Council of the European Union
General Secretariat

Interinstitutional files:
2023/0212 (COD)

Brussels, 17 May 2024

WK 7116/2024 REV 1

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 - Working Party meeting on 30 May 2024 - Presidency Note on privacy and data protection

Correction of numbering typos (points under sub-section 2.A and question numbers)

Presidency's discussion note on privacy and data protection under the digital euro Regulation

Presidency note for the Council Working Party - 30th of May 2024

1. BACKGROUND

This presidency note discusses the provision of Chapter VIII of the draft Regulation and the processing of personal data by PSPs, the Eurosystem and providers of support services, as well as the purposes for which these entities may process personal data.

2. ARTICLE 34 – PROCESSING BY PAYMENT SERVICE PROVIDERS

A. PURPOSES OF PROCESSING

Article 34(1) establishes that PSPs perform a task in the public interest when they process personal data for the purposes mentioned in this Article. The Presidency analyses more closely the mentioned purposes, taking account of the opinion of the EDPB and the EDPS that the purposes should not be expressed in general terms, but rather in a clear and precise manner and be objectively connected to the tasks entrusted to PSPs under the Regulation[1].

a) Provision of digital euro payment services

In the view of the Presidency, the following services mentioned in Annex I could entail a processing of personal data by PSPs: enabling digital euro users to access and use the digital euro, enabling digital euro users to initiate and receive digital euro payment transactions and providing digital euro users with digital euro payment instruments, and managing digital euro payment accounts.

These services are, however, not mentioned in Article 34(1). In this connection, Recital 73 appears to suggest that processing of personal data in the context of these activities would be covered by the provisions of PSD2[2] and hence not specifically regulated under the digital euro Regulation.

The question arises whether this approach should be endorsed, or whether the Regulation should specifically provide for the processing of personal data by PSPs for all of these activities. It should be noted that several Member States have questioned the right-out application of the provisions of PSD2 to the provision of digital euro payment services; this may also extend to the application of the PSD2 provisions on data protection.

b) Enforcement of limits

As suggested by the EDPB and the EDPS[3], the purpose of enforcement of limits may be expressed in more clear and precise terms. Rather than merely enforcing limits, PSPs are under a legal obligation to implement and apply the limits referred to in Article 16. In the view of the Presidency, this entails the verification whether prospective or existing digital euro users already have digital

1 See Joint Opinion 02/2023 on the Proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro, paragraph 69: "Therefore, the EDPB and the EDPS recommend that Article 34(1)(a) and (c) refer exhaustively to the relevant tasks entrusted to PSPs for which personal data may be processed under the Proposal."

2 See also Article 13(1): "Within the framework of Directive 2015/2366, PSPs may provide the digital euro payment services set out in Annex I to …"

3 Joint Opinion, paragraph 69.

euro accounts with the same or with other payment service providers (as well as their dedicated pre-defined holding limit(s)), where necessary by consulting the single access point.

c) Funding and defunding

According to Article 13(2), (3) and (4), PSPs may process personal data for all purposes of funding and defunding, i.e., manual and automatic funding as well as application of waterfall and reverse waterfall functionalities.

d) Provision of services for offline digital euro

PSPs may process personal data for the purpose of providing offline digital euro, including the registration and de-registration of local storage devices. The Regulation furthermore specifies that the processing of personal data by PSPs is limited to the processing of funding and defunding data as referred to in Article 37(4). PSPs are, in other words, not allowed to process offline transaction data.

e) Provision of additional digital euro payment services

According to Annex 1 (e), PSPs should be allowed to process personal data for the purpose of providing additional digital euro payment services on top of basic payment services. Where PSPs offer additional digital euro payment services, they would do so on the basis of Article 6(1)(b) GDPR (processing is necessary for the performance of a contract to which the data subject is party) or of Article 6(1)(a) GDPR (the data subject has given consent). It might be useful to explicitly mention this in the Recitals of the digital euro Regulation[4].

f) Compliance with specific legislation

According to Article 34(1), points (d) and (e), PSPs are allowed to process personal data for the compliance with Union sanctions and with specific obligations under, among others, AMLD and DORA, in so far as they concern the digital euro. The EDPB and the EDPS note the absence of listed categories and types of personal data for these purposes and recommend that the co-legislators further elaborate on lists of categories and specific types of personal data to be processed for these purposes in Annex III[5]. However, it should be noted that, in accordance with Article 6.3 GDPR, the legal basis for processing personal data in compliance with a legal obligation or for a task in the public interest may (but must not) contain specific provisions such as on the types of data which are subject to the processing. GDPR does not impose an obligation to describe in detail all the types of personal data which may be processed by PSPs.

