IDP messages on Commissions proposal for a framework for Financial Data Access

26.10.2023

Insurance & Pension Denmark
Philip Heymans Allé 1
DK-2900 Hellerup
Phone: +45 41 91 91 91
fp@fogp.dk
www.fogp.dk

Sigrid Floor Toft
Head of Digital Policy

Case No. GES-2021-00052
DocID 472220

Insurance & Pension Denmark (IPD) has the following comments on the proposal for a regulation for Financial Data Access (FIDA).

Open Finance has the potential to positively impact both consumers and the financial sector if the framework is designed right. However, IPD is generally critical of the Commission's approach to increased data sharing in the financial sector. Although the proposal focuses on a number of positive aspects about customers' opportunities to exchange their own data with other companies, it is particularly problematic that the Commission extends the concept of "customer data" beyond the personal data that is already covered by the GDPR and the right to portability there, because it could potentially mean that the companies are forced to exchange business sensitive information.

It is necessary to distinguish between different categories of customer data and to specify which categories of customer data are covered by the data sharing requirement. For example, certain data submitted by the customer themselves and general product information are suitable for sharing, whereas the opposite applies to a number of enriched categories of data based on information that differs from company to company, e.g. risk assessments, tariffs, etc.

In addition, the exchange of such a vast amount of data requires the establishment of a digital infrastructure. We are concerned that the broad approach to the scope of data will be a significant cost driver for the industry to the detriment of customers. Furthermore, it will require significant investments and digital resources in each company to become compliant with FIDA. Resources that could otherwise have been put to more effective use in implementing DORA for instance.

While there is room for remuneration for making data available, this does not address the costs of setting up consent dashboards or adapting companies' own digital infrastructure to new requirements. With the current definition of customer data, the requirement for data sharing is expected to require major and costly technical changes, as it will require direct electronic access to a large number of data sources internally at every financial institution as well as their business partners and suppliers. Smaller institutions may not even have digitized alle the relevant information. In relation to business partners and suppliers, the requirement for data sharing will also require significant contractual and technical changes.

Furthermore, there is a significant risk, that with the obligation to make such large datasets readily available at once, there will not be a sufficient number of companies, who can use the data commercially and would be willing to pay for them. The cost of participating in schemes will rise with the amount of data being made available within the scheme. This could deter FinTech's from joining the schemes and supports the argument of starting with a narrower scope for FIDA, to establish actual business cases as the basis for the data sharing framework.

Existing data sharing schemes

The Danish insurance and pension industry already has a number of initiatives that ensure customers the opportunity to share data across the sector and which have been established without regulatory intervention. These are, for example, Forsikringsguiden and Pensionsinfo, which is a tool that makes it easier for customers to get an overview of payments and coverage in the event of pension, illness and death and to share their data with the actors with whom they may wish to share it. It is a collaboration between all Danish banks, pension funds, LD, Udbetaling Danmark (State employees) and pension and insurance companies.

It is important that the proposal takes into account the industry-specific solutions that have already been developed, including that PensionsInfo, for instance, can be given the status of a data scheme. The financial actors should be able to use existing schemes without any additional requirements for API's or data standards being imposed, as there is otherwise a risk of having to develop additional overlapping schemes.

Field of application

The regulation covers both banking, insurance and pensions. In the area of insurance and pensions, access to customer data must be granted in the following areas:

• Non-life insurance products (with the exception of health and health insurance) including data collected for use in needs assessment, cf. art. 20 of the IDD and suitability assessment according to art. 30 of the IDD.
• Pension rights covered by Solvency II and the IORPS directive.

• Pension rights covered by the PEPP rules.

Customer data is broadly defined as both personal and non-personal data that is collected, stored and processed as part of a regular customer relationship and covers both data provided by the customer himself and data generated as a result of the interaction with the financial company - i.e., significantly broader than the GDPR and the right to portability.

The proposal also seems to include both retail and business customers. However, the focus of FIDA should primarily be on retail customers and should exclude commercial customers. This would align the proposed framework with the portability rights under GDPR.

We support the exemption of certain categories of sensitive personal data in relation to sickness and health insurance. However, insurers process different kinds of special and sensitive personal data such as medical/health data and data concerning possible fraud. It should be clear that these categories of data should not fall within the scope of FIDA because of their sensitivity and the risk associated with sharing this kind of data.

