Council of the European Union
General Secretariat

Interinstitutional files:
2023/0212 (COD)

Brussels, 04 November 2025

WK 14030/2025 INIT

LIMITE

EF
ECOFIN
UEM
CONSOM
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 (Digital Euro Package) Financial Services Attachés
Subject:	Presidency discussion note on the fraud detection and prevention mechanism (Article 32), WP 18.07.2025 - Replies by 20 MS

DK PCY Questionnaire following the Digital Euro WP 18 July 2025 Deadline: ***31.07.2025***
From: ES, EL, EE, DK, DE, CZ, CY, AT, SK, SI, SE, PT, PL, NL, LT, IT, IE, HR, FR, FI **Updated: 08/08/2025 14:54**

Guidelines to be followed

Please kindly provide your contributions in the table below.

Drafting suggestions: you may use '**track changes**'* or formatting (for example **bold-underline** for additions and ~~strike-through~~ for deletions, **where necessary, in a different colour**). *Track changes can only be connected once the cursor is placed in editable areas (Drafting or Comments columns).

To make it feasible to consolidate all contributions, the structure of the table must not be changed, so **no rows can be added or deleted.**

New provisions may only be added in any of the **'existing cells'.**

Name of document*:* please add the **two initials** of your delegation's country followed by a space to the MS Word document name, for example, for Austria: **AT name of the document … .docx**

Thank you for your cooperation!

DK PCY Questionnaire	MS Comments
Presidency discussion note on the fraud detection and prevention mechanism (Article 32) **WK 9765 / 2025**	NL (MS Comments): **NL general comment**: we appreciate the information provided by the ECB on their fraud detection and prevention mechanism for online transactions in the recent technical seminar. To us, this is a step in the right direction regarding the matter of privacy, and to bringing this matter to a close. In order to finalise this topic and as stated in the CWP of 18 July, we believe it would be helpful to receive more information on fraud detection and money counterfeiting for offline transactions.]

DK PCY Questionnaire	MS Comments
-Privacy and the functioning of a fraud detection and prevention mechanism	
Q1. Do Member States consider that the technical clarifications provided by the ECB offer sufficient assurance that privacy will be preserved in the implementation of Article 32?	ES (MS Comments): Yes EL (MS Comments): **EL:** Yes, we consider that relevant ECB technical clarifications in the June 30 technical seminar as well as in previous seminars, provide sufficient assurance for the protection of privacy. EE (MS Comments): EE: We believe that technical clarifications provided by the ECB offer sufficient assurance that privacy will be preserved in the implementation of Article 32. However, we would be open to any further clarifications if other Member States deem appropriate. DK (MS Comments): Yes, ECB's technical clarifications offer assurance that privacy will be preserved in the implementation of Article 32. DE

DK PCY Questionnaire	MS Comments
	(MS Comments): It is our understanding that in the context of fraud detection, the ECB will only receive pseudonymized data on individual customers and transactions. It is also our understanding, based on the ECB's technical seminar in March, that the ECB cannot under any circumstances resolve these pseudonyms using other data. As a result, it would then be impossible for the ECB to identify individual customers. Only the payment service provider can assign the pseudonyms to specific customers. In our view, it should also be further clarified in the text of Article 32 (4) that payment service providers must carry out pseudonymization in accordance with the GDPR. The current text only speaks in general terms of "appropriate technical measures, including state-of-the-art security and privacy-preserving measures". This wording leaves a lot of leeway and should be clarified. In our view, it is very important to add an explicit reference to pseudonymization as defined in Article 4 (5) GDPR. Further, we believe it should be made clear that not only "appropriate" measures must be taken, but "all necessary measures". Moreover, we would like to point out that fraud detection and prevention measures are not only impractical for the Eurosystem in offline scenarios, but PSPs themselves will also face limitations in fulfilling PSR's fraud prevention

DK PCY Questionnaire	MS Comments
	requirements. This should be clearly acknowledged. It is critical to avoid any situation in which PSPs are compelled to collect transaction data in order to meet legal obligations, as this would directly contradict the privacy promise associated with offline payments. In this context, we would clearly welcome a follow-up seminar by the ECB focusing on how privacy-by-design principle will be implemented for the offline use. One key open question for us remains what data the user must transmit to the PSP during the reconciliation process. CY (MS Comments): Yes, ECB's technical clarifications offer assurance that privacy will be preserved in the implementation of Article 32. AT (MS Comments): Yes. SK (MS Comments): We would like to thank ECB for the clarifications provided. SI (MS Comments):

DK PCY Questionnaire	MS Comments
	Yes, we agree. SE (MS Comments): We only have one more overarching note on this issue. We thank and take note of the clarifications made by the ECB and the presidency. Privacy issues for users in this regard are important, but we also want to be mindful not to create a mechanism that doesn't fulfill its intended purpose. We also think that some flexibility is important here going forward as we have seen that fraudsters adapt fast and use new devious ways to deceive users. As outlined, trust in the system is crucial and fraudsters can easily break this trust if given the opportunity to exploit the system. PT (MS Comments): PT believes the provided clarifications are sufficient. PL (MS Comments):

DK PCY Questionnaire	MS Comments
	PL: Yes, we are of the view that the technical explanations indicate a well-considered approach to data protection. Although we are aware that the typology will evolve, we believe that a minimum should be introduced to avoid legal uncertainty. Commission delegated acts will complement this minimum. Limiting data processing to the minimum necessary (ID hashing, transaction metadata, IP ranges), no direct access to personal data, and data segregation provide a solid foundation. However, it could be considered to strengthen these guidelines through independent compliance audits and regular infrastructure security reviews. NL (MS Comments): **NL comment**: We think the technical clarifications provided by the ECB sufficiently address our concerns with regard to privacy, for online transactions.] LT (MS Comments): We do. IT (MS Comments):

DK PCY Questionnaire	MS Comments
	Yes, we do. IE (MS Comments): IE is satisfied with the clarifications provided by the ECB. Given the evolving nature of fraud risks and technological developments, it will be important to maintain adaptability in the mechanism's design and governance. IE would also suggest that clear and enforceable deterrents for misuse or breaches could help strengthen public trust and ensure the long-term integrity of the mechanism. HR (MS Comments): Technical clarifications provided by the ECB during ECBs technical seminar regarding data in the digital euro infrastructure held on 6 March 2025 offer sufficient information that privacy will be preserved in the implementation of Article 32. But as it is stated in the DK PRES discussion note, we support the statement that a combination of contractual and technical safeguards (clear segregation of data between relevant actors and an allocation of responsibilities) are important between the providers of support services and the Eurosystem to prevent the linking or onward transmission of personal data between them. FR

