SUERF
The European Money and Finance Forum

SUERF Policy Note
No 385, December 2025

Should Open Finance exclude gatekeepers in the EU? A proportionate path through reinforced supervision


Judith Arnal | CEPS and ECRI
Fredrik Andersson | CEPS and ECRI

Keywords: Open finance, open banking, data, gatekeepers, DMA, FIDA

JEL codes: G28, K23, L86

Abstract

The EU's proposed Financial Data Access Regulation (FIDA) aims to extend data sharing beyond payments to the broader financial sector, building on the foundations of Open Banking. However, ongoing legislative debates have raised the question of whether companies designated as "gatekeepers" under the Digital Markets Act (DMA) should be excluded from obtaining Financial Information Service Provider (FISP) licences. This policy brief argues that such categorical exclusions would be legally inconsistent, economically counterproductive, and misaligned with FIDA's objectives of promoting competition and innovation. While the concerns motivating these proposals are legitimate, they can be more effectively addressed through reinforced supervision and risk-based safeguards. A proportionate regulatory approach would preserve legal coherence, foster innovation, and ensure that Open Finance develops within a framework that protects consumers while harnessing technological progress.

Disclaimer: This policy note is based on "Assessing regulatory approaches to gatekeeper participation in EU open finance", CEPS. The views expressed are those of the authors and not necessarily those of the institutions the authors are affiliated with.

1. Introduction: from Open Banking to Open Finance

The digital transformation is an unstoppable process and data is at its core. Data-driven innovation can bring enormous benefits to the public sector, companies and citizens. Still, the right conditions in terms of connectivity, processing and data storage, computing power, cybersecurity and adequate governance structures for handling the data need to be in place to grasp the full potential of the digital economy. Significant progress has been made in the EU. At cross-sectoral level, the General Data Protection Regulation (GDPR) in 2016, the Regulation on the Free Flow of Non-Personal data (FFD) in 2018, the Cybersecurity Act (CSA) and the Open Data Directive in 2019. In 2020, the European Commission tabled a European Strategy for Data, building on recently passed cross-sectoral regulations like the Data Governance Act and the Data Act.

But on top of trying to put in place the conditions at cross-sectoral level to unleash the power of data, the EU has also adopted a sector-specific dimension – and finance is a case in point here. One of the first steps was the Payment Services Directive 2 (PSD2), approved in 2015, which established Open Banking, giving third party providers (TPPs) access to payment accounts and leading to the creation of Account Information Service Providers (AISPs) and Payment Initiation Service Providers (PISPs).

According to data released by the European Commission, 5% of consumers have been taking advantage of Open Banking by 2021. This is expected to increase to more than 14% in 2025. This is due to trust, security, and technical issues. The European Commission tries to tackle these issues through the proposed PSD3 and PSR but has not limited itself to proposing improvements to Open Banking. Indeed, the Commission has gone a step further by proposing a new Regulation, known as FIDA (Financial Data Access), whose approval would legally establish Open Finance[1].

While Open Banking involves the sharing of payment account data, Open Finance would imply the possibility of sharing a much broader category of data, continuously and in real time, with consumer's consent. Specifically, the FIDA proposal envisions the sharing of data on loans, savings, investments, pensions, and non-life insurance products. Although Open Banking and Open Finance share a similar philosophy, they differ on an important point: while Open Banking is based on a non-contractual right of access at no cost, in the case of Open Finance, the FIDA proposal require entities holding the data and entities using the data to reach contractual agreements for the sharing of financial data, where the data holders can demand reasonable compensation for the costs of making it available.

FIDA establishes a carefully controlled framework for data access, limiting access rights to two categories of entities that meet stringent regulatory requirements.

The first category comprises entities already subject to EU financial services regulation. Examples of such entities are credit institutions and electronic money institutions; investment firms and crypto-asset service providers; insurance and reinsurance undertakings; and asset management companies and pension providers. These entities benefit from existing regulatory oversight and consumer protection frameworks, providing a foundation of trust for data sharing arrangements.

Under FIDA, a new category of regulated entity is introduced, the Financial Information Service Provider (FISP). FISPs represent the regulation's mechanism for enabling innovative companies to access financial data whilst ensuring appropriate consumer protection. To obtain a FISP licence, entities must demonstrate proper corporate governance and internal control mechanisms; compliance with digital operational resilience requirements; adequate professional indemnity insurance or initial capital of €50,000; and clear operational procedures and customer complaint handling systems.