In this connection, the question arises whether it is even practically possible to list in the digital euro Regulation the types of personal data that PSPs may need to process for the application of other types of legislation. One could believe that this is not a realistic expectation and that the reference to points (d) and (e) of Article 34(1) could altogether be deleted or an "including, but not limited to" provision could be added. Where PSPs need to process personal data on the digital euro in compliance with the said legislation, that processing should take place in accordance with the specific data protection provisions of the said legislation and, more generally, in accordance with GDPR. On the other hand, the digital euro Regulation should be relatively detailed and prescriptive when it comes to the processing of personal data in compliance with the provisions of the Regulation itself.

4 See Joint Opinion, paragraph 73.

5 Joint Opinion, paragraph 76.

g) Other purposes

The Presidency believes that PSPs should be explicitly allowed to process personal data for other purposes that are presently not mentioned in Article 34(1). Thus, PSPs may process personal data when exchanging messages for the resolution of disputes (Article 27(2)), switching and emergency switching purposes (Article 31), for the provision of information to and the consultation of the fraud detection and prevention mechanism (Article 32(4)) and for the provision of information to and the consultation of the single access point (Article 35(8)). It might be useful to explicitly mention this in the digital euro Regulation.

h) Summary

Based on the preceding considerations, and without prejudice to any subsequent amendments to Annexes I and II, the Presidency believes that the purposes for which PSPs may process personal data could be framed along the following lines:

> Payment service providers comply with a legal obligation where they process personal data for the following purposes:
> (a) provision of payment services referred to in points (a), (b), (c) and (d) of Annex I / referred to in Annex II;
> (b) the implementation and application of limits referred to in Article 16 and Article 37(5), where necessary by consulting the single access point referred to in Article 35(8);
> (c) switching of digital euro payment accounts as referred to in Article 31, where necessary by consulting the single access point referred to in Article 35(8);
> (d) the provision of information to the fraud detection and prevention mechanism as referred to in Article 32(4), and its consultation in view of the detection and prevention of fraud;
> (e) the provision of information to the single access point as referred to in Article 35(8);
> ~~(f) compliance with Union sanctions as referred to in Article 29;~~
> ~~(g) the obligations of payment service providers under Directive (EU) 2015/2366 related to the execution of transactions and the prevention and detection of fraud, combatting money laundering and terrorist financing under Directive (EU) 2015/849, taxation compliance under Council Directive 2006/112/EC, Directive (EU) 2011/16/EU and relevant national law, the management of operational and security risks under Regulation (EU) 2022/2554 and obligations under Directive (EU) 2014/92/EU, in so far as they concern the digital euro~~.
> (h) the exchange of messages for the resolution of disputes as referred to in Article 27(2).
>
> Where payment service providers provide additional digital euro payment services referred to in point (e) of Annex I, processing of personal data is allowed to the extent necessary for the performance of a contract to which digital euro users are a party or to the extent a digital euro user has given consent.
>
> Payment service providers shall under no circumstances process personal data on offline digital euro payment transactions.

Questions to Member States:

1. *What are Member States views on points (d) and (e) of Article 34(1)?*
2. *Do Member States otherwise agree with the Presidency's list of purposes for which PSPs may process personal data? Would Member States add any other purposes to this list?*

B. ARTICLES 34(3) AND (4)

According to Article 34(3) of the Proposal, PSPs must be considered as the controllers for the personal data processing carried out for the purposes referred to in Article 34(1) of the Proposal. The EDPB and the EDPS had no substantial comments to this provision.

With regard to Article 34(4), the EDPB and the EDPS recommend specifying that state-of-art security and privacy-preserving measures should ensure that personal data are pseudonymised in such a manner that these data can no longer be attributed by the Eurosystem to an individual digital euro user without the use of additional information[6].

