Council of the European Union
General Secretariat

Brussels, 28 May 2024

Interinstitutional files:
2023/0212 (COD)

WK 7554/2024 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:	French delegation
To:	Working Party on Financial Services and the Banking Union (Digital Euro Package) Financial Services Attachés
Subject:	Digital euro - WP meeting on 30 May 2024 - French delegation's Non-Paper on selective privacy for offline and online digital euro transactions

24/05/2024

Regulation on the establishment of the digital euro
Non-paper on selective privacy for offline and online digital euro transactions

Executive summary

Eurogroup Ministers expressed their support for a digital euro with a high level of privacy while complying with other policy objectives such as preventing money laundering. They stated that a risk-based approach could be followed to allow for more privacy in the case of less risky transactions, which could ensure a wider adoption of the digital euro among citizens with a stronger preference for privacy[1]*.*

The regulation proposed by the Commission would allow enhanced privacy features for offline transactions only. Yet, from an ML/FT perspective, offline transactions are not inherently less risky than online transactions. Consequently, this non-paper argues that the relevant distinction is between proximity and remote transactions and not between online and offline transactions. Therefore, as transactions carried out in proximity below a certain amount, whether online or offline, present the same risks, these transactions should benefit from the same privacy framework. Online proximity transactions should benefit from selective privacy, along the same lines as offline transactions.

The approach of selective privacy for proximity transactions presents real opportunities for consumers' and businesses' digital euro experience. Such selective privacy appears to be technologically viable and practically feasible.

In this sense, it seems essential that:

1. *the Eurosystem start working now to further explore such selective privacy from a technical point of view and potentially experiment with it, particularly during the current preparatory phase. Such analytical works would anticipate the technical characteristics of a digital euro with greater privacy for offline and online transactions. Addressing this issue right from the design stage of the digital euro would guarantee maximum efficiency from the outset;*
2. *the regulation (article 37) be amended along these lines, without changing its AML/CFT core equilibrium (selective privacy). This non-paper therefore puts forward proposals to this effect;*
3. *Member States share a common understanding of the trade-offs that a privacy framework, be it for offline or online, implies, notably in terms of AML/CFT, consumer's choice and experience or business model. This may require further discussions in the Council to include new provisions in the Regulation, if deemed necessary.*
4. *dedicated consultation efforts be undertaken to get the views of stakeholders (PSPs, merchants and consumers) on these trade-offs in parallel to the technical and legislative works.*

[1] See Eurogroup statement on the digital euro project, 16 January 2023

Contents

1. Privacy for the digital euro: key objectives and narrative

Privacy of digital euro transactions is an essential part of the digital euro project, in that it meets a legitimate demand from the general public[2] and European organisations[3] that aim to guarantee privacy rights for European consumers[4]. Such feature would also meet the demands made by Ministers in the Eurogroup[5] and follow G7 CBDCs guidelines[6]. It is also part of the digital euro core narrative, as presented by the Commission and the Eurosystem: it is an element of differentiation and therefore of attractiveness of the digital euro. For this privacy offer to be real, effectively used and attractive, it must be easy to use and easily understood by consumers.

Appreciating enhanced privacy matters in the context of online or offline transactions between digital euro accounts is therefore key. It is deemed as commonly agreed that the digital euro will comply with data protection and the right to respect for private life, in accordance with EU regulation. Personal data required when opening a digital euro account or processing digital euro transactions will be dealt with in accordance with the GDPR. In addition, the architecture of the digital euro project would ensure that the Eurosystem will not, in any case, have direct, immediate and transparent access to personal data (especially through an anonymisation/pseudonymisation process of all transaction data within the digital euro architecture).

However, we deem interesting to tend towards the highest possible degree of privacy, *i.e.* to transactions delivering “zero information” (e.g. regarding the amount of the transaction, payer and payee etc.) to any actor in the transaction which is not either the final payer or the final payee (the Eurosystem, the PSPs, etc.), whether for online or offline transactions. **In that sense, the digital euro would tend to resemble cash to the extent possible given the technical constraints.**

In this context, the scope and extent of privacy must comply with other policy objectives such as preventing money laundering, illicit financing, tax evasion, and ensuring sanctions compliance, for the digital euro framework to be consistent with other public policy objectives. In particular, the digital euro must not create new illicit loopholes, which would undermine the new framework negotiated in the AML package. Else, it could also have strong reputational consequences for the digital euro, which could prove singularly detrimental.

