Assessing regulatory approaches to gatekeeper participation in EU open finance

Judith Arnal and Fredrik Andersson

In-Depth Analysis

Summary

The Financial Data Access Regulation (FIDA) is entering a decisive phase in negotiations. FIDA is the EU's attempt to expand data portability in financial services. Building on open banking, it tries to go one step further by increasing its scope to include a wider range of financial services to achieve true open finance.

This ECRI In-Depth Analysis reviews one of the most contentious aspects of the ongoing negotiations, the explicit exclusion of 'gatekeepers' (as defined under the Digital Markets Act) from obtaining a Financial Information Service Provider (FISP) license. It examines whether categorically excluding gatekeepers would be a proportionate response to the market challenges that large tech companies – such as Apple or Meta – represent in financial services.

By analysing the legal basis and conducting a regulatory comparison with other jurisdictions (the US, UK, Switzerland and Australia) this In-Depth Analysis paper aims to contribute to the discussion and highlight why a blanket ban of gatekeepers would undermine innovation and market competition. Instead, it suggests that to reduce risks, it could be wiser to introduce targeted safeguards that protect the market from the systemic vulnerabilities and privacy concerns posed by large technology companies.

1. Introduction

The regulation of financial data sharing in the EU is entering a decisive phase with the Commission's proposal for a Financial Data Access Regulation (FIDA). Building on the experience of PSD2 and open banking, FIDA seeks to expand data portability across a wide range of financial services, setting the foundations for open finance in Europe. Yet one of the most contentious issues in the ongoing legislative negotiations concerns whether companies designated as 'gatekeepers' under the Digital Markets Act (DMA) should be excluded from obtaining Financial Information Service Provider (FISP) licences or accessing financial data more broadly.

This ECRI In-Depth Analysis paper examines whether categorically excluding gatekeepers represents a proportionate response to the challenges posed by large technology companies in financial services, or whether alternative regulatory approaches might better balance innovation objectives with consumer protection concerns.

Employing a doctrinal legal analysis methodology, this in-depth analysis examines the compatibility of proposed FIDA restrictions with EU primary law through systematic interpretation of Treaty provisions, Charter rights, and relevant Court of Justice of the EU (CJEU) case law. The analysis applies established proportionality tests developed in European jurisprudence to assess whether categorical gatekeeper exclusions satisfy legal requirements of appropriateness, necessity, and proportionality in a narrow sense.

The research combines black-letter legal analysis with comparative regulatory examination across four key jurisdictions (Australia, Switzerland, the UK, and US) to contextualise EU approaches within global regulatory trends. Primary sources include legislative texts, Commission proposals, regulatory guidance and supervisory reports, supplemented by academic literature on financial regulation and digital markets.

The legal assessment is informed by policy analysis of market developments and regulatory objectives, drawing on reports from European Supervisory Authorities (ESAs), central banks and competition authorities to evaluate the practical implications of different regulatory approaches for innovation, competition, and consumer protection.

Section 2 of this In-Depth Analysis outlines FIDA's foundations and objectives. Section 3 introduces the DMA framework, its rationale and the specific restrictions being debated in the context of FIDA, with reference to the Data Act precedent. Section 4 places European legislative discussions in a global perspective, contrasting the EU approach with those of the US, the UK, Switzerland and Australia. Section 5 analyses the role of large technology companies in European financial services, highlighting their benefits and risks. Section 6 assesses whether the proposed exclusions satisfy fundamental tests of proportionality, consistency and legal coherence. Finally, Section 7 develops an alternative, more proportionate approach based on risk-sensitive supervision and enhanced safeguards, followed by a short Conclusions section

This paper's central contribution is to demonstrate that categorically excluding gatekeepers under FIDA fails the EU's legal proportionality test and risks undermining innovation and competition. We advance a novel regulatory alternative – a risk-sensitive supervisory framework that preserves openness to innovation while addressing legitimate concerns about data concentration and systemic risk.

This In-Depth Analysis does not underestimate the risks of concentration, systemic vulnerabilities and privacy concerns posed by large technology companies; rather, it argues that these risks must be tackled through proportionate and targeted safeguards instead of blunt categorical prohibitions.

