Council of the European Union
General Secretariat

PUBLIC

Interinstitutional files:
2023/0212 (COD)

Brussels, 24 October 2025

WK 14308/2025 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:	Digital euro - WP meeting on 30 October 2025 - Presidency discussion note on privacy, technical proofs and resilience

Danish Presidency
Council of the European Union

PUBLIC

Presidency discussion note on privacy, technical proofs and resilience

Working Party on Financial Services and the Banking Union

30 October 2025

Proposal for a regulation on the establishment of the digital euro

Meeting on 30 October 2025

PUBLIC

1. Introduction

Discussions on privacy protection and resilience have evolved progressively across Presidencies, reflecting the importance of ensuring both a high level of data protection for users and a robust operational framework capable of withstanding exceptional circumstances. Privacy has been a central concern for Member States and was most recently discussed in the Council Working Party (CWP) meeting in April 2025 under the Polish Presidency.

During these discussions, Member States provided extensive written comments on the privacy-related provisions in the legacy text, seeking further clarity on the envisaged privacy framework and the division of responsibilities between payment service providers (PSPs) and the Eurosystem. To respond to these requests, the ECB organised dedicated technical seminars in March and June 2025 to present the envisaged data flows and privacy-preserving mechanisms within the Digital Euro Service Platform (DESP). At these seminars, the ECB explained that the technical design ensures a clear segregation of data between PSPs and the DESP, and that only the minimum data necessary to processing digital euro payments would be shared, with digital euro users' identities remaining pseudonymised.

Following these explanations, several Member States expressed confidence in the proposed approach, while others underlined the importance of translating these assurances into the legal text, in particular through targeted adjustments to Articles 34, 35, 36 and Annex V.

In parallel, recent developments in Union law, namely a **judgment by the Court of Justice of the European Union (CJEU), have clarified the conditions under which the recipient of pseudonymised data is not to be regarded as processing personal data**, and therefore not subject to the Union legislation on the protection of personal data. The Presidency considers it appropriate to align the privacy provisions in the Regulation with this ruling.

The topics of privacy, technical proofs and resilience are closely linked. Member States have broadly supported the Presidency's overall direction on these areas but have requested further clarifications, including **the scope and storage technical proofs**, as well as on the procedures and division of responsibilities under the safeguard measures set out in in the resilience articles, in particular through targeted adjustments to Articles 22, 31, 34 and accompanying recitals 67 and 67a.

Finally, **the question of safeguarding the digital euro against counterfeiting and preventing double spending was most recently discussed under the Belgian Presidency**. In light of the

PUBLIC

ECB's announcement of the selected digital euro service providers[1], the Presidency considers it timely to revisit Article 37 of the draft Regulation to provide additional **clarity on the data processing responsibilities of the Eurosystem in relation to offline digital euro payment transactions** and to propose targeted adjustments to this provision.

Against this background, and building on Member States' comments, **the Presidency has prepared this note setting out proposed amendments aimed at fostering common grounds among Member States on these topics**. With the aim of ensuring a complete overview of the proposed changes, the Presidency has provided the amended Recitals and Articles in full as an Annex to this note.

[1] Press release: https://www.ecb.europa.eu/press/intro/news/html/ecb.mipnews251002.en.html

PUBLIC

Chapter I

1.1 Article 34 – Processing by payment service providers

The Presidency recalls that Article 34 establishes the framework governing the processing of personal data by PSPs, ensuring that such processing is carried out in accordance with the General Data Protection Regulation (GDPR) and other relevant Union legislation. The article also clarifies that PSPs act under a public interest mandate when performing these activities.

The Presidency notes, that for the provision of offline digital euro in accordance with Article 34(1)(c), which also encompasses supporting the integrity checks, PSPs will need to process two additional categories of data that are necessary to ensure the integrity and security of the offline digital euro:

a) attributes of the authenticity of the local storage device, to ensure that the device is authentic;
b) attributes of the authenticity of offline digital euro, to ensure the authenticity of the offline digital euro as a liability of the ECB or the NCBs, comparable to "serial numbers" associated with offline digital euro units.

To reflect these elements, **the Presidency proposes a new Article 34(1)(c'), and to include the corresponding data categories in Article 2 and Annex III**. In addition, to further strengthen the privacy and protection of the digital euro users' data, the Presidency proposes to specify in Article 34(1) and Annex III that processing of personal data by PSPs may also cover activities related to funding and defunding. It is further proposed to specify that for the purposes of letter (c) and letter (c'), PSPs shall not monitor the use of the offline digital euro user interface, except to the extent it is strictly necessary to ensure the integrity of the offline digital euro.

Question 1-2 to Member States:

Q1. *Do Member States agree with the Presidency's proposed changes to Articles 2 and 34?*

Q2. *Do Member States agree with the Presidency's proposed changes to Annex III?*

PUBLIC

Drafting suggestions

BE Presidency in *black*
DK Presidency in *green*

Article 2 - Definitions

[…]

37. (new) 'attributes of the authenticity of the local storage device' means security features embedded in the local storage device that authorise holding offline digital euro, as well as performing digital euro transactions, including requesting and transferring offline digital euro;

38. (new) 'attributes of the authenticity of the offline digital euro' means security features embedded in offline digital euro holdings, proving they are a liability of the European Central Bank or the national central banks;

Article 34 - Processing **of personal data** by payment service providers

1. Payment service providers perform a task in the public interest where they process personal data for the following purposes:

(a) the **implementation and** enforcement of limits~~**, including the verification of whether prospective or existing digital euro users have digital euro accounts with another PSP,**~~ as referred to in Article 16**, including by providing information to and consulting the single access point referred to in Article 16(7a)**;

(b) funding and defunding as referred to in Article 13(2) and (3), and digital euro payment transactions as referred to in Article 13(4);

(c) the provision of offline digital euro, including the registration and de-registration of the local storage devices as referred to in letter (b) of Annex I;

(c') to comply with the anti-money laundering rules applying to offline digital euro in accordance with Article 37(3).

[…]

For the ~~**provision**~~ **funding and defunding** of offline digital euro, the processing of personal data by payment service providers is limited ~~**to funding and defunding**~~ **to**

PUBLIC

personal data referred to **in** ~~**accordance with**~~ Article 37 ~~**paragraphs 3,**~~ (4) ~~**and 5**~~ **and Annex III**.

For the purpose of letter c and c', payment service providers shall not monitor the use of the offline digital euro user interface, except to the extent it is strictly necessary to ensure the integrity and security of the offline digital euro.

ANNEX III - Personal data processed by payment service providers

1. For the purpose of ~~**point (a) of**~~ Article 34(1)**(a)**, processing shall be limited to:

(i) the user identifier;

(ii) the user authentication;

(iii) information on digital euro payment accounts, including the unique digital euro payment account number;~~ **and**~~

(iv) information of non-digital euro payment accounts, including the account number of the linked non-digital euro payment account~~.~~**; and**

(v) funding and defunding data as defined in Article 37(4).

[…]

3. For the purpose of ~~**point (c)**~~ Article 34(1**)(c) and (c')**, processing shall be limited to:

(i) the user identifier~~,~~**;** including the name of the local storage device holders;~~ and~~

(ii) information on the local storage device, including the identifier of the local storage device;

(iii) attributes of the authenticity of the local storage device; and

(iv) attributes of the authenticity of the offline digital euro.

PUBLIC

1.2 Article 35 and 36

1.2.1 Alignment of privacy provisions with recent CJEU case law

On 4 September 2025, the Court of Justice of the European Union issued its judgment in case C-413/23 P – EDPS v. Single Resolution Board (SRB). The Court clarified the conditions under which the recipient of pseudonymised data is not considered to be processing personal data and is, therefore, not subject to the Union legislation on the protection of personal data.

