The European Commission’s Proposal for a Digital Euro – A Preliminary Personal Data Protection and Privacy Analysis

By Andrés Chomczyk Penedo*, Michaël Van den Poel*, Pablo Trigo Kramcsak*
The Brussels Privacy Hub publications are intended to circulate research in progress for comment and discussion. Available at https://brusselsprivacyhub.com/. Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged.

DISCLAIMER

The opinions expressed in this paper are those of the author/s.
Contents

1 Introduction .............................................................................................................................................. 4

1.1 The EU’s Embrace of Digital Transformation in the Financial Sector ................................................. 4

1.2 The Launch of the Digital Euro Initiative ............................................................................................... 5

1.3 Global Financial Landscape and the Role of Digital Currencies ......................................................... 6

1.4 The Imperative of Data Protection in Finance ......................................................................................... 6

1.5 The Digital Euro as an account-based CBDC ......................................................................................... 8

1.6 Critique and Complexity in Design ...................................................................................................... 9

2 Preliminary Assessment ............................................................................................................................. 10

2.1 The Role of EU Data Protection Law and Authorities (Article 5.2 Proposal) ...................................... 10

2.1.1 Background and Overview of the Gap or Issue .............................................................................. 10

2.1.2 Proposed Solution or Mitigation .................................................................................................. 12

2.2 Fraud Detection and Data Protection (Article 32.2 Proposal) ............................................................. 13

2.2.1 Background and Overview of the Gap or Issue .......................................................................... 13

2.2.2 Proposed solution or mitigation .................................................................................................. 15

2.3 Processing by Payment Service Providers (Article 34 Proposal) ....................................................... 16

2.3.1 Background and Overview of the Gap or Issue .......................................................................... 16

2.3.2 Proposed Solution or Mitigation .................................................................................................. 18

2.4 Processing of Personal Data by the European Central Bank and the National Central Banks (Article 35 Proposal) ...................................................................................................................... 19

2.4.1 Background and Overview of the Gap or Issue .......................................................................... 19

2.4.2 Proposed solution or mitigation .................................................................................................. 21

2.5 Processing by providers of support services (Article 36 Proposal) .................................................... 22

2.5.1 Background and overview of the gap or issue ............................................................................. 22

2.5.2 Proposed solution or mitigation .................................................................................................. 24

2.6 Retention of offline transactional data for AML/CFT purposes (Article 37(2) Proposal) .................. 24

2.6.1 Background and overview of the gap or issue ............................................................................. 24

2.6.2 Proposed solution or mitigation .................................................................................................. 25

3 Conclusions .............................................................................................................................................. 26

3.1 Summary of Key Findings .................................................................................................................. 26

3.2 Significance and Implications ............................................................................................................. 26

3.3 Recommendations and proposed changes ........................................................................................... 26

3.4 Concluding remarks .......................................................................................................................... 27

4 References .............................................................................................................................................. 28
1 Introduction

1.1 The EU’s Embrace of Digital Transformation in the Financial Sector

In an era marked by rapid digital transformation, the European Union’s Digital Finance Strategy (‘DFS’) emerges as a critical policy element to address the changes occurring in the financial services industry.¹ This strategy is not just about leveraging the potential of digital innovation within the financial sector but also about managing the inherent risks that come with such advancements.

Traditionally, the introduction of new technologies has been subject to supervision by financial services authorities. However, fintech and Big Tech companies have made their way into the financial services industry,² through different business models.³ Their presence has been an increasing source of digital novelties in the finance sector,⁴ putting stress on the controlled inflow of data-driven solutions. Therefore, the DFS acknowledges this change and, among many objectives, focuses on the need for vigilant data protection and privacy management, recognizing these as key pillars of a trustworthy and secure digital financial environment.

---

¹ ‘Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Digital Finance Strategy for the EU’ (European Commission 2020) Communication from the Commission (2020) 591.
1.2 The Launch of the Digital Euro Initiative

Since its publication in 2020, the DFS has slowly produced different regulatory instruments, such as Regulation (EU) 2023/1114 (‘MiCA’),\(^5\) and Regulation (EU) 2022/2554 (‘DORA’).\(^6\) However, specific key objectives still lacked their respective regulatory proposals. In late June 2023, many of these instruments were finally unveiled.\(^7\) Most notable was the introduction of a groundbreaking initiative, particularly pushed by the European Central Bank (ECB): the digital euro. This initiative aims to develop a digital form of the euro, promising to revolutionize the landscape of digital payments and secure the role of this currency within the evolving Digital Single Market against the advancements by privately issued e-money, particularly stable-coins.\(^8\)

The core of the digital euro initiative lies in creating a digital currency equivalent to the physical banknotes and coins currently in circulation. This ambitious project encompasses several objectives, including improving the efficiency and inclusivity of payment systems while safeguarding the euro’s essential position in a swiftly evolving digital economy. The potential impact of the digital euro on the European economy is profound – it is poised to transform digital commerce, reshape financial services, and redefine monetary transactions. The regulatory proposal for a digital euro (the ‘Proposal’) published by the European Commission was thus much anticipated.\(^9\)

---


\(^8\) ‘Report on a Digital Euro’ (European Central Bank 2020).

1.3 Global Financial Landscape and the Role of Digital Currencies

The digital euro initiative does not emerge in a vacuum. It is part of a global context characterized by the dynamic evolution of public Central Bank Digital Currencies (CBDCs) and privately issued stablecoins and other cryptocurrencies. These digital assets, each with their unique mechanisms and regulatory frameworks, are reshaping the financial landscape, presenting new opportunities and challenges. It is noteworthy the meteoric rise of cryptocurrencies (including stablecoins, whose value is pegged to another external traditional asset), especially those with privacy-enhancing (or even anonymity-enhanced) mechanisms built-in. These have amplified the public’s interest in the right to private payments.

