

17 November 2023

Transitioning from Open Banking to Open Finance: DIGITALEUROPE's position on the Financial Data Access Regulation (FIDA)

Executive Summary

DIGITALEUROPE supports the shift from Open Banking to Open Finance through an expansion of strategic data-sharing partnerships. The Financial Data Access Regulation (FIDA) can bring multiple benefits to the EU economy and society, contributing to financial inclusion, enhanced transparency, accessibility and accountability for consumers, and ultimately, building trust in data-sharing in the financial services industry.

FIDA should provide industry with the necessary incentives and tools it needs to productively engage in data-sharing.

Any data-sharing framework should be voluntary, customer-centric and cross-sectoral to harness the potential of the data economy. This includes alignment with the Data Act – to avoid asymmetries to the detriment of the financial sector. This also includes granting industry sufficient time to develop data-sharing schemes. A too-short timeline leading to the Commission adopting binding data-sharing measures via a Delegated Act to specify the modalities will lead to inconsistent schemes that are not fit for purpose.

It is vital to improve FIDA. We call on the EU to focus on the following:

1. **Data-sharing schemes:** Establish minimum requirements to develop schemes, to avoid a patchwork of different rules and

modalities per schemes and increase the timeline for industry to develop schemes (Art.9).

2. **Customer data:** Provide a clear and unambiguous definition of customer data in scope, to be made available by data holders. The scope should explicitly exclude derived, inferred, or otherwise further processed data (Art.3(3)).
3. **Legal certainty on the rights and obligations for data holders and data users:** The definitions of data holders and data users should be clarified to for instance prevent a situation where a data user might become a data holder by simply accessing or collecting customer data.
4. **Alignment with the Payment Services Regulation (PSR)**
Proposal: FIDA and the PSR must be aligned in their obligations for data holders to make available permission dashboards for customers/data owners (Art. 8).
5. **Compensation:** Ensure that FIDA allows for compensation models that allow both for data holders to be compensated for making data available and managing data access, providing incentives at the industry level, as well as a model that allows data users to participate in the Schemes (Art.10(1)(h)).

 **Table of contents**

- **Executive Summary 1**
- **Table of contents..... 3**
- **Scope and Definitions..... 4**
 - Calling for a use-case based approach 4**
 - Categories of data under scope 4**
 - Entities and Clients under scope 6**
- **Data Access (Art.4 and Art.5) 7**
- **Permission dashboards (Art. 8) 9**
- **Financial Data Sharing Schemes (Title IV)..... 11**
- **Eligibility criteria (Title V) 13**

Scope and Definitions

Recommendation: *FIDA should be explicit and unambiguous about the data included in scope. The current wording of the regulation leaves room for interpretation, which can lead to inconsistencies in its application and enforcement. A clear and precise definition of the scope of data will provide legal certainty for all stakeholders, ensuring fair and consistent compliance.*

Calling for a use-case based approach

DIGITALEUROPE understands the objectives set out in the FIDA Proposal in support of the transition from Open Banking to Open Finance. However, **we call on regulators to first define distinct end goals, in the form of well-defined use cases, like the approach taken in the insurance sector.**¹

The lessons from PSD2 underscore **the need to establish use cases as the starting point and working backwards from these.** This will allow us to visualise the practical impacts of open finance² and to understand which data sets should be made accessible. This approach will help to avoid replicating a scenario where (as in PSD2) datasets were made available via provisions placed on industry, without first understanding the why.

Categories of data under scope

Increased data-sharing and data usage raises the complexity of accurately establishing data ownership and ensuring legal compliance and that the right safeguards are observed by the parties across the value chain.

FIDA revolves around the sharing of financial data and thus, such ‘data’ should be clearly defined.

