Council of the European Union
General Secretariat

PUBLIC

Interinstitutional files:
2023/0205 (COD)

Brussels, 24 September 2025

WK 12286/2025 INIT

LIMITE

EF
ECOFIN
CODEC

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	Presidency
To:	Working Party on Financial Services and the Banking Union (Open Finance/FIDA) Financial Services Attachés
N° Cion doc.:	ST 11220 2023 INIT
Subject:	Working Party on Financial Services and the Banking Union (FIDA) 1.10.2025 - Presidency note

PUBLIC

Presidency note on FIDA for WP on 1 October 2025

Working Party on Financial Services and the Banking Union

Date: 24. Sep 2025

Financial Data Sharing (FIDA)

Executive summary

This note seeks to address the remaining issues identified by the **Danish Presidency (PCY**). The note will address the following: the introduction of a reversed-demand approach; supervision; gatekeepers; the Level 2 and Level 3 mandates; and implementation deadlines.

This note lays the ground for an **overall compromise** that recognises that balance across issues is the key to a successful outcome. While individual topics may remain sensitive, the PCY believes that this package may offer a balance that reflects MS priorities. Progress on one element should be seen as reinforcing gains in another, ensuring that no delegation leaves the table empty-handed. The PCY is confident that, by focusing on the value of the agreement as a whole, MS can transform potential divisions into a shared success that strengthens the framework and delivers tangible benefits across the Union.

In addition, the PCY once again emphasises the need for simplification and reduction of administrative burdens. At the same time, it stresses the need to maintain an appropriate balance with the objectives of the framework.

After each section of this paper, delegations will be invited to express their views on the respective issues and drafting suggestions, as provided by the PCY.

PUBLIC

1. Reversed-demand approach

At recent WP meetings, MS have discussed various ways in which to reduce burdens and adjustment costs for the sector. As such, MS have already agreed to exclude certain entities from the scope and, to ensure proportionality, have also agreed to clear delimitations of the data in scope.

However, some MS continue to raise the need for FIDA to be more demand-driven. As exemplified by the long string of discussions – most recently on the PCY's suggested submissions on the implementation of data-sharing schemes – it has not proven to be an easy topic in which to bridge the divide.

To accommodate both the MS that favour a more demand-driven approach and those MS that have raised concerns about it, the PCY has been working to find a compromise between the various positions. As a result, the PCY proposes to introduce a reverse demand approach.

The original **COM proposal** requires data holders to become members of a scheme for sharing data under the scope of Article 2(1). The provision entails that for all data categories within the scope of FIDA, entities need to share customer data under all data categories listed in Article 2(1).

The Council mandate and EP position are consistent with the COM proposal regarding the scope of data to be shared under Article 2(1).

The five MS non-paper proposes that each scheme should determine, within its own governance framework, which data categories are subject to data sharing based on market demand (market-driven approach). In this proposal, the requirement for schemes to share data with data users across all data points would be removed, and schemes would instead be responsible for defining which data points are to be shared, based on market demand.

During the **WP meeting on 17 May 2025**, MS expressed differing views on the demand-driven approach, particularly regarding how schemes should decide which data points are made available to customers and data users. **The COM** and **several MS** pointed out that a key challenge to this proposal is that demand is difficult to define in a market that has yet to materialise. Additionally, **some MS** raised concerns that implementing such an approach could undermine the objectives of FIDA by making it more difficult for customers and data users to access data.

The purpose of this section in the note is to introduce a third option that seeks to strike a balance between, on the one hand, the key objectives of FIDA and, on the other, the

PUBLIC

costs associated with data sharing. Thereby the **PCY** seeks to facilitate a compromise within the Council on this issue.

The PCY proposes to apply a reversed-demand approach to the FIDA framework. The principal idea is to combine the Council mandate with the approach to only have data in scope for which there is demand.

Under the reversed-demand approach, all data categories remain in scope as a baseline, as currently stated in the **Council mandate**. However, if a scheme demonstrates that there is no demand for certain categories of customer data, these categories may be exempted from the obligation to share them with data users under Article 5 of FIDA.

The objective is to ensure that customer data is shared where there is demand. In a nutshell, data holders are not to be required to bear the costs of making customer data accessible to data users when no demand exists.

The reversed-demand approach relies on a **"no-demand test"**, which will be explained in the following section. This approach will require amendments to the Council mandate, which also will be detailed further.

1.1 The no-demand test

With the reversed-demand approach, the principles and objectives of FIDA remain unchanged but schemes are given the option to exclude specific data categories from their data-sharing obligations. The default position is that all customer data is presumed to be in demand. Only if a scheme can demonstrate and prove, through a no-demand test, that there is no demand, it may exclude certain data categories that would otherwise be subject to sharing.