According to the judgment, **the recipient of pseudonymised data is not processing personal data when the risk of identifying individuals is, in practice, insignificant** - for example, when identification is prohibited by law or could require a disproportionate effort. This could be the case when the recipient has no legal or practical access to the pseudonymisation key or other information that would enable re-identification.

The Presidency notes that the CJEU's ruling provides additional legal clarity regarding the interpretation of pseudonymised data in Union law. The judgment specifies that, where recipients of pseudonymised data do not have access to identifying information, they cannot, as a matter of law or in practice, identify individual users. It also provides useful indications on the data protection safeguards that could be reflected in the legislative text to ensure a consistent application of data protection principles in the context of the digital euro. The Presidency further notes that this clarification provides additional legal certainty regarding the interpretation of pseudonymised data. It is consistent with the privacy-by-design approach foreseen for the digital euro and further delineates the respective roles of PSPs and the Eurosystem, under which the ECB and NCBs would not have access to information enabling identification of individual users.

To align the draft Regulation with this development, **the Presidency proposes limited and clarifying adjustments to Articles 35 and 36 and their related recitals**. The intention is to clarify that the ECB and NCBs would process personal data to perform the tasks set out in Article 35(1) only if this cannot be exclusively achieved by processing non-personal data. This point is further clarified in Recital 76, where it is proposed to spell out that as a general rule and insofar it is possible, the ECB and NCBs will perform their tasks without processing personal data. In addition, the Presidency proposes to delete Recital 76a, as its contents is now reflected in the operative provisions.

In addition, the Presidency proposes to clarify Article 35(4) to ensure a clear segregation between the data processed by PSPs, which allow the identification of digital euro users, and the personal data processed under the control of the ECB and the NCBs. The amendment would specify that **the Eurosystem shall not be in a position to lift these safeguards during any processing under its control and shall not be able to attribute the data to a specific user**, including by cross-checking with other information. It would also

PUBLIC

clarify that **the ECB and the NCBs cannot request or use information obtained as part of other tasks under Union or national law to identify individual users**. The aim is to reflect the Court's reasoning and ensure that the Regulation provides clear, enforceable safeguards consistent with the technical design of the digital euro.

Finally, the **Presidency proposes to align Article 36(5) with Article 32(1) by removing the reference to NCBs**, as Article 32(1) already provides that the ECB alone may designate the providers of support services.

1.2.2 Article 36 - Processing by providers of support services

The Presidency notes that only a limited number of technical comments were received from Member States on Article 36. Taking these into account, the Presidency proposes minor drafting adjustments to paragraphs 36(1)(a) and 36(4) to reflect Member States' requests and align the wording with Article 32(3) in the legacy drafting from the Belgian Presidency.

Questions 3-4 to Member States:

Q3. *Do Member States agree with the Presidency's proposed adjustments to Articles 35(1), 35(4), 36(5), recital 76 and recital 76a to align the draft Regulation with the CJEU ruling?*

Q4. *Do Member States agree with the Presidency's other proposed drafting changes to Article 36?*

Drafting suggestions

ES Presidency in *red*
BE Presidency in *black*
PL Presidency in *blue*
DK Presidency in *green*

Article 35 - Processing of personal data by the European Central Bank and the national central banks

1. The European Central Bank and the national central banks perform a task in the public interest or exercise official authority where they process personal data for the following purposes **and insofar as these purposes cannot be exclusively achieved by processing non-personal data**:

(a) provision of access for payment service providers to the digital euro settlement infrastructure and support the exchange of messages between payment service providers;

PUBLIC

(b) settlement of online digital euro payment transactions;

(c) safeguarding the security and integrity of the digital euro settlement infrastructure and of local storage devices;

(ca) protection of the digital euro against counterfeiting and prevention of double-spending of digital euros;

(d) supporting ~~**verification by**~~ **the implementation and enforcement of limits by** payment service ~~providers **of whether a prospective user already has digital euro payment accounts with other payment service providers in order to prevent the circumvention of limits**~~**,** in accordance with Article 16**(7a)**;

(e) ~~**in exceptional circumstances as defined in Article 31 (2),**~~ authorising ~~**payment service providers in**~~ **and supporting the** switching **of** digital euro payment accounts **in accordance with Article 31(2) and (3)**~~**held with a payment services provider to another payment service providers designated by the digital euro user.;**~~

(f) facilitating the exchange of messages for the resolution of disputes in accordance with Article 27;

(g) facilitating the fraud detection and prevention tasks of payment service providers in accordance with Article 32.

2. ~~**For the purposes referred to in paragraph 1,**~~ Annex IV lays down the types of personal data **that the European Central Bank and the national central banks may process for the purposes referred to in paragraph 1, points (a) to (e). Annex V lays down the types of personal data that the European Central Bank and the national central banks may process for the purposes referred to in paragraph 1, points (f) and (g).**

3. The Commission is empowered to adopt delegated acts in accordance with Article 38 to ~~**update**~~ **supplement or amend, including deletion,** the types of personal data listed in Annex IV **and Annex V**.

4. **Without prejudice to Article 34(4), the European Central Bank and the national central banks** ~~**Personal data processed for tasks referred to in paragraph 1**~~ shall ~~**be supported by**~~ **adopt and implement** appropriate technical and organisational measures including state-of-the-art security and privacy-preserving measures ~~**when processing personal data for tasks referred to in paragraph 1**~~. Th**ese** ~~**is**~~ shall include the ~~**pseudonymisation and**~~ clear segregation ~~**of**~~ **between, on the one hand, the** ~~**personal**~~ data **processed by** ~~**to ensure that**~~ the European Central Bank and the national central banks **and, on the other hand, the personal data held by the payment service provider that allow to identify a digital euro user. The European Central Bank and the national central banks shall not be in a position to lift these measures during any processing of**

PUBLIC

the data which is carried out under their control. These measures shall prevent the European Central Bank and the national central banks from attributing the data to the data subject including by recourse to other means of identification such as cross-checking with other factors, in such a way that the person concerned is not identifiable by the European Central Bank and the national central banks. ~~**cannot directly identify individual digital euro users.**~~ **In particular, the European Central Bank and the national central banks shall not request from the payment service providers any information, and shall not use any information obtained as part of other tasks enshrined upon them by Union or Member States law to identify individual digital euro users.**

5. The European Central Bank shall be considered the controller of personal data **under** as regards **to** the purposes referred to in paragraph**s** 1 ~~**and 8 of this Article**~~. When the European Central Bank carries out a task referred to in paragraph**s** 1 **and 8** jointly with the national central banks, they shall be joint controllers for that task.

6. This Article is without prejudice to the processing of personal data involved in the performance of the other tasks and powers, including for the supervision of credit institutions and the oversight of payment systems, of the European Central Bank and the national central banks.

~~**7. Where the European Central Bank decides not to confer tasks referred to in Articles 27 and 32 upon providers of support services, the European Central Bank may process the types of personal data referred to in Annex 5 subject to the requirements referred to in paragraph 4 of this Article.**~~

8. ~~**For purpose of supporting the task of payment service providers to enforce the holding limits in accordance to Article 16(1) and ensuring the emergency switching upon the request of the user in accordance with Article 31(2), the ECB may alone or jointly with national central banks establish a single access point of digital euro user identifiers and the related digital euro holding limits as referred to in point (4) of Annex 4.**~~ For purpose of supporting the task of payment service providers to enforce the holding limits in accordance to Article 16(1) and ensuring the emergency switching upon the request of the user in accordance with Article 31(2) or in the circumstances of Article C, the European Central Bank may alone or jointly with national central banks establish a single access point of digital euro user identifiers and the related digital euro holding limits as referred to in point (4) of Annex IV. The European Central Bank ~~and the national central banks~~ shall implement appropriate technical and organisational measures including state-of-the-art security and privacy-preserving measures to ensure that the identity of individual digital euro users cannot be inferred from the information accessed via the single access point ~~referred to in Article 16(7a) and Article 31(3)~~ by entities other than payment service providers whose customer or potential customer is the digital euro user.