2. FIDA – its foundations and objectives

The Financial Data Access Regulation (FIDA), proposed by the European Commission in June 2023, aims to establish a comprehensive framework for sharing financial data beyond payment accounts, building on the foundations laid by the revised Payment Services Directive (PSD2). FIDA represents the EU's ambition to transition from limited open banking to comprehensive open finance.

As such, FIDA pursues three fundamental objectives:

1. Enhanced customer control. The regulation seeks to empower customers – both individuals and businesses – with greater control over their financial data, enabling them to decide when, how and with whom their information is shared.

2. Standardised data sharing. By establishing common technical and operational standards, FIDA aims to eliminate the current fragmented approach to financial data sharing, reducing costs and complexity for market participants.

3. Innovation and competition. The framework is designed to level the playing field between incumbent financial institutions and innovative newcomers, spurring the development of new financial products and services that better serve customer needs.

FIDA also covers an extensive range of financial data categories, including:

- Mortgage credit agreements, loans and accounts (excluding payment accounts).
- Savings and investment products, including crypto-assets and insurance-based investment products.
- Pension rights in occupational schemes and pan-European personal pension products.
- Non-life insurance products.
- Creditworthiness assessment data collected during loan applications.

This broad scope reflects the regulation's ambition to enable comprehensive financial data portability, allowing customers to benefit from data-driven financial services across all aspects of their financial lives.

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 EUR 50,000; and clear operational procedures and customer complaint handling systems.

A licensed FISP must process data only for purposes that customers have explicitly consented to; implement robust data security measures; provide transparent information about data usage; and enable customers to withdraw their consent at any time.

FISPs benefit from a European passport, allowing them to operate across all Member States following a simple notification procedure, thus facilitating scale and competition.

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

In a previous analysis, we identified several concerns with the Commission's original FIDA proposal that merit careful consideration. These include uncertainties around the broad definition of 'customer data', which creates ambiguity about what information will be accessed and how data security is guaranteed. We also highlighted potential risks to the current credit ecosystem, where allowing consumers to selectively share only their positive financial information whilst withholding negative data could cause data quality to deteriorate, ultimately leading to higher borrowing costs for all consumers as creditors compensate for increased risk through higher interest rates.

Additionally, we have questioned whether FIDA's 'Big Bang' approach, attempting to revolutionise financial data sharing across all sectors simultaneously, is warranted, particularly given the rather low uptake of Open Banking. Instead, we have advocated for a more measured use-case approach, beginning with specific applications and expanding based on demonstrated success and market acceptance.

This In-Depth Analysis focuses specifically on one of the most contentious aspects of the current legislative negotiations – the proposal to exclude companies that are designated as gatekeepers under the Digital Markets Act (DMA) from obtaining FISP licences.

3. The DMA and proposed FIDA restrictions

3.1. Understanding the DMA

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 EUR 7.5 billion, market capitalisation exceeding EUR 75 billion, providing Core Platform Services (CPS) to more than 45 million monthly active end users, and serving more than 10 000 active business users on an annual basis.

Crucially, the DMA applies a targeted approach, regulating only designated CPS rather than companies as a whole. These CPS include online intermediation services, online search engines, online social networking services, video-sharing platform services, number-independent interpersonal communications services, operating systems, web browsers, virtual assistants, online advertising services and cloud computing services.

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, all covering various core platform services.

3.2. The Data Act precedent

The Data Act, 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, those who use 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, connected cars, smart home appliances and other connected products.

Their exclusion is comprehensive, applying to all IoT data regardless of the device manufacturer or the gatekeeper's existing market presence in that sector.

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

The gatekeeper exclusion was incorporated into the Commission's initial proposal for the Data Act and accompanied by detailed recitals describing why it was needed and its objectives. The regulation states that without the exclusion, the benefits for SMEs would be limited, reflecting concerns about ensuring the fair distribution of data value across different types of market actors.

3.3. Proposed FIDA restrictions

Against this background, 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.