In this regard, heightened privacy measures and advanced cryptographic features can encourage greater user trust, driving engagement and adoption of specific digital currencies over alternative options. This evolving scenario presents a complex interplay between privacy in financial transactions and the need for regulatory oversight.

1.4 The Imperative of Data Protection in Finance

Protecting privacy and personal data is imperative in digital finance. Besides the legal requirement to do so, it is also seen as necessary by users, with 43 per cent of respondents to an ECB public consultation marking privacy as the most important aspect of a digital euro. Financial data can reveal a lot about a person, including special categories of personal data;

12 Auer, Cornelli and Frost (n 10).
16 This legal requirement stems from both primary (article 7 and 8 of the Charter of Fundamental Rights of the EU and article 16 of the Treaty on the Functioning of the EU) and secondary (GDPR) EU law.
as such, the safeguards to be developed in the digital financial landscape are crucial. Protecting this data is thus not just about meeting regulatory requirements; it is about maintaining consumers’ and users’ trust and the integrity of the entire financial system. Therefore, stringent data protection measures are imperative, not only to safeguard individual privacy and ensure secure financial transactions but also to empower individuals with a sense of autonomy and control over their personal financial information.

The relationship between financial services regulation and data protection has historically been fraught with tension. Traditionally, financial institutions upheld client confidentiality under bank secrecy obligations. However, these duties have diminished as banks are increasingly compelled to disclose client information for tax reporting, anti-money laundering (AML), and countering the financing of terrorism (CFT) purposes. In transactions involving regulated financial institutions, individuals now often anticipate personal data-sharing with government agencies.

Contrastingly, cash transactions, facilitated through banknotes and coins, have somewhat remained exempt from such disclosure requirements due to their peer-to-peer nature and absence of an intermediary. As a ‘privacy-by-default’ means of payment, cash has faced governmental restrictions on its usage, in favour of more traceable digital transactions. Examples include a stop in printing 500 euros bills for its supposed association with illegal activities, as well as restrictions on cash payments above certain amounts.

---

18 Lana Swartz, New Money: How Payment Became Social Media (Yale University Press 2020).
21 See for example the Belgian limit of 3 000 euros for cash transactions, article 67§2 Law of 18 September 2017 on Preventing money laundering and terrorist financing and limiting the use of cash, BS 6 October 2017.
1.5 The Digital Euro as an account-based CBDC

Turning back to the Proposal, the digital euro has Article 133 TFEU as its primary law basis.\(^{22}\) This avoids fragmentation by establishing the digital euro as a single currency across the euro area. Designed as a public digital means of payment, the digital euro aims to foster a more competitive and innovative European retail payments market.\(^{23}\)

Money, under its classic definition,\(^{24}\) has four functions: a medium of exchange, a unit of account, a means of payment, and a store of value. As such, it is possible that certain financial instruments are not money because they fail to provide one of these functions. In this respect, the Proposal intends the digital euro to meet all the classical definitions of money.

While not directly discussed in the Proposal or explanatory memorandum, CBDCs can be organized in different manners, primarily around a token-based or an account-based approach. Account-based CBDCs such as the digital euro involve a model similar to that of e-money, with a central authority controlling balances, ownership, and the transfer of funds. Token-based CBDCs, conversely, imply a model resembling cryptocurrencies, where these operations are usually conducted on a peer-to-peer basis after the initial issuance of money.\(^{25}\) In contrast to intrinsically hard-to-trace cash payments, the design choice to implement an account-based digital euro as opposed to a token-based scheme implies a stark difference with traditional cash.\(^{26}\)

The ECB, along with national central banks, will be responsible for issuing the digital euro.\(^{27}\) The distribution of the digital euro will occur through payment service providers (PSPs), credit institutions, and other entities.\(^{28}\) To operate the digital euro, it will be necessary an interface, to be created by either PSPs or the ECB, leaving to users which one to choose.\(^{29}\) Alternatively,

\(^{22}\) Article 133 TFEU requires the Council and Parliament to ‘lay down the measures necessary for the use of the euro as the single currency’ and already serves as the legal basis for the establishment of the present euro.
\(^{23}\) Recital 1 Proposal.
\(^{25}\) Frédéric Tronnier, ‘Privacy in Payment in the Age of Central Bank Digital Currency’ in Michael Friedewald, Stefan Schiffner and Stephan Krenn (eds), Privacy and Identity Management (Springer International Publishing 2021).
\(^{26}\) Auer, Cornelli and Frost (n 13).
\(^{27}\) Article 4 Proposal.
\(^{28}\) Articles 13 and 14 Proposal.
\(^{29}\) Article 28 Proposal.
the Proposal prescribes the interoperability or integration of the European Digital Identity Wallet as an interface.\textsuperscript{30} This would allow users to link digital euro accounts to their European Digital Identity platform. When such a link is created with the offline digital euro, its intended cash-like privacy characteristics could be neutralised.