PUBLIC

9. The European Central Bank and national central banks shall not have access to information stored pursuant to Article 34(5).

Article 36 - Processing **of personal data** by providers of support services

1. Where the European Central Bank decides to confer tasks referred to in Articles **22**, 27 and 32 upon providers of support services providers of support services shall provide payment-related services across PSPs. In such a situation, **providers of support services** ~~**payment service providers**~~ perform a task in the public interest**,** where they process personal data for the following purposes:

(aa) supporting the use of the unique digital euro payment alias number together with ~~**optional**~~ **user aliases in accordance with Article 22(3a);**

(a) supporting the **securing of payment information and the** prevention and detection of fraud across payment service providers in accordance with Article 32;

(b) supporting the exchange of messages for the resolution of disputes in accordance with Article 27.

2. For the purposes referred to in paragraph 1, Annex V lays down the types of personal data.

3. The Commission is empowered to adopt delegated acts in accordance with Article 38 to ~~**update**~~ **supplement or amend, including deletion,** the types of personal data listed in Annex V.

4. ~~**The processing of personal data for the purposes referred to in paragraph 1**~~ **The European Central Bank, national central banks and providers of support services shall** ~~**only**~~ take ~~**place when**~~ appropriate technical and organisational measures including state-of-the-art security and privacy-preserving measures ~~**are implemented**~~ to ensure that the providers of support services cannot directly identify individual digital euro users. **This shall include the pseudonymisation and clear segregation of personal data.**

5. The providers of support services shall be considered to be the controllers of personal data as regards the purposes referred to in paragraph 1 of this Article**,** ~~**unless the European Central Bank and the national central banks were to take upon them the responsibility of controller**~~**. This paragraph is without prejudice to t**The European Central Bank ~~**and the national central banks**~~ **shall not process personal data when** appointing the operators of any payment-related services across ~~**PSPs**~~ **payment service providers** and **when** auditing ~~**of**~~ the service performance level **of providers of support services** ~~**without processing any personal data**~~.

PUBLIC

Recitals

(76) **The European Central Bank and the national central banks should as a rule only process non-personal data to ensure the proper functioning of the digital euro. Where this cannot be achieved by processing of non-personal data only,** ~~**I**~~the The European Central Bank and national central banks may process personal data in so far as it is necessary to fulfil tasks that are essential to the proper functioning of the digital euro. In the framework of this regulation, the processing of ~~**personal**~~ data for the purposes of the settlement of digital euro payment transactions~~**, and**~~ the management of the security and integrity of the digital euro **settlement** infrastructure**, the protection of the digital euro against counterfeiting and the prevention of double-spending of digital euros** ~~**are**~~ **is a** task~~**s**~~ in the public interest that ~~**are**~~ **is** essential for the protection of citizens making use of the digital euro as well as for the stability and integrity of the Union's financial system. The task of maintaining the security and integrity of **the** digital euro infrastructure includes activities related to ensuring the stability and operational resilience of the digital euro. The European Central Bank and national central banks would be the controller**s** of personal data as regards these tasks. The European Central Bank and national central banks would process ~~**personal**~~ data for these tasks ~~**using**~~ **that have been subject to** state-of-the-art security and privacy-preserving measures, such as pseudonymisation or encryption, to ensure that data cannot be used to directly identify a specific digital euro user. **The European Central Bank and the national central banks should not request the payment service providers any information, such as encryption or pseudonymisation keys, nor should they use any information obtained as part of other tasks enshrined upon them by Union or Member State law to identify individual digital euro users.**

~~**(76a) While processing personal data in the public interest, the European Central Bank and the national central banks should apply technical measures to ensure compliance with the principles of purpose limitation, data minimisation and storage limitation, as laid down in Regulation (EU) 2016/679, including technical limitations on the re-use of data and use of state-of-the-art security and privacy-preserving measures, including pseudonymisation, segregation or encryption. In this regard, the Eurosystem should consider applying organisational measures, including training on the processing of special categories of data, limiting access to special categories of data and recording such access. The Eurosystem should also consider establishing a data protection risk management, control and governance framework specifically targeted at monitoring compliance of the digital euro's data protection operations, processing activities and procedures with the applicable rules on data protection. The ECB should report on the implementation of these safeguards and privacy-preserving measures prior to the issuance of the digital euro.**~~

PUBLIC

1.3 Annex V – Personal data processed by providers of support services

Several Member States requested clarification on whether Annex V is intended to provide an exhaustive or indicative list of the personal data categories concerned. The Presidency notes that, in accordance with the GDPR, Annex V defines an exhaustive list of data categories rather than individual data points, which explains the wording "shall be limited to." As the ECB explained during the technical seminar on 30 June 2025, the distinction between data categories and data points is necessary to allow timely responses to evolving fraud techniques, while ensuring that any data points processed remain in the scope of the defined categories.

Against this background, **the Presidency clarifies that the fraud detection and prevention mechanism may process data points only within the scope of the exhaustive list of data categories set out in Annex V**. To support this clarification, **the Presidency proposes an editorial adjustment to Annex V by deleting the reference to "the data required for the prevention and detection across payment service providers**," as this element is already covered by point (a) of Article 36(1). The amendment would also confirm that the list of data categories is exhaustive (shall be limited to) and align its formulation with that of the other annexes.

Finally, the Presidency notes that in accordance Article 36(3), the Commission is empowered to adopt delegated acts in accordance with Article 38 to update the types of personal data listed in Annex V – this means, supplement or delete data categories. The Presidency recalls, as explained by the ECB, that such processing would be limited to pseudonymised data and only to the minimum extent necessary for fraud detection and prevention purposes. In addition, the ECB can consult with the EDPS to ensure the necessity and proportionality during the mandatory checks are respected, should the purpose not be achievable without processing of personal data.

Question 5 to Member States:

Q5. *Do Member States agree with Presidency's proposed adjustments to Annex V?*

Drafting suggestions

DK Presidency in *green*
ANNEX V - Personal data processed by providers of support services

PUBLIC

For the purposes of point (a) of Article 36(1), processing shall be limited to ~~the data required for the prevention and detection of fraud across payment service providers~~:

(i) information on digital euro payment accounts, including the unique digital euro account identifier;

(ii) information on online digital euro payment transactions, including the transaction amount; and

(iii) information on the transaction session of a digital euro user, including the device internet protocol address-range.

1.4 Article 37 – Offline digital euro payment transactions and AML requirements

The question of safeguarding the digital euro against counterfeiting and preventing double-spending was last discussed under the Belgian Presidency in April 2024. The topic has not been revisited since, as the ECB was still assessing the technological options for the offline functionality. As noted by the ECB during the Council Working Party on the 17 October 2025, as part of the preparation phase for the digital euro, the ECB has selected providers for several digital euro components and related services, including providers for the offline solution, thereby bringing further clarity to the technical process for offline digital euro payment transactions.

The Presidency considers, in line with Member States' comments, that the Eurosystem should only have access to the data strictly necessary to perform the tasks related to the prevention and detection of counterfeiting. Given that the **offline functionality is intended to provide cash-like privacy to digital payments**, information on payment transactions between users made with the offline digital euro should remain known only to the payer and payee involved. At the same time, it is **essential that the Eurosystem can apply effective measures to prevent and detect counterfeiting, as a form of cyberfraud, and double-spending** of offline digital euro in order to preserve the integrity of the digital euro. The first line of defence will be the technical measures ensuring the security and integrity of the local storage devices.

