GDV German Insurance Association

POSITION PAPER

Position Paper

of the German Insurance Association (GDV)
ID-number 6437280268-55

on the proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a **framework for Financial Data Access** and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010, (EU) No 1095/2010 and (EU) 2022/2554

GDV

Gesamtverband der Deutschen Versicherungswirtschaft e. V.
German Insurance Association
Wilhelmstraße 43 / 43 G, 10117 Berlin
Postfach 08 02 64, D-10002 Berlin
Phone: +49 30 2020-5000 · Fax: +49 30 2020-6000

Rue du Champ de Mars 23, B-1050 Brussels
Phone: +32 2 28247-30 · Fax: +49 30 2020-6140
ID-number 6437280268-55
www.gdv.de

Contact
Operations and IT

E-Mail
bdit@gdv.de

Executive Summary

The German insurance industry does not support the FIDA Regulation in its current form. The proposed legislation lacks provisions to appropriately protect customers' personal data and requires tremendous international standardization. As such, the regulation is a significant intervention in the business of insurers. There is no evidence that customers will request data from financial institutions on such a large scale. However, as there is an obligation to transfer data, and thus to design and implement the required data standardizations and systems, considerable costs and use of IT-capacities is unavoidable. The financial risk for this initially lies with the insurers.

FIDA comes at a critical time for the industry. On the one hand, the implementation of the more recent EU regulations is tying up considerable capacities (e.g. DORA, SFDR, AI Act, Data Act), while on the other hand, international competitors are investing heavily in new, AI-supported business applications. European insurers must be able to invest in the future on a comparable scale if they are not to be left behind by the competition.

Substantial improvements are still needed to make the regulation a success for data holders, data users and customers. **We do ask to continue the constructive discussions and not to conclude the procedure prematurely.**

Key points for improving the regulation

1. Narrowing the scope of the regulation

→ **Exclude accident insurance** from the scope, similar to health and life insurance, due to the processing of sensitive personal data
→ **Limit the definition** of customers **to consumers and micro enterprises**
→ **Exclude large risks,** as defined in relevant EU regulations, from the scope
→ Support the definition for **occupational pension schemes** that requires **accessibility** for all **interested consumers**

2. Strengthening the role of Financial Data Sharing Schemes (FDSS)

→ Ensure **data access** occurs **only within defined Financial Data Sharing Schemes** for transparency and control

3. Limiting the amount of data to be shared

→ **Narrow** the **definition** of customer data to raw data provided by customers to protect competitive advantages and trade secrets
→ Clarify that only customer's own data, **not third-party data**, must be shared
→ **Completely exclude data under Art. 9 GDPR** from the scope
→ **Define** and clarify that **real-time data** should only be provided where relevant and feasible
→ **Do not** further **extend** the scope of the **data use perimeter**

4. Clarifying the role of financial information service providers

→ Require that only EU subsidiaries of third-country providers can be authorized as FISPs

5. Making the implementation feasible

→ Support a **cut-off date** to ease the technical burden and costs of implementation
→ Set up a **phased implementation** by product category with no insurance-specific products at "level 1"
→ Clarify the **relationship** between the obligations under **FIDA and** the **GDPR**

1. Narrowing the scope of the regulation

FIDA's scope of application is not only a challenge for data holders, but also unfeasible given the vast amount of data included. According to GDV's estimates, up to 400 million life and non-life insurance contracts could be affected in the German market alone. Both the large number of contracts and the variety of products they contain are a significant impediment in its implementation as well as a cost driver for the companies implementing the regulation.

For the success of the regulation, it is therefore crucial to achieve a product-related restriction of the scope of application. From the insurance industry's point of view, there are several starting points for this:

→ Accident insurance

Since the Commission sees special risks for customers in the sharing of health insurance and life insurance data, apart from IBIPs, PEPPs and occupational pension products, the FIDA proposal excludes these products from the scope of application. The exclusion is of paramount importance because special categories of personal data within the meaning of Art. 9 GDPR are typically processed on a large scale within the scope of these products.