This dual approach ensures that only properly regulated and supervised entities can access customer's financial data while maintaining high standards of consumer protection and enabling innovation.

[1] Arnal, J., Andersson, F., & Pozo, B. (2025). *Boosting competitiveness in EU retail payments: A strategic policy agenda.* Journal of Payments Strategy & Systems, 19(3), 277-290. https://doi.org/10.69554/UDCF2161

As part of ongoing negotiations, different proposals are circulating to exclude companies designated as gatekeepers under the Digital Markets Act (DMA) from obtaining FISP licences[2].

Against this background, this note reviews the DMA and the Data Act as precedents for data access restrictions, discusses the proposals to exclude DMA-designated gatekeepers from the FISP regime under FIDA, and then examines the role of large technology companies in European financial services. Building on this analysis, the note evaluates the legal consistency and proportionality of proposed gatekeeper exclusions and concludes by setting out a risk-based supervisory approach that aligns with FIDA's objectives.

2. The DMA and precedents of gatekeeper restrictions

The DMA, which entered into force in 2022, aims to ensure contestable and fair digital markets by regulating large online platforms that act as "gatekeepers" between businesses and consumers. The regulation designates certain companies as gatekeepers based on specific quantitative thresholds: annual European Economic Area turnover exceeding €7.5 billion, market capitalisation exceeding €75 billion, providing Core Platform Services (CPS) to more than 45 million monthly active end users, and serving more than 10,000 yearly active business users.

Crucially, the DMA applies a targeted approach, regulating only designated CPS rather than companies as a whole.

The DMA imposes specific obligations on designated CPS, including prohibitions on combining personal data across services without explicit consent, requirements to provide business users with access to data generated through their platform use, obligations to ensure interoperability with third-party services, and restrictions on self-preferencing and tying practices.

Currently, seven companies have been designated as gatekeepers: Alphabet (Google), Amazon, Apple, Booking.com, ByteDance (TikTok), Meta (Facebook), and Microsoft, covering various core platform services.

The Data Act[3], adopted in 2023, includes provisions excluding gatekeepers from certain data access rights, providing the most relevant precedent for gatekeeper exclusions in EU data legislation.

Under the Data Act, users of connected products and related services have the right to access and share data generated by these products with third parties. However, companies designated as gatekeepers under the DMA are explicitly excluded from these data access rights. This means that gatekeepers cannot benefit from the Data Act's provisions that would otherwise allow them to request access to data generated by Internet of Things (IoT) devices.

The exclusion applies to gatekeepers seeking to access data as third parties, but does not prevent them from providing connected products or services themselves. Importantly, the exclusion does not prevent gatekeepers from accessing the same data through other lawful means, such as voluntary commercial agreements with data holders.

The Data Act's gatekeeper exclusion aims to protect small and medium-sized enterprises (SMEs) from potential exploitation in data sharing negotiations, recognising the significant bargaining power imbalances that could arise between SMEs and large technology platforms. The regulation's framework heavily relies on contractual arrangements between parties, where gatekeepers' significant market power and resources could be leveraged to secure disproportionately favourable terms.

[2] European Commission (2022), Regulation 2022/1925 on contestable and fair markets in the digital sector OJ L 265.
[3] European Commission (2023), Regulation 2023/2854 on harmonised rules on fair access to and use of data OJ L.

Table 1. Gatekeepers and respective Core Platform Service

Gatekeeper	Core Platform Service
Alphabet	Google play
	Google Maps
	Google Shopping
	YouTube
	Android Mobile
	Alphabet's online advertising service
	Google Chrome
Amazon	Marketplace
	Amazon Advertising
Apple	AppStore
	iOS
	Safari
	iPad OS
Booking	Booking.com
ByteDance	TikTok
Meta	Facebook
	Instagram
	WhatsApp
	Messenger
	Meta Ads
Microsoft	LinkedIn
	Windows PC OS

Source: Author's own elaboration based on European Commission data.

3. Proposed FIDA restrictions

Legislative discussions surrounding FIDA have increasingly focused on whether companies designated as gatekeepers under the DMA should be permitted to obtain FISP licences or access financial data more broadly[4].