Furthermore, the Presidency considers it important that the Eurosystem can assign security attributes to offline digital euros at issuance and verify their authenticity at the end of their lifecycle, **similar to the logic under which central banks currently apply checks to confirm the authenticity of banknotes**. These security attributes would not contain any information

PUBLIC

relating to individuals or to the offline digital euro payment transactions in which the offline digital euro is expended.

Against this background, **the Presidency proposes an addition to Annex IV and a clarification to Article 37(2) to reflect the necessity for the Eurosystem to process certain data for the purpose of verifying the authenticity of offline digital euro payment transactions, without accessing any payment transaction data**. Furthermore, the Presidency proposes editorial adjustments to the title of Article 37, as the current title refers only to AML requirements for offline transactions, while the scope of the article is broader.

Drafting suggestions

BE Presidency in *black*
PL Presidency in blue
DK Presidency in *green*

Article 37 - **Offline digital euro payment transactions and ~~A~~a**nti-money laundering rules applying to offline digital euro payment transactions

1.Payment services providers shall apply paragraphs 2 to 6 to offline digital euro payment transactions.

2. **Payment ~~I~~t**ransaction data **pertaining to offline digital euro payment transactions** shall not be retained by payment service providers or by the European **C~~c~~**entral **B~~b~~**anks and the national central banks.

3.Payment service providers shall retain data of funding and defunding for storing digital euros on payment instruments in accordance with Article 40 of Directive (EU) 2015/849 and national provisions transposing that Article. Payment service providers shall, upon request, make those data available to the Financial Intelligence Unit and other competent authorities as referred in Article 2(**~~3~~44**) of Regulation **(EU)2024/1624 ~~[please insert reference – proposal for Anti-Money Laundering Regulation - COM/2021/420 final].~~**

4.For the purposes of paragraph 3, the funding and defunding data means the following:

(a)the amount funded or defunded;

(b)the identifier of the local storage device for offline digital euro payment;

(c)the date and hour of the funding and defunding transaction;

PUBLIC

(d)the accounts numbers used for funding and defunding.

5.The Commission ~~**is empowered to**~~ **shall** adopt implementing acts setting offline digital euro payment transaction limits**,** ~~**and**~~ **offline digital euro** holding limits **or both**. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39. **Official digital euro holding limits shall respect the limits established in accordance with Article 16.**

6.Transaction and holding limits shall take into account the need to prevent money laundering and terrorist financing while not unduly restricting the use of the offline digital euro as a means of payment. The Commission, when drawing up the implementing acts referred to in paragraph 5, shall take into account in particular the following:

(a)an assessment of the money laundering and terrorist financing threats, vulnerabilities and risks of the digital euro when funding and defunding their payment instrument;

(b)relevant recommendations and reports drawn up by international organisations and standard setters with competence in the field of preventing money laundering and combating terrorist financing;

ANNEX IV - Personal data processed by the European Central Bank and national central banks

1. For the purposes of point (a) Article 35(1), processing shall be limited to:

(i) information on digital euro payment accounts, including the unique digital euro payment **alias** ~~**account**~~ number; and

(ii) information on online digital euro payment transactions. information linked to an unique digital euro payment **alias** ~~**account**~~ number, including the transaction amount.

2. For the purpose of point (b) of Article 35(1), processing shall be limited to:

(i) the user alias;

(ii) the user authentication;

(iii) the reference to digital euro holdings to debit; and

(iv) the reference to digital euro holdings to credit

PUBLIC

3. For the purpose of point (c) of Article 35(1), processing shall be limited to the data required for counterfeit analysis of offline digital euro payment transactions: information on the local storage device, including the local storage device number.

4.For the purposes of points (d) and (e) of Article 35(1), and the single access point referred to in Article 34(8), processing shall be limited to:

(i)the user identifier;

(ii)the user authentication, related to user's existing digital euro holdings; and

(iii)information on digital euro payment accounts, including the unique digital euro payment **alias** ~~**account**~~ number, digital euro holdings of the user, the holding limit selected by the user and the type of digital euro account.

5. For the purpose~~s~~ of point (ca) of Article 35(1), processing shall be limited to:

(i) attributes of the authenticity of the offline digital euro;

Question 6 to Member States:

Q6. *Do Member States agree with the proposed adjustments to Article 37 and Annex IV?*

PUBLIC

Chapter II

2.1. Technical proofs

The Presidency recalls that the issue of technical proofs has been discussed during several CWP meetings and most recently at the July CWP meeting. The Presidency notes that several Member States raised a number of questions regarding the function, purpose, and legal status of technical proofs. Against this background, **the Presidency is proposing amendments clarifying the obligations for the PSPs to provide continued access to the technical proofs and amendments in relation to the PSPs' back-up requirements.**

2.1.1 Clarification of function and legal status

The Presidency recalls that technical proofs are cryptographic elements used by PSPs to establish a secure link between the identity of a digital euro user (known only to the PSP) and the user's digital euro holdings recorded in the Eurosystem settlement infrastructure. **In itself, the technical proof does not contain any information about the user and does not allow to identify him or her.**

First, to ensure privacy, digital euro holdings are recorded in the Eurosystem-operated settlement infrastructure without direct link to the user's identity. PSPs are the only entities able to connect the user's identity with the corresponding holdings. The technical proof is the "bridge" between the user information held by the PSP and the record of holdings maintained in the settlement infrastructure.

Second, to ensure resilience and users' fundamental right to property, users must have continuous access to their digital euro holdings, including when their PSP is not operationally available. In such cases, users should be able to regain access to their online holdings through another PSP ("emergency switching"). To enable this, a mechanism is needed that does not rely on any input from the unavailable PSP.

2.1.2 Storage of technical proofs

The Presidency recalls that, at the July CWP meeting, it proposed that PSPs distributing the digital euro should securely store a copy of each user's technical proof, in addition to the copy held by the user. The purpose of this obligation is to **ensure that users can always regain access to their technical proof, and through it, to digital euro holdings**, even in cases of PSP unavailability. This would therefore enhance the overall resilience of the system.

The Presidency notes that this obligation would not prescribe how PSPs implement the storage obligation. PSPs would retain flexibility to use their own infrastructure or shared

PUBLIC

arrangements with other providers, provided that security and operational resilience requirements are met. The approach builds on existing obligations under the Digital Operational Resilience Act (DORA), which already requires financial entities to maintain appropriate risk management processes, as well as backup and recovery mechanisms.

Several Member States welcomed the clarification and the reference to DORA. Some delegations nevertheless questioned whether a mandatory obligation would be proportionate or whether users should be given the option to decide ("opt-in"). Other delegations highlighted the importance of ensuring consistency with the data-protection framework and avoiding duplication with DORA requirements.

The Presidency notes that the **technical proof is required to re-establish access to users' online holdings in situations where a PSP becomes unavailable** ("emergency switching"). In such cases, the new provider must be able to use the technical proof, together with standard identity verification of the user, to retrieve the user's holdings from the settlement infrastructure. The Presidency further notes that, while the user must identify themselves to the new PSP for the purpose of switching, the provider only transmits a hashed user identifier to the settlement infrastructure. This identifier does not constitute data that allows the identification of the user and serves solely to link the user's holdings in the ledger. This mechanism is not necessary for regular switching, where both providers are operationally available and can exchange information directly.

Furthermore, the Presidency notes that an **optional or user-only storage model could lead to situations where users bear sole responsibility for maintaining access to their holdings**. As these holdings represent non-visible entries on a central-bank ledger, users themselves would not have the means to demonstrate ownership if their provider becomes unavailable and they cannot provide the technical proof. Such an arrangement would not ensure the integrity or reliability of access to the digital euro.