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

- **Complete FISP exclusion**. Some proposals would categorically exclude gatekeeper-designated companies from obtaining FISP licences, regardless of their compliance with authorisation requirements or operational safeguards.
- **Group-Wide restrictions**. More extensive proposals would extend restrictions to any entity owned or controlled by a gatekeeper, even if that entity operates independently in financial services and holds the appropriate financial services licences.

Proponents of these restrictions have expressed 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.

It has also been argued 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. Some argue that gatekeeper participation could stifle rather than promote innovation by creating entry barriers for smaller, more specialised fintech companies.

4. European legislation on financial data in a global context

The EU's approach to open finance and gatekeeper regulation represents one of several distinct strategies that are emerging globally. As financial services become increasingly digital, jurisdictions across the world are grappling with how to balance innovation with consumer protection and, crucially, how to address the role of large technology companies in financial services.

This section examines four key jurisdictions with markedly different approaches: the US pursues fragmented initiatives that have faced implementation challenges; the UK takes a measured, post-Brexit transition approach; Switzerland maintains a voluntary, market-led framework; while Australia demonstrates cautious sectoral expansion through its Consumer Data Right, notably keeping the door open to Big Tech participation.

These varied approaches highlight the global debate over whether large technology platforms represent opportunities or threats in open finance ecosystems – a central tension in EU discussions around FIDA's proposed gatekeeper exclusions.

4.1. Open finance regulation in the US

There are multiple pieces of regulation in the US that cover both data access and combatting the dominant positions of large tech companies.

The Consumer Financial Protection Bureau (CFPB) is responsible for regulating financial services. Under Section 1033 of the Dodd-Frank Act, consumers' right to access financial data are defined. According to the Act, entities included are to make personal data available upon the request of the user. This includes transactional data, consumer financial products and services obtained from an entity covered by the Act.

Section 1033 is, compared to EU legislation, more narrowly defined and market led. Unlike FIDA, it includes no technical standards and does not include the creation of centralised infrastructure.

The final rule was published on 22 October 2024 and was supposed to enter into force by 30 June 2026. However, the ruling was blocked shortly after its publication following a lawsuit in May 2025. The lawsuit was raised under the claim that the legislation exceeds the regulator's statutory authority, citing risks to competition, consumer privacy concerns and account security caused by the poor oversight of third party access. Following the lawsuit, an assessment confirmed the current proposal's limitations, resulting in it being withdrawn. A new CFPB consultation is currently underway.

The US has over the last few years discussed multiple legislative proposals to avoid digital gatekeepers gaining significant market dominance, with none of them successfully completing the legislative process. One of these proposals is the American Innovation and Choice Online Act. It proposed prohibiting large online platforms from favouring their own products on their own platforms. Another proposal is the Open App Market Act, which aimed to limit gatekeepers' power over the modern app-dependent economy by increasing choice and reduce costs for consumers. A final proposal was the Ending Platform Monopolies Act, to ban large online platforms from offering products to consumers from another business owned by the platform.

These divergent approaches reflect broader philosophical differences in digital policy: the EU favours proactive regulatory intervention to prevent market failures, while the US relies more on market self-regulation and *ex-post* antitrust enforcement.

4.2. Open finance regulation in the UK

In the UK, the baseline for sharing financial data is what was defined in open banking under PSD2 and the resulting Payment Services Regulation. Since Brexit, there has been no new legislation on accessing financial data. However, the Financial Conduct Authority (FCA) has committed to publishing research and a roadmap to pave the way to open finance in the UK by the end of 2025.

This timeline suggests the UK is taking a more cautious, evidence-based approach compared to the EU's more comprehensive FIDA framework, potentially allowing it to learn from early European implementation experiences.

British authorities have further developed a multi-layered framework for digital markets competition. May 2024 saw the passing of the Digital Markets, Competition and Consumers Act, with the date for entry into force being set to January 2025. Under the Act, the UK Competition and Markets Authority (CMA) can designate firms as having a strategic role (‘*Strategic Market Status*’ (SMS)). For SMS designated firms, the CMA is empowered to impose specific conduct requirement or introduce pro-competitive interventions to ensure the market remains competitive with a good business environment. Unlike the EU’s DMA, which applies predetermined obligations to designated gatekeepers, the SMS framework allows for more tailored, case-by-case interventions, reflecting the UK's preference for flexible regulatory responses over standardised rules.