Questions to Member States:

3. *Do Member States agree with the recommendation of the EDPB and the EDPS regarding Article 34(4)?*
4. *Do Member States have any other comments to Article 34(3) and (4)?*

3. ARTICLE 35 – PROCESSING BY THE EUROSYSTEM

A. PURPOSE OF PROCESSING

According to Article 35(1), the Eurosystem would perform a task in the public interest or exercise official authority when processing personal data for the following purposes: providing PSP access to the digital euro settlement infrastructure, settlement of online digital euro payment transaction, safeguarding the security and integrity of the settlement infrastructure, supporting PSPs in the implementation and application of (holding) limits and authorising emergency switching.

In this connection, several Member States underlined the importance of ensuring a high level of privacy for digital euro users and considered that the Eurosystem, as is the case for cash, should not be able to see any personal data of digital euro users.

It should be pointed out, however, that segregated or pseudonymised data (as prescribed in Article 35(4)) would still be theoretically considered as personal data for GDPR purposes if the Eurosystem were to be able to combine it with other data sources that it has reasonable means to obtain[7] [8].

---

6 Joint Opinion, paragraph 78. See also paragraph 54: " … the EDPB and the EDPS point out that the Proposal does not establish a binding obligation that would ensure pseudonymisation of transaction data vis-à-vis the ECB and the national central banks. The EDPB and the EDPS therefore recommend introducing an explicit obligation to pseudonymise transaction data vis-à-vis the ECB and the national central banks in the enacting terms of the Proposal, instead of only referring to it in Recital 76 of the Proposal."

7 See Recital 26 of GDPR: "Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable."

8 Where independent operators may reasonably have at their disposal the means enabling them to link information to an identified or identifiable natural person, that information constitutes personal data for them, even if the

This explains why Article 35(1) must mention the purposes for which the Eurosystem may process personal data, even if the data to which the Eurosystem has access for these purposes do not allow it to directly identify individual digital euro users.

Article 35(7) stipulates that the Eurosystem may also need to process personal data for the following purposes, in case they are directly pursued by the Eurosystem itself rather than by providers of support services: (i) supporting the prevention and detection of fraud across PSPs, and (ii) supporting the exchange of messages for the resolution of disputes (see Article 27). It may be clearer to directly add these purposes to the list of Article 35(1).

Questions to Member States:

5. *Do Member States agree to adding the fraud detection and prevention mechanism, the dispute mechanism to the list of purposes for which the Eurosystem may process personal data?*
6. *Do Member States have any other comments on Article 35(1)?*

B. ARTICLE 35(4) – PRIVACY-PRESERVING MEASURES

According to Article 35(4), personal data should be clearly segregated (and possibly also pseudonymised) so as to ensure that the Eurosystem cannot directly identify individual digital euro users. Several Member States have questioned how this provision should be interpreted, and who would in particular be responsible for applying the segregation and/or pseudonymisation techniques. The Presidency believes that PSPs should apply segregation or pseudonymisation before data are communicated to or accessed by the Eurosystem. The latter obligation is already laid down in Article 34(4).

Article 35(4) could, nonetheless, be further clarified and contain additional safeguards to ensure that the Eurosystem does not identify (neither directly nor indirectly) any digital euro users. The following can be considered:

- an obligation for the Eurosystem to design the digital euro and adopt measures, rules and standards in such a way that it cannot directly identify individual digital euro users;
- more specifically, the Eurosystem 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, or encryption[9];
- an explicit prohibition for the Eurosystem to identify individual digital euro users, either directly or indirectly;
- an obligation for the Eurosystem to apply organisational measures, including training on processing special categories of data, limiting access to special categories of data and recording such access, applying Chinese walls between digital euro staff and other Eurosystem staff, segregating the operation of digital euro components between different entities;
- an obligation for the Eurosystem to establish a data protection risk management, control and governance framework specifically targeted at monitoring compliance of the digital euro's data

information is not, in itself, personal data for them (judgement 09 November 2023, *Scania*, C-319/22, EU:C:2023:837, paragraph 49).

9 This proposal is inspired by Article 80 of PSDR (Proposal for a Regulation on payment services in the internal market).

protection operations, processing activities and procedures with the applicable rules on data protection.