Finally, the Presidency recalls that the **obligation concerns the information necessary to identify the Eurosystem's direct liability towards digital-euro users**. This technologically neutral concept provides a clear legal basis for determining responsibility for storing and ensuring access to the relevant information, while detailed technical and procedural elements will be further defined in the digital euro Rulebook.

Against this background, **the Presidency proposes to ensure greater consistency between the DORA requirements and the storage of technical proofs under this Regulation**. More specifically, several Member States underlined that the storage of technical proofs should be consistent with the backup requirements under the DORA. The Presidency also notes that the responsibility for supervising and enforcing the requirements set out in DORA falls to the national competent authorities of the supervised entities, in this case, the PSPs. One Member State proposed clarifying, particularly, how to ensure a common approach that

PUBLIC

safeguards the storage of technical proofs according to consistent requirements throughout the euro area while ensuring access to them at all times, including during exceptional circumstances. In response**, the Presidency proposes to clarify in a new Article 34(6) the requirements on backup obligations, while safeguarding the digital euro user's right to access their copy of the technical proof**. This would aim at ensuring that such information remains securely stored, segregated from other ICT systems, and can be retrieved at all times, including during exceptional circumstances. In light of these adjustments, the Presidency also proposes editorial amendments to Recital 67 and to delete the similar provision in Article C(7) as well as obligations to inform users of the consequences of not authorising the sharing of technical proofs 31(3b), which would both become redundant.

Furthermore, the Presidency notes that previous drafts related to the technical proofs was exclusively made in the context of switching. From an operational perspective, the use of such technical proofs would indeed be limited to switching purposes. However, situations may arise where a user, having lost their technical proof, wishes to request access to a new copy of it from their PSP, without necessarily intending to initiate switching at the time of request. The Presidency has reflected on this issue and recognises the risk of potential misinterpretations that a replacement copy could only be provided in connection with an actual switching process. Therefore, **the Presidency proposes the inclusion of a new paragraph 3bis in Article 22, clarifying that PSPs must create and provide the technical proof to the user upon opening a digital euro account and must ensure continued access to this information, including in cases where the user has lost their copy**. Finally, the Presidency proposes to broaden the wording of Article 34(1)(cb) and to introduce an editorial amendment of Article 34(5), to ensure that data processing also covers the provision of a new copy of the technical proof to users, or the receiving PSP on their behalf, as referred to in Article 22(3bis), implying that it is not limited to switching. The Presidency notes that, should Member States agree to the proposed adjustment, **corresponding amendments to Article 31 might also be required**.

Question 7 to Member States:

***Q7**. Do Member States consider that the Presidency's proposed adjustments on technical proofs sufficiently address the concerns raised by Member States?*

Drafting suggestions

BE Presidency in *black* **PL Presidency in *blue*** **DK Presidency in *green***

PUBLIC

Article 22 - Accessibility and use

[…]

3bis. When opening a digital euro account payment service providers shall give digital euro users the information necessary to identify the direct liability in digital euro of the European Central Bank or of national central banks towards the digital euro user. Payment service providers shall ensure continued access of users to that information, including at their request.

Article 31 - Switching of provider of digital euro payment ~~accounts~~ services

[…]

~~**3b. The payment service providers shall inform digital euro users about the consequences of not authorising the sharing of the information necessary to identify the direct liability in digital euro of the European Central Bank or of national central banks towards the digital euro user in the conditions established in paragraph 2 of this Article.**~~

3**b~~c~~**. Any outsourcing arrangements or arrangements between PSPs and third parties for the storing of the relevant information as referred in paragraph 1(f) of Article 34 of this regulation should include adequate safeguards to ensure a high level of data protection, in accordance with Regulation (EU) 2016/679, and apply high-level cyber-security requirements in accordance with the Regulation (EU) 2022/2554.

[…]

Article 34 - Processing **of personal data** by payment service providers

[…]

(cb) ensur~~e~~**ing** access to **and use of online** digital euro **holdings**, **in particular** as foreseen in **Article 22(3bis),** Article 31(2)**,** and in exceptional circumstances as defined in Article C.

[…]

5. For the purposes referred to in paragraph 1 (cb) of this Article, payment service providers shall store a copy of the information necessary to identify the direct liability in digital euro of the European Central Bank or of national central banks towards digital euro users in order to ensure that digital euro users**, or the receiving payment service provider on the digital euro user's behalf,** can retrieve this information at all times.

PUBLIC

6. Without prejudice to the payment service provider's obligations pursuant to Regulation (EU) 2022/2554, for the purposes referred to in paragraph 1, point (cb), payment service providers shall include in the scope of the data that is subject to the backup obligations set out in Article 12 of Regulation (EU) 2022/2554 a copy of the information necessary to identify the direct liability in digital euro of the European Central Bank or of national central banks towards digital euro users.

Payment service providers shall ensure that the information necessary to identify the direct liability in digital euro of the European Central Bank or of national central banks towards digital euro users is stored on IT systems that are physically and logically segregated from the payment service providers source ICT systems and that digital euro users, or the receiving payment service provider on the digital euro user's behalf, can retrieve this information at all times, including during exceptional circumstances as referred to in Article A. Where digital euro users have given their permission to share the information necessary to identify the direct liability in digital euro of the European Central Bank or of national central banks towards the digital euro user in accordance with Article C(5), payment service providers shall ensure that the payment service providers designated by a Member State in accordance with Article D(1) can retrieve this information during exceptional circumstances.

Article C - Emergency switching in exceptional circumstances

[…]

~~**7. Any outsourcing arrangements or arrangements between PSPs and third-parties for the storing of the relevant information as referred in paragraph 5 of Article 34 in this Regulation, should include adequate safeguards to ensure a high level of data protection, in accordance with Regulation (EU) 2016/679, and apply high-level cyber-security requirements in accordance with the Regulation (EU) 2022/2554.**~~

Recital 67

(67) […] The obligation of storage of the information necessary to identify the direct liability of the European Central Bank or of national central banks towards the digital euro users in order to facilitate switching should be subject to the requirements of Regulation (EU) 2022/2554, **and additional digital euro-specific safeguards**, which ~~**sets out requirements to**~~ ensure the digital operational resilience of financial entities, including for PSPs offering digital euro payment services.

PUBLIC

2.2 Resilience

The Presidency recalls that Articles A–D establish the framework for exceptional measures to ensure continuity of digital euro payment services in the event of exceptional circumstances. Several Member States underlined the importance of providing a clear and operational framework while maintaining legal certainty regarding the division of responsibilities between the Commission, the European Central Bank and Member States.

2.2.1 Article A – Possibility to adopt certain measures in exceptional circumstances
Discussions highlighted the need to clarify the process and division of responsibilities for triggering and adopting exceptional measures. The Presidency recalls that these measures are not unilateral actions by Member States, but form part of a legally framed process set out in Articles A–D. The Presidency also notes that, when justified in terms of effectiveness, the Commission also retains the possibility to act on its own initiative, only as regards the measure of increasing of digital euro offline holding or transaction limits.

To address Member States' calls for stronger involvement, **the Presidency proposed to clarify in recital (A) that, the main responsibility for triggering exceptional measures would lie within Member States**.

Furthermore, to ensure consistency in terminology and alignment with the operative provisions in Article 37, the **Presidency proposes to adjust the wording of Article A(a) to explicitly refer to "raising offline digital euro holding and payment transaction limits.**".

Finally, some delegations suggested introducing a general provision to specify when and how exceptional measures should be terminated once the circumstances referred to in Article A no longer apply. The Presidency recognises the intention to provide legal clarity and ensure a timely return to normal conditions. In this context, the **Presidency considers that provisions on the termination of measures could be more appropriately reflected within each relevant article**, in order to maintain coherence with the procedural framework.