However, the reference in the text is to the products (i.e. health and sickness insurance) and not the data itself. This means that the sensitive health-related data of customers could still be subject to data sharing requirements in the context of other insurance products.

FIDA should therefore clearly exclude from the scope of any data sharing obligations any insurance lines which also cover personal data related to health, for the same reasons that health and sickness insurance are excluded. This would include, for example, accident insurance, disability insurance, long-term care insurance, etc.

Too broad and unclear definition of customer data

IPD finds it highly problematic that data is so vaguely defined and also includes other customer-related data that arises in the interaction with the financial company. This is a problem because it can be interpreted to mean that, as a starting point, it includes enriched data, e.g. the assessments and analyses, which are central elements in the insurance and pension companies' value proposition to customers, which is not reasonable simply to demand that it be handed over to competitors. It is competition-sensitive information and, according to the existing wording, it can include, for example, risk assessments, suitability assessments according to IDD, tariffs, etc. Nor would it necessarily benefit the consumer if all this data were passed on to other companies and it should therefore be clarified in the legal text that it is raw data that the regulation relates to. We would therefore urge the Commission to exclude enriched or proprietary data from the field of application.

We propose a different wording of art. 3, (3) of the proposed act and propose a deletion of the reference to “data generated as a result of customer interaction with the financial institution”. Alternatively, the definition could explicitly stat that the definition does not include enriched data, trade secrets or business sensitive information.

It must also be made clear that the results of the "suitability and appropriateness" assessment, as well as the "needs and demands assessment" under IDD is not included in the concept of "customer data" and that it is only the data that provided by the customer in this process, which should be covered by the term.

In general, we want a much clearer definition of customer data. Perhaps the scope could be limited to data given to the customer in the customer relationship, cf. IDD (Insurance Distribution Directive) (e.g. IPID), but not the result of the needs and suitability assessments according to Art. 20 and 30. However, this does not solve the problem for B2B insurance where there are no standard solutions or IPID.

The term "customer" should also be defined more clearly, as the definition currently is unclear. In insurance, there are many categories of persons/legal entities that use the financial products. It is the person who has the policy, other insured persons, beneficiaries, injured parties, etc. In relation to the purpose of this regulation, it should only be the person who has taken out the policy who is referred to as the customer and this should be made clear in nature. 3 (1) (2).

It is a real concern that the financial burden for the companies by starting with such a broad area of application becomes significant and can become a severe financial burden for the individual company, which is not proportional to the desired goals that are sought to be achieved with FIDA. This applies to everyone, but especially the smaller companies that are covered by the regulation's scope of application as "data holders", when it comes to the implementation of common data standards, development of APIs and consensus dashboards.

IPD therefore prefers the proposal to a use-case-driven approach, where data sharing in specifically defined areas is tested before the broad approach that the Commission has chosen. There is a provision for review after 4 years, which allows the Commission to extend the scope of application with more data or to exclude categories of data - however, there may be areas where there is no interest in the data in question or any business justification for sharing the data, but the industry will presumably still be required to build the infrastructure for sharing this data before the Commission finds that the data should have been excluded to begin with. For instance, data relating to accident insurance, which may contain information of a sensitive nature,

such as health information, which is currently is excluded from the scope of application.

In addition, data should always be retrieved at the "source", so that the data that the companies, for example, buy from other companies/data brokers cannot be accessed free of charge by simply retrieving it via a data holder in a scheme.

No protection of business sensitive data and unlimited access for technology companies

There are no restrictions on the large tech companies' (gatekeepers') ability to retrieve data in this regulation, and we are concerned about the consequences this may have for industry and customers, in relation to getting large technology-driven companies into this market.

At a minimum, we want the same restrictions on access to data as found in the Data Regulation - where "gatekeepers", covered by the Digital Markets Act, cannot access data. Furthermore, there is a restriction in the upcoming Data Regulation on the possibility of using the acquired data to offer competing products, which should also be included here if the Commission also insists that enriched data must be shared.

At the same time, we would like to appeal to the Commission to look at the cross-sectoral rules in the data regulation and ensure consistency between the two regulations when it comes to general rules on the sharing of data. If customer data also contains business-sensitive information, then the provision in the data regulation should also be introduced here – it contains a form of protection of trade secrets (if the company can demonstrate the risk of a financial loss, they can refuse to hand over data that can categorized as trade secrets).