To ensure this balance, and according to the principles guiding the AML/CFT policies, a **risk-based approach** needs to be followed to allow for more privacy in the case of less risky transactions. It would ensure a wider adoption of the digital euro among citizens with a stronger preference for privacy. The digital euro must therefore benefit from **selective privacy,** enabling

[2] The ECB's 2022 Study on the payment attitudes of consumers in the euro area (SPACE) highlights anonymity and privacy as the top three benefits of cash for European consumers, with a 40% preference. (See Study on the payment attitudes of consumers in the euro area (SPACE) – 2022, ECB, page 44 chart 22). Furthermore, in the Eurosystem's report on its 2021 public consultation on the digital euro project, privacy is by far the most preferred feature of the digital euro among European consumers who responded to the survey. (See Eurosystem report on the public consultation on a digital euro, ECB, April 2021, page 12, chart 4).

[3] Right to privacy and protection of personal data (Articles 7 and 8 of the Charter of Fundamental Rights of the European Union)

[4] See regular position taken by the BEUC.

[5] See Eurogroup statement on the digital euro project, 16 January 2023

[6] See G7 Public policy Principles for Retail Central Bank Digital Currencies (CBDCs), 2021, Principle 3

a balance to be struck between the fundamental objective of privacy attached to public money, as it is today for cash, and the objectives linked to other public policies.

2. The case for integrating online transactions within a framework of enhanced selective privacy: rationale based on ML/FT risk-based approach

The Commission's draft regulation distinguishes between two types of transaction mechanisms, with different privacy and data protection framework applied thereof:

(i) Offline digital euro transactions that would necessitate proximity to be performed, as the settlement will be made locally between two local storage devices. Neither the PSP nor the Eurosystem would see any transaction data. PSP would only see data related to funding and defunding requests from their clients.[7] Those transactions would be capped by a maximum amount (which is still to be determined in the regulation);

(ii) Online digital euro transactions that could be carried out both in physical proximity and remotely: the PSP would see transaction data and the Eurosystem may see some pseudonymised data (without seeing the identity of the payer/payee), notably to settle transactions[8].

Offline transactions are not inherently less risky than online transactions. One could argue that proximity can mitigate the ML-TF risks in that potential wrongdoers run a greater risk of being caught when they are to meet in person to carry out a transaction as they can't hide behind screens. **Yet, proximity digital euro transactions can be achieved both via offline transactions and online transactions. Therefore, the relevant distinction in terms of ML/FT risks is not between online and offline transactions but between proximity transactions and remote transactions.**

Indeed, digital euro online transactions can correspond to payment transactions at the point of sale – therefore performed in physical proximity – with both the digital euro holdings of the payer and the merchant recorded in the Eurosystem settlement infrastructure, therefore being "online" -. **In that case, as this transaction would entail the same risks as an equivalent transaction performed offline, it shall benefit from the same enhanced privacy as an offline transaction.**

This approach is explicitly supported by the EDPB and EDPS in their joint opinion as they "recommend that the specific regime which would apply to the offline modality (which AML/CFT checks only for funding and defunding) should be extended to the online modality for low-value transactions, thereby establishing a privacy threshold, or in other words, a threshold under which no tracing of transactions for AML/CFT purposes would occur."[9]

The Eurosystem also supports the idea of a "selective privacy" for online transactions as well: "For the online model of the digital euro, while the current proposal provides for a level of

[7] See Article 34, paragraph 1.

[8] See Article 35, paragraph 1(b).

[9] As the EDPB and EDPS point out, the level of AML/CFT risks should be analysed precisely, not in the abstract, but in relation to the characteristics of the digital euro. In particular, the EDPB and EDPS state that the AML/CFT risks for online transactions need to be analysed in greater depth, taking into account various mitigating measures such as transaction limits. In this sense, these institutions consider that a certain number of measures are sufficiently interesting and appropriate to reduce the risks incurred. See EDPB-EDPS, *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,* adopted on 17 October 2023, paragraph 89, 90 and 94

privacy comparable to existing cashless means of payment, the ECB also suggests considering the possibility of offering increased privacy for certain low-risk, low-amount payments in digital euro."[10]

Therefore, the future form of the euro shall not be deprived from this opportunity from the outset: a higher level of privacy can also exist for online transactions, along the same lines as for offline transactions.

3. The case for integrating online transactions within a framework of enhanced privacy: opportunities and challenges

a. Opportunity for digital euro users (consumers and merchants)

For citizens, a distinction between proximity and remote transactions would be much clearer than a distinction between online and offline transactions. It would therefore favour a much wider adoption of the digital euro.