This also applies to the German accident insurance[1], as this is a product in which sensitive personal data is typically processed to a considerable extent, especially in the event of a claim. The considerations that apply to health insurance and the parts of life insurance not covered by the FIDA regulation (e.g. term life insurance, occupational disability insurance) are also valid here. This assessment is reflected, for example, in the fact that in Germany special confidentiality obligations apply to life, health and accident insurance in accordance with section 203 of the German Criminal Code (StGB). In the German translation, recital 19 of the FIDA proposal also provides for equal treatment of accident insurance with health and life insurance. For all these reasons, we strongly recommend reflecting this in the legal text by excluding accident insurance from the scope of application in the same way as life and health insurance.

→ Corporate customers

The purpose of the FIDA Regulation suggests that the new data sharing mechanisms are primarily aimed at private end customers. Contrary to this, however, business customers and large risks are also part of the scope of application. An

[1] German private accident insurance primarily provides a lump-sum or pension benefit if an accident results in permanent mental or physical impairments or leads to death. It provides coverage world-wide and around the clock.

alignment by narrowing the scope is therefore justified.

Business customers generally receive customized insurance solutions tailored to the specific situation of the respective company. Insurers' inhouse and external experts are involved to develop offers and solutions in close communication with these companies. The contracts are the result of individual and complex risk assessments and contain business secrets of insurers and their customers.

Also from an operational perspective, there are challenges with business customers. For each company, any number of employees might be granted permission to work with FIDA. Thus, completely new, and costly authorization management systems would have to be created, the maintenance and upkeep of which would be bureaucratic and time-consuming for both sides.

Due to the small number of contracts in conjunction with the low level of standardization, business customers are neither FIDA-ready nor FIDA-suitable. We therefore propose to restrict the customer definition in Art. 3 (2) to consumers and micro enterprises.[2]

→ Large risks

In addition to business customers, large risks are also implicitly covered by FIDA. These are defined in Article 13 of Directive 2009/138/EC on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II) and respective local laws, e.g. § 210 German VAG. Large risks include transport and aviation risks, i. e. rail vehicles, aircraft, ships and goods in transit.

Due to the clear commercial nature of large risks and the strong and worldwide co-insurance concept of these insurance markets, those insurance risks need to be excluded.

Large insurance risks have historically been treated differently due to their size and international nature, as reflected in various regulations such as the non-life insurance directives, the Rome I and Brussels I Regulations, and the Solvency II Directive. These regulations establish a clear distinction between insurance contracts that require protective measures and those, like large risks, where such protections are not necessary, allowing greater contractual freedom. The Solvency II Directive and the Insurance Distribution Directive (IDD) similarly exempt large risks from certain regulatory obligations, aiming to prevent unnecessary bureaucratic burdens on insurers.

[2] ECON Report, 30.04.2024, Art. 3 – Par. 2

For this reason, it is prudent to exclude large risks from the scope of the FIDA Regulation. To this end, the product definition in Art. 2 (1) (e) should be expanded as follows: *"non-life insurance products [...]* ***with the exception of large risks in accordance with Directive 2009/138/EC.****"*

→ Occupational pension schemes

In line with the ECON report[3] and the Council progress report[4], we support the amended definition of occupational pension schemes, and particularly the clarification regarding the accessibility to all interested consumers.

The reason for that is that national tracking systems in a growing number of Member States already achieve the objective of pension tracking and providing comprehensive information for these products in one place.

2. Strengthening the role of Financial Data Sharing Schemes (FDSS)

→ Exchanging data only through FDSS

The aim of the EU Commission is to give consumers and firms better control over access to their financial data.[5] To this end, data holders and users are to provide the infrastructure required for exchanging the data and organize themselves in so-called Financial Data Sharing Schemes (FDSS).

The idea of FIDA is that FDSS are based on a common contractual framework, clear and transparent governance rules and mechanisms for compensation, dispute resolution and liability. This way, the FDSS is intended to enable a standardized exchange of data that complies with the applicable data protection regulations.