The no-demand test entails three cumulative conditions: (a) no data user has requested that data category to be included in the scope of that data-sharing scheme; (b) no data user has been accessing that data category through a customer interface; and (c) that the corresponding data category is not included in any other scheme in the EU.

These conditions are designed to provide certainty that there is no demand for specific data categories of customer data. If any data user within a scheme has requested access or obtained access to a certain data category of customer data via customer interfaces, it cannot be excluded. Furthermore, the requirement that a data category is not included in any other EU scheme serves to ensure that data users can still access data that is deemed relevant in another scheme. This avoids fragmentation across schemes.

PUBLIC

To avoid requiring data holders to incur costs for preparing data that is not in demand, data holders may conduct a no-demand test during the transitional phase, as provided for in Article 36 of the Council mandate. During this start-up phase of FIDA, data holders are able to demonstrate that the three conditions for exemption are satisfied. During this period, data users and customers must request access to data within the FIDA framework if they wish to obtain it. The PCY notes that including **the EP position** on a staggered approach during the transitional phase could be beneficial, as the EP position divides the transitional phase into three separate stages.

The PCY finds that the three conditions are necessary to demonstrate the absence of market demand and thereby to ensure adequate protection of data users' access to data.

The general provision for the no-demand test is proposed for inclusion in Article 5, which sets out the obligations for data holders. The draft provision clarifies that data holders are not obliged to share data for which there is no demand. **The PCY** notes, that the provision is exclusively added to Article 5, meaning it applies only to data holders sharing data through schemes, and does not affect the right of customers to access data under Article 4.

The proposal provides that the scheme is responsible for assessing the status and accuracy of the conditions set out in the no-demand test on an annual basis. In addition, the competent authority is empowered to assess whether the information supplied by the scheme is correct and reliable. However, **the PCY** does not consider it necessary for the no-demand test to be formally approved by the competent authority, as their role is only to ensure that the description of the no-demand test is correct. These measures are added in the drafting of Recital 10 (line 22).

1.2 Further proposals

The PCY proposes to amend Article 10(4) by including an obligation to notify the competent authorities when a category of customer data will not be covered by the scheme because of lack of demand. This amendment will ensure that competent authorities maintain a clear overview of which data categories of customer data are exempted in a scheme.

To ensure alignment with **the Council mandate, the PCY** proposes to add a subparagraph to Article 11 removing the COM empowerment to intervene with a delegated act for categories of customer data where no demand has been demonstrated.

Based on the PCY proposal, the PCY proposes the following drafting suggestions. The drafting is based on the Council mandate. The PCY notes that the drafting would need to be reworked in order to ensure that the no-demand test takes place during the

PUBLIC

transitional phase and find that inspiration could be sought also in the EP text as mentioned above. Yet, this also relates to implementation deadlines and the gradual approach in general, why it can be accommodated at a later stage.

The PCY invites MS to comment on the PCY proposal on reversed-demand approach and indicate whether MS agree with the drafting.

- **Recital 10 (line 22) [Based on the Council mandate, PCY drafting in red]**

The sharing of the customer data in the scope of this Regulation should be based on the permission of the customer. The legal obligation on data holders to share customer data should be triggered once the customer has requested their data to be shared with a data user. This request can be submitted by a data user acting on behalf of the customer. Where the processing of personal data is involved, a data user should have a valid lawful basis for processing under Regulation (EU) 2016/679. The customer's data can be processed for the agreed purposes in the context of the service provided. The processing of personal data must respect the principles of personal data protection, including lawfulness, fairness and transparency, purpose limitation and data minimisation. A customer has the right to withdraw the permission given to a data user. When data processing is necessary for the performance of a contract, a customer should be able to withdraw permissions according to the contractual obligations to which the data subject is party. When personal data processing is based on consent, a data subject has the right to withdraw his or her consent at any time, as provided for in Regulation (EU) 2016/679. **When a data-sharing scheme can demonstrate, by satisfying a number of conditions, that there is no demand by any data user for a particular category of customer data, data holders should not be obliged to share such categories of customer data, as doing so would add unnecessary costs and administrative burden.**

A scheme's demonstration of compliance with the three conditions needs to be done in the transitional phase according to implementation provisions. Data users, customer organisations and consumer associations may, during this period, request data under each data category. If no data under a data category is requested during the transitional phase, the data holders can choose not to prepare the data for sharing.

Competent authorities do not need to approve the scheme's decision not to share the data categories for which there is no demonstrated demand. Competent

PUBLIC

authorities should, however, have the power to request additional information and should be able to reject the exemption of the obligation to share categories of customer data where the schemes do not demonstrate compliance with the applicable requirements of this Regulation, including where the information is insufficient or misleading.

- **Insert new Article 5(4) (new line 140a) [Based on the Council mandate, PCY drafting in red]**

(4) The data holder is not obliged to make the data listed in Article 2(1) available to a data user, where it has been demonstrated that there is no demand for this category of data.