This account-based approach exposes transactions to potential analysis by the wide range of intermediaries responsible for managing the digital euro ledger. The role of and risk of the involvement of these different intermediaries to privacy and data protection will be further explained below. However, the Proposal is adamant and explicit in ruling out a potential ‘programmable’ euro, ensuring its unrestricted use.\textsuperscript{31} Such programmable money would enable entities to limit the use of the currency through technical means.\textsuperscript{32}

As with any other financial transaction, a final settlement, i.e., a conciliation of accounts between different system parties, of operations is necessary to minimize unnecessary movement of funds between the operators. In this respect, settlement will be handled within the Eurosystem for online payments,\textsuperscript{33} while offline transactions will be settled locally.\textsuperscript{34}

1.6 Critique and Complexity in Design

Despite the intention to implement the digital euro as a form of digital cash-alternative, various organisations have raised concerns about the digital euro being potentially problematic for privacy and data protection; central to these concerns is the digital euro’s unnecessary complexity.\textsuperscript{35} While digital assets like cryptocurrencies demonstrate the possibility of direct end-user acquisition from the source, the proposed structure for the digital euro introduces a complex web of intermediaries, which some argue is not fundamentally different from existing digital payment solutions.\textsuperscript{36} These concerns become even more prevalent when considering

\textsuperscript{30} Article 25 Proposal.
\textsuperscript{31} Article 24(2) Proposal.
\textsuperscript{33} Article 30.2 Proposal.
\textsuperscript{34} Article 30.3 Proposal.
\textsuperscript{36} ‘Digital Euro and Right to Cash Policy Analysis from a Human Rights Perspective’ (n 35).
the potential interaction of the digital euro with other structures and tools, such as digital wallets. The web of intermediaries runs counter to the principle of proportionality. Applied to the digital euro, it requires maintaining a degree of anonymity in the digital euro system, particularly guaranteeing non-traceability for lower-value transactions that would typically be associated with cash-based transactions. Sufficient safeguards for these transactions are crucial, as low-value transactions should offer ‘cash-like privacy’.

From a data protection perspective, and despite its complex architecture, the digital euro in its current configuration and design is nothing more than a dataset that will keep a track on account balances assigned to given (natural) persons, like many other forms of digital money. 37 While the Proposal is extensive, and there are significant data protection and privacy challenges across its text, this report aims to dissect some of the core issues and propose concrete changes to the current wording of both the recitals and articles in question.

2 Preliminary Assessment

2.1 The Role of EU Data Protection Law and Authorities (Article 5.2 Proposal)

2.1.1 Background and Overview of the Gap or Issue

Money, and by extension all operations that involve some sort of monetary value, can be considered as data. 38 When this information relates to an identified or identifiable natural person, the GDPR rules regarding personal data processing become applicable. 39 More importantly, monetary transactions can reveal special categories of personal data. 40 Whether directly or indirectly, 41 the digital euro will process personal data, especially under the account-based approach. Even when the personal data processed does not fall under the defined special

---

37 Lee (n 32).
39 Article 4(1) GDPR
41 This refers to personal information related to an individual who is not the primary user of a particular digital currency or its associated services/infrastructure. This is considered as the processing of ‘silent party data’ (see ‘Guidelines 06/2020 on the Interplay of the Second Payment Services Directive and the GDPR’ (European Data Protection Board 2020) 1.0.)
categories of the GDPR, it might still be deemed sensitive due to the higher risks involved in the processing of financial data. Examples include the inference of certain behavioural data from financial transactions by individuals. As potential high-risk data processing will take place to implement the digital euro, data protection rules, including the GDPR should come to the foreground. The current safeguards offered in the Proposal seem quite weak in this regard.

As the EDPB and EDPS note in their Joint Opinion, the importance of privacy and data protection in the implementation of the digital euro should mean that ‘data protection by design and by default should be embedded in the design of the digital euro from the outset’. As the Commission proposal remains vague on many of the technical details, the ECB is tasked with implementing ‘detailed measures, rules and standards’.

This delegates responsibilities, which require a careful consideration of fundamental rights to the ECB, a body that has substantially less democratic legitimacy than the co-legislators, given that their authorities are not directly elected by EU citizens. The fundamental rights to privacy and data protection lay thus in the hands of the ECB in the current Proposal’s version.

As a safeguard, the parties involved will not only have to consider data protection legislation but will also be subject to supervision by data protection authorities. The EDPS retains its full competences under the EUDPR, which is applicable to the ECB. This includes article 40 EUDPR requiring prior consultation with the EDPS for high-risk processing and the relevant provisions on supervision of the national central banks and PSPs would also be scrutinised for their compliance with data protection rules. As important players defining technical and operational details not covered by the Proposal and as co-designers and distributors of the digital euro, respectively, they are subject to the GDPR. This includes supervision by national supervisory authorities in the member states where these actors are established.

---

42 Article 9 and 10 GDPR.
44 Article 5(2) Proposal.
46 The role and supervision of the national central banks should be nuanced, as when acting together as part of the European System of Central Banks, they might be considered as an institution for the purpose of data protection supervision, placing them under scrutiny of the EDPS applying the EUDPR. See Annelieke Mooij, 'Digital
In an effort to include the views of data protection authorities, Article 5(2) of the Proposal requires the ECB to ‘consult’ the EDPS when adopting these measures affecting data protection.\textsuperscript{47} Despite the EDPB and EDPS welcoming this provision,\textsuperscript{48} the wording of this provision seems rather limited, in view of the extensive responsibilities that data protection authorities will and should have in the implementation of the digital euro.

\subsection*{2.1.2 Proposed Solution or Mitigation}

The design of the digital euro conditions how the rights to privacy and data protection will be safeguarded. The Proposal has already settled for an account-based approach, which exposes personal data to trusted intermediaries. As such, taking a different approach that is more aligned with data protection and privacy would constitute redrafting the whole Proposal. Because of this, it is necessary to ensure that adequate safeguards are incorporated into the Proposal. While the involvement of the EDPS under Article 5(2) constitutes a solid start, building on the existing applicable provisions in the EUDPR, there is room for improvement.