To strengthen the role of the FDSS, the Belgian Council Presidency proposed to add a paragraph to Article 6(1), stipulating that data may only be exchanged within the defined FDSS[6]. We fully support this proposal, as it prevents the emergence of uncontrolled data flows, strengthens the transparency of data flows, and avoids risk for consumers and other stakeholders.

In contrast, non-standardized traffic outside the FDSS will result in the customer only having a limited overview of their data and less control over the data sharing. In addition, the complexity of the overall system increases, which may lead to acceptance problems for the customer.

[3] ECON Report, 30.04.2024, Art. 2 – Par. 1 (c)
[4] Council Progress Report, 14.07.2024, Art. 2 – Par. 1 (c), p. 79
[5] EC Proposal for a Regulation, 28.06.2023, Explanatory Memorandum
[6] Belgian Presidency's Progress Report on the Financial Data Access Regulation, 14.06.2024, No. 25 in conj. with Art. 6

Also, from an operational point of view, there are good reasons against data exchange outside the FDSS. For example, the requirement in Title II to provide the data continuously and without undue delay can hardly be fulfilled without an orderly and structured framework.

There is also a risk of misguided incentives and evasive maneuvers, as no remuneration is provided for data access outside the FDSS. This could jeopardize the success of FIDA as a whole, since many data users could avoid joining the schemes if there is an alternative way to receive the data free of charge and without investing in necessary software interfaces. From the data holder's perspective, a standardized approach limits the risks in case of data delivery. If there is no assurance for the data holder that data needs to be provided in line with the standards, data transmittal may have to be refused.

→ Operationalizing the FDSS

For an FDSS to work effectively, clear and effective governance rules are an important prerequisite. FIDA provides that contractual arrangements on the data to be shared within the schemes are to be agreed upon. The draft regulation gives no indication what legal form such an agreement should have.

In our view, it is important that the data holders are appropriately represented in the internal decision-making processes of the FDSS, as stated in the EU Commission's draft (Art. 9 Para. 1 a, i). A one-sided ability[7] of a minority of data users to expand the data sets to be shared in a FDSS would contradict the balanced approach and should therefore be rejected.

3. Limiting the amount of data to be shared

→ Narrower definition of "customer data" within the meaning of Art. 3 No. 3

The Commission's draft regulation provides for an almost unlimited, very broad definition of customer data in Art. 3 No. 3, according to which, in addition to the personal and non-personal data transmitted by the customer, data generated as a result of the customer's interaction with the financial institution is also covered. We fully support the view that this definition is not clear enough and is too broad.

Customer data should only be raw data that the customer has provided to the financial company. It should be ensured that enriched and processed data is excluded from the scope of the regulation. The preparation, enrichment, digitalization, structuring etc. of data provided by the customer is part of the company's internal economic value creation. This should not have to be passed on to competitors

[7] ES & SE Non-paper, 14.05.2024, p. 3

because otherwise it would distort competition. Furthermore, there is a risk that competition-sensitive information of the data holder and data that may also contain business secrets will fall within the scope of the regulation. It is therefore important to effectively prevent reverse engineering.

We think that even the amended wording proposed by the Council presidency is not sufficiently clear. It should be made explicit in the wording that only raw data provided by the customer to the data holder is covered by the definition.

In particular, the new wording, which refers to transaction data and no longer to "data generated as a result of customer interaction with the financial institution", does not make it possible to determine with certainty which data is covered by the term "transaction data". This does not fulfil the Council's objective of sharing only the data that the customer has made available to the company. The definition should describe the relevant data explicitly in this way.

→ No sharing of third-party data

The Council presidency has addressed the issue that data of third parties could be processed by the data holder. If more than one customer is involved, the Presidency is considering clarifying in a recital that the additional customer must consent to the transmission of their data.[8]

Third-party data is also affected in other practically significant constellations in the insurance industry. For example, in third party liability insurance not only data of the insurance customer but also information about third parties injured by the customer is stored, including particularly sensitive health data. In legal expenses insurance, the insurer has information about the opponent in a lawsuit for which legal expenses insurance covers the costs. It cannot be at the customer's discretion whether the data of these persons is passed on to a data user in accordance with Art. 5 of the FIDA Regulation. This applies in particular to personal data, but also to business secrets. Third party data is also involved if a beneficiary is entered into the contract.