It could be argued that digital euro users willing to benefit from a high degree of privacy will be able to opt for offline transactions and that this choice could be sufficient. Limiting a privacy framework to offline transactions only would however appear relatively problematic from a consumer experience point of view.

Indeed, in practice, for consumers, the need to fund their local storage device before being able to carry out a transaction that benefits from privacy would represent important friction. In addition, the need for a consumer to activate the offline modality, depending on these characteristics, could be an additional source of friction. Finally, exercising privacy over offline digital euros would involve a deleterious trade-off for a payer, between the desire to benefit from enhanced privacy on the one hand and the possibility of loss when storing digital euros offline, with no possibility of recovering the funds lost, on the other hand (loss or alteration of smart cards or telephones carrying digital euros stored offline).

Furthermore, the need for regular reconnection of an offline digital euro device would add another layer of friction for the end-users. It would imply transmission of data. Indeed, such reconnection will be needed both (i) for reasons of money supply management in particular to avoid double spending and (ii) to prevent counterfeiting or misuse of local storage devices for fraudulent purposes. It will also be needed because of the limited storage capacity of local storage devices. From a consumer perception perspective, such need would already blur the lines between the privacy of a digital euro offline euro and the framework for digital euro online transactions if the two frameworks were not aligned.

In order to accept offline digital euro payments, merchants will have to provide local storage devices on each of their terminals: consumers will only be able to benefit from greater privacy if a retailer has actually equipped itself to accept offline payments. This configuration would also present constraints, as funds received from offline transactions would automatically have to be defunded to the merchant's online account, due to the lack of capacity to hold digital euros in accordance with the orientations already presented by the Eurosystem. Both the strong dependence on retailers' equipment and the interactions with holding capacities and online digital euro accounts could present significant frictions, and could as a consequence undermine the privacy framework of digital euro transactions. We understand that the

[10] See First progress on the investigation phase of a digital euro (europa.eu), Section 2.2, as well as Opinion of the European Central Bank of 31 October 2023 on the digital euro (CON/2023/34) (europa.eu), Paragraph 16.3

Eurosystem is deepening its technical work in this direction, to reduce these frictions. However, in any case, offering an online digital euro with privacy features would appear to be a way of extending the framework of privacy offered to users.

In total, payments in digital euro, whether offline or online, should be seamless. Therefore, privacy should be extended to online transactions in order to enhance the convenience of a digital euro and make it more attractive for the users who value privacy.

b. Technological viability

Because of the way an offline digital euro would work, it is true that the fact that authorisation and settlement take place in the local storage devices of the payer and payee makes it relatively easy to create the conditions for enhanced privacy. In fact, unless the user explicitly reconnects to its PSP network or the settlement infrastructure, no information whatsoever can be transmitted to the PSP, a third party, or the Eurosystem. No transaction data can *in practice* be retained by payment service providers or by the Eurosystem, except when the user funds or defunds its offline digital euro device.

However, this technical characteristic inherent to the offline digital euro is not the only one capable of organising a privacy framework for digital euro transactions: sufficiently mature technologies are identified to enable the building of a privacy framework for online transactions. In particular, **zero-knowledge proofs (ZKP) technologies** could provide such a framework. Indeed, using ZKP technologies, transaction requests, authorisations and settlements can be processed without having to reveal any personal data, including amounts, while ensuring that transaction amounts do not exceed a given maximum amount.[11] These technologies are already the subject of proposals relating to the digital euro from the private sector, payment experts[12], academics[13] and international organizations[14]. In addition, at the end of 2019, the ECB was already recognising the opportunity to explore these technologies[15] and continued to do so in 2021[16]. Other jurisdictions are also exploring such technologies for their CBDCs.[17]

[11] These methods are based on a stochastic evaluation of the quality of the response to a test based on the Ali Baba cave model. For more details, see Quisquater, JJ. et al. (1990). How to Explain Zero-Knowledge Protocols to Your Children. In: Brassard, G. (eds) Advances in Cryptology — CRYPTO' 89 Proceedings. CRYPTO 1989. Lecture Notes in Computer Science, vol 435. Springer, New York, NY

[12] See IBM Consulting whitepaper – *Implementation of the digital euro,* August 2023 and *A Framework for Resilient, Transparent, High-throughput, Privacy-Enabled Central Bank Digital Currencies,* Androulaki et al. Cryptology ePrint Archive, Paper 2023/1717, 2023 that shows that transactions processing and settlement efficiency can be achieved with stronger privacy guarantees, even with computation-heavy privacy-preserving protocols.