We suggest the incorporation of the following wording as part of Article 5(2):

a. ‘When adopting a particular measure, rule and/or standard pertaining to the digital euro and how personal data will be processed, if the EDPS has indicated a preferred safeguard, then the ECB shall adopt such measure, rule and/or standard. In the event that EDPS has not indicated a preference, and if the ECB has several options to select from, it shall only adopt the one that affects the process the least amount of personal data, regardless of if that option requires additional efforts to be carried out, taking especially into account the data minimisation principle’.

b. ‘If the measure, rule and/or standard will have to be co-decided and/or implemented by national central banks and PSPs, the relevant supervisory authorities will be involved in the process’.

\textsuperscript{43} A prior example of the ECB engaging in a prior consultation with the EDPS can be found here: EDPS opinion on a prior consultation requested by the European Central Bank on their new customer-management-system [2021] European Data Protection Supervisor Case 2021-0528.

Point a. is proposed to further limit the ECB’s discretionary powers in a sensitive topic as digital cash, with a focus on addressing concerns raised by citizens, especially in light of investigations conducted by the ECB. As for point b., it is necessary to keep in mind that the operation of the digital euro implies several other local stakeholders, who are accountable to different supervisory bodies in each Member State.

Aligned with these considerations, while there are several Recitals that refer to the importance of the rights to privacy and personal data protection, there is room for improvement. In that sense, it is suggested that the text below be added at the end of Recital 70:

‘While the ECB is independent in carrying out its primary competences, such independence cannot compromise the rights to privacy and data protection. The ECB shall thus be subject to the supervision of the EDPS according to the EUDPR. Additionally, when having an option in the concrete design choices for the digital euro operation, particularly the offline part, the option that guarantees the highest level of privacy and personal data protection shall be selected, regardless if that carries an additional burden on other lawful objectives to be pursued by it and the national central banks’.

### 2.2 Fraud Detection and Data Protection (Article 32.2 Proposal)

#### 2.2.1 Background and Overview of the Gap or Issue

One of the basic digital services for natural persons, according to Annex II of the Proposal, is the ‘(...) initiation and reception of digital euro payment transactions (...) in the following use cases: (...) point-of-interaction digital euro payment transactions, including point-of-sale and e-commerce’. As such, the digital euro is intended to facilitate both offline and online payments. Particularly in the online Digital Online Market, fraudulent transactions can be a concrete and real barrier to the effective development of e-commerce. To counter fraud using the digital euro, the Proposal incorporates mechanisms for fraud detection and prevention.

The Proposal would introduce a broad mandate for the ECB to establish a ‘general fraud detection and prevention mechanism’. According to its provisions, the ECB would be free to
choose whether it operates this mechanism itself or delegates this responsibility to designated ‘providers of support services’. PSPs would provide this mechanism with personal account and transaction data. The involvement of PSPs builds upon previous legislation, which is used as an argument for its transposition to the digital euro. A blind copy-paste of fraud mitigation measures from other regimes would neglect data protection law considerations, which is even more relevant due to the data-driven solutions used. In this sense, the necessity of the proposed measures and the existence of appropriate privacy safeguards should be scrutinized.

Detecting and preventing fraud implies a potential compromise on the fundamental right to data protection, which is subject to the requirements of article 52(1) of the Charter of Fundamental Right of the EU (‘CFR’). The Proposal, as discussed before, intends to create a digital equivalent to cash to meet the needs of the digital economy. However, due to its anti-fraud measures, the text significantly differs from the privacy standards provided by cash. Reviewing transactions, particularly ex-ante, to detect patterns that might give away suspicion involves processing the personal data of the parties to such transactions. This is particularly far-reaching when compared to cash operations, whose features either provide effective anonymity or enable enhanced data subjects’ privacy. The awareness of implementing an ex-ante control system could create a chilling effect that runs counter to the freedom that cash, and its digital counterpart, should provide. This effect should thus be weighted with the necessity of the measures imposed in the Proposal.

As the EDPB and EDPS note in their Joint Opinion, Article 32 of the Proposal does not meet the requirement of necessity required by article 52(1) CFR. The Proposal ‘does not provide

---

51 Article 32(1) Proposal.  
52 Article 32(4) and Annex 5 Proposal.  
53 Recital 5 Proposal.  
54 Under the current e-payments landscape, detecting and prevent fraud falls upon trusted third parties. PSD2s obligates the collection of consent for the execution of transactions on their behalf proper client authorization is collected. See article 5(i) and (j) PSD2.  
56 Recital 5 Proposal.  
for clear and precise rules governing the scope and application’ of the fraud detection mechanisms, which causes ambiguity regarding the roles of the ECB and that of PSPs in turn resulting in a lack of foreseeability. Finally, necessity requires a careful analysis of less intrusive measures. If algorithmic profiling is used for this purpose, it does not go without risk, as illustrated by past instances like the SyRI case in the Netherlands, where AI-based systems demonstrated the potential adverse impacts of such technology.

Adopting a balanced approach, including necessity and proportionality criteria, involves establishing specific thresholds to differentiate between high-risk and low-risk cases. This assessment considers the severity and scope of the infringement, ensuring a nuanced response tailored to the level of risk involved. More importantly, and given the rapid development of this field, these measures should follow international trends and developments on Privacy Enhancing Technologies and safeguards.