In order for the first subparagraph to apply, the data-sharing scheme which the data holder is a member of must demonstrate the following:

(a) No data user that is a member of the data-sharing scheme has requested that data category to be included in the scope of that data-sharing scheme;
(b) No data user that is a member of the data-sharing scheme has been accessing that data category through a customer interface;
(c) The data category is not included in any other data-sharing scheme listed in the EBA register of schemes according to Article 15(1) point (c);

Points (a) to (c) must be assessed and confirmed yearly by the data-sharing scheme which the data holder is a member of. Where a subsequent review establishes that there is demand for the sharing of a data category previously excluded under the first subparagraph, the data holders of that scheme will make the data available in line with the provisions under Article 10 within [X – the original implementation timeframe applicable to the corresponding data sets] months from the outcome of the review held pursuant to the previous subparagraph.

- **Insert new Article 5(5) (new line 140b) [Based on the Council mandate, PCY drafting in red]**

(5) The competent authority receiving a notification pursuant to Articles 10(4) must be satisfied that points (a) to (c) have been demonstrated by the data-sharing scheme.

PUBLIC

- **Article 10(4) (line 205) – Council [Based on the Council mandate, PCY drafting in red]**

The notification **needs to** include information regarding the scope of products and services covered by the scheme**, including, where applicable, whether a category of customer data will not be covered be the data-sharing scheme as provided in Article 5(4)~~, as well as~~. It should also specify the** geographic scope, and the calculation to prove that the scheme represents a significant proportion of the market. **The financial sharing scheme needs to notify the national competent authority of any changes identified in relation to the review of Article 5(4) point (a) to (c), in accordance with Article 5(5).**

- **New Article 11(2) (new line 213c) [Based on the Council mandate, PCY drafting in red]**

(2) Paragraph 1 shall not apply where the members of a data-sharing scheme demonstrate that there is no demand for the sharing of one or more categories of customer data listed in Article 2(1), as provided in Article 5(4).

Q1: Do MS support the proposed approach? If not, please explain.

2. Supervision

As preparation for the upcoming trilogue, the **PCY** has reviewed the EP's proposals on supervision and put forward recommendations for the Council's position in the negotiations.

Article 7 – Data use perimeter and Article 17, 18 – designation of competent authority and general supervisory powers

Articles 17 and 18 of the FIDA proposal establish the designation of competent authorities and set out their general supervisory powers. These provisions do not explicitly confer supervisory responsibilities over data users. However, such responsibilities follow indirectly from the fact that competent authorities are tasked with enforcing compliance with the Regulation, including the obligations imposed on data

PUBLIC

users. Neither the **COM proposal** nor the **Council mandate** contains specific provisions on the supervision of the data use perimeter.

The **EP position,** however in Article 7(4c) (line 157c) proposes that the ESAs should undertake regular comprehensive review of data users' compliance with Article 7(1) about data use perimeters.

Article 10 – Scheme governance and content

In the **COM proposal,** it is the competent authorities in the MS that has been empowered to receive the notification of the scheme and carry out the assessment in Article 10(6). Where the three most significant data holders are established in different MS the scheme should be notified to all of these authorities which must agree on which authority should carry out the assessment in Article 10(6) (line 207).

The **Council mandate** has no changes to the COM proposal on supervision, but specifies in Article 10(4) that disagreements between authorities should be resolved under Article 27(1). Furthermore, it proposes in Article 10(6) that the competent authority should inform EBA if the scheme no longer satisfies the provisions of Article 10(1).

The **EP position** proposes greater involvement of the ESAs by stating in Article 10(3) (line 204) that after a data holder has communicated to the national competent authority which scheme it is part of, the competent authority of the MS must communicate this notification to the ESAs as applicable, based on their respective competences. Furthermore, the EP proposes in Article 10(4) (line 205a) that schemes with members established in more than one MS shall be notified directly to the ESAs which shall carry out the assessment in article 10(6) (line 207), and that the relevant ESA shall be notified where the membership of a scheme changes due to the addition of data holders and data users that are established in another MS, whereafter the ESA might proceed to a new article 10(6) assessment. Furthermore, the EP proposes that where the competent authorities assess compliance of a scheme limited to one MS, the competent authority should consult the ESAs. Lastly, the EP proposes that the ESAs should undertake regular comprehensive reviews of compliance with Article 10(1) about schemes governance arrangements in Article 10(6a) (line 208b).

Article 14 – Granting and withdrawal of authorisation of FISPs

In the **COM proposal** and the **Council mandate,** it is the competent authority that is empowered to grant and withdraw authorisations of FISPs. Article 14(7) specifies the situations when a competent authority may withdraw an authorisation with Article 14(7)(c), stipulating that an authorisation can be withdrawn if the provider no longer

PUBLIC

meets the conditions for granting the authorisation or fails to inform the competent authority on major developments in this respect.