Several forms of restriction have been proposed during the legislative process:

- **Complete FISP exclusion**. Some proposals categorically exclude gatekeeper-designated companies from obtaining FISP licences, regardless of their compliance with authorisation requirements or operational safeguards.

[4] Computer & Communications Industry Association (CCIA Europe). (2025, 23 de mayo). Commission services non-paper on simplification of the Regulation on Financial Information Data Access (FiDA) limits consumer choice, hurts competition, and stifles innovation. https://ccianet.org/wp-content/uploads/2025/05/CCIA-Europe-Letter-Commission-services-non-paper-on-simplification-of-the-Regulation-on-Financial-Information-Data-Access-FiDA-limits-consumer-choice-hurts-competition-and-stifles-innovation.pdf

- **Group-Wide restrictions**. More extensive proposals extend restrictions to any entity owned or controlled by a gatekeeper, even if that entity operates independently in financial services and holds appropriate financial services licences.

Proponents of these restrictions cite several concerns. There are fears that large technology companies could leverage their existing market power and technical capabilities to dominate emerging open finance markets, potentially squeezing out traditional players and innovative startups. Related to this are concerns that gatekeepers could combine financial data with their existing vast datasets, creating unprecedented levels of consumer profiling and potentially undermining privacy and consumer autonomy. Arguments are also made that traditional financial institutions would face an uneven playing field, being required to share data with gatekeepers whilst receiving no reciprocal access to the technology companies' customer data.

4. The role of large tech companies in European Financial Services

Large tech companies' activities in the EU are broad. In the EU, large tech companies have entered financial services, regulated as non-bank payment firms or lenders[5]. Historically, gatekeepers have mainly been providing payment solutions to European consumers, but have over the last years expanded their activities to credit, investments and asset management. Their expansion follows global patterns observed in markets like China and the United States, where big tech firms have achieved significant market penetration in financial services using platform-based models and data-driven approaches[6]. This expansion is generating questions for legislators because of the potential they have in changing the market landscape.

In 2023, six large tech companies subsidiaries were registered e-money institutions (Alphabet (Google), Meta, Amazon, Alibaba, Uber and NTT Docomo), two authorised payment institutions (Google and Tencent (WeChat)), two credit institutions (Orange and Rakuten), three insurance intermediaries (Amazon, Apple and Orange), and two insurance undertakings[7] (Tesla and Vodafone). Thanks to the passporting regime they have been able to offer their services throughout the entire union.

4.1 What are the incentives for large tech companies

Large technology companies enter the financial sector driven by multiple incentives and supported by significant competitive advantages. Their vast reach reduces the barriers to entry that would otherwise deter new competitors[8], enabling them to challenge a sector long dominated by traditional banks. Technology companies enter financial services with different business models than traditional banks. While banks typically generate revenue primarily from lending margins and fees, technology platforms view financial services as part of broader ecosystem strategies that may prioritise user engagement and data collection alongside direct revenue generation.

A first key advantage lies in data access and utilisation. By interacting continuously with millions of users, large tech companies hold unprecedented volumes of behavioural and transactional information. This allows them to design highly tailored products and to monitor user behaviour more effectively.

Another major driver is the role of network effects. As platforms expand their user base, they generate self-reinforcing growth: the larger the network, the greater the value for consumers and merchants. This is particularly evident in

[5] European Parliament (2024) Bigtech finance, the EU's growth model and global challenges. https://www.europarl.europa.eu/RegData/etudes/IDAN/2024/755724/IPOL_IDA(2024)755724_EN.pdf
[6] Frost, J., Gambacorta, L., Huang, Y., Shin, H. S., & Zbinden, P. (2019). BigTech and the changing structure of financial intermediation. *Economic Policy*, 34(100), 761-799.
[7] Joint European Supervisory Authorities (2024), Report on 2023 stocktaking of BigTech direct financial services provision in the EU https://www.esma.europa.eu/sites/default/files/2024-02/JC_2024_02_Joint_ESAs_Report_on_2023_stocktaking_of_BigTech_direct_financial_services_provision.pdf
[8] Brühl, V. (2023). Big Tech, the platform economy and the European digital markets. *Intereconomics,* 58(5), 261-270.

payment services, where merchant acceptance and consumer adoption reinforce one another in virtuous cycles[9] that traditional financial institutions struggle to replicate.

