strategy. In this context NFU sees the greatest challenge of the planned open finance legislation in the blurring of lines between financial services and other industries. One of the aims of the legislation should be to organise the collaboration between financial services and data protection authorities. A market-focused model, which would prioritise only the emergence of a market for data, while regulatory interventions are limited to the correction of market failures and to the protection of critical interests, such as national security is no practicable way forward for NFU, as the EU has already followed a different regulatory approach, which focuses on individual rights and privacy. NFU acknowledges that the general data governance framework of the EU has evolved around these core priorities:

(i) the prevention of data concentration in the hands of a handful of dominant firms; and more recently and

(ii) the promotion of sufficient technological capacity to promote the growth of the internal market. Starting with a series of data protection and privacy directives primarily focused on protecting consumers (EU data subjects), the data governance framework expanded in scope and influence.

Consequently, NFU promotes an open banking strategy, which maintains the individuals' control over their data, as financial institutions can share them with authorized third parties only if requested by customers. Finally, NFU sees two challenges: Firstly, the adoption of a cohesive legislative framework in the Open Finance Framework, which requests financial institutions to enable actual control and sharing to facilitate the ideal of Open Banking/Open Finance/ Open Data and second building the necessary technological infrastructure to make it actually work in practice.

The role of finance employees – finance employees as officers of data handling

With further opening up of data sharing in the finance sector, more responsibilities will be placed on finance employees to handle data in a secure, trustworthy and ethical way. It is likely to assume that finance employees will be the ones that must decide on how to handle the data, if or not the data should be used, and prevent misuse of the data. Of course, a lot of this work might also be automated, creating another level of complexity for employees in need for competence development. With this line of new or deepened responsibilities, finance employees will need new competences and skills. Further, the legislation must address the employee perspective and employees should never be held liable for misuse of data. A key feature for the upcoming regulation will be that it comes with clear guidelines within the legislation itself and through European Supervisory Authorities on how data should be handled and managed.

Further, the term "data ethics" will play a major role as finance employees will be given the role or handling automated processes to assess, protect and use customer data. Finance employees will face ethical dilemmas when handling data, putting pressure on them to handle it in a trustful and responsible way. However, the term "ethical" can be problematic as it might be too abstract. Finance employees should use GDPR as a tool for protecting customer data. Many finance employes have a basic knowledge of GDPR but the need for deepened understanding will increase. Here, employers have a large responsibility in providing training of employees in deeper understanding of GDPR and its relationship to Open Finance. Further, we see a potential problem of trust for the financial sector if the customers financial data will be able to flow out of the sector to actors under less sever regulatory realities. Data ethics will play a major role in this data sharing process. The implications for the financial sector are huge if data stemming from the sector is being transferred to third parties in an extensive manner.

We see a need for clear guidelines on interpretation and implementation on how to handle and manage data as part of the legislation. The ethics and responsibility in using and handling customer data is important, first and foremost, for customers but also for the employees as they will be the ones in charge of the customers data. This employee perspective is crucial to bring to the legislative process. Trade union representatives have an important role to be involved in implementation processes to bring this perspective of employees work and stress level.

NFU strongly advocates for implementation and interpretation guidelines for the sector along with the proposal, at the latest after the adoption of the respective legislative acts. Clear guidelines on how data handling and managing should be done is needed for employees to handle their changed role. Employers must provide competence development and training in GDPR and data handling for finance employees.

Finally, NFU looks forward to the legislative proposals promised for summer 2023 and will update this initial analysis accordingly. Credit institutions and their employees enjoy a high level of customer confidence in data protection and security and have established and widely accepted infrastructures with online and mobile banking in consumer relationships. Thus this up-coming legislative package has to be carefully calibrated to prevent a loss of confidence and trust through external data access.