It should therefore be explicitly clarified in Article 3 (3), or at least in a recital thereto, that customer data is only data of the customers themselves, but not data of third parties. In the event that third-party data is collected, it must at least be ensured that the data holder only has to transfer the data if the customer or data user clearly proves that there is a legal basis for the data transfer in their relationship with the third party and that, in the case of personal data, there is a basis for authorization for the data transfer under the GDPR.

[8] Hungarian Presidency Note, 03.07.2024, No. 6.1.

→ Mitigating the risks associated with special categories of personal data

Special categories of personal data within the meaning of Art. 9 (1) of Regulation EU (2016/679) should be expressly excluded from the scope of the FIDA Regulation. The corresponding proposal by the Spanish Council Presidency was rightly taken up by the Belgian Council Presidency, as it met with no resistance from the Member States.[9]

As the loss or unlawful use of sensitive data can lead to considerable disadvantages for customers, the Council's position should be maintained on all accounts. This will also prevent any inferences being drawn from this data that could be detrimental to consumers. The proposed wording from the ECON Committee's draft report[10] would not achieve this goal, as it only regulates what is already applicable law under the GDPR.

→ Practice-oriented definition of “real-time” data

A clearer definition of real-time data should be included in the FIDA Regulation. On the one hand, the term as used currently, is perceived very differently by different stakeholders. On the other hand, the definition of real-time is a major prerequisite for the design of the IT systems, network infrastructure and APIs underlying the data exchange in FIDA.

To improve legal certainty, we therefore propose amendments to two points:

Firstly, it should be clarified in Art. 4 and 5 that real-time data delivery only must take place where this is "relevant and feasible". While there is a very high transaction density for payment transaction data (several times a day), this is not the case for insurance contracts. In insurance, relevant changes to data records only occur occasionally, depending on the type of policy.

Secondly, real-time should refer to the period between the request for data by the data user or customer and the provision of the data by the data holder. Therefore, the following definition of real-time data should be included in Article 3: *"Real-time data means the state of the data as it exists in the data holders' systems at the time of the customer's or data user's request. No new data ought to be created because of the request."*

[9] Belgian Presidency’s Progress Report on the Financial Data Access Regulation, 14.06.2024, No. 33
[10] ECON Report, 30.04.2024, Art. 2 – Par. 3b

→ **Maintaining the status quo of the data use perimeter**

In GDV's view, the EU Commission's original proposal on the data use perimeter should be retained.

Firstly, the Commission proposes guidelines, which are a suitable instrument because product and market requirements can change quickly. EIOPA has the necessary expertise to be able to respond appropriately with the guidelines. More importantly, technical regulatory standards would be less effective, as they do not have the necessary flexibility.

Secondly, the intended scope of the data use perimeter is based on recital 18, according to which the EU Commission sees an increased risk in data processing in life, health, and sickness insurance[11]. Accordingly, the data use perimeter is restricted to the aforementioned insurance sectors and rightly does not include non-life insurance.

Regarding the objective of the data use perimeter, it must be taken into account that any intervention in the risk assessment and pricing can have a significant and lasting impact on companies' business models. Unlike social insurance, the private insurance model is not about a systematic redistribution between people with high and low risks. Because taking out private insurance is mostly voluntary and a matter of personal choice, one of its fundamental principles is the orientation of the premium paid in relation to the risk or the expected benefit from the insurance contract. Risk-relevant factors therefore have an impact on the decision to take out an insurance policy and the level of premiums. Higher premiums or, in extreme cases, exclusion from insurance cover are therefore not unlawful discrimination, but a permitted and even necessary differentiation to the benefit of the community of insureds.