2.2.2 Proposed solution or mitigation

As with the previous provision analysed, further wording in the text of Article 32(2) Proposal can be introduced to ensure that these systems take the least intrusive approach to the privacy capabilities that EU citizens are expecting from the digital euro. In this respect, while EDPS can steer ECB in its tasks, the EU legislator has a possibility to add concrete limitations to the dangers posed by these systems. In this respect, we suggest the following wording to be added:

‘In formulating the operational framework for the fraud detection and prevention mechanism to be adopted by the ECB, the selection of methods shall consistently prioritize those that involve the minimal processing of personal data, in accordance with the principles of necessity and proportionality and taking due count of the guidance and opinions of data protection supervisory authorities. If there is a foreseeable risk that these measures might exclude vulnerable populations from utilizing the digital euro, then such mechanisms should not be implemented. Moreover, any impact assessment conducted by the ECB shall not dispense any

59 Ibidem.
61 For example, see Project Tourbillon for pro-payer privacy CBDC design, https://www.bis.org/about/bisih/topics/cbdc/tourbillon.htm, last accessed 5 December 2023.
other party that engages in fraud detection and prevention activities to conduct their own impact assessment, where applicable, under Regulation 2016/679 and/or any other relevant legislation.’

Further improvements can be made in the Recitals to guide the correct implementation of this provision. In that sense, we suggest incorporating the following text into Recital 68:

‘This mechanism shall only be considered for implementation if there are empirical grounds to support a collective and general approach, always ensuring the use of the least intrusive method necessary for maintaining trust in the digital euro’.

2.3 Processing by Payment Service Providers (Article 34 Proposal)

2.3.1 Background and Overview of the Gap or Issue

Article 34 of the Proposal highlights several crucial aspects concerning the processing of personal data by PSPs, who are key stakeholders in the digital euro infrastructure. The article addresses various elements including: (i) the legal basis for data processing of certain activities; (ii) a group of key activities that will be carried out by PSPs; (iii) types of personal data that can be processed in regards to these activities; (iv) the capacity in which the PSPs will engage with regards to personal data involved in these activities; and (v) the adoption of safeguards to avoid the communication of personal data to the ECB. As for the first element contained in Article 34 Proposal, and in contrast to other EU regulations and directives dealing with the Digital Finance Strategy, the text clearly indicates the legal basis that should be used for certain processing activities when personal data is involved in the PSPs’ activities with regard to the digital euro: public interest.

However, there exists a potential conflict regarding the appropriate legal basis applicable. In this sense, Article 34 Proposal refers to ‘public interest’, including the provision of the offline digital euro capabilities; as noted by EDPB and EDPS, the selection of this legal basis might not be the most appropriate, since the Proposal would be imposing an obligation on PSPs to engage in the distribution and operation of the digital euro rather than extending an invitation to the system. At the same time, Article 13(6) Proposal makes it seem that the legal basis for

---

62 For example, the FiDA proposal and, previously, PSD2.
the digital euro services would be a contractual arrangement between the digital euro user and the PSP. In the same vein, EDPB and EDPS have pointed out that Recital 73 would also follow this approach around a contractual basis, particularly for additional services built on top of the digital euro.\textsuperscript{63}

Regarding the second element identified, questions can be raised whether other tasks not included in Article 34 Proposal can be performed. Such tasks would need to be structured around a different legal basis such as consent or the performance of a contract, both of which can prove difficult. In a similar sense, as the EDPB and EDPS note, the inclusion of the word ‘including’ in Article 34(1)(a) and (c) is not appropriate, as it leaves legal uncertainty regarding the exact tasks for which PSPs can process personal data.\textsuperscript{64}

Another concern relates to the registration and deregistration by PSPs of local offline clients provided for in Article 34(1)(c) Proposal. In this respect, Recitals 34 and 35 indicate that PSPs ‘should’ perform these activities and, also, Recital 73 would seem to tie this activity, alongside others, to the compliance with AML/CFT legal obligations, just like using an ATM. However, and in contrast to ATMs and cash, the offline digital euro would be hosted in local storage that, at some point, would have to (re-)connect with PSPs, either for funding or de-funding. This is another situation where the decision to adopt an account-based approach puts stress on securing the protection of the right to personal data protection. As AML/CFT activities are data-intensive and they have been criticized for their lack of success in achieving their objectives,\textsuperscript{65} it is possible to wonder if stricter measures, such as limiting the activities related to these objectives to merely the registration and de-registration of devices to block balances in case of, for example, theft, should be adopted in the proposed text to protect end-users from undue intrusions and potential unlawful uses of their personal data.

Moving on, the Proposal also provides extensive powers to the Commission to determine the categories of personal data that can be processed for the provision of the aforementioned

\textsuperscript{64} ibid 24.
services. These powers present a challenge due to the uncertainty surrounding the scope of activities and services that will fall under the digital euro framework. While, on the one hand, this possibility under Article 34(3) Proposal allows room for the improvement of the digital euro, it does so at the expense of legal certainty to the digital euro users. Yet again, the digital euro proves to be a field of uncertainty in comparison with the cash it tries to emulate, with details such as specific safeguards being able to be defined down the line.

Turning to the capacity in which PSPs will engage within the digital euro framework, we can identify a notorious tension between the definition of controller under GDPR and the actual activities that PSPs perform. Under the GDPR, a controller defines the means and purposes for processing personal data. This includes deciding all matters pertaining to the lifecycle of personal data for a given activity. Under the digital euro framework, while PSPs have been chosen as the primary outlet for distribution, they are left without much room to determine how the processing of personal data will take place. As noted above, the ECB and national central banks retain a considerable margin for determining how the digital euro operates in practice. Therefore, it is, at least, questionable that these entities do not share any responsibility over how personal data is processed. Moreover, the safeguards mentioned in the article are somewhat ambiguous, giving what appears to be a broad discretion to the ECB.

