European Commission
“Have your say”

EU Transparency Register 022027817030-67
Date: 23.10.2023
Your ref.: COM (2023)360

EU commission proposal Regulation of Financial Data Access 2023/0205

Finance Norway notes that the EU Commission (COM) has deemed it necessary to further regulate the rights given to data owners in the General Data Protection Regulation to share customer data with third parties. The proposed regulation has been developed over time and has been open to stakeholder input on several occasions. As shown in our input during the consultation last summer, Finance Norway has demonstrated that the sharing of data from the financial sector is possible and can be made safe also without this regulation. Finance Norway appreciates the possibility to give our input also at this juncture.

The rapid development of machine learning and Artificial Intelligence in production lines and consumer interfaces throughout the economy has highlighted the importance of access to high quality and relevant data. Finance Norway acknowledges and supports the large body of work that the COM has undertaken to level the playing field and increasing market participants’ access to data. The current proposal fits into this overall endeavour, by acknowledging that financial data is generated in a highly regulated setting and ensuring an appropriate prudential environment also when data is shared. This is essential to maintaining trust in the financial system.

However, we are still not entirely convinced that all aspects of the playing field have been levelled with this proposal. The European financial sector is at a disadvantage when it comes to customer behavioural data in comparison to the large global, unregulated institutions that are usually referred to as BigTech. The obligation to share data *from* the financial industry should be complimented by a clear obligation to also share data *with* the financial industry. The implementation of the Digital Markets Act does not fully alleviate these concerns.

Finance Norway welcomes the introduction of “schemes” into the regulation. This facilitates efficient and pragmatic paths forward for the sharing of data. The sharing of cost for technical solutions is enabled, as is the delineation and standardisation of the data to be shared. Schemes, defined and executed in a flexible way, will enable a market led development of financial information services. However, the prerequisites defined in the proposal belies the ability for the financial services industry to develop the sharing of financial information as demand develops.

In reading the proposal, Finance Norway has envisaged how the dynamics of innovation would play out once the regulation is in place. A Financial Information Service Provider (FISP) – a data user – will develop a service and market that service towards a group of customers. To produce the service, the FISP needs a specified data set. The customers that are interested in the service, may be customers in several different financial institutions – data holders. The data user (FISP) therefore turns to the data

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

holders to access the specified data through the technical solution developed by the data holder, under the rules agreed on in the scheme. The notion that the data holder should already be prepared to deliver the specified data points is not realistic.

The customer data in the financial services industry develops over time, and while there may be an established scheme that could provide governance for sharing of this data, there might not be any demand for all data points. While the image of an unlimited market for data might be enticing, one should remember that markets suppliers need to gage demand interest before deciding what to offer. When there is no demand, delivery of data and development of rules and standards in the scheme to govern this will in fact be a cost without a benefit. Mechanisms for identification and qualification of demonstrated demand are therefore important.

Our members believe that market driven innovation on a level playing field is the best way to strengthen European competitiveness in the digital economy, also when it comes to financial services and financial information services. Facilitating the workings of the market through creation of infrastructure with market pricing for resource allocation must be the way forward.

Scope

It is vital that the data covered by the obligation to share customer data should be limited to the personal data that has been provided by or made available to the customer. Any ambiguities in this regard risks creating legal uncertainty followed by delays in market developments. The second part of the definition of customer data in Art 3(3), "…data generated as a result of customer interaction with the financial institution" covers data inferred or derived by financial institutions. The financial institutions have added value to the data in such cases, and the data should not be at the disposal of customers or other market participants, and not be in the scope of the regulation. "The sharing of customer data in the scope of this Regulation should respect the protection of confidential business data and trade secrets." is mentioned in recital 9. Given the importance of this concept, we consider the wording in Recital 9 not to suffice. We would suggest to including it in an article. Additionally, it should be clearly mentioned in the articles that other Union regulation regarding data sharing or protection, must be followed.

The choice of data points collected by the financial institutions generally reflects the process the financial institution uses the data in. There are of course many commonalities in different processes, but each individual financial institution uses different data points for their own processes. These processes are an integral part of the institutions business models and competitive tools. To ensure that competition is not depleted, and the quality of the customer assessment processes isn't weakened, it must be possible to safeguard the structure of the customer data. In addition to the data used for risk assessment in insurance underwriting, examples of this are suitability and appropriateness assessment within the meaning of Art. 25(2) and 25(3) of MiFiD II and the data collected by a bank for credit assessment purposes.