¹ EIOPA, *Discussion paper on Open Insurance: an exploratory use case in the insurance sector* (24 July 2023): <https://www.eiopa.europa.eu/system/files/2023-07/EIOPA%20Open%20Insurance%20use%20case%20-%20Insurance%20Dashboard.pdf>

² DIGITALEUROPE, *The digital finance revolution: unleashing the power of inclusion, growth, sustainability & security* (18 April 2023): <https://www.digitaleurope.org/resources/the-digital-finance-revolution-unleashing-the-power-of-inclusion-growth-sustainability-security/>

- ▶▶ **Clear definitions:** First, DIGITALEUROPE believes it is essential to enhance clarity on the data-sharing schemes (including on the number of them, who their participants will be, participation requirements) as well as on the definition of a Financial information Service, and a Financial information service Provider (FISP). This will ensure that the Council and the European Parliament outline a more workable, precise definition of in-scope customer data under Art.3(3) of FIDA.

Regarding the definition of customer data, mandated data sharing should be restricted to ‘raw’ data, i.e. data that has not undergone any processing beyond mere collection. The scope should exclude derived, inferred or otherwise further processed data as this would inherently impinge on proprietary information, commercial confidential data, trade secrets, and intellectual property rights. This is in line with our position on the Data Act and in line with the EDPS opinion³ on FIDA.

- ▶▶ **Including payment account data within FIDA:** Once FIDA has been set up and is functioning well, it would be **valuable to consider whether its scope should be expanded to include payment data (that is currently in scope of PSR/PSD3) and to establish one framework.** The establishment of two different frameworks and sets of rules for what falls under the umbrella of financial data may lead to compliance and regulatory complexity. In the interim period, the search for consistency across regulations should be a clear objective (e.g. in the way data-sharing is presented to customers through the permission dashboards). Payment data can provide invaluable insights into consumer behaviour and financial health, thereby fostering financial innovation and reducing financial exclusion risk.
- ▶▶ **‘Suitability and appropriateness data’ collected by financial institutions for the purpose of carrying out assessments should be excluded from the scope of FIDA:** This data is tailored to the internal processes of each entity. A data user applying the same data to other procedures may carry the risk of making incorrect investment or advice decisions. Furthermore, the details of each entity's suitability and appropriateness assessments constitute a distinctive feature of each entity's advice, and the standardisation of these procedures can lead to low quality of services. Likewise, it should be clarified that the

³ EDPS Opinion 38/2023 on the Proposal for a Regulation on a framework for Financial Data
Access: https://edps.europa.eu/data-protection/our-work/publications/opinions/2023-08-22-edps-opinion-382023-regulation-framework-financial-data-access_en

results of the suitability and appropriateness assessments, as well as the demands and needs assessment under the Directive on insurance distribution (IDD), should not be within the scope of customer data. Only the data that is provided by the customer as part of this process should be included. We are concerned that the FIDA framework may increase the current IDD obligations regarding information gathering in respect of the clients' demands and needs assessment.

- ▶▶ **The scope of the creditworthiness assessment data should be clarified:** Data may vary from one entity to another. Risk assessment is a distinctive factor of each entity that must be maintained to guarantee a wide credit offering and diversity. **The data used to assess the creditworthiness of natural persons must remain outside the scope of the Regulation, as stated in recital 9.**
- ▶▶ **The list of data derived from investment accounts should be limited,** eliminating the part of the proposed Article 3(9) which refers to *“other data points relating to lifecycle events of that instrument”* which is disproportionately broad, as are its implications.

Entities and Clients under scope

- ▶▶ **Certification of FISPs:** We welcome FIDA introducing an authorisation regime for third parties to access data through the creation of the Financial Information Service Providers (FISPs). However, we would point to a few shortcomings that should be addressed by legislators and to the **need for clarification on what constitutes a FISP**. This is also mentioned under paragraph 43 of the EDPS opinion of FIDA⁴, which compares it to an account information service (AIS) under PSD2 where, unlike under FIDA, there is a clear definition of what the service entails.
- ▶▶ **Data holder and data user definitions:** The definitions of “data holders” and “data users” should be clarified further to prevent a situation where a data user might become a data holder by simply accessing or collecting customer data.
 - **Additionally, the proposal does not acknowledge the potential for FISPs to play a dual role:** to wear the data user

⁴ EDPS Opinion 38/2023 on the Proposal for a Regulation on a framework for Financial Data
Access: https://edps.europa.eu/data-protection/our-work/publications/opinions/2023-08-22-edps-opinion-382023-regulation-framework-financial-data-access_en

“hat” in one scheme and the data holder “hat” in another – or even, wear both “hats” within the same scheme. **This raises ambiguity on how they are to manage their roles effectively in a way that ensures transparency in their operations.**

- ▶▶ **Interplay between PSR and FIDA:** If PSR and FIDA were ever to be merged in the future, **the existing rights of licensed entities should be properly taken into account in order not to disrupt existing downstream business models**, such as accounting.