There is generally a need to put in place clear safeguards and specific provisions to protect trade secrets or business sensitive data. Insurance companies should not be obliged to share trade secrets, company-sensitive information or enriched/proprietary data that they themselves have generated and enriched and which is the result of their own work, e.g. building risk profiles or insurance and claims models. This type of data represents an important competitive factor and innovation driver, and it must be seen in the context of an insurance company's strategy and portfolio, which differs from insurance company to insurance company.

It will not be possible to protect business secrets, especially on price models and negotiated partner prices, if the company's internal information is subject to mandatory data sharing. There is a risk that aggregation of this information will enable "reverse engineering" of the underlying price models.

These are important business secrets in the insurance industry and should therefore be kept secret.

In order to protect the insurance company's know-how, it is necessary to further specify the scope of the regulation so that it only includes raw data related to the customer and omit any result of internal data processing (enriched data) from the scope of FIDA.

Data schemes

IPD is pleased that the Commission has listened to the wishes of the industry to ensure a clear framework for responsibility and management and has focused on ensuring that the same activity and the same risk must be covered by the same regulation. Therefore, it is also positive that FISPs should meet the requirements of DORA and be subject to an approval regime at the Financial Supervisory Authority. To ensure customer data are handled with the utmost level of care and high levels of cyber security, FISP's that are not liable to fall under the DORA framework, should still demonstrate a high level of cybersecurity in order to be able to handle customer data securely.

It is our expectation that our members will also be data users themselves, and that there will be a fair amount of data exchange between the companies in the industry.

The regulation obliges data holders (financial companies) to make customer data available free of charge to the customer at his request continuously and in real time. However, data users who obtain the customer's consent to retrieve data must cover the costs of this if the financial company from which they retrieve data is a member of a data scheme. If the data holder and data user are members of different schemes, it should be the data holder who dictates which scheme applies.

We welcome an approach that seeks to ensure that standards are developed but at the same time providing that the further development of such standards is industry-led. The concept of financial data sharing schemes is therefore positive, as it leaves room for industry to develop the modalities for data sharing including data formats and API's. However, we still find it critical that the Commission has established such a broad application area and only proposes subsequently to assess whether there is a need for an exception for certain types of data.

IPD calls for a narrower approach, where the Commission would start with one or two use cases (as the Commission did with PSD II), to test whether it has the desired effect. The type of data to be shared can then be gradually expanded based on periodic evaluations of the Regulation, taking into account both the benefits and costs of making data available. A gradual imple-

mentation would also make the implementation of the regulation less burdensome for financial institutions and easier to foresee the consequences thereof.
The proposal allows for a review after 4 years, which gives the Commission the opportunity to exclude categories of data from the scope of application. However, it would have been preferable to start with a narrower scope that could be expanded after 4 years, when the need and demand has been demonstrated.

It is also important that the scope of data schemes is clearly defined, as it is otherwise left to the individual schemes to define the extent of the (customer) data to be shared. The consequence may be that it leads to schemes with different definitions of covered data – customers risk being treated differently depending on which scheme the data holder and data user are covered by.

However, the regulation should not introduce restrictions on the companies' possibilities to share data on a contractual or voluntary basis outside of data sharing schemes. The insurance industry therefore welcomes the acknowledgment in recital 50 that the proposed FIDA regulation does not affect access to, sharing and use of data on a purely contractual basis without making use of FIDA's data scheme obligations. However, such a key aspect should be included directly in the legal text rather than only being mentioned in the preamble.

FISPs must also be subject to requirements for sharing customer data

In addition, there is a lack of reciprocity in relation to FISPs, who are given access to retrieve customer data, but are not obliged to make customer data available as data holders. FISP's should also be considered a "data holder" with an obligation to pass on customer data in data sharing schemes, to ensure reciprocity in the requirements for data sharing and a level playingfield. That should be clarified in art. 3(1)(5) and art. 3 (1) (7).

Timeline

The time frame for the implementation of the regulation and the data arrangements is unrealistic. In particular, the 18 months given to get an operational data-sharing scheme in place is unrealistic and will be a challenge for most markets. The experience from PSD I, was that it took at least 4 years to get the infrastructure and APIs in place.

Being able to feed data into a data scheme will probably take even longer, as it requires adaptation of the digital infrastructure in the individual company. It is also unclear whether these costs in connection with making data available through a scheme will be covered by the remuneration clause.