DK PCY Questionnaire	MS Comments
	(MS Comments):
	Privacy will be guaranteed on the basis of analyses by data protection agencies and independent audits. As the new PSR regulation reminds us, the fight against fraud is crucial. Combating bank fraud requires a great deal of experience and an extensive track record: any new means of payment is exposed to a high risk of fraud. We need to ensure that the digital euro is safe. If not, we are exposing the euro to a risk of loss of confidence.
	FI (MS Comments): Yes
Q2. Do Member States find it necessary to further amend Annex V?	ES (MS Comments): No. However, it could be useful to be able to review the list contained in Annex V, regarding the list of personal data that can be processed by PoSSs through a Commission delegated act, to be able to update some of the categories if it is considered necessary after the procurement proceedings. We could also refer the list to the EDPS prior to the implementation of the mechanism to ensure that everything is compliant with GDPR. EL (MS Comments):

DK PCY Questionnaire	MS Comments
	EL: No, we see no need for further amendments to Annex V. EE (MS Comments): EE: We have not identified a need for further amendments. However we are open to proposals for improvements. DK (MS Comments): Cyprus opinion is that the text should remain flexible avoiding the definition of a specific list of data categories in the regulation itself. DE (MS Comments): We understand that Annex V deliberately defines broad categories of data rather than specific data points. That approach is meant to provide flexibility to amend the selection of relevant data points, thereby allowing for quick reactions in a constantly evolving threat environment. We think that in general, this is a sensible approach. However, we think that the current wording of Annex V requires further clarification. The draft currently stipulates that data that is "required" for fraud detection can be evaluated. At the same time, Annex V contains a list of relevant data. It is unclear whether this list is exhaustive or just illustrative for

DK PCY Questionnaire	MS Comments
	data which are usually required for fraud detection. This point should be clarified. In our view, the list of data categories should be exhaustive - especially in light of the above-mentioned approach of defining broad categories of data. Moreover, we find the definitions of data allowed to be processed in this context in annex V to be rather vague. For example, annex V (i) allows the processing of "account information". This is a very broad term. What does it comprise? If taken at face value, wouldn't this allow the ECB (or PoSS) to process data which allows to identify the account holders? That said, we are concerned that the current provisions would – in theory – allow for very large data collections. Article 35 (7) in connection with annex V would essentially allow the ECB (or a PoSS) to create comprehensive payment profiles. A crucial question for us will be what exactly are "state-of-the-art security and privacy-preserving measures" in this context? CY (MS Comments): Cyprus opinion is that the text should remain flexible avoiding the definition of a specific list of data categories in the regulation itself. AT

DK PCY Questionnaire	MS Comments
	(MS Comments): We suggest the following amendment to cater more explicitly for the pseudonymized personal data process: […] i) information on digital euro payment accounts, including the pseudonymized unique digital euro account identifier in accordance with Article 32 (4); SI (MS Comments): / PT (MS Comments): At this stage, PT does not identify the necessity to introduce further amendments to Annex V. PL (MS Comments): PL: We are of the view that the current form of Annex V may be sufficient, provided that flexibility is maintained in its updating. In addition, however it would be worth considering clarifying the terminology to ensure consistency between the Articles and the Annexes and introducing a short explanatory note for each category of data. Therefore, taking into

DK PCY Questionnaire	MS Comments
	account the answer to question 1, we see the possibility of further changes to Annex V based on the level of detail of the data and the establishment of a precise minimum. NL (MS Comments): **NL comment:** No, we do not think this is necessary.] LT (MS Comments): We do not find it necessary to further amend Annex V. IT (MS Comments): No, we don't. IE (MS Comments): IE is satisfied with the current drafting of an Annex V; however, IE recognises that fraud detection and prevention technologies are constantly evolving. Therefore, IE foresees the need to make use of the empowerment under Article 36 (3), allowing the Commission to adopt delegated acts to update Annex V as necessary. This will ensure the framework remains adaptable and future proofed in response to technological developments.

DK PCY Questionnaire	MS Comments
	HR (MS Comments): No, we find that it is not necessary to further amend Annex V. FR (MS Comments):
	No, but we are open to proposals from other Member States.
	FI (MS Comments): No
Q3. Do Member States find it necessary to conduct further amendments to Article 32?	ES (MS Comments): No EL (MS Comments): **EL:** No, we do not consider further amendments to Article 32 to be necessary. EE (MS Comments): EE: We have not identified a need for further amendments. However we are open to proposals for improvements. DK

DK PCY Questionnaire	MS Comments
	(MS Comments): No strong views from Cyprus. DE (MS Comments): Currently, the draft legal text only envisages a role for the EDPS "prior to developing on the operational elements of the fraud detection and prevention mechanism" (Art. 32(2)). From our perspective, if the approach taken under Annex V is maintained, the EDPS role should be clarified to ensure its involvement prior to, or in the intermediate aftermaths of, substantial amendments to the operational details of the fraud mechanism (e.g. change of data points or of objectives of the mechanism). In our view, it would make sense to further clarify the wording of Article 32 (4): o In particular, it should be stated that fraud detection may only be carried out in accordance with the requirements of the GDPR and that all entities involved in fraud detection must comply with the requirements of data protection law (e.g. in a Recital). o We also noticed that reference is made to "support service" while the appropriate term appears to be "provider(s) of support service". That aspect should be addressed.

DK PCY Questionnaire	MS Comments
	CZ (MS Comments): It should be clarified the interplay between DER and PSD3/PSR. CY (MS Comments): No strong views from Cyprus. AT (MS Comments): Article 32 (4) does not further specify or give any clarifications which privacy preserving measures are sufficient. The term "privacy-preserving measures" is not legally defined. Wording suggestion reg Art 32 (4): […] including state-of-the-art security and privacy-preserving measures, such as pseudonymization in accordance with Article 32 (1) (a) GDPR, to ensure that the support service shall not be able to directly identify the digital euro users […] SK (MS Comments): We do not find it necessary to amend Article 32 further. SI (MS Comments): No. PT

DK PCY Questionnaire	MS Comments
	(MS Comments): At this stage, PT does not identify the necessity to introduce further amendments to Article 32. PL (MS Comments): PL: The current wording of Article 32 seems to be sufficient. Nevertheless, it would be worth considering adding an operational review clause in the future, which would allow the provisions to be updated on the basis of experience gained in implementing the mechanism. NCBs should be able to operate a general fraud detection and prevention mechanism, as suggested by the BE Presidency. The involvement of national central banks in this matter is important given their knowledge of the specificities of their national markets and their ability to assess and take appropriate action. Cooperation between the ECB and NCBs is a key factor in effectively combating fraud. NL (MS Comments): **NL comment**: We do not.] LT (MS Comments):

DK PCY Questionnaire	MS Comments
	We do not. IT (MS Comments): It would be beneficial to amend Article 32 to include a provision for regular information exchange between PSPs. This would allow them to pool their experiences and share the choices they've made regarding fraud detection and prevention. Moreover, this article should be aligned with the PSD3/PSR provisions on this aspect; a cross-reference may be beneficial, and it should be evaluated in the light of the final text of those legislative texts. IE (MS Comments): IE is satisfied that the drafting of Article 32 is broadly sufficient but would underline the importance of maintaining flexibility, given the evolving nature of fraud, particularly as new risks may emerge in the specific context of the digital euro. FR (MS Comments):
	We have not identified any other subjects.
	FI