Large tech firms also exploit economies of scale in technology and data processing[10]. Their cloud infrastructures and AI capabilities allow them to deliver financial services at significantly lower costs than those borne by banks, which often remain constrained by legacy systems.

Finally, while the share of revenues that financial services contribute to large tech firms is still relatively limited, their strategic importance goes far beyond direct profit generation. Financial services support broader goals, such as expanding the pool of data for advertising optimisation, reinforcing customer lock-in within the ecosystem, and enhancing overall platform monetisation.

4.2 Market developments observed with technology company participation

Technology companies' participation in financial services has coincided with increasing participation rates in capital markets —an area that remains a European Commission priority through the investment and savings union[11]. Research suggests that data-driven business models may enable more detailed auditing of decision-making processes, compared to current systems that lack transparency for consumers and regulators. However, whether technology company participation would strengthen or complicate supervisory capacity remains a subject of regulatory debate.

The competitive dynamics introduced by fintech and technology companies appear to have influenced incumbent banks' digital transformation strategies. This competitive pressure coincided with improvements in digital service quality and financial inclusion, which aligns with EU single market objectives for financial services[12].

4.3 Risks and challenges of large tech participation

The growing role of large technology companies in financial services is not without significant risks. Market concentration represents the most immediate concern: firms dominating digital ecosystems could replicate similar dominance in financial services, thereby reducing long-term competition and consumer choice[13].

Equally critical are data protection and privacy issues. The combination of highly sensitive financial information with behavioural, social, and geolocation data could create unprecedented levels of consumer profiling and surveillance[14]. This raises the risk of discriminatory practices in credit or insurance, and of manipulative targeting that undermines individual autonomy.

A related concern involves the potential for regulatory capture or circumvention. Large technology companies possess significant resources for regulatory engagement and have demonstrated sophisticated approaches to compliance that exploit ambiguities or gaps in existing frameworks. The complexity of their business models, spanning multiple jurisdictions and sectors, make effective supervision challenging for national competent authorities.

A further challenge lies in systemic risk. As large platforms become embedded in critical financial infrastructures, their failures or sudden market withdrawals could transmit shocks across the financial system[15]. This concern is amplified

[9] Milne, A. (2005). What is in it for us? Network effects and bank payment innovation. *Journal of Banking & Finance*, 30(6), 1613-1630. https://doi.org/10.1016/j.jbankfin.2005.05.014

[10] Keuschnigg, M., & Nielsen, K. R. (2022). Demand-side economies of scope in big tech business modelling and strategy. *Journal of Open Innovation: Technology, Market, and Complexity*, 8(4), 246. https://doi.org/10.3390/joitmc8040246

[11] European Commisison (2025) Savings and investments union: connecting savings and productive investments https://finance.ec.europa.eu/regulation-and-supervision/savings-and-investments-union_en

[12] De la Mano, M. and Padilla, J. (2018), 'Big Tech banking', Journal of Competition Law & Economics, Vol. 14, No 4, pp. 494-526.

[13] Bank for International Settlements. (2019). Big tech in finance: opportunities and risks. *BIS Annual Economic Report 2019*, Chapter III.

[14] Borgesius, F. Z., Gray, J., & van Eechoud, M. (2022). Digital technologies: Tensions in privacy and data. *Journal of the Academy of Marketing Science*, 50(6), 1299-1323.

[15] Financial Stability Board. (2019). BigTech in finance: Market developments and potential financial stability implications. FSB Report.

by their dual role as providers of cloud, communications, and data services, making them potential single points of failure[16].

Moreover, the ability of large tech firms to leverage their platform power to privilege their own services poses threats to contestability. Even if consumers appear to enjoy wider choice, self-preferencing practices could marginalise smaller competitors and erode the innovation that open finance seeks to stimulate[17].

Finally, the network effects that benefit large technology platforms can create significant barriers to entry for new competitors. Once a platform achieves critical mass in financial services, the switching costs for consumers and the advantages of being part of a large network make it extremely difficult for innovative startups to gain traction, stifling the very innovation that open finance policies promote.

The preceding analysis has shown that large technology companies bring both clear benefits and material risks to European financial services.

Against this background, the question is not whether large tech companies participation in Open Finance creates challenges, but whether the proposed blanket exclusions of DMA-designated gatekeepers represent a proportionate and legally consistent response to those challenges.