This may be coupled with an obligation for the ECB to report on the implementation of these safeguards and privacy-preserving measures prior to the issuance of the digital euro. This obligation could be inserted in Article 40(2) of the Regulation.

Questions to Member States:

7. *Do Member States agree with the clarifications of Article 35(4) and additional safeguards as proposed by the Presidency? Would Member States propose other additional safeguards?*

C. ARTICLE 35(5) – JOINT CONTROLLERS

According to this provision, the ECB and the national central banks shall be considered joint controllers when they jointly carry out a task referred to in paragraphs 1 and 8 (single access point).

The EDPB and the EDPS pointed out that this raises the question of how the obligation of transparency and the exercise of data subjects' rights will be ensured by the ECB or national central banks when processing personal data for the purposes listed in Article 35(1). In particular, the EDPB and the EDPS consider that cooperation between PSPs and the ECB or national central banks on this matter will be essential to ensure the effectiveness of data subjects' rights as required by the GDPR, and thus build the high level of trust sought in the Proposal.

The Presidency believes this practical issue does not need to be dealt with in the Regulation itself, and that it can be clarified at a later stage, e.g., in a Decision of the ECB.

Questions to Member States:

8. *Do Member States have any comments on Article 35(5)?*

4. ARTICLE 36 – PROCESSING BY PROVIDERS OF SUPPORT SERVICES

A. PURPOSE OF PROCESSING

Article 36(1) describes that providers of support services may process personal data in the situation where the ECB decides to confer them with the task of managing a dispute mechanism function (Article 27) or tasks in relation to the fraud detection and prevention mechanism (Article 32).

B. ARTICLE 36(4) AND (5)

Article 36(5) specifies that providers of support services are to be considered as controllers when providing the said support. Several Member States have questioned the designation of providers of support services as controllers, and argued instead that they may only be considered processors while the Eurosystem would continue to take up the role as controller. The EDPB and the EDPS pointed out that the determination of the role of the controllers in legislative acts must be aligned with the actual responsibilities attributed to these actors in these legislative acts, which cannot be determined on the basis of the current wording of the Regulation. It was therefore recommended to further specify the responsibilities attributed to the providers of support services with regard to

these mechanisms that would justify their role as controllers, or to remove from Article 36(5) the qualification of these providers as controller in all cases, such qualification having to be assessed at a later stage in the light of the actual tasks entrusted by the Eurosystem to the providers of support services. Since it seems premature to specify the exact responsibilities to be attributed to providers of support services, the Presidency would like to ask Member States if they can agree to amend Article 36(5) so as to determine the role of the controllers in line with the actual responsibilities attributed to these actors:

> *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 as defined in [GDPR Art. 4(7)].*

Furthermore, to avoid potential contradiction of the second sentence of paragraph 5 ("This paragraph is without prejudice to the European Central Bank and the national central banks appointing the operators of any payment-related services across PSPs and auditing of the service performance level without processing any personal data.") with the principles of GDPR, this sentence could therefore be rephrased so as to merely entail a prohibition for the Eurosystem to process any personal data when auditing the service performance level of providers of support services.

Questions to Member States:

9. *Do Member States agree to amend Article 36(5) so as to determine the role of the controllers in line with the actual responsibilities attributed to these actors?*
10. *Do Member States agree to rephrase the second sentence of Article 36(5) so as to merely entail a prohibition for the Eurosystem to process any personal data when auditing the service performance level of providers of support services?*
11. *Do Member States have any other comments to Article 36(4) and (5)?*

5. ANNEXES III TO V

A. TYPES OF PERSONAL DATA

Annexes III to V lay down the types of personal data that PSPs, the Eurosystem and providers of support services may process for the purposes identified in respectively Article 34(1), 35(1) and 36(1). Subject to an agreement on the final drafting of these Articles, the Annexes will need to be reviewed accordingly. To ensure completeness, the Commission is empowered to adopt delegated acts in accordance with Article 38 to update the types of personal data listed in Annexes III-V. The EDPB and the EDPS consider in any case that all three Annexes would benefit from further specifications as to the exact type of data that can be processed[10].

Questions to Member States:

12. *Do Member States have any comments on Annexes III to V?*

10 Joint Opinion, paragraphs 75– 76, 81 and 85 – 86.