2.3.2 Proposed Solution or Mitigation

To address the issue described above, we suggest the following modifications to Article 34. In that sense, firstly, we recommend incorporating the following text as Article 34.2 Proposal:

‘For any other processing activity that the payment service provider carries out regarding the provision of the digital euro, the processing will be based on the performance of a contract, relying on Article 6(1)(b) Regulation 2016/679, between the digital euro user and the payment service provider. In the event that the processing involves special categories of personal data, then it shall be necessary to obtain consent from the data subject’.

---

66 Article 34(3) Proposal allows the Commission to adopt delegated acts changing the categories of personal data processed for the tasks described in article 34(1) Proposal.
Next, the word ‘including’ in Article 34(1)(a) and (c) should be removed. Therefore, the provision should be as follows:

‘(…) (a) the enforcement of limits, and the verification of whether prospective or existing digital euro users have digital euro accounts with another PSP, as referred to in Article 16; (…)’

(c) the registration and de-registration of the local storage devices as referred to in letter (b) of Annex I; (…)’.

To contribute to further clarity, we also suggest that Article 34(1) Proposal introduces the following text to link its provisions with the relevant Articles from GDPR:

‘Payment service providers comply with their obligations under this Regulation, relying on Article 6(1)(c) Regulation 2016/679, where they process personal data for the following purposes:

On a final note, Article 34(3) Proposal should be deleted and, instead, provide a more detailed elaboration on the categories of personal data. This should encompass specific details regarding the planned operation of the digital euro framework.

2.4 Processing of Personal Data by the European Central Bank and the National Central Banks (Article 35 Proposal)

2.4.1 Background and Overview of the Gap or Issue

Moving on to Article 35 Proposal, it delineates several critical points regarding personal data processing by both the ECB and national banks. As was the case for article 34 Proposal, Article 35 tackles a number of personal data-related issues, such as: (i) the legal basis for a range of activities; (ii) the categories of personal data that will be involved; (iii) the necessity to segregate personal data to avoid identification of end-users; (iv) the capacity in which the PSPs will engage with regards to personal data involved in these activities; and (v) the establishment of a single access point of digital euro users.

The Proposal is reasonably clear in the legal basis used by the ECB and national central banks when processing personal data according to Article 35 Proposal.68 The text mentions that

---

68 Which refers to Annex IV Proposal for a list of types of personal data, which can be updated by the Commission through the adoption of delegated acts. See article 35(2) and (3) Proposal.
these central banks ‘perform a task in the public interest or exercise official authority where they process personal data’ for the listed purposes but does not explicitly refer to processing on the ground contained in Article 6(1)(e) GDPR and Article 5(1)(a) EUDPR. This leads the EDPB and EDPS to call for the inclusion of an explicit reference in Recital 76 Proposal.\textsuperscript{69}

As with PSPs, the Proposal lists a number of processing activities in Article 35(1)(a) through (e), which leads to the same consideration of whether this is an exhaustive list or not. If not, the same question regarding the applicable legal basis for other processing activities comes to the foreground. Besides this, there are concerns over the key activities. In this respect, ‘safeguarding the security and integrity of the digital euro settlement infrastructure and of local storage devices,’\textsuperscript{70} poses a challenge to ensure that the offline digital euro acts like cash, as supposedly intended by the Proposal. As discussed previously, the current structure of the offline digital euro incorporates the idea that it can (and requires at some point) a connection with a third party that exposes natural persons’ personal data, leading up to their full identification.

In connection with this, Article 35(4) Proposal presents a major challenge in the digital euro logic. Its latter part states that for the performance of the tasks indicated in Article 35(1), the measures to be adopted with regards to personal data ‘(…) shall include the clear segregation of personal data to ensure that the European Central Bank and the national central banks cannot directly identify individual digital euro users’. If the ECB and the national banks are not intending to have access to personal data, then this provision is, at least, unnecessary. As it will be further elaborated, the supposed ‘artificial walls’ that certain scholars argued the ECB will put in place,\textsuperscript{71} are absent in the Proposal. Even if implemented, the Proposal contains elements, which suggest possibilities to breach these ‘artificial walls’.

This is tied with our comments in the previous section. If the ECB and the national central banks have such vast powers to determine the means and purposes for which personal data can be processed within the digital euro framework, then they meet the definition of controller, with the PSPs acting as their processors. In our opinion, in the current configuration the ECB

\textsuperscript{70} Article 35(1)(c) Proposal.
\textsuperscript{71} Mooij (n 41).
and national central banks could be joint controllers together with other digital euro operators in light of the extensive definition of joint controllership in the case-law of the European Union Court of Justice.

On a final note, while these issues parallel those identified in related discussions, Article 35 Proposal brings to light two additional major concerns for the digital euro system under Article 35(7) and (8), each with a corresponding risk data protection: (i) the potential re-centralization of its infrastructure, and (ii) the creation of a single access point for the digital euro.

1. **Re-centralization of Infrastructure**: Article 35(7) allows the ECB to provide directly a dispute mechanism as well as a general fraud detection and prevention mechanism. Therefore, there is a risk of consolidating control and data processing in a smaller number of entities, potentially undermining the decentralized nature that digital currencies typically aspire to achieve and, thus, increasing the impact that a single data breach can have.

2. **Single Access Point**: Article 35(8) allows for the adoption of a single access point, which raises questions about data security, access control, and the implications for user privacy. It implies a focal point through which all digital euro transactions could be monitored or processed, posing significant data protection and cybersecurity challenges.

Both concerns are at odds with the intention to deploy a digital equivalent to cash. However, certain safeguards can be adopted to counterbalance this.

**2.4.2 Proposed solution or mitigation**

Regarding the text of Article 35, the following changes can be proposed to mitigate the identified risks. First and foremost, it is necessary to limit what the ECB and the national central banks can do. Article 35(1) Proposal should include a final paragraph in the following sense:

‘These shall be the only activities that the ECB and the national central banks will be able to carry out within the context of this Proposal.’