The UK's approach represents a middle path between the EU's prescriptive framework and the US' fragmented initiatives. By maintaining operational continuity through existing open banking infrastructure, it simultaneously tries to develop bespoke competition tools. The UK could be positioning itself by completing its legislation and associated regulation faster than the US, while hoping to avoid some of the implementation complexities facing FIDA in the EU.

However, this measured approach could also imply that the UK is falling behind open finance in the EU, should the EU’s initiatives gain significant market traction before British regulatory frameworks are finalised.

4.3. Swiss regulation of open finance

Switzerland has opted for a market-oriented framework that is voluntary and industry led. Financial institutions in Switzerland are under no legal obligation to make financial data available to third parties – even when requested by a customer.

The Federal Department of Finance is responsible for monitoring the Swiss market. As it recorded sufficient developments self-initiated by market players, it suggested that it was not necessary to introduce additional measures. This *laissez-faire* approach stands in stark contrast to the EU and UK’s regulatory interventions, reflecting Switzerland's traditional preference for minimal regulatory interference in financial markets, being more in line with the US.

However, Switzerland's voluntary approach may face pressure as neighbouring EU regulations like FIDA become operational. Swiss financial institutions operating across borders may find themselves at a competitive disadvantage if they cannot offer the same level of data portability and open finance services as their EU counterparts. The current ‘wait-and-see’ stance may need reassessment as crossborder financial services are become increasingly data-dependent and regulatory arbitrage opportunities diminish.

4.4. Open finance in Australia

Australia has had a progressive approach to regulating how consumer data is shared. The current regulation is an evolution of the Consumer Data Right initially based on open banking and now moving towards open finance. It allows consumers to decide which service providers to share their data with. Third party entities that can access data are required to be accredited and must be listed on an open database. In 2025, data is limited to banking and energy data, with an expansion to non-bank lenders underway.

Currently, no large tech companies are accredited for data access. The regulation is nevertheless framed to allow for future accreditation. This contrasts notably with some of the proposals being discussed for the EU's FIDA framework, which would explicitly exclude DMA-designated gatekeepers from obtaining FISP licenses.

On regulating digital markets, the Australian Competition and Consumer Commission has conducted regular inquiries into services provided by digital platforms, publishing their latest report in 2025. The proposed code introduces interoperability requirements, prohibits self-preferencing practices and limits pre-installation agreements. Australia's Competition and Consumer Commission has suggested further stronger consumer protection. While the proposed regulation would take inspiration from the DMA in how to manage gatekeepers, the proposal does not include a blanket ban on gatekeepers.

The Australian framework demonstrates a pragmatic middle ground – more structured than the US' fragmented approach and Switzerland's voluntary model, yet more flexible than the EU's comprehensive regulatory intervention. This may allow Australia to benefit from regulatory experimentation while maintaining closer alignment with its major trading partners in the Asia-Pacific region, where attitudes towards big tech regulation tend to be more accommodating than in Europe.

5. The role of large tech companies in European financial services

Large tech companies' undertake a wide variety of activities in the EU. This includes financial services, being both active and regulated as non-bank payment firms or lenders. Historically, gatekeepers have mainly provided payment solutions to European consumers but over the last few years have expanded their activities to credit, investments and asset management. Their expansion follows global patterns observed in markets like China and the US, where big tech firms have achieved significant market penetration in financial services through platform-based models and data-driven approaches. This expansion to other services is generating questions for legislators because of their potential to change the market landscape.

In 2023, six large tech companies' subsidiaries were registered as e-money institutions[1], two as authorised payment institutions[2], two as credit institutions[3], three as insurance intermediaries[4], and as

[1] Alphabet (Google), Meta, Amazon, Alibaba, Uber and NTT Docomo.
[2] Google and Tencent (WeChat).
[3] Orange and Rakuten.
[4] Amazon, Apple and Orange.

two insurance undertakings[5]. Due to the passporting regime they have been able to offer their services throughout the entire EU.