DK PCY Questionnaire	MS Comments
	(MS Comments): No
Presidency discussion note on mobile device access (Article 33) **WK 9764 / 2025**	
-Fair, reasonable and non-discriminatory access to mobile devices (Article 33)	NL (MS Comments): **NL general comment**: The offline digital euro is a **key priority** for the Netherlands as it guarantees the digital euro's added value to the European payment infrastructure. Having the offline functionality available from the initial launch remains key for us. We do understand that launching this can be challenging and that certain decisions need to be made to achieve this goal. Therefore we are willing to give this matter further attention and are open to discuss possible solutions. We understand that the European Digital Identity Wallet (EDIW) will need access to the Secure Environment for offline functionalities as well and is facing similar challenges. We therefore think this issue should be addressed more comprehensively in a different, broader legal framework, such as the Digital Markets Act or the Data Act. Of course, certain aspects still could be addressed in the Digital Euro Regulation, for example, in case it is necessary

DK PCY Questionnaire	MS Comments
	to ensure that the digital euro will get sufficient storage capacity within the Secure Environment. We welcome any substantiation of FRAND-access in an implementing or delegated act in case this supports PSPs and/or the Eurosystem in gaining access to the required technology to make the offline digital euro functionalities a success from the first issuance of the digital euro. In case the online functionalities are ready for launch but more time is needed to ensure access to offline functionalities for a majority of users which have access to SEs, we would consider postponing the launch of the digital euro until these functionalities are available. Moreover, we are contemplating whether it would be suitable for the ECB to take a leading role in the negotiations with Secure Element providers.
Q1. Do Member States consider that the current FRAND-based framework in Article 33 provides sufficient legal clarity and guarantees to ensure effective and equitable access to secure environments for digital euro services?	ES (MS Comments): As a general comment on the offline functionality: • We strongly support the offline functionality of the digital euro for resilience and financial inclusion reasons. • We prefer to introduce a best-effort clause obligation on the Eurosystem: We believe that the offline functionality should be delivered as soon as possible, if possible, from day 1 of the introduction of the digital euro. We are nevertheless aware of the

DK PCY Questionnaire	MS Comments
	difficulties in the development of the functionality. We deem it is of extreme importance that the offline functionality offers the highest levels of security against hardware and software attacks, with well selected secure environments that provide this adequate level of security and do not present storage capacity complications. We also want to avoid that the deployment of the offline functionality derives in undesirable dependencies on third country providers, affecting the objective of strategic autonomy that the D€ project aims to reach. For this reason, we would prefer a best-efforts clause on the Eurosystem to provide the offline functionality as soon as possible. We think that our objectives as co-legislators and the Eurosystem's objectives are aligned in this matter: provide a secure, easy to use and valuable offline functionality that contributes to the objectives of the D€ (resilience, strategic autonomy and financial inclusion) as soon as possible. Answering the question: We think that FRAND terms seem more proportionate than requiring OEMs to provide access free of charge. Also, for bigger OEMs, considered gatekeepers by the DMA, the access will need to be provided for free. We see also that article 12b of the EUDIWs Regulation only foresees free access by gatekeepers. However, we have some concerns on the FRAND-based access, given the difficulty to determine what are FRAND terms and also given the different bargaining power in the determination between smaller PSPs and large OEMs.

DK PCY Questionnaire	MS Comments
	We see that the FRAND access is regulated in other pieces of legislation (the EU data act and the DMA) and that it will be necessary for providing other services such as the EUDIW. For this reason, we could see value in addressing this issue from a broader perspective and learning from the texts that are already on the table regarding this matter. We could include elements similar to those foreseen in the Data Act: - developing model contractual clauses to promote balanced negotiations. Also, we could think of fostering joint negotiations by PSPs. - empowering the COM to intervene when access conditions are structurally unfair or discriminatory - mandating the COM to introduce guidance on what may constitute FRAND terms EE (MS Comments): EE: An offline digital euro is a key goal from the first issuance of the digital euro. Therefore, we support further discussion and finding a robust and holistic solution to enable it. DK (MS Comments):

DK PCY Questionnaire	MS Comments
	Cyprus supports the Presidency's judgment that while the FRAND-based framework provides a useful basis, further clarification would help reduce legal uncertainty and facilitate uniform application across Member States. DE (MS Comments): General remark on privacy and the offline version For Germany, it is of key importance that the offline version of the digital euro will be available from day one. Reaching this goal has highest political priority. In Article 23 of the Proposal this political goal is clearly linked to a legal obligation to make offline available as of the issuance. We trust that the ECB will make offline available as of the first day of the issuance. In our view, the responsibility to implement the offline version in technical terms rests with the ECB. The legislative framework shall provide a clear legal basis and shall serve as an enabler for both the ECB and the PSPs. To this effect, we support a strong and robust legal framework which provides all necessary guidance to make the offline version available from day one.

DK PCY Questionnaire	MS Comments
	In our understanding, the digital euro is not the only European initiative which will require a legal framework enabling the use of a Secure Hardware Element. When assessing Article 33, we would like to draw the attention to the fact that another very important European digitalisation project, the European Union Digital Identity Wallet (EUDIW), will also benefit from access to the Secure Hardware Element. In this context, the European Digital Identity Cooperation Group was established under the eIDAS Regulation. The Group is working on concepts for a secure mobile platform that can host the EUDI wallet on the user's mobile device. We believe that the technical work of the ECB and the process launched there would benefit from a closer alignment, where possible. Art. 25 of the Digital Euro Regulation foresees that the digital euro and the EUDI Wallet shall be interoperable. Hence, technical alignments should be ensured here. Potentially, there could be positive spill-over effects, both in legal terms and in technical terms. Moreover, in the PSD3/PSR trialogues a proposal was tabled by the European Parliament which seeks to enable FRAND access to technical features (e.g. Near Field Communication) needed for payment processing within the context of the PSD3/PSR. Likely, PSD3/PSR would enter into force before the digital

DK PCY Questionnaire	MS Comments
	euro. Hence, valuable time and experience with the FRAND conditions could be gained in the context of PSD3/PSR. Given the importance of those parallel initiatives, we call for a closer alignment of these workstreams. Finally, the costs for PSPs will play a key role. If accessing the Secure Element would come at high costs, these costs would, again, have to be factored in when discussing the compensation model. Therefore, we support an effective but also affordable access for PSPs to the necessary Secure Hardware Elements. In response to Q1: We support a solid legal framework which ensures an effective and affordable access to the Secure Hardware Elements. The legal framework of Article 33 shall ensure clarity and set the right benchmarks. It shall prevent discriminatory or excessive pricing and shall not lead to implementation uncertainties.