5. Legal and regulatory analysis of proposed gatekeeper exclusions

This section examines whether the proposed gatekeeper exclusions comply with EU law across multiple dimensions: internal market freedoms, fundamental rights, proportionality requirements, and regulatory coherence. The analysis demonstrates that blanket restrictions may violate Treaty freedoms and Charter rights while failing to achieve FIDA's core objectives.

5.1 Compatibility with internal market freedoms

The proposed gatekeeper exclusions could violate Article 56 TFEU[18], which prohibits restrictions on the freedom to provide services within the internal market. As established in Case C-76/90 Säger[19], any measure which prohibits, impedes or renders less attractive the exercise of the freedom to provide services constitutes a restriction requiring justification.

The exclusions would prohibit gatekeepers from providing financial information services across the EU, impeding their exercise of fundamental Treaty freedoms. To the extent that FIDA grants data access rights to all eligible companies except gatekeepers and entities controlled by them constitutes a prohibition on providing services that rely on financial data received under FIDA.

For such restrictions to be justified under EU law, they must pursue an overriding public interest and be proportionate to that objective, as established in Case C-55/94 Gebhard[20]. The proposed exclusions appear to fail this test as they would undermine FIDA's core public interest objectives of promoting competition and innovation in financial services. Excluding innovative technology companies would restrict competition, contrary to the regulation's stated aims.

[16] Claessens, S., Cornelli, G., Gambacorta, L., Manaresi, F., Segoviano, M., & Zakrajšek, E. (2022). Why risks from big tech interdependencies require attention. *VoxEU CEPR Policy Portal*.
[17] Financial Conduct Authority. (2024). Potential competition impacts from the data asymmetry between Big Tech firms and firms in financial services. *FCA Feedback Statement FS24/1*.
[18] European Commission (2012), Consolidated version of the Treaty on the Functioning of the European Union OJ C 326, 12012E/TXT
[19] Case C-76/90 - Säger v Dennemeyer (1991).
[20] Case C-55/94 - Gebhard v Consiglio dell'Ordine degli Avvocati e Procuratori di Milano (1995).

5.2 Fundamental rights considerations

The proposed restrictions violate multiple fundamental rights and general principles of EU law that form the constitutional foundation of the Union's legal order.

Freedom to conduct a business. The exclusions could infringe Article 16 of the Charter of Fundamental Rights[21], which recognises the freedom to conduct a business. As established in Case C-283/11 Sky Österreich[22], this freedom includes the right to exercise economic or commercial activity and access markets on equal terms. The exclusions would deny gatekeepers and entities controlled by them equal access to European financial data markets, effectively creating a two-tier system of market access based solely on DMA designation. This discriminatory treatment lacks objective justification, as DMA designation relates to specific platform services unrelated to financial data processing capabilities or consumer protection concerns in financial services.

Principle of equality and non-discrimination. The exclusions also violate the fundamental principle of equal treatment enshrined in Article 20 of the Charter and developed through extensive case law including Case C-148/02 Garcia Avello[23]. This principle requires that comparable situations not be treated differently unless objectively justified. Gatekeepers and entities controlled by them are in a comparable situation to other companies seeking FISP licences. Their DMA designation relates to entirely different business activities and bears no relevance to their capability to provide financial information services or comply with FIDA's consumer protection requirements.

Proportionality principle. Under Article 5(4) TEU[24] and established case law including Case C-112/00 Schmidberger[25], any restriction on fundamental rights must satisfy strict proportionality requirements: appropriateness, necessity, and proportionality in the narrow sense. The proposed exclusions would fail all three tests. They could fail the appropriateness test to not effectively address the concerns they purport to resolve, as excluding innovative companies from European Open Finance may reduce competitive pressure on incumbent financial institutions. The restrictions would fail the necessity test because FIDA already contains comprehensive safeguards including regulatory supervision, standardised technical interfaces, explicit customer consent requirements, and data protection obligations to address any legitimate concerns without wholesale exclusions. Finally, the restrictions would impose manifestly disproportionate burdens by categorically barring some of the world's most innovative companies from European financial services.

5.3 Proportionality assessment under EU law

Article 114 TFEU empowers the EU to adopt measures for the establishment and functioning of the internal market, with particular emphasis on promoting innovation and competitiveness.