The **EP position** is similar. However**,** in a new Article 14(7a) (line 271b), the EP proposes that the ESA or the competent authority of any host MS at any time may request the competent authority of the home MS to examine whether the financial information service provider still complies with the conditions under which authorisation was granted, when there are grounds to suspect that this may no longer be the case.

PCY analysis

The **PCY** takes note of the proposals by the EP but finds that the current Council mandate ensures the right level of supervision and strikes the right balance by keeping supervisory powers at the national level. The Council mandate also involves the ESAs only where necessary. The **PCY** therefore proposes to retain and defend the current Council mandate.

Q2: Do MS support the proposed approach? If not, please explain.

3. Gatekeepers

Considering the recent progression on FIDA, the **PCY** considers it timely revisiting the issue of gatekeepers.

The **WP meeting on 16 July 2025** demonstrated that a wide range of considerations need to be taken into account, reflecting differing priorities among MS. These considerations translated into divergent policy choices, illustrating the complexity of striking the right balance and highlighting the necessity for a timely and robust resolution. Among MS**,** some saw merit in a full or a partial exclusion. Others advocated keeping Gatekeepers within the framework of FIDA. The **PCY** are aware of the need for caution when considering this policy choice in view of the current geopolitical context.

The **COM non-paper** acknowledges the considerable economic power of gatekeepers and accordingly also their competitive advantages. It recommends that co-legislators pursue two measures that would align FIDA with the horizontal data framework and rely on the rules already established in the Data Act and the Digital Markets Act. Firstly, gatekeepers designated under Article 3 of the DMA could be excluded from obtaining the Financial Information Service Provider (FISP) licence. Secondly, the non-paper suggests

PUBLIC

cross-referring to the relevant provisions of the Digital Markets Act (in particular, Articles 5(2) and 6(2)) to ensure that gatekeepers do not obtain an unfair advantage over other market participants. Article 5(2) prohibits gatekeepers from combining and cross-using personal data from other core platform services, unless the end user has given consent. Article 6(2) prohibits the gatekeeper from using, in competition with businesses, any non-public data that is generated by those businesses in the context of their use of core platform services.

The **Council mandate and the EP position** include safeguards and limitations on gatekeepers. According to the EP position, gatekeepers should not be eligible to become a FISP. The Council mandate allows for gatekeepers to become FISPs, but places certain safeguards through the assessment included in Article 18. The Council mandate and the EP position both include a special assessment carried out by the national competent authorities, and certain safeguards and limitations against data users that are owned or controlled by gatekeepers. The Council mandate and the EP position also prohibit combining customer data with data from outside of this Regulation and to ensure data is not shared to other entities that are part of the same group as the gatekeeper.

The **non-paper by one MS** calls for a full exclusion of gatekeepers and entities owned or controlled by gatekeepers as data users, stating that the current envisaged system of individual assessments is overly complex, bureaucratic, and unlikely to produce effective outcomes in practice.

Based on the previous work in the Council, the **PCY** has identified three main concerns regarding gatekeepers. Firstly, the competitive advantage held by gatekeepers and their subsidiaries, as highlighted by the industry and a majority of MS, suggests that including gatekeepers within the FIDA framework would result in *disproportionate* effects on small and medium-sized enterprises (SMEs). This is due to the market power and digital capabilities of gatekeepers, as well as their ability to leverage large volumes of data. Secondly, several MS have raised concerns as regards the need to ensure a high level of *consumer protection* in the framework. Thirdly**,** the inclusion of gatekeepers in the FIDA framework could present challenges in the *supervisory* work of the national competent authorities. In addition, the special assessment as advocated in the **Council mandate and the EP position** is, as above mentioned, complex and at risk of being ineffective in practice.

Based on these considerations, the PCY has developed two sets of drafting options: (A) full exclusion of gatekeepers and (B) partial exclusion of gatekeepers.

Drafting proposal (A) is based on the **non-paper by one MS** and would entail a full exclusion of gatekeepers as data users. The proposed rewriting of recital 10a in drafting option (A) mirrors the considerations set out in recital 40 in the Data Act (EU/2023/2854)

PUBLIC

ensuring that similar concerns are duly reflected in FIDA and that the framework would be disproportionate on SMEs. If MS opt for a full exclusion of gatekeepers, the special assessment by the NCAs, as currently provided for in the Council mandate, should be deleted.

Drafting proposal (B) is based on the **proposal from the COM non-paper** which is a partial exclusion. The partial exclusion is based on excluding gatekeepers from obtaining the Financial Information Service Provider (FISP) licence. It would also prohibit gatekeepers from combining and cross-using personal data from other core platform service, as well as any non-public data that is generated by those businesses in the context of their use of core platform services.