DK PCY Questionnaire	MS Comments
	Therefore, we **welcome any initiative to further improve Article 33**. The **goal is very clear to us: In accordance with Article 23, offline must be available from the day of the first issuance.** In practical terms, we are wondering how the FRAND access would be implemented in practice? Would each PSP need to conclude bilateral agreements with every single OEM? **What role might the scheme, i.e. the ECB, play here?** We are wondering whether there is a **possibility that the Commission and/or the ECB would conclude framework agreements with the OEMs** which would set the price limit for all PSPs? In particular with regard to smaller PSPs, a centralised pricing framework would be of great importance. CY (MS Comments): Cyprus supports the Presidency's judgment that while the FRAND-based framework provides a useful basis, further clarification would help reduce legal uncertainty and facilitate uniform application across Member States. AT (MS Comments): - SK

DK PCY Questionnaire	MS Comments
	(MS Comments): We would like to raise additional point with regards to the proposal of the European parliament on art. 88a of the PSR, which basically extends art. 33 of Digital euro Regulation to payment services in general. We supported this from the beginning, but we also acknowledge that this may be limiting for the availability of offline Digital euro payments due to the capacity limitations of the hardware. We believe that this should be discussed within Digital euro working party together with the ECB to better assess the possible implications and to coordinate our approach. SI (MS Comments): The current FRAND-based framework in Article 33 is not sufficient for two reasons: i) an effective provision must be established to prevent discriminatory or excessive pricing for PSPs accessing secure environments on the devices, especially smaller providers or Member States with less bargaining power vis-à-vis large device manufacturers and ii) it should be ensured that smaller PSPs are not obliged to negotiate individually with large device manufacturers, but that such matters are resolved at a higher, coordinated level to avoid unnecessary burdens and preserve a level playing field. SE

DK PCY Questionnaire	MS Comments
	(MS Comments): We want to reiterate our position that access to secure elements in mobile devices is one aspect of the regulation where we think it would be beneficial to also include non-euro CBDCs, since it is in some respects an internal market issue. This could be important to enable inter-operability between a digital euro and a possible non-euro member state CBDC. PT (MS Comments): Based on the analysis conducted, PT does not identify at this time possible improvements to include in the drafting of Article 33 to enhance the clarity and precision of the suggested FRAND framework. Notwithstanding, and considering the described lack of precedents, we believe that only based on effective market experience it would be possible to evaluate whether any additional concrete requisites or safeguards need to be previewed. PT further highlights that the obligation laid down in Article 33(3), on the

DK PCY Questionnaire	MS Comments
	publication of general conditions of effective interoperability and access, greatly contributes towards transparency and will be essential to assist front end entities to secure the wished access. On a final note, PT will remain open to evaluate further amendments deemed relevant. PL (MS Comments): PL: The current wording on the application of FRAND principles may not provide sufficient regulatory clarity. In practice, the wording used may be interpreted in different ways, which may lead to disputes between payment service providers and mobile device manufacturers or operating system operators. We recommend: • clarifying the provisions, for example by providing examples of criteria for assessing FRAND conditions, such as access costs, availability of interfaces, implementation time, and technical transparency, • considering the possibility of issuing guidelines by the European Commission; these guidelines could harmonize the application of FRAND principles and reduce the risk of divergent interpretations between Member States,

DK PCY Questionnaire	MS Comments
	• developing model contractual clauses, including defining standard licensing and technical conditions, which could speed up negotiations between entities and ensure a level-playing field. NL (MS Comments): **NL comment:** we think that the FRAND-based framework is a good starting point for ensuring effective and equitable access to secure environments, however, we currently cannot be sure that expanding this framework will be the right solution to provide access. In case it improves the negotiating position of PSPs and/or the Eurosystem, we welcome further substantiation of the article or, preferably a delegated or implementing act. LT (MS Comments): We consider that the current FRAND-based framework in Article 33 does not provide sufficient legal clarity and guarantees to ensure effective and equitable access to secure environments for digital euro services. We would appreciate additional clarifications. IT (MS Comments):

DK PCY Questionnaire	MS Comments
	We are open to evaluate any improvement of article 33 in order to grant sufficient legal clarity and guarantees to ensure effective and equitable access to secure environments for digital euro services. IE (MS Comments): Generally, IE supports the premise of Art. 33 but recognises that it is likely not strong enough to ensure legal clarity and guarantee all PSPs have effective and affordable access to the secure environments (provide by OEMs) needed to support offline digital euro payments (without potentially encountering excessive fees from the OEM). A lack of clear definitions for "fair" and "reasonable" creates uncertainty. The security exception could be used by OEMs to block access without independent oversight and while dispute resolution is included, ADR is typically non-binding, so may not prevent real-world barriers to access. IE has a concern if legal certainty regarding effective and affordable access is not achieved, PSPs could experience expensive fees being charged by OEMs. It could see a situation developing, where PSPs would also have to negotiate individual contracts with OEMs and considers this may a burdensome task.

DK PCY Questionnaire	MS Comments
	IE considers that the DER may not be best placed to ensure access to secure environments as it considers this a broader matter with widespread implications (e.g. eIDAS2, PSR and PSD3). IE would welcome insights from the CLS in this regard. HR (MS Comments): According to the information stated in the DK PRES discussion note and ECB technical seminar held on 30 June 2025 we find that current FRAND-based framework in Article 33 does not provide sufficient legal clarity and does not guarantee effective and equitable access to secure environments for digital euro services. Current reference to access on FRAND terms lack sufficient clarity what constitutes "fair and reasonable" under FRAND terms which will prevent discriminatory or excessive pricing and could lead to implementation uncertainties or litigation. This is especially important for smaller providers or Member States with less bargaining power vis-à-vis large device manufacturers. Also, we support the statement in the DK PRES discussion note that the requirement under Article 23 for offline functionality to be included from the first issuance of the digital euro may amplify these dynamics, as a potentially large number of PSPs would need timely and consistent access to secure

DK PCY Questionnaire	MS Comments
	environments. These considerations may have implications for market functioning, access conditions, and the overall viability of broad PSP participation. In that regard, we find that FRAND terms and strictly necessary and proportionate measures should be prescribed in implementing or delegated act to specify the economic conditions for access and supporting effective and equitable access in practice. FR (MS Comments):
	France considers that the 'Digital Euro' regulation should only deal with payment issues and that telephone technology issues should be dealt with via other channels such as the DMA and DSA regulations or the prerogatives of DG COMP. We are therefore happy with the current framework.
	FI (MS Comments): We would support a further study on regulatory approaches on this matter, since this is a broader topic that is not only related to digital euro.
Q2. Do Member States support further specification or adjustment of the economic conditions for access to mobile devices under Article 33, with a view to ensuring legal clarity, proportionality and practical enforceability?	ES (MS Comments):

DK PCY Questionnaire	MS Comments
	As stated in the precious question, we could include elements similar to those foreseen in the Data Act: - developing model contractual clauses to promote balanced negotiations. Also, we could think of fostering joint negotiations by PSPs. - empowering the COM to intervene when access conditions are structurally unfair or discriminatory - mandating the COM to introduce guidance on what may constitute FRAND terms EE (MS Comments): EE: We support. DK (MS Comments): Yes, Cyprus supports the proposal to explore further specification of the economic access conditions. Such refinement would promote legal clarity, ensure proportionality, and support the practical enforceability of the regulation. DE (MS Comments): We would welcome further specifications and adjustments.