Excluding companies with proven track records in developing user-friendly, secure, and scalable digital services directly contradicts this innovation imperative. Gatekeepers possess significant technical capabilities in data processing, cybersecurity, user experience design, and AI applications that could benefit European consumers. Their exclusion risks creating a technological gap that leaves European consumers with inferior services compared to other global markets.

5.4 Regulatory coherence concerns

The proposed restrictions create significant inconsistencies within EU law, undermining legal certainty and regulatory coherence. The DMA was designed with a targeted approach, applying only to specific CPS as emphasised in Recital 15's reference to "targeted set of harmonised rules." Expanding these restrictions to entirely different business activities contradicts this targeted approach.

[21] European Commission (2000), Charter of fundamental rights of the European Union, 2000/C 364/01 OJ C 326, 12012E/TXT.
[22] Case C-283/11 - Sky Österreich (2012).
[23] Case C-148/02 - Garcia Avello (2003).
[24] European Commission (2012), Treaty on European Union OJ C 326, 12012M/TXT.
[25] Case C-112/00 – Schmidberger (2003).

Creating sector-specific exclusions for entities already regulated under the DMA risks fragmenting EU digital policy in violation of Article 114 TFEU's internal market objectives. As established in Case C-120/78 Rewe-Zentral[26] (Cassis de Dijon), measures that hinder market access must be justified by overriding requirements and be proportionate to their objectives.

5.5 Distinguishing features from the Data Act context

Several key factors distinguish FIDA from the Data Act context, undermining arguments for similar exclusions. Unlike the Data Act's largely unregulated bilateral negotiations, FIDA subjects all data users to comprehensive regulatory supervision. It scheme-based approach with common technical standards reduces scope for exploiting bargaining power imbalances that concerned Data Act legislators.

First, the nature of the data covered by the two regulations differs significantly. The Data Act primarily deals with data in an area that previously was largely unregulated, where contractual asymmetries between device manufacturers and users were acute. By contrast, the financial data covered by FIDA is already embedded within a dense regulatory framework, including prudential supervision, consumer protection, and sector-specific confidentiality rules. FIDA's requirement for explicit and revocable customer consent further ensures compliance with Article 8 of the Charter and with Article 6(1)(a) GDPR, providing additional protection against potential abuse. This substantially reduces the risk of unregulated bargaining power abuses that motivated the Data Act's gatekeeper exclusion.

Second, the relationship between market actors is markedly different. Under the Data Act, the concern was that powerful gatekeepers could extract disproportionate advantages from small manufacturers or SMEs in bilateral negotiations. In FIDA, all market participants must obtain a licence as a FISP and comply with uniform supervisory, governance, and operational requirements. This harmonised regime addresses the asymmetries that justified the Data Act's more categorical restrictions.

Finally, the risks identified in FIDA differ substantially from those in the Data Act and are already partially mitigated by the safeguards embedded in the proposal — notably explicit and revocable consumer consent, purpose limitation, common technical standards, and regulatory supervision of licensed entities. This existing framework provides a much stronger baseline than the largely unregulated contractual setting of the Data Act. Where legitimate concerns remain, particularly in relation to data concentration or systemic relevance, they call for proportionate reinforcement of these safeguards rather than for categorical exclusions.

5.6 Implementation complexity and practical concerns

The proposed restrictions raise significant implementation challenges that further demonstrate their inappropriateness. Determining which entities qualify for restrictions and monitoring compliance across complex group structures presents substantial administrative complexity for national competent authorities.

Creating sector-specific exclusions generates legal uncertainty about the scope and application of DMA designations beyond their intended context. Market boundary issues arise for entities that may become gatekeepers in the future or operate across multiple business lines, creating uncertainty about the continuity of FISP licences and market access rights.

The restrictions could also lead to regulatory arbitrage, where gatekeepers structure their operations to circumvent exclusions, potentially creating less transparent and accountable corporate structures that serve neither regulatory objectives nor consumer interests.

[26] Case C-120/78 - Rewe v Bundesmonopolverwaltung für Branntwein (1979).

6. A more proportionate path: safeguards over categorical exclusions

Blanket exclusions of DMA-designated gatekeepers from the FISP regime are neither legally justified nor aligned with the objectives of FIDA. This does not mean that the concerns motivating such proposals should be dismissed. Rather, they call for a more precise regulatory response that addresses specific risks without undermining the coherence, innovation potential and legal integrity of the framework.