The **PCY** invites MS to indicate which approach they prefer.

Option A:

- **Article 3(6) (Line 142) [Based on the council mandate, PCY drafting proposal in red]:**

(6) 'data user' means any of the entities listed in Article 2(2) who, following the permission of a customer, has lawful access to customer data listed in Article 2(1) **with the exception of entities designated as a gatekeeper or owned or controlled by an entity designated as a gatekeeper as defined in Article 3 (28)(c) of this Regulation.**

- **Recital 10a (Line 22 a) [Based on the council mandate, PCY drafting proposal marked in red]**

(10a) ~~**This Regulation contains rules on gatekeepers designated pursuant to Article 3 of Regulation (EU) 2022/1925. These rules apply to data holders and data users, including entities that apply for authorisation in accordance with Article 12, that are gatekeepers, or are owned or controlled by gatekeepers to ensure that gatekeepers do not circumvent these rules. A data holder and data user, including entities that apply for authorisation in accordance with Article 12, that is a gatekeeper or that is owned or controlled by a gatekeeper should be subject to a special assessment by the national competent authority of its registered office, after a consultation of the ESAs and the European Commission, to ensure its eligibility under this Regulation. Gatekeepers should not engage in behaviour that would undermine the effectiveness of the prohibitions and obligations laid down in this Regulation.**~~

A small number of very large enterprises have emerged with considerable economic power in the digital economy through the accumulation and aggregation of vast volumes of data and the technological infrastructure for monetising them. Those

PUBLIC

very large enterprises include undertakings that provide core platform services controlling whole platform ecosystems in the digital economy and which existing or new market operators are unable to challenge or contest. Regulation (EU) 2022/1925 of the European Parliament and of the Council aims to redress those inefficiencies and imbalances by allowing the Commission to designate an undertaking as a 'gatekeeper'. In addition, the Regulation imposes a number of obligations on such gatekeepers, including a prohibition to combine certain data without consent. One such obligation is to ensure effective rights to data portability under Article 20 of Regulation (EU) 2016/679. In accordance with Regulation (EU) 2022/1925, and given the unrivalled ability of those undertakings to acquire data, it is not necessary to achieve the objective of this Regulation. It would therefore be disproportionate for data holders made subject to such obligations to include gatekeepers as beneficiaries of the data access rights as 'data users'.

It is likely that such inclusion would also limit the benefits of this Regulation for SMEs, linked to the fairness of the distribution of data value across market actors. This means that an undertaking that provides core platform services, and that has been designated as a gatekeeper, cannot be a data user pursuant to this Regulation. However, it does not prevent those undertakings from obtaining and using the same data through other lawful means. The access rights provided for in this Regulation contribute to a wider choice of services for consumers. As voluntary agreements between gatekeepers and data holders remain unaffected, the limitation on granting access to gatekeepers would not exclude them from the market or prevent them from offering their services.

Option B: Partial exclusion

- **Recital 34c (Line 46c) [Based on the council mandate, PCY drafting proposal marked in red]**

(34c) A small number of very large enterprises have emerged with considerable economic power in the digital economy through the accumulation and aggregation of vast volumes of data and the technological infrastructure for monetising them. Those very large enterprises include undertakings that provide core platform services controlling whole platform ecosystems in the digital economy and which existing or new market operators are unable to challenge or contest. Regulation (EU) 2022/1925 of the European Parliament and of the Council aims to redress those inefficiencies and imbalances by allowing the Commission to designate an undertaking as a 'gatekeeper', and imposes a number of obligations on such gatekeepers, including a prohibition to combine certain data without consent and

PUBLIC

an obligation to ensure effective rights to data portability under Article 20 of Regulation (EU) 2016/679. In accordance with Regulation (EU) 2022/1925, and given the unrivalled ability of those undertakings to acquire data, it is not necessary to achieve the objective of this Regulation. It would therefore be disproportionate for gatekeepers to be allowed to apply for a financial information service provider authorisation or to include gatekeepers as beneficiaries of the customer data access right. It is likely that such inclusion would also limit the benefits of this Regulation for SMEs, linked to the fairness of the distribution of data value across market actors. This means that an undertaking that provides core platform services, and that has been designated as a gatekeeper, cannot apply for a financial information service provider authorisation pursuant to this Regulation. As voluntary agreements between gatekeepers and data holders remain unaffected, the limitation on granting a financial information service provider authorisation to gatekeepers and entities owned or controlled by gatekeepers would not exclude them from the market or prevent them from offering their services, including when they hold an authorisation to provide financial services in accordance with Union law.