4. Clarifying the role of financial information service providers

The Council is currently discussing whether FISPs from third countries should only be authorized if they have a subsidiary or branch in the EU. The need for a subsidiary in the EU is correctly described as a prudent and proportionate measure that ensures control over European consumers' data, effective supervision and a level playing field with FISPs based in the EU.[12]

Another argument for the exclusion of FISPs from third countries – without a respective subsidiary in Europe – is the difficulties under data protection law, which make it impossible to exchange personal data within a reasonable time frame in a

[11] EC Proposal for a Regulation, 28.06.2023, Recital 18
[12] Presidency Questionnaire, 03.07.2024, Exclusion of third-country FISPs

permissible manner.

The transfer of personal data to third countries under Art. 44 et seq. GDPR is only possible under strict conditions. Following the Schrems II judgement of the European Court of Justice[13] the examination of the legality of the transfer of personal data to countries without an adequacy decision by the EU Commission requires considerable effort. Assessing the legal situation in third countries and examining the measures required by the EDPB to protect the rights and interests of data subjects is time-consuming and seldom leads to a legally certain result.

Consent in accordance with Art. 49 para. 1 lit. a) GDPR can justify the transfer of data. However, it is uncertain whether the requirements of the data protection authorities for such consent, in particular its sufficient transparency, can be met. At the very least, this also requires a time-consuming examination, which stands in the way of a rapid data transfer.

A complete exclusion of FISPs in third countries avoids these problems.

5. Making the implementation feasible

→ Cut-off date for existing contracts and historical data

FIDA does currently not distinguish between new and existing insurance policies. The implicit inclusion of existing contracts places a disproportionate burden and great technical effort on data holders. Due to the historically evolved IT landscapes in conjunction with the long-term nature of the insurance business, companies generally use several generations of portfolio administration systems in parallel. In the case of older tariff generations, these systems are often in a so-called passive maintenance mode. The systems are maintained for as long as the existing contracts are active and then gradually switched off. Far-reaching technical interventions would be required by data holders in order to make these databases compatible with FIDA. This would not be economically viable.

Hence, we strongly support the implementation of a cut-off date for existing contracts. A reasonable compromise would be to opt for the date of entry into force as the cut-off date. Due to the two-year transitional period until the law becomes applicable, a balanced number of existing contracts would still fall within the scope of application.

A further reduction of the data to be shared by removing historical data from the canon of data should also be supported, as this would reduce the initial burden on data holders when implementing the FIDA regulation. In any case, the

[13] ECJ, 16.07.2020, case C 311/18

decision for or against historical data should be dealt with at the level of the regulation to ensure a consistent implementation across all schemes.

→ **Phasing in accordance with the FIDA-readiness of the product categories**

GDV welcomes the discussions on a phasing in of the FIDA regulation according to the FIDA-readiness of the different product categories in Art. 2 (1).

This approach ensures that data owners can implement the extensive requirements of the regulation in a staggered process. It also takes account of the fact that insurance products in the scope of application are highly complex and have a low degree of standardization.

Motor insurance, for instance, should not be classified as FIDA-ready, as it encompasses a wide range of contract types, policies, and individual customer needs. The data processed in motor insurance, which includes driving behavior, claims history, and insurance information, originates from various sources such as telematics data, garage reports, and damage assessments. This diversity makes it challenging to establish uniform standards that apply to all scenarios, which is why motor insurance is not fully FIDA-ready.

We strongly recommend that insurance products are not categorized in the so-called ‘level 1’ of the phasing-in.

→ **Clarification of the relationship between the obligations under FIDA and the GDPR**

The interaction of the obligations under FIDA and the GDPR may lead to practical challenges that need to be resolved before the regulation enters into force. Specifically, the data holder must be able to ensure that there is a valid legal basis under the GDPR in cases where personal data is requested under FIDA Art. 5. For example, he must be able to rely on the fact that consent fulfils all the requirements of the GDPR, in particular that it is informed and freely given. It must also be clear what role the dashboard plays in informing the customer in accordance with Art. 13 (3) or Art. 14 (4) GDPR and the data protection implications of withdrawing the permission via the dashboard.

Berlin, 27 August 2024

Contact: Operations and IT

Email: bdit@gdv.de