6.1 Risk-based supervision and enhanced authorisation procedures

A more coherent and proportionate alternative to blanket gatekeeper exclusions would consist in applying reinforced supervisory measures to any FISP applicant that exhibits characteristics associated with elevated risk. Rather than relying on external classifications under other regulatory frameworks, such as the DMA, this approach would ground its scrutiny in objective indicators of risk, including market power, cross-sectoral data capabilities, or systemic reach. In this model, entities applying for a FISP licence would be subject to the same baseline requirements, but national competent authorities could impose additional obligations on firms whose structure, operations or scale raise particular concerns for consumer protection, data security or fair competition.

Such a system could build on established practices in EU financial regulation, where supervisors exercise discretion in tailoring authorisation processes and ongoing obligations based on the specific risk profile of the applicant. This would allow for case-by-case assessments while preserving a level playing field, avoiding arbitrary distinctions based on group affiliations alone. The European Banking Authority could provide guidance and support to ensure convergence and consistency in supervisory approaches across Member States.

6.2 Safeguards to prevent data overconcentration and abuse

In cases where heightened scrutiny is triggered, competent authorities could impose additional safeguards to mitigate identified risks. These might include reinforced requirements on data ringfencing, preventing the combination of financial and non-financial datasets without explicit and granular customer consent. Firms could be required to implement enhanced internal governance and auditing mechanisms to ensure compliance with data usage restrictions, especially in relation to profiling and cross-service monetisation. Obligations to provide detailed transparency reports on data flows and data-based business models could further support accountability and offer customers and regulators a clear view of how financial data is used.

These measures would be grounded in the general principles of the GDPR and in the existing safeguards embedded in the FIDA proposal, including explicit consent, purpose limitation and technical standards. Rather than inventing a new regulatory regime for certain firms, it would reinforce the existing one where justified, maintaining coherence and proportionality.

7. Conclusions

Moving away from group-based exclusions towards a risk-based supervisory model offers a more coherent and proportionate solution for the future of Open Finance in Europe. Transposing DMA designations into the financial domain risks undermining FIDA's objectives and fragmenting the single market. The DMA was conceived as a targeted instrument for specific core platform services; extending its logic to financial data access would stretch its intent and create unnecessary legal and operational complexity.

Anchoring supervision within the financial regulatory framework, where proportionality, consumer protection and prudential oversight already coexist, would strengthen legal certainty and market coherence. A risk-based approach allow supervisors to address genuine concerns such as data concentration and systemic relevance, while avoiding arbitrary barriers that stifle innovation and competition.

By enabling capable and compliant firms to participate under reinforced safeguards, the EU can cultivate a financial data ecosystem that is both innovative and resilient. Open Finance will not thrive through blanket exclusions, but through supervision that adapts to the systemic relevance of each participant. A framework where larger players face reinforced oversight, consistent with their risk profile, will better protect consumers and foster competition while allowing technological progress to unfold within clear and predictable boundaries.

About the author(s)

Judith Arnal is Board member at the Bank of Spain, as well as a member of its Audit Committee. She is an Associate Senior Research Fellow at CEPS and ECRI, a Senior Research Fellow at the Elcano Royal Institute and a member of its Scientific Committee. She conducts extensive research on financial and European policy affairs and is a regular contributor to financial media.

Fredrik Andersson is a Researcher in the Financial Market and Institutions unit at CEPS. He is also a Researcher in the European Credit Research Institute (ECRI), where he is focusing his research on payments, consumer credits and digital finance.

SUERF Policy Notes and Briefs disseminate SUERF Members' economic research, policy-oriented analyses, and views. They analyze relevant developments, address challenges and propose solutions to current monetary, financial and macroeconomic themes. The style is analytical yet non-technical, facilitating interaction and the exchange of ideas between researchers, policy makers and financial practitioners.

SUERF Policy Briefs and Notes are accessible to the public free of charge at https://www.suerf.org/publications/suerf-policy-notes-and-briefs/.

Editorial Board: Ernest Gnan, David T. Llewellyn, Donato Masciandaro, Natacha Valla

Designed by the Information Management and Services Division of the Oesterreichische Nationalbank (OeNB)

SUERF Secretariat
c/o OeNB, Otto-Wagner-Platz 3A-1090 Vienna, Austria
Phone: +43 1 40 420 7206
E-Mail: suerf@oenb.at
Website: https://www.suerf.org/