- **Article 6(4a) (Line 151c) [Based on the council mandate, PCY drafting proposal marked in red]**

(4a) Data users that have been designated as gatekeepers or owned and controlled by an entity designated a gatekeeper pursuant to Article 3 of Regulation (EU) 2022/1925 shall not process, combine, cross-use or use customer data referred to in Article 2(1) of this Regulation in any of the ways described in Articles 5(2) and 6(2) of Regulation (EU) 2022/1925;

- **Article 12(3a) (235C) [Based on the council mandate, PCY drafting proposal marked in red]**

(3b) Undertakings providing core platform services for which one or more of such services has been designated as a gatekeeper pursuant to Article 3 of Regulation (EU) 2022/1925 shall not be eligible for obtaining an authorisation referred to in paragraph 1.

Q3: Which of the options do MS prefer as regards gatekeepers, please elaborate:

Option A: Full exclusion of gatekeepers

Option B: Partial exclusion of gatekeepers

PUBLIC

4. Empowerments for L2 and L3 mandates

In accordance with the shared agenda on simplification and burden reduction, the **COM non-paper of 16 May 2025** advocates limiting the L2 and L3 mandates to what is essential for the effective functioning of FIDA, cautioning against adding further mandates that would increase complexity and burdens. However, the COM non-paper showcases a willingness to expand guidelines in specific areas where co-legislators agree on the need to address consumer protection. The **PCY** considers the limitation of L2 and L3 mandates as an essential part of delivering on the simplification agenda and cutting red tape for authorities and businesses.

MS at the **WP meetings on 27 May** and **16 July 2025** indicated openness to reducing binding L2 RTS and non-binding L3 guidelines where mandates do not provide sufficient value relative to the additional complexity and administrative burden, provided that the necessary clarity can be secured in the Level 1 text.

By contrast, it is the impression of the PCY that the **EP** considers the mandates valuable and is reluctant to delete any of them. However, this viewpoint may have changed given the focus on simplification and burden reduction.

The **PCY** has therefore assessed the mandates and will, at the end of this section, present a possible Council direction for the trilogue negotiations.

Article 6(2c): Data user permission request

Article 6 sets out the general conditions under which a data user may access customer data. The **COM proposal** does not include a L2 or L3 mandate.

The **Council mandate** proposes adding specific criteria to the Level 1 text, requiring that permission requests be clear, objective, accurate, and easily understandable for customers. It specifies the information that must be included in the data user permission request, the design of the request and the deletion of customer data by data users (Article 6(2)(a)-6(3), line 143a-143j).

The **EP position** proposes empowering the ESAs to develop RTS on how data users should design their data access permission requests, including rules on pre-ticked boxes and behavioural nudges. In this process, the ESAs must formally consult the European Data Protection Board (EDPB). The PCY notes that the EP mandate on RTS in Article 6(2c) is not framed or drafted in enough detail for an RTS.

PUBLIC

At the **WP meeting 27 May 2025,** the PCY noted overall positive feedback from MS to keep down the number of L2 and L3 mandates as advocated in the COM non-paper and some MS specifically mentioned that the Article 6(2c) mandate could be deleted.

PCY analysis
The **PCY** finds that the conditions set out in the Council mandate already ensure sufficient clarity in level 1. On this basis, the PCY, as the first option, recommends retaining the Council mandate and removing the EP's proposed L2 mandate. As a second option, the PCY will seek explanations from the EP and as a compromise introduce further clarity in the level 1 text, if there are no other ways to accommodate EP concerns.

Article 7(1a), 7(2), 7(3) and 7(2a): Processing of customer data – (EBA, EIOPA and ESMA)

Article 7 regulates the data use perimeter, meaning how data users process customer data.

Article 7(2) in the **COM proposal** authorises EBA to develop L3 guidelines on data use perimeters specifically for consumer credit scores, stipulating in Article 7(4) that EBA should cooperate closely with the EDPB when preparing the guidelines. The COM proposal states that EIOPA are to develop L3 guidelines for products and services related to risk assessment and pricing of a consumer in the case of life, health and sickness insurance products (Article 7(3), line 156), cooperating closely with the European Data Protection Board when preparing the guidelines.

The **Council mandate** authorises EBA to develop guidelines for products and services related to the creditworthiness assessment of consumers. Furthermore, the Council mandate allows for EBA or ESMA to develop guidelines for other products and services if necessary for the protection of customers. The Council mandate retains the mandate for EIOPA to develop L3 guidelines, but specifies that these guidelines should be on both life and non-life insurance and should include provisions on how data may be used to avoid excessive granularity that undermines the "risk sharing" principle of insurance. Additionally, the Council mandate requires EIOPA to prepare a report within two years on the impact of climate risk and natural disaster-related data, with the possibility to update the guidelines based on this assessment.

