EU Commission
DG FISMA

EU Transparency Register 022027817030-67
Date: 05.07.2022
Our ref.:
Your ref.:

Targeted consultation on open finance framework and data sharing in the financial sector

With reference to the targeted consultation on open finance and data sharing in the financial sector issued by the European Commission on 10 May, Finance Norway outlines its view on the need for an Open finance framework in this position paper. Finance Norway is the business organisation for banks and insurance companies in Norway. In addition to our own contribution, we participate in the consultation work in the European Banking Association, EBF, the European Savings Banking Association, ESBG and in the European Insurance Association, Insurance Europe.

Finance Norway represents several types of stakeholders in the data value chain. Our members are data managers (holder of customer data), data users (User of customer data), in addition to the fact that Finance Norway itself is in the category «other».

Our understanding of Open Finance
As there is no clear and uniform definition of Open Finance, we have worked on the assumption that Open Finance means accessing and sharing finance-related personal and non-personal data via a predefined technical solution. Data is shared with third party are service providers who need data to provide a range of financial services and information services. It also expands access to data between players in the industry.

The GDPR already allows consumers to ask financial institutions to share data, whenever technically possible. Business customers do not have the same rights. An Open Finance framework will oblige the financial institutions to establish general technical solutions for data sharing or facilitate technical access in some areas clearly identified areas.[1]

Finans Norge's assessment
The Norwegian financial industry is concerned with data security and integrity for its customers, and thus also for its business. The Norwegian financial sector is highly digitized. The development has been rapid, and a basic care for customers' security, integrity, data and consumer protection has enabled the industry to develop many modern, good user experiences. A well-functioning electronic identification method, through BankID, has been a basic prerequisite for this. The GDPR is also one of the basic preconditions.

[1] One such area has already been identified with the introduction of the PSD2.

Hansteens gt. 2, Oslo . P.O.Box 2473, N-0202 Oslo, Norway . Phone +47 23 28 42 00 . Org.no 996 549 488 . finansnorge.no

The term "data" is not unambiguous or exhaustive. Individual data, which is information customers have provided to the financial institution, or which is generated through the customer's interaction with the financial institution is one thing. Portfolio data is when customer data is added together. Sharing portfolio data raises several additional issues that deal with competition, trade secrets and obtaining consent. Another distinction is between the data provided by the customer and data developed in the company based on that data, i.e., proprietary data. In its response to the EU Commission, Finance Norway has focused on individual customer data. Some principally designed answers also include portfolio data and proprietary data.

1. Should financial institutions be obliged to share customer data with third parties if the customer so wishes?

Finance Norway approaches this question with the premise that customer owns their own data. In principle, the customer should be able to make customer data in a financial institution available to another service provider. The principle is not limited to the financial industry but applies to all areas of life. Conversely, data linked to third parties, as in liability insurance, should not be made available for compulsory sharing since consent is not given by the third party.

Requirements should be set for how the customer's consent is obtained and verified. It should also be possible for the financial institution that submits data to verify that the customer wishes to transfer data. This could be done by the data holder (i.e., the financial institution) either requesting the customer's consent to transfer, or at least being given the opportunity to verify the consent that is given to third parties. The financial institution has responsibility under the GDPR not to transfer customer data without a sufficient basis. Regarding data other than personal data, requirements should be set for how the recipient processes and stores data.

There are many ways to share data, and it has proven to be beneficial for customers and society to create solutions where data is shared to third parties when the customer wants it. In the Norwegian financial industry, there are many good examples of contract-based solutions where specific data are included in a joint project for the benefit of customers. However, high development costs and the need for scalability in solutions mean that for small players it may be important to have regulation that paves the way for more active data sharing in and with the financial industry.

The financial industry collects a lot of sensitive data about its customers. This is necessary for the credit and risk assessment on which the industry bases many of its products. Trust in the industry's handling of customer data is therefore an important prerequisite for the industry's operations. It must control all data sharing and set the conditions for how sharing can take place. In assessing the need to expand the obligation to share data beyond the PSD2 Finance Norway underlines the need to carefully assess the role of data in risk-assessment and other financial services that are conceptually different from PSD2, and the potential consequences to production of these services.[2]

Financial institutions should therefore be able to enter into agreements on data exchange with third parties when customers so wish. This should also include the commercial establishment of technical solutions that make this type of exchange simple and standardized, but still sufficiently secure for both the customer and the financial institution as the issuing party.

[2] EIOPA has worked on the concept of Open Insurance for some time, and Finance Norway points to Insurance Europes views on a possible open finance framework, and the further discussion triggered by this work.