Big technology companies with significant investments in financial services are already subject to European Central Bank oversight under the Payment and Intermediary Services Act (PISA) framework. This existing supervisory structure provides an additional layer of regulatory oversight beyond the sectoral authorisations mentioned above, demonstrating that these entities do not operate in an unregulated environment but are already embedded within established EU supervisory mechanisms.

In payments, the role of large tech companies has become especially prominent when it comes to digital wallets and pass-through wallets. By facilitating the check-out process at the point of interaction and for online purchases, they have garnered a high uptake rate throughout the EU. In numerous Member States they are among the preferred payment options in e-commerce, with user rates surpassing those of other national alternatives.

Another area where large tech companies are starting to play an increasingly important role is the provision of credit intermediation. Mainly provided by e-commerce platforms, the most common customers for credit provision have been smaller firms. Large platforms have allowed firms to gain simpler and faster access to credit. The providers also benefit from additional tools to ensure that credit is reimbursed according to the specified conditions.

As the platform is likely to be the place of choice for firms to carry out their activities, they would automatically become aware of the importance of repaying the loan, with non-payment possibly resulting in temporary de-listing. Research shows that credit provided by large tech companies appears to be largely complementary, rather than substitutive, to traditional bank lending.

5.1. What are the incentives for large tech companies

Large technology companies enter the financial sector due to multiple incentives and have significant competitive advantages. Their vast reach reduces the entry barriers that would otherwise deter new competitors, enabling them to challenge a sector long dominated by traditional banks. While banks typically generate revenue primarily from lending margins and fees, technology platforms often 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 use. By continuously interacting 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. This can help them to match financial services to users' real financial situations. Academic research highlights that companies' comparative advantage by relying on Big Data rests on their ability to combine transactional data with behavioural and social network information, thus allowing them to create more comprehensive risk profiles than traditional credit assessments.

Another major driver is the role of network effects. As platforms expand their user base, they generate self-reinforcing growth – in short, the larger the network, the greater the value for both consumers and merchants. This is particularly evident in payment services, where merchant acceptance and consumer adoption reinforce one another in virtuous cycles that traditional financial institutions struggle to replicate.

[5] Tesla and Vodafone.

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

Finally, while revenue shares from financial services are still relatively limited for tech firms, their strategic importance goes far beyond profit generation. Financial services support broader goals for tech firms, such as expanding the pool of data for advertising optimisation, reinforcing customer lock-in within the ecosystem and enhancing the platform's overall monetisation.

5.2. Market developments observed with technology company participation

Tech companies' entry into European payment services has coincided with several market developments. Technology companies have introduced digital payment solutions that often feature lower transaction costs, streamlined user interfaces and enhanced mobile functionality. Academic studies suggest that fintech competition has spurred incumbent banks to modernise their legacy systems and expand their digital service offerings.

Tech companies' participation in financial services has coincided with their increasing participation in capital markets – an area that remains a European Commission priority through the Investment and Savings Union. Data-driven business models may enable more detailed auditing of decision-making processes, compared to current systems that may lack transparency for consumers and regulators. However, whether tech companies' participation would strengthen or complicate supervisory capacity remains a subject of regulatory debate.

The competitive dynamics introduced by fintech and tech companies have influenced incumbent banks' digital transformation strategies. This competitive pressure has coincided with improvements in the quality and expanded financial inclusion of digital services, particularly among younger consumers, which aligns with the EU's single market objectives for financial services.

5.3. Risks and challenges of large tech participation

The growing role of large tech companies in financial services is not without significant risks. Market concentration represents the most immediate concern, namely that firms that already dominate digital ecosystems could also become dominant in payments, credit and/or asset management, thus reducing long-term competition and consumer choice.

Equally critical are data protection and privacy issues. Combining highly sensitive financial information with behavioural, social and geolocation data could create unprecedented levels of consumer profiling and surveillance. This risks discriminatory practices in credit or insurance, and of manipulative targeting that undermines individual autonomy.

Regulatory capture or circumvention is another concern. Large tech companies possess significant resources for regulatory engagement and have demonstrated sophisticated approaches to regulatory compliance that may exploit ambiguities or gaps in existing frameworks. The complexity of their business models, spanning multiple jurisdictions and sectors, can make effective supervision challenging for NCAs that may lack the technical expertise or resources to monitor cross-platform data flows and algorithmic decision-making processes.