Art. 5.3.(e) and Art. 6.4.(b) foresees an obligation for both data holders and data users to maintain the confidentiality of trade secrets and intellectual property rights when accessing customer data pursuant to Art. 5.1. However, neither the data holder nor the data user could provide a guarantee for the protection of business secrets in relation to the customer data, since only the (company) customer knows whether access to certain data affects its business secrets or intellectual property rights. In addition, such an obligation could involve a great potential liability for the data holders and data users concerned to a completely unclear extent. Moreover, a need for protection of trade secrets should

rather exist for the data holder. After all, the collection and processing of customer data to an extent individually specified by the data owner or according to a provider-specific system can be a differentiating feature in competition and thus affect its trade secrets or IP rights. In the name of level playing field, a similar exclusion for the sharable data should be made as in Data Act where the data holder can withhold from sharing trade secrets.

Customer data pertaining to the categories of data specified in Art.2 is not a precise definition of what the obligation to share entails. Finance Norway surmises that this means that any scheme can define the scope of the obligation and negotiate what data holders will be willing to share beyond the obligation. Finance Norway would welcome further specification on the principles for the sharing obligations. Financial institutions assessment of price towards the individual customer illustrates the data holders' internal processes and is sensitive also with regards to competition. The obligations to share such data should therefore be explicitly regulated and any further processing of pricing data, except for one-time transactions serving individual customer's needs, should be prohibited.

Financial Information Service Providers

Finance Norway believes that while sharing of financial data with other market participants can facilitate innovation and dynamic economic development, the case for customers sharing data from other markets participants to financial services is as strong.

By proposing FIDA, the Commission acknowledges that the GDPR is not sufficient grounds for data sharing to happen. There is a need for «rules and tools to manage data sharing permission", "rules governing such sharing are either absent or unclear" and "data sharing is made more costly as both the data itself and the technical infrastructure are not standardised…". Finance Norway acknowledges that this is true for data generated through customer interaction with financial services. Indeed, that is why we have successfully built a string of collaborations to make information sharing more efficient. But this is also true for other sectors in the economy. Data from other sectors of the economy could be equally important to build not only financial information services, but also benefit the development of new products and services within the financial sector itself. Behavioural data from telecoms or power could enhance customer analysis in financial services. We therefor regret that the obligation to create systems and rules for sharing customer data is only directed towards the financial industry.

This argument can also be applied to 3rd country entities, who might be financial services providers in their jurisdictions, who may limit their regulatory exposure to that of being data users only in the internal market.

Finance Norway acknowledges the reciprocity of data access being created with gatekeepers defined through the Digital Markets Act. However, the DMA definition is at the present time limited to seven companies. No reciprocity is established with other companies that hold a FISP-licence.

We understand that the registered Account Information Service Providers (AISPs) (art. 2.2(b)) could benefit the same rights provided by FIDA as other data users. We would prefer FIDA to either require AISPs, already registered as such but wishing to access financial data, to also apply for FISP's authorisation regime, or introduce a single common authorization regime for both AISPs and FISPs.

Schemes
Finance Norway welcomes the concept of schemes. We believe that a principles-based, light touch regulation of schemes could facilitate market driven data sharing while being essential to assist data holders safeguarding that data is only shared with licenced data users. In the payments area, there are several well-functioning schemes in place. These have been developed over many years, and innovation and new specifications have been assigned to well established bodies for further development. The current proposal requires participation from market actors that do not participate in schemes, and where cooperative mechanisms, like schemes, have been developed only to a varying degree.

We are, however, struggling to understand the reasoning behind the timeline set up for the establishment of schemes. We fear that the delineation creates a static model that will rupture the demand driven model that should be driving the sharing of data.

Existing schemes, and existing products and ideas for products by members of such schemes could probably comfortably be developed within the time frame given. Yet longer timelines are needed for the development and negotiation of new schemes; 18 months is not feasible. To take this into account and the specificities of each product area (e.g., financial products are heterogenous across member states), the different actors, the costs and time necessary to centralize and the broad range of data, a gradual approach with different timelines should be introduced per type of data under Art.2.

Article 10 (1) h sets out principles to balance the financing of a scheme ensuring that it is non-discriminatory. However, in the last paragraph to Article 10 (1) h the proposal introduces a particular regulation of compensation from data users that are micro-, small, or medium enterprises. The material difference between the compensation limit in Article 10 (1) h (i) and Article 10 (1) h last paragraph is not quite clear, and the reason for differentiating between scheme participants due to their size should be examined from a competition law perspective.