Question 8 to Member States:

Q8*. Do Member States agree with the proposed amendments to Article A and Recital A?*

Drafting suggestions

PL Presidency in blue
DK Presidency in green

PUBLIC

Article A - ~~p~~Possibility to adopt certain measures in exceptional circumstances

One or more of the following measures may be adopted pursuant to the provisions of this chapter, as appropriate, in situations where there is widespread and severe disruption of the continuity of digital payments, ~~or~~ including digital euro payments ~~operations,~~ or a **credible and imminent** risk of such disruption **that affects or threatens to affect, in whole or in part, a Member State or the euro area**:

a) raising offline digital euro holding and payment transaction limits;

b) emergency switching;

c) enhancing the distribution of the digital euro;

The measures listed in the first subparagraph, points (a), (b), and (c), shall be limited in time, duly justified and proportionate. The~~se~~ measures shall be applied during the period of time that is necessary in view of the exceptional circumstances in question.

Recital A

(A) To strengthen the resilience of digital euro payments in exceptional circumstances, **such as natural disasters, major cybersecurity incidents or other events of comparable impact,** and to leverage on the digital euro resilience for the benefit of ensuring the continuity of payments, it is appropriate to provide for measures aimed at safeguarding the continuity of digital euro payments. These measures, which consist of the possibility to increase offline limits, activate emergency switching and enhance the distribution of the digital euro, should be limited in time, duly justified and proportionate. They may only be adopted when credible and substantial risks of disruptions to the continuity of **digital** payments, including digital euro payments, are growing to a level where actions are needed or when widespread and severe disruptions are already present, whether affecting, in whole or in part, one or more Member States of the euro area or the euro area as a whole. The measures should cease to apply as soon as they are no longer necessary in view of the exceptional circumstances justifying them. **The Member States have the main responsibility to assess whether a situation of exceptional circumstances prevails and to communicate it.** This Regulation is without prejudice to national procedures that Member States may establish for the purpose of requesting the adoption of the measures under this Chapter, to procedures under national law to declare national emergencies, or to their power to adopt other measures regarding the continuity of payments within their own sphere of competence.

PUBLIC

2.2.2 Article B – Procedures for raising the offline holding and transaction limits

The Presidency recalls that discussions on Article B showed broad support for maintaining the existing notification process set out in Article B. Some delegations suggested that Member States should directly notify other Member States in parallel with the Commission and the European Central Bank to expedite procedures. The Presidency considers that the current drafting already allows Member States to provide parallel notification, should they deem it useful for ensuring timely coordination.

Several delegations suggested providing greater clarity on the procedural elements of Article B, including the information to be contained in requests and the details to be specified in the implementing act. In response**, the Presidency proposes to clarify in paragraph 1 that requests for measures should also indicate the envisaged start and end dates which shall not exceed three months whereafter the Member State may resubmit a request where justified**. The Presidency also suggests specifying in paragraph 3 **that the implementing act adopted by the Commission should set out the temporary increase of offline holding and transaction limits, together with the corresponding territorial scope and timeframe of application**.

To reflect comments on ensuring regular review, the Presidency proposes to adjust paragraph 5 to include a cross-reference to paragraph 2, **allowing the same 24-hour consultation process to apply to any amendment or renewal of the measure**.

Question 9 to Member States:

Q9*. Do Member States agree with the proposed amendments to Article B and Recital B?*

Drafting suggestions

PL Presidency in blue
DK Presidency in green

Article B - Procedures for raising the offline holding and transaction limits

1. In the circumstances set out in Article A ~~O~~**one or more Member States may submit a request to the Commission for a temporary increase of the applicable offline digital euro payment transaction limits and offline digital euro holding limits**, within the limits ~~, which shall respect the limits~~ **to the use of the digital euro as a store of value set out in accordance with Article 16.** ~~**The**~~ **Such a request shall specify, and be limited to, the relevant** ~~**territories and**~~ **categories of users under the jurisdiction of the requesting Member State or Member States,** ~~**.**~~**and shall contain the grounds justifying that measure and the envisaged** ~~precise~~ ~~**timeframe**~~ **start date and end date** for its application. **The**

PUBLIC

duration of the measure shall not exceed three months. Upon expiry of that period, the Member State concerned may submit a renewed request in accordance with this Article, where duly justified.

2. The European Central Bank and~~/or~~ the Member States other than those requesting the measure envisaged in paragraph 1 may submit their opinions on the proposed measure without undue delay and in any event **within a limit of [24] hours from the notification of the request by the Commission.**

3. If **the circumstances as referred to in Article A are present and** the conditions **set out it in this Article** for the adoption of the measure are met, ~~T~~**the Commission shall adopt its implementing act setting out the temporary increase of the digital euro offline payment transaction and holding limits, the territorial scope of application and the timeframe of that increase,** without undue delay and in any event **within [48] hours after receiving the request referred to in paragraph 1. In case of a negative decision, the Commission shall provide grounds for it. In adopting such an implementing act, the Commission shall take into account the principles referred to in Article 37(6).**

4. The Commission may adopt such a measure also on its own initiative. Paragraph 2 shall apply mutatis mutandis.

5. The measure shall cease to apply at the end of the timeframe provided for in the Commission implementing act. In duly justified cases, where the circumstances set out in Article A justifying the adoption of the measure continue to exist, change or cease to exist, the Commission shall, without undue delay, adopt a new implementing act under paragraph 3 amending or repealing the measure. **Paragraph 2 shall also apply.**

Recital B

(B) To strengthen the resilience of society, payment systems, and the euro, and to support the use of the digital euro in exceptional circumstances, it should be possible to temporarily increase the applicable offline digital euro payment transaction limits and offline digital euro holding limits. These limits should in any event respect the limits to the use of the digital euro as a store of value that are set out in accordance with Article 16. Such a decision may be adopted by the Commission either at the request of one or more Member State concerned or at the Commission´s own initiative**. In its request, a Member State may indicate whether the temporary increase should apply to individual users, business users, or both within its jurisdiction.**

The adoption by means of a Commission implementing act should allow for a rapid activation, also by specifying the relevant deadlines for consultation of the Commission**, the**

PUBLIC

affected Member States and other Member States as well as for the adoption. The Commission implementing act should take account of the need of balancing its possible impact on money laundering/terrorist financing risks with the need to maintain the usability of the digital euro in exceptional circumstances, and it should allow for input from **the affected Member States,** other Member States and the European Central Bank. **The Commission implementing act should allow for subsequent amendments, including adjustments to its timeframe, the affected jurisdictions and the applicable limits, as circumstances evolve. To this end, there should be close monitoring of the situation in the affected Member States and an ongoing exchange of information between the Commission and those Member States, in order to ensure that the measures remain appropriate.**

2.2.3 Article C – Emergency switching in exceptional circumstances

The Presidency recalls that discussions on Article C focused on ensuring that the framework for emergency switching provides an effective and proportionate response in cases of exceptional circumstances. Delegations generally supported maintaining a rapid and automatic mechanism to preserve continuity of service for users, while emphasising the need to clarify the duration, legal effects, and procedural safeguards linked to such measures.

Some delegations suggested **adding "without undue delay" in paragraph 1** to underline the need for swift implementation and have accommodated the addition for clarity.

To improve legal coherence, and respond to the request on having a clearing framework on when measures cease to apply**, the Presidency proposes clarifying in paragraph 3 that emergency switching measures are temporary and remain in force only as long as justified under Article A and no longer than three months whereafter the Member State may resubmit a request where justified**. Where the underlying circumstances change or cease to exist, the measure should be amended or repealed through the same procedure used for its adoption. This would aim at ensuring that temporary emergency switching, whose total duration may be difficult to define when the measure is first requested, provides sufficient flexibility for the Member States to manage the situation. It would also ensure that the end of these exceptional circumstances serves as the final backstop for the measure, and a benchmark for return to normal conditions.