[13] See for instance *Design Choices for Central Bank Digital Currency: Policy and Technical Considerations,* Sarah Allen, Srđjan Čapkun, Ittay Eyal, Giulia Fanti, Bryan A. Ford, James Grimmelmann, Ari Juels, Kari Kostiainen, Sarah Meiklejohn, Andrew Miller, Eswar Prasad, Karl Wüst, and Fan Zhang, NBER Working Paper No. 27634, August 2020 – page43 or research under the Digital currency initiative of the MIT, that notably explores ZKP or private information retrieval modalities of CBDC privacy.

[14] See for instance Project Tourbillon: exploring privacy, security and scalability for CBDCs (bis.org)

[15] See ECB, *Exploring anonymity in central bank digital currencies,* IN FOCUS, Issue n°4, December 2019, p.10

[16] See *Digital euro experiment Combined feasibility – tiered model*, July 2021

[17] Notably, under the second phase of Project Aurum initiated by the BIS Innovation Hub Hong Kong Centre, in collaboration with the Hong Kong Monetary Authority, those institutions intend to explore and enhance privacy by design for retail CBDC around pseudonymisation and ZKP. The project is said to

In concrete terms, this privacy framework for online transactions would mean that both PSPs and the Eurosystem will not be authorised to view online transaction data. This needs to be the subject of an in-depth feasibility study, in particular to ensure effective settlement and operationalisation of the technologies mentioned. It could require only the pre-reading of certain data to identify that the transaction qualifies for enhanced privacy. In any event, the data transmitted will have to be reduced to what is strictly necessary in order to be as closely aligned as possible with the offline framework (no data transmitted, unless reconnected), subject to the Eurosystem clarifying the technical feasibility. This framework must go further than pseudonymised data.

<u>It seems essential to work now to explore this innovative technological opportunity further: the Eurosystem should therefore explore the technical feasibility of these technologies and potentially experiment them. Privacy by design of the digital euro would guarantee maximum efficiency from the outset.</u>

c. Identification of payments made in physical proximity

Providing for a specific selective privacy framework for online transactions requires the payer's PSP to be able to distinguish between transactions carried out in physical proximity and those carried out remotely. **Even if specific work by the Eurosystem is still needed to develop this field further, it already seems technically possible to make this distinction, given both the existing possibilities for payment solutions already used on the market and the technological possibilities offered by the digital euro**.

<u>For existing digital payment transactions,</u> it is already possible to distinguish between transactions carried out by close contact and those carried out remotely, i.e. without direct contact. Notably,

- <u>for payment cards</u>, transaction data can be used to identify the initiation channel, both for the payer's PSP and for the payee's PSP. In more detail, the data accompanying a card-based transactions contains data that can be used to determine whether the transaction was carried out via a payment terminal, including tokenised cards - i.e. carried out in close proximity -, or via an e-commerce interface – i.e. carried out remotely.
- <u>for credit transfers</u>, SEPA data does not include any specific information on the initiation channel, which means that the beneficiary's PSP is not able to identify the initiation channel. However, the payer's PSP is able to determine the initiation channel (whether an IBAN on a banking app, a QR code, another interface using a specific proxy), which makes it possible to know whether this channel guarantees the existence of proximity, so that the PSP can apply selective privacy to this transaction. While this will require further technical expertise, at this stage, it seems satisfactory enough.

<u>For most current payment technologies, the payer's PSP is able to identify whether the transaction is remote or performed in physical proximity, thanks to knowledge of the payment initiation channel: by extension, such a distinction in practice does not appear to be an insurmountable difficulty for the digital euro.</u>

<u>Therefore, for online digital euro transactions</u>, based on these elements, flag data specifying the initiation channel used and therefore the proximity/remote nature of the online transaction would enable the payer's PSP to know which privacy framework to apply.

intend to investigate how these technologies can be integrated into CBDC systems without compromising system performance or regulatory compliance.

With regard specifically to initiation via a QR code, in order to be able to distinguish between a transaction carried out in proximity and one carried out remotely, it seems necessary to ensure that a QR code cannot be scanned remotely. The existence of dynamic QR codes – created on the spot - or other QR code functionalities would make it possible to ensure that a scanned QR code is indeed scanned in physical proximity. Further analytical work is needed there.