DK PCY Questionnaire	MS Comments
	The presidency note mentions model contractual clauses or possibilities for the Commission to intervene when unfair market conditions prevail (under the Data Act). In addition, we would welcome a **thorough analysis** – both practical and legal – **from the Commission** of what is possible. We take note that the **Digital Markets Act** and the Data Act are both recent Regulations launched at EU level. The Digital Markets Act not only introduces the **FRAND access but, under certain conditions, also an access free of charge.** In our understanding, Article 6 (7) of the Digital Market Act introduced free of charge access to certain hardware and software elements. This provision became relevant with regard to the access to the NFC module of a certain OEM. Also, the Commission has extensive experience with **legal disputes** with some of the OEMs. In addition, we would like to emphasize that **Article 12b of the eIDAS Regulation** also establishes a legal framework for interoperability and access to hardware and software features of OEMs when providing European Digital Identity Wallet services. According to Art. 12b of the eIDAS Regulation, effective interoperability and access shall be allowed free of charge. This raises the question of why Article 33 should follow a different approach, and

DK PCY Questionnaire	MS Comments
	what the reasoning behind this should be, since, in our understanding, the required technical solutions will most likely be very similar. Here, we would like to highlight one general thought: The need for addressing economic conditions and their definition by regulation depends largely on the concept defined for the secure mobile platform. Therefore, the intended technical solution should be considered now when deciding on the legal framework accompanying it. For example, the "Secured Applications on Mobile" (SAM) initiative, a standardization driven by GSMA and GlobalPlatform, aims for example to expand the use of secure elements beyond traditional services (like telecom). With SAM, these chips evolve into secure platforms for sensitive digital applications like electronic IDs, ticketing, or mobile payments. To achieve this, a specially protected and isolated security domain (called SAM-SD) is created within the secure element. This domain functions independently of both the user's mobile network operator and their device manufacturer, ensuring consistent hardware-level security across different systems. As a result, users benefit from improved data protection and broader access to trustworthy digital services. The SAM-concept would allow self-management of the secure mobile platform by the PSP or an independent intermediary. The cost and effort of OEM would be limited to providing feasible SE from

DK PCY Questionnaire	MS Comments
	trustworthy SE-vendors and to deploy the required software interfaces to connect to these SE. Overall, we would welcome more guidance from the Commission on these issues: What options are available? What would be the implications of FRAND access vs. free of charge access? Judging from the Commission's experience, what are the key elements which must be ensured? Based on this input, further amendments of Article 33 shall be analysed. CZ (MS Comments): Technological specification and economic conditions should be as universal and future-oriented as possible. CY (MS Comments): Yes, Cyprus supports the proposal to explore further specification of the economic access conditions. Such refinement would promote legal clarity, ensure proportionality, and support the practical enforceability of the regulation. AT (MS Comments):

DK PCY Questionnaire	MS Comments
	Yes, we agree. Further specifications or adjustments of the economic conditions for access to mobile devices under Article 33 are warranted to ensure legal clarity, proportionality and practical enforceability. SI (MS Comments): Yes, as indicated in the previous comment. PT (MS Comments): PT does not identify the necessity to introduce further specification or adjustments in this regard but would remain open to consider concrete suggestions. PL (MS Comments): PL: Yes. In our view it would be beneficial to further clarify the economic conditions of FRAND, e.g. by referring to reference costs (benchmarking against other MNO/OEM services) and indicating the entities responsible for dispute resolution. NL (MS Comments):

DK PCY Questionnaire	MS Comments
	NL comment: we would support further specification or adjustment of Article 33 in a delegated act, as this would make the regulation future-poof. We believe specifying these terms in the regulation would limit our flexibility unnecessarily.] LT (MS Comments): We support. IT (MS Comments): We support further specification or adjustment of the economic conditions for access to mobile devices under Article 33. On this point, we are concerned especially that FRAND principles might not effectively protect PSPs from the application of excessive fees. This would be inappropriate especially for the functioning of the offline functionalities as basic services that PSPs provide for free. We would welcome Commission and Council Legal Services support in order to evaluate the best, legally sound, solution. Perhaps we should look at other European regulatory frameworks and evaluate the possibility of introducing a provision that effectively protects PSPs from the fees charged by OEMs (e.g. free access for basic services). In this regard, the regulation should at least specify what fair access means.

DK PCY Questionnaire	MS Comments
	IE (MS Comments): IE supports further specification of the economic conditions under Article 33. Clearer rules on pricing and access terms are essential to avoid disputes, ensure proportionality, and make the obligations practically enforceable, especially for secure environments. HR (MS Comments): Yes, we support further specification or adjustment of the economic conditions for access to mobile devices under Article 33, with a view to ensuring legal clarity, proportionality and practical enforceability. FR (MS Comments):
	We are not in favour of opening up this subject, which will not be easy to deal with and could have repercussions on the Union's trade negotiations. Indeed, if we force manufacturers to open up access to the chip free of charge, this could trigger economic reprisals in the current context. This kind of subject cannot therefore be dealt with in the Euro Digital Regulation, but under the other channels mentioned above, in the hands of the Commission. As the ECB noted, the EU has a strong technological dependence on smartphones, but we cannot change this state of affairs in the short term.

DK PCY Questionnaire	MS Comments
	FI (MS Comments): See Q1
Q3. Would Member States agree with empowering the Commission with the possibility to introduce guidance on what may constitute FRAND terms, similar to Article 41 of the Data Act?	ES (MS Comments): Yes. EL (MS Comments): **EL:** The FRAND framework could be specified further. One way of doing this could be a mechanism similar to art 41 of the Data Act, we note however the non-binding nature of the terms envisaged in that article, which may not suffice in the case of the digital euro. EE (MS Comments): EE: We agree. DK (MS Comments): Cyprus agrees with empowering the Commission with the possibility to introduce guidance on what may constitute FRAND terms. DE (MS Comments): Yes, we would welcome this initiative.