A further challenge lies in systemic risk. As large platforms become embedded in critical financial infrastructures, their failure or sudden market withdrawal could send shockwaves across the financial system. This concern is amplified by their dual role as providers of cloud, communications and data services, marking them as potential single points of failure.

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

Finally, the network effects that benefit large tech platforms can create significant entry barriers 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 can make it extremely difficult for innovative startups to gain a foothold, again potentially stifling the very innovation that open finance policies aim to promote.

The above analysis has shown that large tech companies bring both clear benefits (innovation, competition, inclusion) and material risks (market concentration, privacy concerns, systemic vulnerabilities) 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 exclusion of DMA-designated gatekeepers represents a proportionate and legally consistent response to those challenges. Section 6 therefore examines why such categorical restrictions are neither justified under EU law nor aligned with FIDA's objectives, and why a more proportionate approach is needed.

6. 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. It demonstrates that these blanket restrictions may violate Treaty freedoms and Charter rights while failing to achieve FIDA's core objectives.

Key considerations include the distinction from Data Act precedents, implementation complexities and being potentially detrimental to European consumers and innovation.

6.1. Compatibility with internal market freedoms

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

The exclusions would effectively prohibit gatekeepers from providing financial information services across the EU, directly impeding their ability to exercise fundamental Treaty freedoms. To the extent that FIDA grants data access rights to all eligible companies, except for gatekeepers and entities controlled by them, this 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. However, the proposed exclusions appear to fail this test as they would actually undermine FIDA's core public interest objectives of promoting competition and innovation in financial services. Excluding innovative tech companies would restrict rather than enhance competition, contrary to FIDA's stated aims.

Proponents argue that excluding gatekeepers would safeguard competition by preventing dominant platforms from pushing out smaller fintechs and innovative newcomers. However, this rationale rests on a narrow, defensive understanding of competition as protection against market concentration. From a broader perspective, competition in open finance should be understood as ensuring contestability and the diversity of actors, where all firms that meet regulatory and supervisory requirements are allowed to participate.

Excluding innovative tech companies restricts, rather than enhances, this type of competition, as it reduces the pool of capable market participants and limits the pressure on incumbents to innovate.

6.2. Fundamental rights considerations

The proposed restrictions violate multiple fundamental rights and general principles of EU law that form the constitutional foundation of the EU's legal order. Applying internal market freedoms to financial data access is an original contribution, as the existing debate has thus far focused primarily on competition law and consumer protection – rather than on Treaty-based service freedoms.

Freedom to conduct a business. The exclusions could infringe Article 16 of the Charter of Fundamental Rights, which recognises the freedom to conduct a business. As established in Case C-283/11 Sky Österreich, this freedom includes the right to exercise economic or commercial activity and access markets on equal terms.

The proposed 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 has not been objectively justified, 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. This principle requires that comparable situations not be treated differently unless such differential treatment is 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 has no relevance to their ability to provide financial information services or comply with FIDA's consumer protection requirements. The proposed differential treatment lacks any objective justification related to FIDA's purposes and objectives. By framing the discussion in terms of Charter rights, this analysis extends beyond policy considerations and grounds the debate in constitutional principles of EU law – an angle largely absent in the current academic and policy discourse over FIDA.

Proportionality principle. Under Article 5(4) TEU and established case law including Case C-112/00 Schmidberger, any restriction on fundamental rights must satisfy strict proportionality requirements: appropriateness, necessity, and proportionality in the narrow sense.

The proposed exclusions could fail all three tests. They could fail the appropriateness test by not effectively addressing the concerns they claim to resolve, as excluding innovative companies from European open finance may actually reduce competitive pressure on incumbent financial institutions, potentially slowing innovation and maintaining higher costs for consumers.

The restrictions could fail the necessity test because FIDA already contains comprehensive safeguards, including regulatory supervision, standardised technical interfaces, explicit customer consent requirements and data protection obligations that could all address any legitimate concerns without wholesale exclusions.