In line with the proposed changes to Recital B on the scope of measures, **the Presidency proposes to amend Article C(1a) to clarify that both individual and business users are in scope for emergency switching**. This is also in line with previous calls from Member States to ensure business continuity.

PUBLIC

Finally, the Presidency proposes refining paragraph 5 to clarify that, for switching to take place, **PSPs shall request users' authorisation to share with designated entities the information necessary to enable the temporary provision of services in accordance with Article D**.

Question 10 to Member States:

***Q10**. Do Member States agree with the proposed amendments to Article C and Recital C?*

Drafting suggestions

PL Presidency in blue
DK Presidency in green

Article C - Emergency switching in exceptional circumstances

1. Upon the reasoned request of a Member State, the European Central Bank or the relevant national central bank ~~may~~shall authorise the emergency switching in the circumstances set out in Article A if, on the basis of the information provided by the requesting Member State, the measure is justified and proportionate for the achievement of one or more of the following objectives:

(a) to ensure the continuity of digital euro payment functions;

(b) to protect the access of digital euro users to their digital euro holdings.

1a. For the purpose of this Article, the emergency switching shall mean an authorisation of the switching of the provision of ~~basic~~ mandatory digital euro payment and mandatory acquiring services, as referred to in Annex II and Annex IIa, from one payment service provider or providers to another payment service provider or providers designated by the Member State in accordance with Article D(1). The receiving payment service provider shall perform the switching upon notification of such authorisation, without undue delay and without the need to exchange information with the unavailable payment service provider.

2. The European Central Bank or the relevant national central bank may discuss with the requesting Member State the proportionate measures to be adopted. They shall only refuse to authorise emergency switching if such authorisation is not justified in view of the achievement of the objectives set out in paragraph 1.

3. The emergency switching under this Article shall be a temporary measure. It shall only apply for as long as the measure is justified in view of the achievement of the objectives set out in paragraph 1. **Where the circumstances set out in Article A justifying the adoption of**

PUBLIC

the measure change or cease to exist, the measure shall be amended or repealed according to the same methods and procedures that led to its adoption. The duration of the measure shall not exceed three months. Upon expiry of that period, the Member State concerned may submit a renewed request in accordance with this Article, where duly justified.

4. When the emergency switching is carried out in accordance with this Article, the digital euro access ~~account~~ number shall be maintained.

5. Upon the opening of a digital euro payment account, payment service providers shall request from digital euro users their authorisation to share, with other authorities or entities designated to provide temporary digital euro payment services according to Article D ~~or other payment service providers or third parties as applicable~~, the information necessary to identify the direct liability in digital euro of the European Central Bank or of national central banks towards the digital euro user in order to facilitate the emergency switching in the conditions established in this article. Digital euro users may also **decide not to give that authorisation to share the information necessary to identify the direct liability in digital euro of the European Central Bank or of national central banks towards the digital euro user** or withdraw it at any time thereafter.

6. The PSPs shall inform digital euro users about the consequences of not authorising the sharing of the information necessary to identify the direct liability in digital euro of the European Central Bank or of national central banks towards the digital euro user in the conditions established in this article, in particular the impossibility to carry out the emergency switching foreseen in this article.

~~**7. Any outsourcing arrangements or arrangements between PSPs and third parties for the storing of the relevant information as referred in paragraph 5 of Article 34 in this Regulation, should include adequate safeguards to ensure a high level of data protection, in accordance with Regulation (EU) 2016/679, and apply high level cyber security requirements in accordance with the Regulation (EU) 2022/2554.**~~

Recital C

(C) To safeguard the operational continuity of digital euro payments in exceptional circumstances and to ensure uninterrupted access for users to their digital euro holdings, it is appropriate to allow the emergency switching. Such emergency switching should be authorised by the European Central Bank or the relevant national central bank, following a reasoned request from the Member State concerned. To this end, Member States may designate payment service providers or entities, located in their national territory or in another Member State, as a backup system to support the temporary provision of **mandatory** digital euro payment and acquiring services. To be able to provide these

PUBLIC

temporary services, the entities should participate in the digital euro scheme and have implemented the necessary preparatory measures. These entities may leverage on existing national backup systems to promote operational efficiency and avoid an unnecessary administrative burden. Emergency switching should be strictly limited in time and should only apply for as long as it is justified in view of the achievement of the relevant objectives **in exceptional circumstances**.

2.2.4 Article D – Enhancing the distribution of the digital euro in exceptional circumstances

The Presidency recalls that discussions on Article D confirmed broad support for the approach previously presented by the Presidency, allowing Member States, during exceptional circumstances, to designate one or more of the entities referred to in Article 1(1), points (a) to (d) and (f) of the PSD2 provide temporary digital euro payment services and payment instruments.

Building on comments received from delegations, **the Presidency proposes to clarify that, to ensure operational continuity, this provision should also cover the temporary provision of services to persons not already holding a digital euro account**, where necessary to maintain access to and continuity of basic payment services. Furthermore, the Presidency recalls that there was broad support from Member States for including the term 'resilient' in Recitals (3), (5), and (16), and therefore proposes to retain these amendments.

Finally, the Presidency notes that, unlike the measures set out in Articles B and C, the measure under Article D is not proposed to be subject to a three-month limitation period, as such a restriction would not reflect the procedural nature of this measure, given that neither the Commission nor other Member States are involved in its application.

Question 11 to Member States:

Q11*. Do Member States agree with the proposed amendments to Article D and Recital D?*

Drafting suggestions

PL Presidency in blue
DK Presidency in green

Article D - Enhancing the distribution of the digital euro in exceptional circumstances

1. In ~~the situations~~ ~~provided for by~~ the circumstances set out in **Article A,** and only for as long as it is justified, **Member States may decide** that ~~they have designated pursuant to Article 14(3)~~ one or more of **the authorities or** ~~bodies~~ other entities referred to in Article 1

PUBLIC

(1) points (a) to (d), and (f) of the Directive (EU) 2015/2366 **shall**~~, in addition to their other tasks,~~ **provide temporary digital euro payment services and payment instruments to** ~~**digital euro users**~~ **the persons and entities referred to in Article 12a(1), points (a) to (f) that are necessary to facilitate the continuity of** ~~**daily**~~ **mandatory digital euro payment**~~**s**~~ **services.**

Recital D

(D) To safeguard the continuity of digital euro payment functions and to protect access of users to digital euro holdings, Member States may designate authorities or other entities to provide temporary digital euro payment services and instruments to digital euro users under exceptional circumstances. These authorities or entities may be the same as the specific entities designated for the distribution of the digital euro in the framework of Article 14(3), but they may also be authorities or other entities within the categories mentioned in that provision. Member States may use service agreements when designating the authorities or other entities to reduce the burden imposed on them. This could create synergies as under normal circumstances, the designated authorities and entities could be tasked with providing ~~**basic**~~ **mandatory** digital euro payment services to these consumers as well as the appropriate face-to-face support. This would ensure access to digital euro payment services to vulnerable groups. Under exceptional circumstances, these authorities or entities could be designated to serve a broader range of users**, including users that are not already their customers,** with digital euro payment services and instruments to facilitate the continuity of ~~**daily**~~ mandatory digital euro payments on a temporary basis. To be able to provide these services, these authorities or other entities should be members of the digital euro scheme and have implemented the necessary preparatory measures. In order to provide guidance on policies, procedures and controls that authorities or other entities designated by the Member States should have in place in exceptional circumstances to balance the need for broad access to the digital euro with robust AML/CFT measures, the EBA and AMLA should issue guidelines.

