European Financial Services Round Table

November 2021

EFR PAPER ON OPEN FINANCE IN THE CONTEXT OF THE EU DATA ECONOMY

The upcoming EU's Open Finance initiative should aim to bring data sharing and third-party access to a wider range of sectors and products. Sharing of standardised product information increases transparency; improves product comparison as customers assess the benefits of products and services. Open Finance refers just to a small building block within a broader set of legislatives initiatives aimed at implementing the EU's strategic digital and data agenda for innovation and better services for EU citizens and businesses. A cornerstone of this strategy is to fully reap the benefits of valuable data exchanges and flows amongst all actors within a clearly articulated framework. This is certainly more fruitful than just focusing on Open Finance, the financial sector representing only a part of the European (Data) Economy.

In fact, sharing and accessing of data is already current practice in the financial sector. It happens in the context of PSD2, as well as in current commercial practices, in particular in ecosystem business models, based on private commercial business contracts that rely on already existing legal frameworks. However, often as a result of sometimes missing legislative clarity (such as legal uncertainties derived from data privacy regulation, lacking/unclear liability considerations, unclear data rights framework for individuals and businesses), these practices are unevenly spread, progress at different speeds and have yet to develop their full potential. Further reasons for the uneven development are: lack of/misaligned commercial incentives (given the often high costs to build and maintain data access), as well as new risks and threats emerging as unintended consequences (such as potential conduct risks, cyber risks, etc).

Consequently, the Commission needs to address persisting challenges by putting a horizontal, cross-sectoral framework in place with specific sectoral add-ons where needed. As a result, there are multiple regulatory initiatives under consideration, which require clarity over how they work together – Data Governance Act (DGA), Digital Markets Act (DMA), Digital Services Act (DSA), Data Act, Common European Data Spaces (such as the Health Data Space, Financial Data Space), European Single Access Point (ESAP), European Digital Identity Framework (eIDAS and Digital Identity Wallet). Establishing robust and ultimately value enhancing principles that govern the access and sharing of data are a leading theme in all of these legislative initiatives. If not considered holistically, all separate pieces could lead to further confusion.

Three basic key principles to heed

An envisaged proposal on the sharing of specific customer data amongst financial institutions and/or other market participants should be based on putting the customer at the centre, which would ultimately protect customer rights, put them in control of their data, and allow for innovation in products and services amongst market participants.

For any data exchange and data flow to deliver broad-based economy-wide benefits as intended by the Commission, three basic key principles need to be at the core of any future regulatory framework:

(1) Accessing and sharing of raw data in this context, generally[1] requires the **consent of customers**. When consent is the lawful basis being relied upon, then full **transparency** is required, **as to how and when such consent can be given or withdrawn**.

(2) **Incentives to innovate** must be preserved for all market actors **by embedding any Open Finance initiative in a horizontal and cross-sectoral framework** for a competitive EU Data Economy. Moreover, it must be **ensured that costly efforts** to enhance and expand the range of products and services through the use of refined data (= inferred data) **remain commensurately rewarded**.

(3) **Trust in the integrity of the accessed or shared data** as well as in any of its further uses needs to be preserved throughout the value chain. Trust is at the core of the customer relationship in financial services and therefore the user must be at the centre of the data framework. This also means that the party working with the data must be able to rely on its integrity and accuracy so it can be used for the benefit of the customer.

[1] Consent is not always required for the sharing of personal data, for example GDPR provides for legitimate interest or compliance with legal obligations. This allows, for example, a financial services organisation to share data with a regulator for a regulatory requirement.

1. Securing consent and transparency

Customers – individuals and businesses - are the data right holders over the data (e.g., name, address, circumstances) they offer and provide when soliciting products and services (also referred to as "volunteered data" by DG COMP[2]). The same is true for the data they generate when interacting with the service, and which can be "observed" by the data controller. The consent and transparency principle means other providers should be able to re-use and re-purpose such raw data in a safe and ethical environment, but only in full alignment with the consumer's interest. A customer of a financial services firm needs to affirmatively agree that a third party can access her or his financial data for a certain purpose, and in return would be able to access new and more personalised products.

Data exchanges can only happen in a clear framework of data rights, which should be horizontal and cross-sectoral, beyond the financial sector. It should allow for safe and real-time exchange of data, via secure, and to a certain degree standardised exchange mechanisms, such as APIs. To facilitate interoperability, given the potentially different standards across different sectors, the European Commission could play a role in fostering the dialogue between different stakeholders across sectors, supported by a common base framework of minimal standards. At the same time, it is important to highlight that APIs are only one of many technological tools for data exchange. Ultimately, the choice of such data exchange mechanisms should be market-led. An Open Framework should therefore remain technology neutral to allow for the ability to develop other mechanisms for data exchange in accordance with the evolution of technology.