The **EP position** expands even further on the COM proposal by requiring EBA to develop both L2 RTS and L3 guidelines not only for consumer credit scores, but also for mortgage credit agreements, accounts (including credit card accounts), and investment products.
The EP position proposes that EIOPA develop L2 RTS and adds motor and home-insurance to the mandate and, like the Council mandate, the EP wants the RTS to include provisions on how to prevent overly granular data use that could undermine the risk-sharing principle (Article 7(3), line 156). The EP position also requires EIOPA to address the "right

PUBLIC

to be forgotten" with L2 RTS for survivors of cancer, chronic diseases, and mental conditions in non-credit related insurance policies (Article 7(3), line 156c).

The **COM non-paper** states that it could agree to expand the EIOPA empowerment to cover both life and non-life insurance.

PCY analysis
For the additional **L2 and L3 mandates in Article 7** (7(1a), 7(2), 7(2a) and 7(3)) on processing of customer data, the **PCY** notes that consensus can be reached on including both life and non-life in the empowerment of EIOPA to develop L3 guidelines in Article 7(3), and also including wording on how to prevent overly granular data use that could undermine risk sharing. The PCY furthermore finds that L3 guidelines provide sufficient guidance, while still being a flexible tool to allow for frequent update in case of market development and addressing new risks should they arise. Therefore, the PCY does not see a need for a mandate for L2 RTS for EIOPA. The PCY would also suggest deleting the report on climate risk from the Council mandate. While agreeing with the importance of the topic, the PCY considers it is well within EIOPA's current mandate to address this as needed, as also stipulated in article 16a of the ESAs regulation which provides the ESAs the mandate to produce opinions, on their own initiative, on all issues related to their area of competence. The PCY would therefore suggest deleting this mandate for a report.

Furthermore, the PCY finds that allowing EBA and EIOPA to develop additional guidelines as needed is the most flexible approach. Therefore, the PCY, as the best option, recommends retaining the current Council mandate for L3 mandates for both EIOPA and for ESMA, EBA if needed. The PCY will seek explanations from the EP and try accommodating EP concerns to providing more clarity in level 1.

<u>Article 7(4a): Processing of non-sensitive KYC data for business customers (ESA)</u>

The **EP position** further introduces Article 7(4a), line 157, which requires the ESAs to develop L3 guidelines on the processing of non-sensitive customer data.

The **COM proposal** and **Council mandate** do not include similar provisions. The **COM non-paper**, as previously mentioned, warns against adding additional L2 and L3 mandates as it is likely that these empowerments would add complexity and administrative burden.

PCY analysis
The **PCY** finds that the conditions set out in the Council mandate already ensure sufficient clarity. On this basis, the PCY, as the best option, recommends retaining the Council mandate and removing the EP's proposed L3 mandate. As a second-best option, the PCY will seek explanations from the EP and as a compromise introduce further clarity in the level 1 text, if there are no other ways to accommodate EP concerns.

PUBLIC

Article 8: Financial Data access permission dashboards

Article 8 regulates the Financial Data Access permission dashboards provided to the customer by the data holder. The **COM proposal** does not provide any L2 or L3 mandates.

The **EP position** proposes that ESAs should develop guidelines in close cooperation with the EDPB, specifying the categories of data so that data are easily understandable for customers. Furthermore, the EP advocates for instructions on the design of the dashboard in the proposed Article 8(2a)(a-c). In addition, the EP position addresses the consequence when a customer decides to withdraw permission for data access as stated in Article 8(2b)(a-c) (line 169f-169m).

The **Council mandate** requires the ESAs, through the Joint Committee, to develop common guidelines on the application of Article 8 (Article 8(4a), line 176c).

PCY analysis
The **PCY** considers that the additions provided by the EP regarding the design of the dashboard in the proposed Article 8(2a)(a-c), as well as the additional provisions for when a customer decides to withdraw permission concerning data access in Article 8(2b)(a-c), provides for a useful clarification to the Level 1 text. Given the positive feedback from MS on limiting the number of L2 and L3 mandates - particularly when sufficient clarity can be provided in the Level 1 text - the PCY proposes, as a best option, to delete the L3 mandate while retaining the EP additions in level 1 in the text. As a second-best option, the PCY will retain the L3 mandate and seek clarifications from the EP on their level 1 amendments in order to find a balanced outcome.

Article 12(4): Application for authorisation as a FISP

The **COM proposal** in Article 12(4) stipulates that EBA in cooperation with ESMA and EIOPA should develop an RTS on the authorisations for FISPs after consulting all relevant stakeholders. The **EP position** aligns with the COM proposal. The **Council mandate** aligns with COM proposal, but empowers the ESAs to develop the standards through the Joint Committee (Article 12(4), line 236).