---

72 Either separately or as part of the ESCB. See Mooij (n 41) 24-25.
As for Article 35(1)(c) Proposal, the words ‘and of local storage devices’ should be deleted, as generally safeguarding the security and integrity of devices belonging to individuals is too broad, and it should not be up to the ECB and national central banks to access personal data stored on these devices beyond what is strictly necessary for the processing of payments.

Finally, Article 35(5) Proposal should refer to the joint controllership of the ECB, national central banks and PSPs, where these parties are jointly designing and putting systems into the field, particularly as mentioned in Article 35(7) and (8) Proposal. This ensures adequate accountability for these controllers to data subjects.

As for Recitals, our analysis suggests potential modifications. In regard to Recital 77, it would be advantageous to propose the following text to replace its current final sentence:74

‘The European Central Bank and national central banks shall adopt measures to ensure that account balances can be redeemed directly by users through the use of a backup code vis-à-vis the use of seed phrases in cryptocurrencies so as to mitigate potential data breaches of the intended single access point and provide a more cash-like experience to users’

Whilst a reference to Article 6(1)(e) GDPR and Article 5(1)(a) EUDPR would be possible to include in the Proposal’s Recital, it should be noted that recitals are not binding.75 In the interest of full legal certainty, it would be advisable to include a reference in the text of Article 35(1) Proposal itself, which could be implemented as follows:

‘The European Central Bank and the national central banks perform a task in the public interest or exercise official authority, on the basis of Article 6(1)(e) Regulation 2016/679 or Article 5(1)(a) EUDPR, where they process personal data for the following purposes:’

2.5 Processing by providers of support services (Article 36 Proposal)

2.5.1 Background and overview of the gap or issue

74 ‘The European Central Bank and national central banks should consider, where appropriate and to minimise the risk of data breaches, the use of decentralised data storage’

Besides the operations discussed above, which will be conducted by the ECB, national central banks and PSPs, Article 36 Proposal introduces rules on the processing by providers of support services. These support services include the following: (i) the provision of fraud prevention and detection capabilities; and (ii) the provision of message exchange capabilities for the settlement of disputes.

The default approach for these services seems to be that the ECB and the national banks will provide these services and, only when opting out, these will be delegated to support services providers. In contrast with Article 35(5) Proposal, which defines the providers of support services as controllers, it should be noted that under Articles 27 and 32 Proposal, the ECB and the national banks are the ones defining the operation of such services. It is, therefore, questionable that they will not be considered the actual controllers when delegating these tasks to these third parties, with the providers of support services acting as joint controllers with these institutions.

Turning to the substantive content of Article 36 Proposal, it follows a similar structure to the previous Articles. In that sense, it tackles: (i) the legal basis to conduct these activities; (ii) the categories of personal data involved; (iii) the adoption of safeguards to ensure that these cannot identify data subjects; and (iv) the capacity in which these support service providers will engage with regards to personal data involved in these activities.

Regarding the selected legal basis for these activities, and in contrast to the activities operated by PSPs under Article 34 Proposal, which have a contractual relationship with data subjects, the use of public interest is reasonable, particularly considering that these activities are intended to ensure a healthy and sound financial system. However, at the same time, it is possible to repeat the same arguments provided for the analysis of the PSPs’ legal basis and consider that compliance with an obligation would be more fitting.

Turning to the activities, the dispute mechanism will only concern activities pertaining to the operation of the digital euro, which, as noted by Recital 60, refers to controversies over ‘(...) situations where the transaction amount differs, where there are duplicates, or where there is no authorization or pre-validation (...) [as well as] situations of identity theft, merchant identity fraud, counterfeit goods.’ Considering that monetary transactions can by themselves be considered as personal data, these disputes are also dealing with personal data.
As for the general fraud detection and prevention mechanism, we refer to the analysis made in Section 2.2.

2.5.2 Proposed solution or mitigation

The issues identified above can be resolved through the application of the remedies described above, applied *mutatis mutandis* to Article 36 of the Proposal. However, and to foster clarity regarding the intended legal basis to be used, we recommend that Article 36(1) Proposal is drafted as follows:

‘Where the European Central Bank decides to confer tasks referred to in Article 27 and 32 upon providers of support services, providers of support services shall provide payment-related services across PSPs. In such a situation, payment service providers comply with a *legal obligation under this Regulation, relying on Article 6(1)(c) GDPR*, where they process personal data for the following purposes:’

2.6 Retention of offline transactional data for AML/CFT purposes (Article 37(2) Proposal)

2.6.1 Background and overview of the gap or issue

As discussed in the introduction, the Proposal envisions a twofold scheme for the digital euro: an online and an offline system. The adoption of an account-based system facilitates the implementation of AML/CFT measures to comply with relevant provisions on the matter. However, if the offline digital euro is intended to operate as a cash equivalent, then this design decision brings along the necessity to adopt further safeguards to ensure its privacy-equivalence. In this respect, the Proposal states in its Article 37(2) that ‘*transaction data shall not be retained by payment service providers or by the European central banks and the national central banks.*’ While the provision is adequate, it has several shortcomings.

First, the Proposal currently lacks a proper definition of what constitutes transactional data within the operation of the digital euro. As noted by EDPS and EDPB,76 the lack of such a definition further increases the uncertainty over the operation of the offline digital euro. In our

opinion, transaction data would at least contain the amounts involved and the local storage devices that took part of the transaction.