DK PCY Questionnaire	MS Comments
	CZ (MS Comments): We support the possibility of empowering the Commission to introduce guidelines on FRAND requirements. CY (MS Comments): Cyprus agrees with empowering the Commission with the possibility to introduce guidance on what may constitute FRAND terms. AT (MS Comments): Yes, we would welcome further guidance by the Commission on what may constitute FRAND terms, similar to Article 41 of the Data Act. SK (MS Comments): We do not oppose empowerment for the Commission. SI (MS Comments): Yes, we agree. PT (MS Comments):

DK PCY Questionnaire	MS Comments
	PT supports this approach, following the example foreseen in the Data Act. We believe a COM guidance would be helpful for stakeholders to operationalize the requirements depicted in Article 33 before implementation. However, we also believe said guidance must embody the possibility to be amended post implementation, so as to be future proof and accommodate needed improvements derived from effective market experience. PL (MS Comments): PL: We are of the view that this would make the rules more consistent and reduce the risk of different interpretations in different Member States. NL (MS Comments): **NL comment**: we would agree with receiving more guidance by the Commission on what these FRAND terms may constitute, in a delegated act.] LT (MS Comments): We agree. It is important to keep in mind that the digital euro is a public good and will have a legal tender status, meaning that PSPs will have an obligation to distribute it and merchants will be required to accept it. Therefore, it would seem sensible to consider the possibility of a uniform European approach, with

DK PCY Questionnaire	MS Comments
	a view to ensuring that each PSP individually would not have to negotiate with OEMs to access the SE. IT (MS Comments): Yes, we agree. IE (MS Comments): IE notes the reference to possible guidance. While this could be helpful for interpretation, IE would point out that guidance is not legally binding and may not provide the level of legal clarity that is ultimately required. FR (MS Comments):
	We are open to this proposal.
	FI (MS Comments): See Q1
Q4. Do Member States support the proposed clarifications to Article 33, in particular the inclusion of "securely processing/executing … transactions", to better reflect the functional and security requirements of the offline digital euro?	ES (MS Comments):

DK PCY Questionnaire	MS Comments
	Yes, we agree, by introducing this broader formulation we avoid the text being too limiting. We understand that the inclusion of *3rd party technical support providers acting on behalf of PSPs* in the wording refers to the trusted service managers that install the offline functionality in the cell phone EL (MS Comments): **EL:** We could support the proposed clarifications. EE (MS Comments): EE: We support. A technology-neutral approach is important. DK (MS Comments): Cyprus supports the proposed clarifications. DE (MS Comments): We welcome this amendment to Article 33. The wording shall be technology neutral and ensure that the transactions will be enabled. We do support the amendment to ensure that atomic operations, such as transaction signing and balance updates, can be executed.

DK PCY Questionnaire	MS Comments
	However, as long as the technical implementation is not clear, an **even more general wording** combined with a non-exhaustive list of features could might work even better. PSPs might, for example, also need the capability to manage and maintain a payment application on the Secure Hardware Element which may need a dedicated design of the SE and supporting software in the mobile device. Therefore, it should be ensured that 'processing/executing of transactions' effectively covers all possible scenarios. CY (MS Comments): Cyprus supports the proposed clarifications. AT (MS Comments): Yes, we support a broad formulation to cover a wider range of requirements. The new wording provides only limited changes to the previous version and further elaborations of functional and security requirements for mobile devices could be warranted. SK (MS Comments): We support the amendment.

DK PCY Questionnaire	MS Comments
	SI (MS Comments): / PT (MS Comments): PT agrees with the PRES DK's stance on sticking with a broader drafting to encompass a wider scope of actions, which would increase probabilities to guarantee the intended access in its entirety. Regarding the concrete amendments, PT supports those as proposed. PL (MS Comments): PL: We support the proposed clarifications to Article 33. NL (MS Comments): **NL comment**: we agree with the clarifications, however, we would like to add the following in bold underlined: *[…]effective interoperability with, and access for the purposes of interoperability to, the hardware features and software features necessary for* ***the secure storing of offline digital euro holdings and*** *securely processing (/executing) online or offline digital euro payment transactions, including the*

DK PCY Questionnaire	MS Comments
	secure *storage and transfer of data, on fair, reasonable and non-discriminatory terms."*] LT (MS Comments): We support the proposed clarifications to Article 33. IT (MS Comments): Yes, we agree. In addition to that, we suggest specifying in article 33 that original equipment manufacturers of mobile devices and providers of electronic communication services shall have no visibility on transaction data nor store them. This is key to be aligned to the offline level of privacy that the digital euro strives to achieve. Transaction data are to be disclosed to no third party. While it is clearly specified that "For offline digital euro payments, the European Central Bank, the national central banks and payment services providers will not gain access to personal transaction data", we would advise to extend this list to any third party, including explicitly OEMs. IE (MS Comments):

DK PCY Questionnaire	MS Comments
	IE supports the new drafting. Processing or executing transactions, including offline, is broader and more accurate than just storing and transferring data. It more accurately reflects the real technical needs of the digital euro. FR (MS Comments):
	We agree.
	FI (MS Comments): Yes
Q5. Do Member States consider that the formulation of Article 33 is sufficient to ensure effective interoperability with the hardware and software features of mobile devices, notably in the case of offline transactions?	ES (MS Comments): The best place could be an Annex or Commission guidelines. Even if the rulebook seems the most appropriate place to determine technical requirements; where the industry has a voice in the Rulebook Development Group, and the state-of-the-art technology is searched. It is not an applicable to OEMs and MNOs, so it is not the best option. The core text of the regulation should remain tech neutral, but an Annex could be more easily modified EL

DK PCY Questionnaire	MS Comments
	(MS Comments): **EL:** We agree with the view of the ECB and the Commission not to overburden the text with technical specifications that may change over time and to have a technology-neutral approach. EE (MS Comments): EE: We are open to further specifying the features in the secondary legislation to ensure that the requirements are future-proof. DK (MS Comments): Cyprus supports the presidency's suggestion of including a broader formulation in order to cover wider range of requirements. DE (MS Comments): We would **welcome further amendments of Article 33** in order to ensure effective interoperability. Again, we would recall also Article 25 which sets out that interoperability with the EUDI Wallet shall be ensured. Regarding other options, we are open to explore all options with regard to the necessary functional and security requirements.

DK PCY Questionnaire	MS Comments
	However, we would believe it would be meaningful to identify first the necessary requirements. In our understanding, the practical implementation of the regulation through the ECB and the PSPs would require a **comprehensive set of technical standards and specifications**. These standards would define the solution to be implemented by the OEM in detail. To ensure secure and sovereign use of secure hardware elements, **relevant technical standards and specifications must be defined**. One way would be through **implementing acts**. Without them, access would rely on proprietary OEM interfaces, limiting openness and independence. Referencing standards helps prevent fragmentation and supports a harmonized digital single market. We would welcome an **update from the ECB on the relevant standards and specifications** which shall be applied. In any event, all measures should be **harmonised across the Union**. Therefore, they should not be issued as guidelines by competent authorities at national level. Rather, they should be **set out in EU legislation** – potentially at level 2, where they can be adapted and updated as needed. Overall, we would welcome **further guidance from the Commission** but also from the **ECB** regarding the technological and legislative needs. To us, it seems crucial to obtain this input without undue delay.