In addition, Article 12 of FIDA requires FISPs to have been authorised by the competent authority of a member state in order to be eligible to access customer data. This approval process means that FISPs will only be able to join a data sharing scheme after a set period of time, which further reduces the time available for all scheme members to discuss and agree upon the scheme's operation and relevant standards. It may therefore be more appropriate to allow a period of 24 months for the setting up of the schemes, identification of use cases and the development of the relevant governance rules of the scheme, as well as the relevant standards.

Once the schemes have been set up, development of the technical infrastructure and IT solutions by data holders will take significant additional time which does not seem to have been taken into account in the proposal. A second stage of 18-24 months would therefore be necessary.

Positive that it is only data with the customer's consent
It is positive that there is more focus on strengthening the customers' consent management, but in general we may well be concerned that some of the requirements in the regulation end up as a cost driver for the sector without necessarily providing more value for the customers.

We agree that it is important to secure customers' trust. Therefore, there is a requirement that data users who gain access are pre-approved by a supervisory authority. However, it is inappropriate that there is no requirement that the FISPs must return data to schemes, as they can also become data users when data is used for their own purposes.

Compensation for making data available
It is also positive that the bill contains provisions on cost recovery in relation to making data available and developing APIs for this – if the incentives for data sharing are to be increased, it is a prerequisite that there is cost recovery – it must be the experiences from the PSD II regulation from the banks, where this has been a challenge.

However, it is important that it is cost-neutral to comply with the requirements to make data available, otherwise it will be the customers who end up bearing the burden in the end. This means that it must be possible to cover both development and operating costs in connection with the establishment of a data scheme.

Again, there is a lack of coherence to the horizontal regulation in the Data Regulation, specifically art. 9, which sets the framework for cost recovery for access to data according to this framework. The method of calculating compensation is more realistic as it allows for remuneration for the costs of formatting data, dissemination of data and investment in collection and pro-

duction of data and may include a margin. This provision should also be included in FIDA, so that there are uniform rules for data sharing across the different sectors in the EU.

Trust in data security is central, and it is important that customers can control where their data is sent and withdraw consent. It is therefore crucial that there are requirements for the data users who gain access, that data is only used for what has been consented to and that they have a sufficiently high level of IT security. This seems to be reflected in the proposal, but the cost of developing consent dashboards can be high, because it will require access to a number of data sources internally within the company and with their partners. These costs are not covered by the remuneration and must be borne by the individual company and eventually their customers.

It is also not clear what is meant by "without undue delay, continuously and in real time" in Article 5. Some types of information may not be fully digitized or available in a structured format, within the company. Exchanging these types of data, would require a manual process or costly it-development.

The protection of business sensitive information is central and the incentive to innovate will be reduced if the insurance companies have to deliver enriched data into a data scheme. It is worth focusing on protecting innovation efforts, as mentioned in recital 28 of the Data Regulation.

No focus on cross-sectoral data sharing

We believe it is a missed opportunity not to have more focus on cross-sectoral sharing of data, as this could greatly benefit both customers and insurance companies. Data from other sectors, such as data from cars, climate data, health data, etc., could promote more innovation within the sector and the development of new and better insurance and pension products.

Need for proportional sanctions

The proposed regulation contains sanctions in art. 20 ff. It is undisputed that the extensive data access and exchange requires a sanctioning mechanism.

However, the measures proposed in the draft law are disproportionately strict in their scope, seriousness and scope. One result of this can be that it puts a damper on innovation and data exchange, because data owners and data users consider the risk of a breach to be too great.

Specifically, the recovery of profit according to Article 20, paragraph 3, letter c), as well as the determination of the maximum compensation amount in accordance with Article 20, subsection 3, letter e), is reassessed. The temporary ban on exercising a management function in a financial company, which can be increased to up to 10 years, also seems very far-reaching in relation to the nature of the violations and there should be more focus on the proportionality of the sanctions. The possibility of daily fines under Article 21 is also

likely to lead to risk aversion, rather than a willingness to innovate on the part of the companies.

In many cases, the data to be shared will be personal data that is already covered by the GDPR and its provisions on infringements. Since there is overlap here, it is positive that recital 36 and art. 5, allows for cooperation between authorities. We encourage the legislature to re-evaluate whether the extensive provisions on fines in FiDA are necessary in this form and are not already sufficiently regulated by the GDPR.