Article 10(2) of the proposal states that if a financial data sharing scheme is not developed for one or more categories within a reasonable amount of time, then the Commission may set up such a scheme. However, there could be various reasons as to why no financial data sharing scheme may be in place, which could range from the short timeline for implementation to the lack of customer demand for data sharing. Moreover, such an approach seems to be at odds with leaving the development of innovative solutions to the market.

Already established schemes
Norwegian financial institutions already share customer data through several established and well-functioning schemes. One example is the pensions dashboard, Norsk Pensjon, that provides the individual with an overview of their three pillars of pension savings. It is provided by a company owned by the pension companies in Norway. The platform functions as a hub where the individual asks the platform to gather information on the personal data, which is shown in real time in the customer interface. No data is stored or processed for other purposes. The licence to gather the data is given each time the platform is activated.

For these schemes, the current proposal will entail a re-regulation. What this will entail in practice is difficult to assess and will vary. To avoid the dissemination of well-functioning services, Finance Norway sees the need for the competent authority to be able to exempt schemes from the scope of the regulation.

Liability
Data holders cannot be held liable for information after the point where it has been shared with a data user. The customer is the one choosing what should be shared, and data holder cannot know what data will be used or misused for. The collaboration foreseen in schemes can only hope to prevent this, so that liability can be allocated precisely and according to what is possible to control. Data users must therefore be held responsible for the confidentiality of the process from the point where they access the data.

Only the data user can assess the relevance and actuality of the data. While this probably also is a discussion between data holders and users envisaged taking place within a scheme, data holders cannot be held responsible for data users' error of judgement in own data needs and the feasibility of meeting these.

Finance Norway also wishes to underline that liability for data correctness and data security can only be upheld if data is accessed by reliable methods agreed upon by the participating parties. Unsecure methods like screens scraping, mobile API re-engineering and other innovative but unauthorized methods disables controls and security systems and data holders cannot be held liable.

Permission dashboards
Art 15 of the GDPR ascertains a degree of insight and control over personal data by customers also in financial institutions. Finance Norway welcomes the elaborations of this tool as specified in Art. 8 of the proposal. However, it is essential to underline that the sharing of data permitted from the data holder is based on a contractual relationship between the data user and the customer. The data holder is not privy to the content and conditions of this contractual relationship. To ask the data holder to explain the purpose of the permission, is therefore not feasible. In this regard, it should be noted that data holders must not be forced to accept requests of making data available where the data holder has not been in control of the identity and access management, and what information that is provided to the customer when the request is submitted.

There is clearly an informational need on the side of the data user as well, and Finance Norway sees a corresponding responsibility – the creation of customer dashboards – for data users as a way forward on this.

This could possibly also alleviate the logical issues arising with the re-establishment of permissions through the dashboard. Re-establishment of sharing must logically be based on a re-establishment of the contract between the customer and the data user, and the dashboard would need a signal from both these parties to re-establish the sharing.

Even though data in the financial sector is far more diverse than the payment data that has been shared for some years now, there needs to be some level of harmonisation with the payment services sharing. The more diverse the permission dashboards universe is, the less accessible and useable it will be for the customer and their actual management of permissions. We also note an asymmetry between this proposal and the EBA stance that ASPSPs cannot revoke consents on behalf of the PSU in a PSD2 setting, as this would undermine the aim of PSD2 to create a level playing field and be in breach of articles 66, 67 and 68 (5) of PSD2.

Chains
It is not uncommon, in the payment services universe, that third party providers act as aggregators and suppliers to other third-party providers. Sometimes also to non-licensed receivers, sometimes further on to a fourth or fifth party. This practice gives rise to questions of liability and control through dashboards in the further financial data information sharing. The licensing and supervision of the FISPs is reassuring, and further sharing of data should also be limited to FISPs. Furthermore, the liability of the data holder in such cases should be clarified. FISPs should also be seen as data holders for data they have obtained directly from their own customers and that falls under the scope of FIDA.

Security and fraud
We welcome the licensing, supervision and the legal requirements placed on the FISPs. Fighting fraud and strengthening cyber security are on top of the agendas for the financial services industry. As data security, access to initiation and other use of customer data as well as delineation of liability on these issues are part of the contractual agreements left to scheme participants to develop, practices and standards will emerge. Maintaining high standards will remain crucial to safeguarding the trust in financial institutions that are data holders, and thus to the financial system as such.

Finance Norway is a member of the European Banking Federation and of Insurance Europe. We support these organisations' contributions to the current "Have your say". This entry aims to further emphasising issues that warrant deeper discussion and underlining issues of specific importance to the Norwegian banks and insurance companies.

Yours sincerely
Finance Norway

Ellen Bramness Arvidsson
Executive Director International Affairs