DK PCY Questionnaire	MS Comments
	In a second step, it shall be analysed whether these requirements shall become part of the legislative proposal and in which form, e.g. a separate Annex or guidelines. CY (MS Comments): Cyprus supports the presidency's suggestion of including a broader formulation in order to cover wider range of requirements. AT (MS Comments): Further elaborations of functional and security requirements for mobile devices could be warranted also in light of the recent technical input during the dedicated seminar on mobile device access highlighting the challenges and limitations regarding mobile device security and the need to ensure adaptability over time as for instance by a Commission delegated act. SI (MS Comments): / PT (MS Comments):

DK PCY Questionnaire	MS Comments
	PT does not identify at this time the necessity to further amend Article 33 but would remain open to consider additional concrete suggestions. Similarly to our stance regarding the FRAND framework, PT would also be willing to accept, if considered necessary, further precising requirements in specific guidelines before implementation. We would avoid expanding and overly prescribing the L1 text in order not to preview complex operational terminology that may not even be future proof. In our view, any issued guidelines should allow for future reviews to benefit from effective market experience, which again we deem crucial to evaluate whether the legislative requisites advanced are fit for purpose. PL (MS Comments): PL: We lean towards the option 5.b (Define those requirements in specific guidelines that would be issued by competent authorities). NL (MS Comments): **NL comment:** Although we believe the proposed clarifications are helpful, we would be open to discussing further clarifications in a delegated act.] LT (MS Comments):

DK PCY Questionnaire	MS Comments
	We consider that the formulation of Article is not sufficient to ensure effective interoperability. We are in favour to define those requirements in specific guidelines that would be issued by the EC or another relevant European institution, as these guidelines should be applied uniformly across the EA. IT (MS Comments): We are open to explore and evaluate any improvement of the text. However, it's important to emphasize that the smartphone world is one in which technology and industrial production are rapidly evolving, and setting overly rigid regulatory frameworks could have an undesirable effect. For this reason, we deem that a flexible regulatory framework, like L2 legislation, would be preferable. IE (MS Comments): IE does not consider the formulation of Article 33 sufficient in ensuring effective interoperability, given the requirements for access have not been determined. IE suggests pursuing a combined approach as outline in option 5c.

DK PCY Questionnaire	MS Comments
	IE supports including core requirements in the regulation to ensure legal certainty, while leaving technical and implementation details to binding secondary legislation such as delegated or implementing acts to ensure adaptability as technology evolves. This option may be a more complex process but offers a balance between enforceability and adaptability. FR (MS Comments):
	As mentioned earlier, the technologies used will be set by the market.
	We don't want to complicate the text with devices based on smartphone technologies FI (MS Comments): We are still assessing this and we are hoping for further discussions and information.
Q6. Do Member States find the envisioned accessibility level of the smartphones form factor to be sufficient in light of the inclusiveness objectives of the digital euro?	ES (MS Comments): - 90% of smartphones with secure environment that accepts offline is high - Also, other form factors like smartcards with bridge devices, that are cheap, can tackle the population that does not have a smartphone with those characteristics. We wonder whether the bridge devices should be provided to those users that choose cards as the option to be provided by

DK PCY Questionnaire	MS Comments
	the PSP as a basic service (not applicable for those who choose cell phones) EL (MS Comments): **EL:** As the ECB explained in the June 30 technical seminar, PSP access to the smartphone's embedded secure environment is critical for the digital euro offline functionality. In this context, we take note that the technical requirements for the offline digital euro cannot be fulfilled by all phone devices, leaving a certain portion of users without access to the specific product. In case any additional measures are proposed to cover this gap, they should take into account the principle of proportionality and could allow for a transitional period. EE (MS Comments): EE: It seems sufficient given that the accessibility level is probably improving over time, and alternatives are in place. DK (MS Comments): Cyprus supports exploring whether additional measures are needed to ensure that secure environments are available across the full range of commonly used devices. These considerations should inform future reflections on how to ensure that the digital euro remains accessible to all users, including those relying on lower-cost devices. DE

DK PCY Questionnaire	MS Comments
	(MS Comments): In general, we believe that the offline digital euro should be available to all users. At first glance, covering 90% of the available smartphone in 2029 already seems to be a rather high number. With regard to the remaining 10%, we would ask for more clarification: Does the ECB plan to introduce also smartcards for online and/or for offline? Albeit only providing an inferior user experience, smart cards could bridge that remaining divide of 10%. We are wondering about the role of cards, in particular at the beginning of the project. Many citizens will be used to pay with their cards and not with their smartphones. Going completely without cards could hamper the digital euro's uptake because users would need to adapt to an entirely mobile device based payment process. The Presidency Note mentions the option to 'explore whether additional measures are needed to ensure that secure environments are available across the full range of commonly used devices'. What would such measures be? Is there a practical and/or legal way to ensure access to all smartphones? Also, we are wondering about the costs for consumers of those lower budget-oriented smartphones? With a view to inclusion, one should bear in mind also

DK PCY Questionnaire	MS Comments
	an increase in the possible cost if Secure Hardware Elements would become mandatory. If the remaining users could rely on alternative form factors such as smartcards combined with bridge devices and that any initiative to further increase the availability of compatible smart phones would likely require another market intervention by the co-legislators, we have a tendency to believe that such a level of availability might be sufficient. CZ (MS Comments): Due to the lack of data, we are based only on the data presented by the ECB. We consider it crucial that the digital euro as a new payment method is available to all interested parties, regardless of the price and brand of their mobile phone. CY (MS Comments): Cyprus supports exploring whether additional measures are needed to ensure that secure environments are available across the full range of commonly used devices. These considerations should inform future reflections on how to ensure that the digital euro remains accessible to all users, including those relying on lower-cost devices.

DK PCY Questionnaire	MS Comments
	AT (MS Comments): Yes, we agree. The potential distribution and availability of form factors such as smartcards (or simpler cards with bridge devices) and their usage in an offline or online scenario, as potential alternatives, still seem unclear to us. SK (MS Comments): As other modes of the payment will be available, we do not see a 10% share of incompatible phones to be of a major concern. The share will likely be decreasing over time. The concern we have is, that subject to article 33 being extended to payment services in general through PSR, the processing capacity of additional share of smartphones could be negatively affected. SI (MS Comments): The remaining 10% of smartphones in 2029, which may not support the offline digital euro, should not pose a problem, as end-users will always have the possibility to use a physical card for offline payments PT (MS Comments):

DK PCY Questionnaire	MS Comments
	PT understands the importance of ensuring full indiscriminate access to the digital euro for all euro area citizens irrespective of their possession of a smartphone that is equipped with the necessary technical and security capabilities. With this setting in mind, we believe options, as described in the note, to enhance that access across all used devices can be evaluated but its pursuance must be based on a cost-benefit analysis. In our view, the mentioned solutions may embody significant operational and financial burdens that perhaps do not justify the added coverage. It should not be forgotten that accessibility does not necessarily imply usage and that, even if complete smartphone coverage is achieved, citizens who do not hold one will probably still not be able to access the offline version of the digital euro. We also deem it as unrealistic the objective to guarantee the same level of user experience, given the very distinct features of smartphones under usage. Therefore, concerning accessibility, we consider the focus should be on firstly guaranteeing that provided solutions meet all required security standards. Trying to bypass those to attain greater coverage may leave certain users vulnerable, for instance being easily targeted for fraud purposes. Additionally, and instead of attempting complete coverage, future users should be provided with transparency on the kinds of devices that support the digital euro, and its offline version. Finally, we note enhanced inclusiveness may not necessarily

DK PCY Questionnaire	MS Comments
	be effective right from the beginning, but rather progressively improved based on verified experience and actual recognised gaps. PL (MS Comments): PL: Generally we find the envisioned accessibility level of the smartphones form factor to be sufficient in light of the inclusiveness objectives of the digital euro. However, it should be born in mind that the remaining 10% of smartphone that are mentioned in the note, located in the lower-cost segment and that may not support the offline digital euro may be held, for instance, by vulnerable groups of the society, this not guaranteeing the inclusiveness of these groups as regards digital euro. NL (MS Comments): **NL comment**: Yes, it is important that the offline digital euro is available to those that want to use it. For the majority this will be possible through mobile phones. For those that are in possession of smartphones that are not compatible with the offline functionality, the offline payment card would still be available. Also, they will still be able to use cash. In our expectation, accessibility of the mobile device offline features will improve over time.