Second, the provision in question merely refer to ‘retain’ as the only prohibited processing activity. Therefore, it would be possible for PSPs, the ECB and national banks to process such personal data in other manners. This is further supported by Annex IV that provides for allowed processing activities to detect counterfeit offline digital euro.

As noted in different EDPS opinions, finding a balance between AML/CFT and data protection is considerably difficult. This balance should take into account the value citizens pay to privacy in their euro payments. Promoting an offline digital euro as identical to cash when its functionality does not align with cash, apart from ethical concerns, amounts to misrepresentation and a failure to meet the transparency obligations expected from the responsible data controllers involved.

2.6.2 Proposed solution or mitigation

To mitigate this, Article 37(2) Proposal should be rephrased in the following terms:

‘Transaction data for offline transactions shall not be processed by payment service providers or by the European central banks and the national central banks.’

Moreover, while a definition in the Articles of the Proposal would be much welcomed, it would be possible to include a definition at the end of Recital 75, as follows:

‘Transaction data shall be understood as any piece of information directly tied to a digital euro account, either online or offline, when used as intended in the context of this Regulation.’

77 For example, Opinion 12/2021 on the anti-money laundering and countering the financing of terrorism (AML/CFT) package of legislative proposals, European Data Protection Supervisor, 24/9/2021
78 See the ECB survey referenced in Section 1.4.
3 Conclusions

3.1 Summary of Key Findings

This report has conducted a preliminary examination of some of the privacy and data protection aspects of the digital euro initiative. We identified significant challenges in the current proposal, especially concerning the account-based design, the involvement of multiple intermediaries, and the handling of transactional data. Our analysis brought to light the potential risks this design poses to user privacy and data protection.

3.2 Significance and Implications

The advent of the digital euro marks a transformative moment in the financial landscape of the European Union. While it promises to enhance payment systems by creating ‘digital cash’, the potential impact on privacy and data protection cannot be overlooked. Our findings highlight the critical need to balance digital innovation with the fundamental rights of individuals.

3.3 Recommendations and proposed changes

In response to these challenges, we propose the following concrete changes to the digital euro Proposal:

1. Modification of Article 5(2): Implement a mandatory adoption of safeguards preferred by the European Data Protection Supervisor (EDPS) in the digital euro's measures, rules, and standards, particularly emphasizing the data minimization principle as well as involvement of data protection supervisory authorities.

2. Enhancement of Recital 70: Explicitly state that the European Central Bank's (ECB) independence must not compromise privacy and data protection rights, ensuring the selection of privacy-centric design choices for the digital euro operation.

3. Strengthening safeguard for Fraud Detection Measures in Article 32: Revise Article 32(2) to prioritize minimal data processing methods in fraud detection and prevention, ensuring they align with data protection principles.
4. **Clarification in Article 34**: Remove ambiguities regarding PSPs’ data processing activities and legal bases, and ensure the activities are strictly necessary and proportionate to their intended purposes.

5. **Revision of Article 35**: Propose clear guidelines for the ECB and national banks regarding the processing of personal data, emphasizing the need for transparency and user privacy.

6. **Reassessment of Article 36**: Review the role and data processing activities of support service providers and the retention of offline transactional data for AML/CFT purposes, ensuring they conform to data protection standards.

7. **Restructuring Offline Digital Euro Operations in Article 37(2)**: Reframe the operational modalities of the offline digital euro to better align with the privacy expectations akin to cash transactions.

### 3.4 Concluding remarks

The widespread acceptance and utilization of the digital euro heavily depend on ensuring its privacy standards mirror those of cash. To achieve this goal, integrating innovative digital payment solutions into the digital euro framework must go hand in hand with robust data protection measures. The proposed changes aim to ensure that the digital euro not only transforms the financial landscape but also upholds the privacy and trust of its users. As the European Union continues to evolve its digital finance strategy, it is crucial to keep data protection and privacy at the forefront of these advancements.
4 References


‘BEUC’s Recommendations on the Legislative Framework for the Digital Euro’ (BEUC - The European Consumer Organization 2023)


‘Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Digital Finance Strategy for the EU’ (European Commission 2020) Communication from the Commission (2020) 591

‘Digital Euro and Right to Cash Policy Analysis from a Human Rights Perspective’ (epicenter.works – for digital rights 2023)


‘ESBG Response to the European Commission Call for Feedback on the Proposed Regulation on the Establishment of the Digital Euro’ (ESBG (European Savings and Retail Banking Group) 2023)

‘Eurosystem Report on the Public Consultation on a Digital Euro’ (European Central Bank 2021)

Fashion ID GmbH & CoKG v Verbraucherzentrale NRW eV [2019] European Court of Justice (Second Chamber) C-40/17, ECLI:EU:C:2019:629

Ferretti F, ‘Open Banking: Gordian Legal Knots in the Uncomfortable Cohabitation between the PSD2 and the GDPR’ (2022) 30 European Review of Private Law 73


Goodell G and Aste T, ‘Can Cryptocurrencies Preserve Privacy and Comply With Regulations?’ (2019) 2 Frontiers in Blockchain 4

‘Guidelines 06/2020 on the Interplay of the Second Payment Services Directive and the GDPR’ (European Data Protection Board 2020) 1.0


‘Report on a Digital Euro’ (European Central Bank 2020)

Swartz L, New Money: How Payment Became Social Media (Yale University Press 2020)

Tronnier F, ‘Privacy in Payment in the Age of Central Bank Digital Currency’ in Michael Friedewald, Stefan Schiffner and Stephan Krenn (eds), Privacy and Identity Management (Springer International Publishing 2021)


EDPS opinion on a prior consultation requested by the European Central Bank on their new customer-management-system [2021] European Data Protection Supervisor Case 2021-0528