Finally, the restrictions could impose manifestly disproportionate burdens by categorically barring some of the world's most innovative companies from European financial services, potentially depriving European consumers of advanced products and services available in other jurisdictions.

6.3. 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. FIDA's stated objectives include fostering innovation and levelling the playing field between incumbent financial institutions and innovative newcomers.

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. Excluding them risks creating a technological gap that leaves consumers with inferior services compared to other global markets.

6.4. Regulatory coherence concerns

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

Creating sector-specific exclusions for entities already comprehensively 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 (Cassis de Dijon), measures that hinder market access must be justified by overriding requirements and be proportionate to their objectives.

6.5. 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. FIDA's scheme-based approach with common technical standards reduces the scope for exploiting the bargaining power imbalances that concerned Data Act legislators.

First, the nature of the data covered by the two regulations is significantly different. The Data Act deals primarily with data generated by connected devices, an area that had previously operated in a largely unregulated environment and 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, however, all market participants – whether incumbents, fintech firms or large technology companies – must obtain a licence as a FISP and comply with uniform supervisory, governance and operational requirements. This harmonised regime already 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 mitigated to some extent 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 Data Act's largely unregulated contractual setting. Where legitimate concerns remain, particularly relating to data concentration or systemic relevance, they call for the proportionate reinforcement of these safeguards rather than for categorical exclusions.

This contrast with the Data Act provides a novel analytical lens – rather than assuming regulatory precedents apply uniformly across domains, it demonstrates why FIDA requires a distinct legal and supervisory approach.

6.6. Consumer and innovation detriment

The restrictions risk being significantly detrimental to consumers and European competitiveness. Excluding gatekeepers limits consumer choice in data-driven financial services, potentially depriving European consumers of innovative products that are successful in other markets. Tech companies' expertise in reaching underserved populations could support financial inclusion objectives that traditional institutions have struggled to achieve.

European open finance risks falling behind international competitors that actively include major tech companies in similar frameworks. Blanket exclusions could discourage broader investment in European fintech, as investors may question the sector's openness to innovation and technological advancement.

6.7. Implementation complexity and practical concerns

The proposed restrictions raise significant implementation challenges that further highlight how inappropriate they are. Determining which entities qualify for restrictions and monitoring compliance across complex group structures would result in substantial administrative complexity for NCAs.

Additionally, restrictions could act as a *de facto* prohibition depending on how the legislative text is drafted, extending beyond explicit exclusions. Regulatory requirements that appear formally neutral – such as disproportionate compliance obligations, excessive capital thresholds or operational constraints tailored to traditional business models – could effectively prevent gatekeepers from participating without formally barring them. Such indirect restrictions would create the same substantive barriers as explicit exclusions while generating additional legal uncertainty about their scope, triggering concerns and creating enforcement challenges for supervisors.

Creating sector-specific exclusions generates legal uncertainty about the scope and application of DMA designations beyond their intended purpose. Market boundary issues would arise for entities that could become future gatekeepers 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 purposely circumvent exclusions, potentially creating less transparent and accountable corporate structures that serve neither regulatory objectives nor consumer interests.

7. A more proportionate path: safeguards over categorical exclusions

The previous section demonstrated that blanket exclusions of DMA-designated gatekeepers from the FISP regime are neither legally justified nor aligned with FIDA's objectives. However, this does not mean that the concerns that spurred these proposals, including risks of data overconcentration, competition distortions and abuse of market power, should be dismissed. Rather, they call for a more precise regulatory response that addresses specific risks without undermining the framework's coherence, innovation potential and legal integrity.

This section outlines a more proportionate approach based on risk-sensitive authorisation, reinforced safeguards and supervisory discretion – preserving FIDA's openness while ensuring appropriate protections.

7.1. Risk-based supervision and enhanced authorisation procedures

A more coherent and proportionate alternative to blanket gatekeeper exclusions would consist of applying reinforced supervisory measures to any FISP applicant that possesses any 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 risk indicators, 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 NCAs, where appropriate, 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 applicant's specific risk profile. This would allow for case-by-case assessments while preserving a level playing field and 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.