Data Access (Art.4 and Art.5)

***Recommendation:** Real-time data sharing should not be mandatory where it is not technically feasible, or where the confidentiality, integrity and availability of data can be compromised.*

Real-time data sharing should not be mandatory where it is not technically feasible or where the confidentiality, integrity and availability of data can be compromised. Just as the GDPR sets limits to real-time sharing, and just as the Data Act acknowledges that real-time data sharing should only occur where relevant and where technically feasible⁵ **the FIDA should at the very least account for the risks and difficulties with sharing large volumes of diverse data in real-time.**

However, **in order for data holders to share in-scope data with customers or third parties (albeit not in real time), DIGITALEUROPE recommends that data be shared through already-existing APIs.** These would allow data access in an efficient and secure way. The implementation of PSD2 has provided industry with a good example of how this could work.

Whilst DIGITALEUROPE members understand and agree that data-sharing is important, mandating that this be done ‘continuously and in real-time’ could pose significant challenges not only for industry but for the EU as a whole. Any data-sharing framework must incorporate proportionality (both on the data user and on the data holder sides), allow for innovation, and align with other

⁵ Data Act, Art.4(1)

data sharing frameworks. **Real-time data sharing presents the following challenges:**

- ▶▶ **Security risks:** Not only does providing continuous and real-time access to data **increase the risk of unauthorised access, data breaches, and other security threats but it is important to highlight that when it comes to financial data-sharing, there is a risk to the entire financial system.** Proper safeguards will have to be implemented to ensure data security for the EU and its citizens.
- ▶▶ **Legal and ethical considerations:** **Personal data privacy, intellectual property rights, and other ethical considerations must be considered** when releasing data.
- ▶▶ **Challenge of managing permissions:** The obligation on the data holder to manage permissions and access in real-time again poses several challenges including **ensuring data security, collecting the appropriate data, integrating distributed data sources, costly resources required to analyse the data,** ensuring scalability, performance of the infrastructure, and maintaining data quality.
- ▶▶ **Operational challenges:** Providing continuous access to data will pose operational **challenges associated with data storage, management, and distribution.**

Alignment with data protection laws: It is essential to ensure that access to, and processing of, personal data by the data user is fully aligned with data protection laws. In doing so, we recommend clarifying that data users can rely on any of the legal grounds under the General Data Protection Regulation (GDPR)⁶ for the processing of customer data under FIDA.

⁶ GDPR, Article 6.

Permission dashboards (Art. 8)

***Recommendation:** Ensure alignment with the PSR proposal's obligation for data holders to make available permission dashboards for customers/data owners.*

We welcome the Proposal's inclusion of the obligation on data holders to offer permission dashboards to customers – dashboards will build trust between customers and data sharers, promote data democratisation, enable easy access to data and insights and more. **To reap these benefits however, a few points must be addressed:**

- ▶▶ **Industry principles for dashboard development:** The requirements for configuring the permission dashboards must be high-level, establishing general principles and leaving flexibility to the Payment Service Provider (PSP) in configuring the details. Permission dashboards can become complex and challenging to manage, especially when dealing with multiple stakeholders across various organisations. The absence of an industry standardised approach to permission management and lack of standardised dashboards pose a significant barrier to enhancing transparency, building trust and truly enabling data-sharing.
- ▶▶ **Consistency of dashboards:** There is a need for the legislator to safeguard the consistency of permission dashboards across FIDA and PSR. This includes **allowing data holders to manage data permissions stemming from both FIDA and PSR through a single permission dashboard.** The establishment of two different frameworks and different rules for financial data sharing (FIDA and PSD3/PSR) would hinder customer permission management and also entail higher operational difficulties for industry as the dashboards will require significant resources to implement (as abovementioned, by including payment account data within FIDA, all financial data could be shared through a single dashboard more easily). **Seamless alignment across both regulations is of the utmost importance to avoid confusion on the consumer side, and unnecessary complexity for industry.**
- ▶▶ **Clarity on duration of access:** Data holders must have clarity on the duration they must provide data access to data users to avoid mismanagement of data permissions.