DK PCY Questionnaire	MS Comments
	We would also like to note that the offline digital euro will never be the only solution to resilience in payments. For example, EU citizens are encouraged to prepare for 72 hours without government support and/or access to online means of payment. We can imagine that people either have offline digital euros available or hold a minimum amount of cash in case of emergencies.] LT (MS Comments): We think that accessibility level is sufficient. IT (MS Comments): Yes, we can broadly agree. However, as emphasized on several public occasions, we expect the digital euro to be inclusive by design and leave no one behind. IE (MS Comments): IE considers accessibility level to be sufficient. Provisions for those who do not use smart phones are being made e.g. physical card. Additionally, IE is aware the ECB's app will cater to the highest degree of accessibility as prescribed by the European Accessibility Act. FR

DK PCY Questionnaire	MS Comments
	(MS Comments):
	France considers that the regulation should only cover payment services and should not extend to the handset market. As explained above, the handset market is global and different from the payment market. We will not be able to influence the technologies available via this regulation. The ECB's 'digital euro' product will have to evolve over time with technologies that will be set by the market. The current level of accessibility proposed is sufficient: citizens who do not have compatible smartphones will still be able to use cash or payment cards.
	FI (MS Comments): Yes
Q7. Should a specific supervisory framework be introduced to ensure compliance with Article 33, for example involving competent authorities designated under Article 6 in the digital euro regulation? If so, how should coordination at EU level be ensured?	ES (MS Comments): We would need to understand how a specific supervisory framework would work in practice. We see that an enforcement at EU level could be more appropriate, with the Commission having an enforcement role similar to the role conferred in the DMA. In any case, we consider it is important that such a regime is compliant with EU law. We could also learn from the enforcement model of the data act, that also foresees enforcement of FRAND terms. We need to better understand to what

DK PCY Questionnaire	MS Comments
	extent a legal text based on article 133TFUE can introduce enforcement and supervisory obligations to national authorities outside the financial scope. EL (MS Comments): **EL:** We are still reviewing this proposal, as it would require additional resources and introduce further complexity. EE (MS Comments): EE: We have no strong opinion at this stage. However, we can support the review clause. DK (MS Comments): Cyprus supports the Presidency's recognition of potential enforcement challenges. At this stage, Cyprus' opinion, it is prudent to first assess the practical need for a dedicated supervisory framework, including the scale of implementation challenges and enforcement gaps. DE (MS Comments): We believe that an enforcement regime on Article 33 is needed and that such a regime should cover both financial and non-financial access conditions to the

DK PCY Questionnaire	MS Comments
	secure environment. Without an enforcement regime, effective implementation of Article 33 may not be achievable. A possible enforcement regime should be established at the European level, potentially involving the Commission, given that virtually all original equipment manufacturers operate across the entire Union. Depending on whether access to the secure environment would be unique to the digital euro or also established for other payment service providers, for instance via the PSD3/PSR, the ECB or the European Banking Authority could play a role in harnessing the contributions of the national competent authorities which could provide data. CZ (MS Comments): We are flexible on this issue. CY (MS Comments): Cyprus supports the Presidency's recognition of potential enforcement challenges. At this stage, Cyprus' opinion, it is prudent to first assess the practical need for a dedicated supervisory framework, including the scale of implementation challenges and enforcement gaps. AT

DK PCY Questionnaire	MS Comments
	(MS Comments): Yes, a specific supervisory framework should be further considered to ensure compliance with Article 33. In our view, a reasonable and harmonized enforcement of Art 33 would be only possible at an EU-wide level. Leaving the competence with national authorities could lead to market fragmentation, hamper level playing field and weaken negotiation power for PSPs. SK (MS Comments): We are not convinced that such framework would be necessary. If specific supervisory framework is introduced, it should be at the EU level. SI (MS Comments): / PT (MS Comments): PT is still assessing this specific issue but would highlight the apparent pertinence in attempting to establish a supervisory framework for the purpose of compliance with Article 33. This can indeed be operationalised at the EU level and be based on notices and complaints from market agents directed at an agreed upon authority.

DK PCY Questionnaire	MS Comments
	PL (MS Comments): PL: We do not have a strong position on that point. Perhaps it is worth considering the need to establish dedicated sectoral supervision with a coordinated role for the European Commission. It may also be beneficial to establish an enforcement contact point in each Member State. NL (MS Comments): **NL comment:** We would propose observing how the current arrangement functions in practice as we could always have the option to make adjustments through a review clause. In our opinion, we should be careful with establishing an entirely new supervisory regime, as this could increase costs and add unnecessary complexity.] LT (MS Comments): We support the EU's approach to supervisory frameworks and coordination. This will make sure that the end-user has the uniform experience in the EA. We do not support that national CA would have competences to supervise compliance with Article 33. IT

DK PCY Questionnaire	MS Comments
	(MS Comments): Given the specificity of the subject matter, the global scope of activity of device manufacturers and their non-financial nature, the authorities designated under Article 6 in the digital euro regulation may not be the most suitable for this task. For this reason and considering what is already provided for in Regulation (EU) 2022/1925 of the European Parliament and of the Council (Digital Market Act), we believe that should be evaluated the possibility that the enforcement of any dedicated framework may be the responsibility of the Commission, possibly with the support of the ECB. IE (MS Comments): IE supports the establishment of a specified supervisory framework to ensure effective enforcement of article 33, given that over 70% of devices are not subject to obligations under the digital markets act and the cross sectoral nature of the issues involved. Competent authorities under Article 6 should have a role, with EU level coordination, ideally led by the ECB and Commission, to ensure consistent application, particularly for access to secure environments. HR (MS Comments):

DK PCY Questionnaire	MS Comments
	We find that supervisory topic is very important for the implementation of the whole Proposal and especially Article 33. We support the proposal that a specific supervisory framework should be introduced to ensure compliance with Article 33, for example involving competent authorities designated under Article 6 in the digital euro regulation. In that regard we would appreciate opinion of the EC how should coordination at EU level be ensured due to its competence for Data Act, Digital Markets Act. FR (MS Comments):
	We are not in favour of adding such a supervisory framework because the supervisory authorities will not have additional resources to carry out these tasks.
	FI (MS Comments): We are sill assessing this. However, if there would be a supervisory framework, we would more in favour of an EU wide approach.