7.2. Safeguards to prevent data overconcentration and abuse

In cases where heightened scrutiny is triggered, NCAs could impose additional safeguards to mitigate the 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 also be required to implement enhanced internal governance and auditing mechanisms to ensure compliance with data usage restrictions, especially relating to profiling and cross-service monetisation. Imposing obligations to provide detailed transparency reports on data flows and data-based business models could further support accountability, while offering consumers and regulators a clear view of how financial data is used and for what purposes.

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

7.3. Avoiding legal uncertainty and regulatory fragmentation

Crucially, moving away from group-based exclusions towards a risk-based supervisory model would avoid the legal uncertainty and operational challenges associated with applying DMA gatekeeper designations to financial services. The DMA's targeted scope, limited to specific Core Platform Services, makes it problematic to use as a proxy for financial data access risk. Gatekeeper status can also change over time and does not necessarily reflect the business model, conduct or market behaviour of subsidiaries operating in the financial domain.

A system that anchors obligations in financial regulation itself, rather than in the extraterritorial reach of digital competition rules, offers greater legal certainty and coherence.

7.4. Preserving openness and fostering innovation

This alternative model would preserve FIDA's original ambition of enabling competition and innovation, ensuring that capable and compliant firms, including those with significant digital capabilities, are not excluded unnecessarily. By assessing and mitigating risks through targeted safeguards, rather than prohibiting participation, the EU would be better positioned to deliver a financial data economy that is both dynamic and trustworthy. Encouraging a diverse range of actors to participate, under appropriate supervision, remains essential to achieving real consumer benefits and driving technological progress in European financial services.

8. Conclusions

The debate over whether DMA gatekeepers should be excluded from FIDA's scope illustrates a central regulatory challenge, namely how to balance innovation, competition and consumer protection in an evolving financial data economy. While concerns about market concentration, data overuse and systemic risk are legitimate, categorical exclusions risk undermining FIDA's core objectives of openness and innovation, as well as creating legal inconsistencies within the EU's regulatory framework.

This ECRI In-Depth Analysis makes clear that the risks associated with gatekeeper participation are serious and require vigilant regulatory oversight. The argument advanced here is not to deny such risks but to show that categorical bans are a blunt instrument that may ultimately weaken both consumer protection and innovation.

A more proportionate approach would not rely on group-based prohibitions but rather on risk-sensitive supervision and targeted safeguards tailored to the specific characteristics of financial data markets. This would enable regulators to address the risks associated with large technology companies while preserving contestability, consumer choice and technological progress.

By demonstrating the legal inconsistency of categorical exclusions and arguing for a proportionate, risk-based supervisory alternative, this In-Depth Analysis contributes to the broader debate on the role of large tech companies in regulated markets. The insights developed and explored here extend beyond financial services, offering a framework that would be relevant to other areas of EU digital regulation where innovation, competition and consumer protection must be reconciled.

European Credit Research Institute

The European Credit Research Institute (ECRI) is an independent, non-profit research institute that develops its expertise from an interdisciplinary team and networks of academic cooperation partners. It was founded in 1999 by a consortium of European banking and financial institutions. ECRI's operations and staff are managed by the Centre for European Policy Studies. ECRI provides in-depth analysis and insight into the structure, evolution, and regulation of retail financial services markets in Europe. Through its research activities, publications and conferences, ECRI keeps its members up to date on a variety of topics in the area of retail financial services at the European level, such as consumer credit and housing loans, credit reporting, consumer protection and electronic payments. ECRI also provides a venue for its members to participate in the EU level policy discussion.

For further information, visit the website: www.ecri.eu.

Centre for European Policy Studies

CEPS is one of Europe's leading think tanks and forums for debate on EU affairs, with an exceptionally strong in-house research capacity and an extensive network of partner institutes throughout the world. As an organisation, CEPS is committed to carrying out state-of-the-art policy research that addresses the challenges facing Europe and maintaining high standards of academic excellence and unqualified independence and impartiality. It provides a forum for discussion among all stakeholders in the European policy process and works to build collaborative networks of researchers, policymakers and business representatives across Europe.

For further information, visit the website: www.ceps.eu.