- ▶▶ **Alignment with GDPR principles:** It is essential to ensure that access and processing of data by the data user is fully aligned with the GDPR principles such as purpose limitation and data minimisation.
- ▶▶ **Dashboards should not replace contract mutation tools for the customer:** Permissions should be managed through the data user, who advises the data holder, who then amends the permission dashboard. This is **because there is a concern that dashboards may create a parallel ‘contract’ universe. A contract exists between parties and any change can be effective only when agreed upon between those parties and a termination must be invoked by the one party to the other.** These are the bases of contract law.

The dashboard allows a customer to make changes to its contract with another party via (the dashboard provided by) the data holder. This should never be the case. The data holder could be held liable by the customer for not correctly/in a timely manner passing on the relevant contract change to the data user, and customers must honour the terms of their contracts with any service provider and can only make changes directly and in agreement with this service provider.

- ▶▶ **Remove Article 8(2)(c):** The provision allowing customers to re-establish any withdrawn permissions via dashboards **could create contractual challenges if the conditions for access have changed since the time the permission was granted.**
- ▶▶ **Clarity of responsibilities:** It is also relevant to define a clear framework of responsibilities among the different participants (especially data holder and data user) other than a model based on best efforts (Art.8.4). There will be cases where the permission, permission withdrawal and potential re-establishing of a permission, will happen bilaterally between the data subject and the data user while the obligation of updating and displaying this lies with the data holder.

Financial Data Sharing Schemes (Title IV)

***Recommendation:** The timeline to develop the data-sharing schemes should be appropriate to the standard pace of business discussions with regards to developing data sharing partnerships between multiple actors.*

The proposed approach for voluntary, industry-driven, flexible, financial data sharing schemes is a positive approach in contrast to earlier suggestions for mandated participation from the outset. However, we see the need for the Commission and the co-legislators to work with industry to establish minimum requirements to guide industry to develop these schemes in a way that is feasible to implement and use for both data holders and data users. **This will allow overarching consistency of the schemes and avoid a situation where multiple memberships in financial data sharing schemes will lead to a patchwork of different rules and modalities per scheme.** For instance, if a data holder/user is participating in four different schemes, will they have to develop and abide by four different compensation models? This would be complex and cumbersome to manage.

Minimum requirements should be established to ensure a minimum level of consistency across all schemes. They should be developed for:

- ▶▶ **Compensation:** Given the added costs for data holders to develop the infrastructure to enable and manage data access permissions as well as enabling data access by third parties, it is urgent to clarify compensation rights. FIDA must allow data holders to develop commercial compensation models, that enable cost recovery at a minimum, in line with the EU Data Act. To align with the Data Act, FIDA should be based on a “reasonable compensation model” that may include a margin. This margin should be understood not as a means to make profit, but as a means to ensure data-sharing mechanisms are sufficiently innovative to improve access to more and better customer data, with better quality and more securely, keeping up with cyber threats.

This will allow for a future-proof framework and for flexibility regarding new financial product development. This will also provide the right incentives for industry participation and fast development of the open Finance ecosystem.

- ▶▶ **Liability:** Liability should be in-line with the GDPR as far as personal data is concerned. For non-personal data, it would be worth considering the value of providing minimum standards, to limit the

variation between schemes. Areas not covered by the GDPR should also be addressed:

- **Data misuse:** The data holder must be expressly exempt from any responsibility for the inappropriate use of data by the data user. For instance, when the customer withdraws the permission through which a data user accessed their data, the data holder no longer has control over the treatment carried out by that user on the data already accessed. Therefore, when the customer withdraws permission, the data holder will ensure that access by that data user to the data is cut off as soon as is technically feasible but should not be responsible for the use that the data user makes of the customer's data, including when it occurs after the withdrawal of permission.
- **Data breach:** FIDA must include clear liability provisions in the case that a data user does not have adequate security measures in place to deal with the data they are processing, leading to a data breach.