At the same time, it is important that the ways for the customers to give, manage and withdraw their consent are simple and fully transparent. For this, links with the new Digital Identity Wallet should be explored.

In order for a consent-based approach to be operable there must be a very clear distinction between the unprocessed / 'raw' data that customers provide to or generate with a service provider (= "volunteered" or "observed data") and "inferred" or "derived data", where financial services firms have enhanced the value of the data through deployment of their own intellectual property.

In this sense, the portability principle introduced through GDPR in 2018 provides for a clear foundation and good starting point to access and share data. According to GDPR:

- Raw data can be transferred on demand of the data subject: An EU individual can obtain a transferrable copy of data he or she has actively provided or "volunteered" (e.g., information provided through the application) or observed data generated by and collected from the person's activities (e.g., speed data recorded on a telematics device). And he has the right to transmit those personal data to another data controller.
- Inferred data cannot be transferred on demand of the data subject as part of the data portability: An EU data subject cannot obtain a transferrable copy of derived or inferred data exclusively generated by the controller (e.g., a driving score based on an analysis of raw data from a telematics device)[3].

However, the aforementioned foundation of GDPR is focused on the legal rights that the regulation actually protects, and many legal gaps and uncertainties still exist for financial market players to reap the full benefits and generate new business from available data. Combining all the above-mentioned concepts (user consent, raw data, real-time exchange of data from one data controller to another, via standardised APIs, GDPR portability right) brings us to the notion of "enhanced portability". A more efficient data portability right applicable for all sectors (as also introduced in the proposed DMA) would give users/individuals more control over who can access and use their data in a very much needed fully-fledged data sharing framework that creates a level playing field. At the same time, an extension of the enhanced portability concept to data that goes beyond the GDPR scope (e.g. IoT data, sales data) is required, in order to include in the framework data that is sharable or portable also for businesses, machines, etc. Those should be clarified in the forthcoming data regulations, horizontally and not only for Financial Services.

2. Cross-sectoral data framework

The European Commission aims to promote data-driven innovation in finance; to facilitate the industry transition to tailored customer solutions; bring efficiencies for consumers, businesses, and authorities; to help integrate European capital markets and to channel investments into sustainable activities (e.g. green financing). This ambition will only be achieved if a new framework preserves incentives to innovate for all market actors based on a horizontal, cross-sectoral framework that levels the playing field for all actors involved (i.e., all players across the entire economy are subject to similar obligations as regards their respective raw data). As an illustrative example, the access to data from the energy and transportation sectors would allow financial services firms to calculate the carbon footprint and offer tailored green loans, in line with the EU sustainable finance strategy. It would facilitate the creation of ecosystems and generally support innovation with partners, as multiple third parties would be able to develop valuable new products and services. In this scenario, increased data sharing, based on facilitating a seamless exchange of raw data generated within and across sectors, while also ensuring costly investments that are translating into valuable new consumer products and services get adequately rewarded, it will be a win-win situation.

---

[2] European Commission - DG COMP 2019 « Competition policy for the digital era »

[3] If that derived or inferred data is deemed to be personal data, the data subject may be entitled to access it, although GDPR does not grant the right to portability of this inferred personal data.

Data sharing in the financial sector should be driven by credible consumer propositions and use cases. Also, the implementation should be proportionate, consistent and carefully coordinated and sequenced with interventions in other sectors; so that other holders of large quantities of client data that are of interest for the innovation in financial services are subject to similar obligations. In any case, provisions of an Open Finance framework regarding banking activities should not deepen the asymmetry in data access introduced by PSD2.

Preserving incentives will require ensuring that proprietary (= inferred) information originating from costly financial investments is appropriately protected from being diluted or poached and excluded from any data sharing obligations. If this is not done, innovation that is beneficial to the overall economy will reduce or cease to be undertaken. Any obligations for data sharing with an Open Finance framework must protect commercial incentives, avoid creating competitive distortions and ensure there is no scope for 'free-riding'.

Further, data localisation requirements and restriction to transfer and use data within the EU present a particular challenge in regard to Open Data, increasing operating costs and hindering scalability. In this regard, it is essential to remove data localisation requirements, allowing companies to store and process data where they choose, of course taking into account due diligence considerations. The localisation restrictions will depend on the level of assurance certified by the cloud service provider. Beyond the EU, the aim should be to achieve global standards across jurisdictions.