PCY analysis
The **PCY** recommends retaining the L2 mandate, as it provides the essential legal basis for L2 RTS needed for consistent and objective authorisation of FISPs in MS across the EU. Removing this mandate would risk legal uncertainty and fragmentation. Furthermore, it is standard practice to provide for an RTS to ensure alignment between NCAs practices and facilitate the application process for authorisation.

PUBLIC

Article 28(4a): Cross-border access to data by FISPs

Article 28 addresses situations where a FISP seeks access to data listed in Article 2(1) from a data holder in a MS other than its home country.

The **COM proposal** and the **EP position** do not include L2 or L3 mandates for this provision.

The **Council mandate**, however, requires the ESAs, through the Joint Committee, to develop RTS specifying the framework for cooperation and information exchange between competent authorities in home and host countries. These RTS would detail the methods, means and specifics of cooperation. These include notification procedures, common terminology and standard templates to ensure a consistent and efficient cross-border notification process (Article 28(4a), line 403a-403d).

PCY analysis
The **PCY** acknowledges the Council's wish to introduce an RTS specifying the framework for cooperation between home and host MS. Given the importance of the topic for the Council, the PCY proposes to retain this RTS.

Summary

As outlined above, the PCY proposed moving forward on the following basis:

- Seek to remove L2 mandate in **Article 6(2c)** on data user permission requests
- Seek to retain L3 guidelines on **7(1a), 7(2), 7(3) and 7(2a)** on the processing of customer data and remove other L2 mandates, while seeking to delete the mandate for a report on climate risk
- Seek to remove L3 mandate in **Article 7(4a)** on the processing of non-sensitive KYC data for business customers
- Seek to remove the L3 mandate in **Article 8** on dashboards
- Seek to retain the L2 mandate in **Article 28** on cooperation between home and host authority

As outlined in the section above, if the first option is not sufficient to secure a compromise with the EP on L2 and L3 empowerments, the PCY will seek to accommodate EP concerns as described.

Q4: Can MS support the PCY approach? If not, please elaborate.

PUBLIC

5. Implementation deadlines

At the **WP meeting on 16 July 2025**, the implementation timelines for FIDA were discussed. The **COM proposal** includes a transitional period for setting up schemes. The **Council mandate** introduces a phased implementation based on data categories, with three stages spread over 48 months (Article 36, line 455f, 455m and 455s).

The **EP position** instead proposes a single implementation deadline of 30 months, with an extended timeline for SMEs (Article 36, line 456-456a). The EP position also sets specific deadlines for scheme implementation in Article9(lines 179-179d), in conjunction with Article 36(1), line 456a. The EP position sets out a phased approach for implementing financial data access schemes. First, within 12 months, members must agree on the general rules for the scheme (development phase). Within 26 months, they must agree on common standards and a compensation model and notify the scheme of the relevant authority (implementation phase). Finally, within 30 months, all elements of the scheme must be fully operational, enabling data sharing in line with the agreed rules and standards (operationalisation phase).

The MS generally still support the Council's phasing-in approach, but some MS suggest extending the deadlines further to provide the industry with additional time, with the **non-paper by one MS** proposing to add six months for both scheme set-up and scheme implementation. This is effectively an additional year (12 months) for each implementation stage. Specifically: Stage 1 would consist of 24 months for scheme set-up + 12 months for scheme implementation, stage 2 would have 36 months for scheme set-up + 12 months for scheme implementation, and Stage 3 would have 48 months for scheme set-up + 12 months for scheme implementation.

The **non-paper by five MS similarly** proposes that the phasing-in should be further extended.

The **COM non-paper** highlighted the accelerating pace of innovation and cautioned against any excessive delays, since postponing the establishment of a functional open finance framework could increase the risk of other actors entering the market and that a simpler framework would facilitate a shorter implementation period.

At the last **WP meeting on 4 September**, MS agreed to empower the ESOs to make voluntary standards. At the same time, they stressed that the implementation periods should be balanced in relation to the time required for adoption of the standards which are estimated to take approximately two years to develop.

The application of ESO standards may have an impact on the implementation timeline. Even so, the **PCY** notes that the actual cost and duration of implementation will depend

PUBLIC

on sector-specific needs and on whether the schemes in certain sectors will use the standards developed by the ESOs, develop standards themselves, or already have an open finance framework in place which includes previously developed standards. Furthermore, the implementation deadlines will also depend on the amount of and timing of level 2 and level 3 mandates, and also on the operationalisation of the "no-demand test", if the Council decides to move forward on this basis.

All in all, the **PCY** finds that the implementation deadlines should strike a balance between, on the one hand, providing sufficient time for preparation for industry, take into account the work by the ESOs as well as L2, L3 mandates and, on the other, ensuring that consumers and market participants can benefit from FIDA without unnecessary delay. Therefore, the **PCY** proposes that the Council mandate be maintained at this stage and the question will be revisited.

Q5: Do MS support the proposed approach? If not, please explain.