Council of the European Union
General Secretariat

PUBLIC

Interinstitutional files:
2023/0211 (COD)
2023/0212 (COD)

Brussels, 11 July 2025

WK 9765/2025 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 18 July 2025 - Presidency discussion note on the fraud detection and prevention mechanism (Article 32)

Danish Presidency
Council of the European Union

PUBLIC

Digital euro – Presidency discussion note on the fraud detection and prevention mechanism (Article 32)

Working Party on Financial Services and the Banking Union

Date: 11 July 2025

Proposal for a regulation on the establishment of the digital euro

Meeting on 18 July 2025

PUBLIC

General fraud detection and prevention mechanism (Article 32)

To support the use of the digital euro and maintain trust in the system, it is essential to establish a general fraud detection and prevention mechanism to **combat fraud and ensure the safety of users when making online payments with the digital euro**. The overall objective of Article 32 of the Commission's proposal is to establish the legal basis for the ECB to develop such a mechanism at infrastructure level. This mechanism is intended to complement the fraud monitoring obligations of payment service providers (PSPs) under PSD2.

Article 32 was at latest discussed during the Council Working Party meeting under the Polish Presidency on 1 April 2025 and the Presidency recalls that Member states broadly support the mechanism as a tool to combat fraud.

At the same time, the Presidency notes that **some delegations reiterated concerns regarding the mechanism's implications for data protection** and requested further clarification on how the foreseen safeguards would ensure a high level of privacy for digital euro users. The Presidency further notes that a majority of Member States did not raise concerns regarding the wording of Article 32.

1. Privacy and the functioning of a fraud detection and prevention mechanism

In response to Member States' concerns, the ECB outlined the procedural and technical safeguards intended to protect end-user privacy during the technical seminar on 30 June 2025.

According to the ECB, **the fraud detection and prevention mechanism only processes the minimum data strictly necessary to assess risk of fraud**. This includes hashed customer identifiers, transaction metadata (e.g. PSP IDs, transaction ID, amount, transaction type), and session data such as a device IP ranges. ECB further explained that only PSPs have access to end-user identities and can link them to specific transactions**.** Therefore, the Eurosystem will not be able to infer identity attributes or associate them with individual transactions or balances.

In addition, the digital euro settlement platform (DESP) is designed to prevent the linking or onward transmission of personal data between the providers of support services and the

PUBLIC

Eurosystem through a combination of contractual and technical safeguards. These include clear segregation of data between relevant actors and an allocation of responsibilities designed to ensure a high level of data protection and preserve the separation of roles.[1]

The Presidency notes that some delegations requested clarification on the categories of data listed in Annex V and to which extent this data is processed. In particular, concerns were raised about the legal certainty, the level of granularity, and the consistency of terminology between Article 32(4) and Annex V. The ECB noted that it may be advisable to avoid defining a specific list of data categories in the regulation itself, to account for the rapid evolution of fraud typologies and the respective mitigation techniques. In relation to the latter, the Presidency has noted that Annex V furthermore provides a possibility for the Commission to update the types of personal data listed in Annex V via Commission delegated acts, as outlined in Article 36(3).

Moreover, the Presidency notes that digital euro regulation provides an additional safeguard by requiring that the ECB consults the European Data Protection Supervisor (EDPS)[2] prior to developing the operational details of the mechanism. The EDPS has the powers of investigating, advising, and enforcing data protection rules, and **the EDPS is expected to provide an opinion on whether there is proportionality between the data point used and the objectives of the mechanism**.

The Presidency invites delegations to consider whether these clarifications provide sufficient assurance that privacy will be preserved at a technical level in the implementation of Article 32. Moreover, the Presidency invites delegations to share whether further amendment to Annex V would be necessary.

BE Presidency in black

Article 32 – General fraud detection and prevention mechanism

1. The European Central Bank may facilitate the fraud detection and prevention tasks that payment service providers shall perform under Directive 2015/2366 by establishing a general fraud detection and prevention mechanism for online digital euro transactions to ensure the smooth and efficient functioning of the digital euro. That general fraud

[1] For more detailed information, see the ECBs technical seminar regarding data in the digital euro infrastructure from the 6 March 2025.

[2] The European Data Protection Supervisor is an independent data protection authority for the European Union. It ensures that EU institutions and bodies respect the privacy and data protection rights of individuals when processing their personal information.

PUBLIC

detection and prevention mechanism may be operated directly by the European Central Bank **and the national central banks** or by the providers of support services designated by the European Central Bank.

2. The European Central Bank shall consult the European Data Protection Supervisor prior to developing the details on the operational elements of the fraud detection and prevention mechanism.

3. The fraud detection and prevention mechanism shall:

(a) assess the exposure to fraud risk of online digital euro transactions in real-time at the exclusive use of payment service providers before the transaction is introduced into the digital euro settlement infrastructure;

(b) support payment service providers in **securing payment information and** detecting fraudulent transactions in online digital euro payment transactions that have been settled.

4. For the purpose of this Article, payment service providers shall provide the fraud detection and prevention mechanism with information referred to in Annex V. Payment service providers shall implement appropriate technical and organisational measures including state-of-the-art security and privacy-preserving measures to ensure that the support service shall not be able to directly identify the digital euro users on the basis of the information provided to the fraud detection and prevention mechanism.

Question 1-3 to Member States:

Q1. Do Member States consider that the technical clarifications provided by the ECB offer sufficient assurance that privacy will be preserved in the implementation of Article 32?

Q2. Do Member States find it necessary to further amend Annex V?

Q3. Do Member States find it necessary to conduct further amendments to Article 32?