3. **Preserving trust in the integrity of the accessed or shared data**

The implementation of Open Finance should not only be proportionate, gradual and phased (in parallel to other sectors, avoiding a one-sided opening in financial services), but – above all – be driven by credible consumer propositions and use-cases. Customers will buy new propositions only if the promises of seamless processes, more personalised services at better and tailored prices ultimately hold without data privacy and security getting compromised. Therefore, a user-centric cross-sectoral data sharing framework should be favoured rather than Finance only approaches.

A secure EU interoperable digital identity, which aims at preserving trust between customer and financial institution, would be a welcome complement.

Prioritising the protection of customer data, and preserving trust, is vital to encourage customer-led data sharing. A cross-sectoral approach should be taken to tackling some of the biggest challenges that increased data sharing introduces – challenges such as data breaches, data loss, data theft, and the subsequent impact on fraud and scams (noting there will be alignment to the Digital Services Act). Therefore, the regulatory framework should establish and apply cross-industry common security standards and requirements for all actors and sectors that participate in a given value chain that builds upon data accessed and shared by third parties.

To mitigate data privacy concerns in sharing data along a potential value chain, so-called privacy enhancing technologies (PETs), such as data synthetisation, anonymisation or differential privacy, are playing an increasingly important role. Their development promises secure processing and exchange of personal data while preserving important correlations and depersonalised information and avoiding the risk of application of de-anonymization procedures which would allow to trace back the person to which data refers. PETs enable business models based on data sharing, like benchmarking services in personal lines insurance based on larger data pools, more informed decision making based on international / market data pools and easier 3rd party data exchange (e.g., with academia). However, it is important that the legal responsibility to apply and deploy sufficient safeguards/ protections, such as trust preserving PETs is clearly assumed by both, the initial data controller and -after having access to the data - by the 3rd party accessing the data.

In addition, the Financial Service Industry will be subject to dedicated robust cyber risk security standards under the Digital Operational Resilience Act (DORA). It will be important to ensure that these standards are not compromised or undermined by the introduction of obligations to establish APIs with third parties. In order to protect the interest of consumers and integrity of the system, the same supervisory standards should be applied to all actors in an open finance framework. In a cross-sector data sharing and portability framework, similar security standards ought to apply.

The user must be at the centre of the Open Finance framework. Trust has always been at the core of the customer relationship, and at the foundation of the Open Finance proposal should be how to help the users (individuals or businesses) to take control over how their data is used and shared, in a secure way and in line with GDPR.

Conclusions and policy recommendations

An Open Finance framework should be encapsulated in a broader open data cross-sectoral framework. Applying the three basic key principles to the regulatory framework should not be limited to the banking or insurance industries but underpin data sharing across the whole economy. Considering a customer-centric approach, disruptive innovation can only come when a variety of data is used.

Following policy recommendations are made to bring the three basic key principles to life:

1. **Transparency and consent**

   - Open Finance data sharing should be based on the principle that customers control the data they supply or directly generate. In this context[4], the access or sharing of such data requires the customers' explicit consent and a fully transparent governance process. The same applies to the data customers provide or generate in other non-financial environments.
   - At the same time, there is a need for a clear framework for non-personal data (e.g. IoT data, or sometimes geolocation data) similar to that provided by the GDPR for personal data, to provide guidance on how non-personal data can be shared, under which conditions, and on who can decide on it.

2. **Incentives for innovation**

- Such a framework should apply not only to financial market players but across sectors to maximise the potential for innovation (access to data from outside of the financial sector can improve the provision of financial services) and avoid regulatory disbalance and unfair competition.
- There must be commercial incentives for open finance-type arrangements between firms and also with other sectors. Those are key to allow investing in innovative products and services, which meet consumers' current and future needs followed by the sustainable ROI for the companies.
- Similar data sharing frameworks for raw data from other sectors (secure, real-time and with certain standards), as envisaged in open finance, should be introduced across the entire economy. This will allow for the rebalancing of the commercial unlevel playing field amongst all actors. Data sharing should be driven by credible consumer propositions and use cases and carefully coordinated and sequenced with interventions in other sectors. Inferred or derived data should not be in scope.
- An incremental approach for data releases should be defined. The scope of such approach is twofold. Firstly, to allow all data owners to set up appropriate PETs for each dataset. Secondly, to dilute the disruption that data sharing can generate on some firms within the financial sector
- Data localisation requirements should be minimised.

3. **Trust**

- The implementation of Open Finance needs to be proportionate, gradual, phased and driven by credible consumer propositions and use-cases.
- The regulatory framework needs to establish and apply industry-wide common security standards for data exchange. In terms of increased focus on privacy and data security ensuring the safety of customer data should continue to be a key objective.
- Rules or meaningful principles that are equal for all market players in scope are needed to complement the existing legislative & regulatory framework.

[4] Noting, as above, that there are instances where personal data can be shared without the customer's consent, e.g. through legitimate interest.