2. Is there a need to regulate access to data from the financial industry beyond what is done in PSD2?
This is a complex question. With a PSD2 solution you create automatic access to data when customers have approved it. For financial institutions to establish standing technical solutions that give third parties access to all customer-related data in the company is very costly and time consuming. It is not a given that there is a demand for all types of data. In addition, it is very intrusive, and has unclear consequences for the financial institutions' business models.

There is therefore a need to delimit the areas where such access should be granted. However, the criteria that should form the basis for such a delimitation are not clear. The rapid development in service production we have seen over the last ten years illustrates that enshrining such a delimitation in law, is too static and would be detrimental to the dexterity and dynamic that an innovative market needs.

The need for regulation is therefore limited to specifying what the preconditions for sharing customer data should look like. These conditions must ensure the security of customer data. Furthermore, there must be regulations that ensure that financial institutions can get a return on the investments they make in data management and processing. These are rules that partly emerge through the Data Governance Act, the Data Act and the regulations on digital markets, and which will apply to all companies. It is currently unclear whether there is a need for special rules for the financial industry in this area.

3. How should the technical solutions for securing data access be designed in regulation?
Finance Norway considers that the technical solutions needed to ensure data access should be developed in the market. Already today, there are regulations for the financial industry's risk management in interaction with third parties. Any regulations should therefore be based on the same type of principled management and risk control technique that exists in other types of financial regulation. The principled approach in the Digital Operational Resilience Regulation (DORA) is an example.

It is not appropriate to introduce new standards that change the preconditions for the extensive ongoing work with development of APIs in the industry. Contract-based data sharing will provide an opportunity to build on the solutions that are available and will therefore be the most cost-effective way to ensure the sharing of individuals.

In any potential open finance framework, it will be important to develop standards to facilitate data sharing. The starting point for any data sharing should be market-led, based on a common taxonomy that is developed in close coordination with industry. These standards must be well aligned with specific national and general industry standards and practices.

Yours sincerely
Finance Norway

Ellen Bramness Arvidsson
Executive Director International Affairs

APPENDIX

Examples of useful measures that use customer data from financial institutions

In the industry and in collaboration with the financial industry, there are many good examples of solutions that use customer data.

Norsk Pensjon AS is a service where the individual's total pension data can be retrieved and displayed in the environment where the customer wants to see it. Norsk Pensjon is based on agreements between the participating parties and has not needed an Open Finance regulatory framework to be put in place. The European Commission points to **this type of pension portal** as an argument for introducing an Open Finance regulatory framework. The fact that data on public pensions is not yet available in the Norwegian solution illustrates the importance of all stakeholders listening to the user needs and delivering to the solutions.

Norsk Gjeldsinformasjon AS is a service that collects information from financial institutions on **individuals' holdings of unsecured debt**. It gives the customer a comprehensive overview of unsecured debt. It also provides an overview to the participating financial institutions. All financial institutions that offer unsecured debt are obliged to share information with the register.

Invidem AB is a collaborative project between several banks in the Nordic countries that is establishing a contact point where the industry can obtain **reliable "know your customer" information** about corporate customers. By combining customer data provided to the bank with data from third parties, the customer receives a proposal for material that they can choose to share with relevant financial institutions.

Consent-based loan applications are based on the customer giving the credit institution permission to collect relevant tax, population register and housing data from public agencies. This limits the information the credit institution has access to, to what is relevant for the risk assessment and simplifies the customer's work with information collection.

Most people have additional, privately produced, insurance coverage **in case of illness or disability**. The individual can consent to the social security authorities sharing information on disability and rehabilitation with insurance companies in order to activate this additional insurance. Since private insurers base the claims on information about decisions made in the public system, such data sharing ensures timely pay out from the additional insurance.

Insurance companies in the Nordics have been working with **embedded insurance**, from information to distribution and claims management, for at least 10 years. Using API products to expose data and functionality to partners and corporate customers is a fundamental and growing part of the insurance companies' business. However, it is essential that the data owners control the content of the API Products and which partners use them to ensure a sustainable insurance industry as well as continuous compliance with laws and regulations.

Another example that increases efficiency in the industry is based on portfolio data. Cooperation against insurance fraud rectifies skewed selections in one company's databases. A skewed selection is not effective when combating other / new types of insurance fraud. **By sending your own databases to "training camp"** in a common database, you increase the predictive power for the individual company. Here, however, it is a question of the third party performing a service for the insurance companies, and not further distribution to new third parties.