2.3 Switching

The topic of switching was most recently discussed during the September CWP meeting. The Presidency recalls that, based on Member States' feedback, several adjustments to Article 31 were proposed, including a clarification that "switching" refers to changing the PSP of digital euro services rather than merely switching accounts. It was also clarified that, in cases of jointly held accounts, any switching request must be made by all account holders. The Presidency notes that most Member States expressed broad support for this approach, while some raised considerations regarding joint account procedures and

PUBLIC

situations involving emergencies or provider unavailability. A number of delegations also underlined the importance of ensuring consistency with existing legislation, in particular the Payment Accounts Directive (PAD).

The Presidency further recalls that the issue of introducing a fixed deadline for completing the switching process was discussed, and that a majority of Member States supported the Presidency's proposal not to include such a deadline in the Regulation.

Furthermore, the Presidency underlines that, notwithstanding the proposed amendments, the concept of 'digital euro payment account' remains part of the draft Regulation. Accordingly, the legislation applicable to 'payment accounts', in particular the PSD3/R, continues to apply to such accounts.

In light of this, **the Presidency proposes to maintain most of the drafting presented at the September CWP meeting, while introducing targeted amendments to provide greater clarity and ensure alignment with existing frameworks**. Specifically, the Presidency proposes editorial adjustments to Article 31(1b) and (2), as well as to Recitals 67 and 67a, to align with the PAD and address Member States' request to remove the reference to a "prolonged period of time." As previously noted, should Member States agree to the proposed adjustment to Article 34(6) on technical proofs, corresponding amendments to Article 31 might also be required.

Question 12 to Member States:

***Q12**. Do Member States agree with the proposed amendments to Article 31(1b) and (2), and Recitals 67 and 67a?*

Drafting suggestions

BE Presidency in *black*
PL Presidency in blue
DK Presidency in *green*

Article 31 - Switching of provider of digital euro payment ~~accounts~~ services

1. **At the request of digital euro users, ~~P~~p**ayment service providers shall ~~**without undue delay enable digital euro users at their request to**~~ switch ~~**their users'**~~ the provision of digital euro payment **services** ~~**accounts**~~ to other payment service providers **without undue delay** ~~**while maintaining the same account identifiers**~~.

PUBLIC

1a. When switching is carried out ~~digital euro payment accounts~~ **in accordance with this Article,** ~~it shall be ensured that~~ the digital euro ~~payment~~ ~~alias~~ access number shall be maintained**.**~~:~~

~~(a) the digital euro payment account number is maintained;~~

~~(b) all the relevant information for providing access to the switched digital euro payment account is transferred to the receiving payment service provider.~~

1b. In cases where the digital euro payment account is held jointly by two or more legal account holders, request for switching shall be ~~made~~ obtained by ~~each~~ all **of them.**

1c. Without prejudice to Directive 2015/2366, the payment service provider to whom the provision of **digital euro payment services are being switched shall, prior to the switching, make available to the digital euro user the list of digital euro payment services it offers beyond the basic services,** that the user is currently receiving **and that** are eligible ~~can~~ to **be switched in addition to the basic services. The digital euro user shall specifically select the services, other than the basic services, that they wish to switch and shall be informed in advance if any fees apply to services other than the basic services.**

1d. Payment service providers shall only exchange the ~~necessary~~ information ~~to enable~~ required for the switching of the digital euro services.

2. ~~In exceptional circumstances~~ ~~w~~**W**here a payment service provider is operationally not in a position to ~~switch~~ **provide** digital euro ~~payment~~ ~~accounts~~ **switching services to digital euro users upon their request as set out in ~~the conditions established in~~ paragraph 1 ~~of this article~~ ~~for a prolonged period of time~~, ~~or where it is likely that a payment service provider will not be in a position to offer this service for a prolonged period of time,~~ or has lost the digital euro payment account-related data concerned,** the European Central Bank **and** ~~or~~ national central banks may authorise the switching of digital euro payment **services** ~~accounts~~ held with that payment service provider to another payment service provider designated by the digital euro user. ~~**That switching shall enable**~~ ~~Based on this authorisation,~~ **This shall enable** the **new** ~~receiving~~ payment service provider ~~shall~~ **to complete** ~~perform~~ the switching ~~upon digital euro user's request~~**,** without ~~**relying on**~~ **the need to exchange information with** the unavailable payment service provider.

~~(3) For the purpose of ensuring switching in accordance with paragraph 2, the ECB may alone or jointly with national central banks establish a single access point.~~

3a. Upon the opening of a digital euro payment account to digital euro users, payment service providers shall request from digital euro users their authorisation to share, with

PUBLIC

other payment service providers or third parties as applicable, the information necessary to identify the direct liability in digital euro of the European Central Bank or of national central banks towards the digital euro user in order to facilitate switching in the conditions established in paragraph 2 of this Article. Digital euro users may ~~also~~ give that authorisation or withdraw it at any time thereafter**, provided that such choice is made in an informed and unambiguous manner through a clear affirmative action**.

~~**3b. The payment service providers shall inform digital euro users about the consequences of not authorising the sharing of the information necessary to identify the direct liability in digital euro of the European Central Bank or of national central banks towards the digital euro user in the conditions established in paragraph 2 of this Article.**~~

3~~**b**~~**c**. Any outsourcing arrangements or arrangements between PSPs and third parties for the storing of the relevant information as referred in paragraph 1(f) of Article 34 of this regulation should include adequate safeguards to ensure a high level of data protection, in accordance with Regulation (EU) 2016/679, and apply high-level cyber-security requirements in accordance with the Regulation (EU) 2022/2554.

~~**(4) The Commission is empowered to adopt delegated acts in accordance with Article 38 in order to supplement this Regulation by specifying the prolonged period of time and identifying the circumstances under which the European Central Bank and national central banks may authorise the switching of digital euro payment accounts in accordance with paragraph 2, as well as the procedural requirements that must as a minimum be observed. When preparing those delegated acts, the Commission shall consult the European Central Bank.**~~

Recital 67

(67) […] The obligation of storage of the information necessary to identify the direct liability of the European Central Bank or of national central banks towards the digital euro users in order to facilitate switching should be subject to the requirements of Regulation (EU) 2022/2554, **and additional digital euro-specific safeguards**, which ~~**sets out requirements to**~~ ensure the digital operational resilience of financial entities, including for PSPs offering digital euro payment services.

Recital 67a

(67a) Where a payment service provider is operationally unable to perform switching ~~**for a prolonged period of time**~~**, or where it is likely that it will operationally be unable to perform switching** ~~**for a prolonged period of time**~~**, including due to having lost the relevant data related to the digital euro payment account, the European Central Bank should be able to authorise the switching of the digital euro payment accounts**

PUBLIC

concerned so that the receiving payment service provider is able to retrieve the information about the digital euro holdings of the digital euro user and perform the switching without the need to exchange information with the unavailable payment service provider. This process should allow a digital euro user to continue accessing its digital euro holdings via the receiving payment service provider. In this case, the switching does not extend to other digital euro payment services that were offered by the unavailable payment service provider, including conditional payments. The provision of those digital euro payment services will therefore have to be re-established, if appropriate, with the receiving payment service provider. The European Central Bank and the national central banks should not be operationally involved in the switching of digital euro payment accounts between unavailable and receiving payment service providers. To support receiving payment service providers in the process of switching digital euro payment accounts from unavailable payment service providers, the Eurosystem may establish a single access point. ~~The Commission should be empowered to adopt delegated acts to supplement this Regulation by specifying what is understood under a prolonged period of time and by identifying the circumstances under which the Eurosystem may authorise switching of digital euro payment accounts, as well as the procedural requirements that should as a minimum be observed.~~