In addition, the proposed 18 months for developing the schemes is too short. This timeline is neither a reasonable nor proportional request for private businesses. Practically, it will be near-impossible to achieve this and thus, becoming members of a financial data sharing scheme within this timeframe is also problematic. We propose:

- ▶▶ The timeline to develop the data-sharing schemes should be **appropriate to the standard pace of business** discussions with regards to developing data-sharing partnerships between multiple actors.
- ▶▶ **A phased approach** that takes into account the different players in the ecosystem and the existing challenges to set up a data-sharing scheme would allow data holders and data users the necessary time to converge around certain use cases (and conduct the necessary analysis, impact assessments, etc.)
- ▶▶ The deadline for the development and establishment of the Scheme should be reviewed in line with the Review Clause (Art.31), in four years' time, to give market the opportunity to develop robust rules around liability and compensation, and for market authorities to better assess market developments and to address specific issues.


The European Payments Council SPAA Scheme acts as an example as to why the proposed 18-month timeline is too short. The SPAA Scheme has taken years to develop and has yet to be finalised. More time will be required to ensure that the scheme is workable and efficient. Additionally, this same proposed timeline to adopt Delegated Acts in the absence of a data-sharing scheme is too short. Industry will require more time to develop efficient solutions.

Eligibility criteria (Title V)

Every entity participating in a scheme and being able to access, store and process customers' data should be bound to the same requirements (including in terms of security). Title V in general, and Article 12(d) in particular, should include detailed obligations for Financial Information Service Providers (FISPs) to comply with to be eligible. This is without prejudice to any liability regime that may be applicable.

FOR MORE INFORMATION, PLEASE CONTACT:

 Vincenzo Renda
Associate Director for Digital Transformation Policy
vincenzo.renda@digitaleurope.org / +32 490 11 42 15

 Laura Chaney
Officer for Digital Transformation Policy
laura.chaney@digitaleurope.org / +32 493 09 87 42

About DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory environment that enables European businesses and citizens to prosper from digital technologies. We wish Europe to grow, attract and sustain the world's best digital talents and technology companies. Together with our members, we shape the industry policy positions on all relevant legislative matters and contribute to the development and implementation of relevant EU policies. Our membership represents over 45,000 businesses who operate and invest in Europe. It includes 98 corporations which are global leaders in their field of activity, as well as 41 national trade associations from across Europe.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Amazon, AMD, Apple, Arçelik, Assent, Atos, Autodesk, Banco Santander, Bayer, Bidao, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, CyberArk, Danfoss, Dassault Systèmes, DATEV, Dell, Eaton, Eli Lilly and Company, Epson, Ericsson, ESET, EY, Fujitsu, GlaxoSmithKline, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, Johnson Controls International, JVC Kenwood Group, Konica Minolta, Kry, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Meta, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nemetschek, NetApp, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Red Hat, RELX, ResMed, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Skillsoft, Sky CP, Sony, Sopra Steria, Swatch Group, Technicolor, Texas Instruments, TikTok, Toshiba, TP Vision, UnitedHealth Group, Visa, Vivo, VMware, Waymo, Workday, Xerox, Xiaomi, Zoom.

National Trade Associations

Austria: IOÖ

Belgium: AGORIA

Croatia: Croatian Chamber of Economy

Cyprus: CITEA

Czech Republic: AAVIT

Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv

Estonia: ITL

Finland: TIF

France: AFNUM, SECIMAVI, numeum

Germany: bitkom, ZVEI

Greece: SEPE

Hungary: IVSZ

Ireland: Technology Ireland

Italy: Anitec-Assinform

Lithuania: Infobalt

Luxembourg: APSI

Moldova: ATIC

Netherlands: NLdigital, FIAR

Norway: Abelia

Poland: KIGEIT, PIIT, ZIPSEE

Portugal: AGEFE

Romania: ANIS

Slovakia: ITAS

Slovenia: ICT Association of Slovenia at CCIS

Spain: Adigital, AMETIC

Sweden: TechSverige, Teknikföretagen

Switzerland: SWICO

Turkey: Digital Turkey Platform, ECID

Ukraine: IT Ukraine

United Kingdom: techUK