These factors (data elements, use of QR codes) indicate that, in most situations, it would be technologically feasible to identify when a digital euro payment is made in close physical proximity. It should be noted that identifying proximity will not require the use of user geolocation data - especially as this would be problematic in terms of privacy and geolocation can easily be modified.

d. Articulation with the current AML/CFT legal framework

Both for offline transactions that benefit from privacy and for online transactions that shall also benefit from a privacy framework, it should be noted that the introduction of such a framework may require the creation of an ad hoc regime based on the existing AML/CFT framework.[18]

Indeed, in this new set-up, the AML legal framework – both present (AML Directive (EU) 2015/849 and Transfer of Funds Regulation i.e. Regulation (EU) 2015/847) and future (AML Regulation, 6th AML Directive and recast of the TFR i.e. Regulation (EU) 2023/1113) - is bound to apply to remote transactions in digital euro. Such transactions will be intermediated by obliged entities and the digital euro arguably falls within the definition of "funds" under Article 2, point (2), of Directive (EU) 2018/1673[19] to which the AML legal texts also refer. In addition, based on the currently-known technical specificities and use cases of the digital euro, it appears that, when carried out remotely, digital euro transactions pose equivalent ML-TF risks as remote banknote, scriptural or electronic money transactions. Besides, recital (78) of the Commission proposal for the establishment of a digital euro indicates that the existing AML requirements apply to online digital euro transactions.

Therefore, if co-legislators agree on a higher level of privacy for certain transactions in digital euro, an ad hoc AML regime needs to be developed. Article 37 of the Commission proposal for the establishment of a digital euro provides for a tailored AML regime for offline payment transactions, with a certain transaction threshold.

Whatever the regime (offline/online or proximity/remote), the threshold should be determined by the Level 1 Regulation itself rather than a Commission implementing act, as is currently provided for.

In a remote/proximity regime, the "cash-like" privacy that benefits offline digital euro transaction under the current legislative proposal shall be extended to all proximity transactions/payments. In an extended privacy regime, AML customer due diligence shall be carried out upon opening

[18] The EDPB and EDPS share such objective: the EDPB and EDPS are of "the opinion that the AML/CFT rules currently applicable to electronic payments, allowing traceability of commercial bank money, need to be adapted to achieve the objective of the digital euro to ensure the highest possible level of privacy." See EDPB-EDPS, *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,* adopted on 17 October 2023, paragraph 88

[19] 'property' means assets of any kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or an interest in, such assets

of a digital euro payment account (and registering of a local storage device for offline digital euros) but shall not apply thereafter to individual transactions when carried out in physical proximity. In addition, no personal data (identity of the person, amount, origin and destination etc.) would be collected, passed on and/or stored onto the (ordering or beneficiary) PSPs' payment systems nor the Eurosystem's infrastructure provided that the transaction is under the threshold.

PSPs would only access funding and defunding data related inter alia to the identity of the user and the amount funded and defunded, similar to personal data processed by PSPs when users deposit or withdraw cash. PSPs would transmit these funding and defunding data, upon request, to Financial Intelligence Units and other competent authorities when users are suspected of money laundering or terrorist financing.

Such ad hoc regime would depart from the features of the anonymous e-money provision foreseen in the current AML Directive (and retained in the future AMLR), mostly applicable to pre-paid cards and which allow for exempting obliged entities from carrying out CDD under certain conditions since the card issuer has a duty to monitor the business relationship with the card holders[20]. Rather, AML-CFT obligations surrounding proximity payments in digital euro would be close/similar to those made in cash with no or very limited traceability (e.g. through ZKP technologies when carried out online) and a payment threshold to mitigate the ML-TF risks[21]. This threshold (below which confidentiality is ensured) would have to be set in a way that prevents smurfing (circumvention of the threshold by breaking down one transaction into several small linked ones just below the threshold).

Yet, as already pointed out by the ECB and the Presidency, the practical enforcement of transaction (and holding) limits should several digital euro payment accounts (and local storage devices for offline digital euro) exist is yet to be worked out. Input from the national central banks and the ECB will be key in this regard.

Finally, the Financial Action Task Force (FATF) has yet to undertake policy work on the impact of the emergence and diffusion of Central Bank Digital Currencies on the AML-CTF global standards (40 recommendations). As a consequence, the latest substantial revision project (that of recommendation 16 on payment transparency[22]) has deliberately chosen to leave aside

[20] Article 15 (CDD) of the new AMLR: " *Supervisors may, directly or in cooperation with other authorities in that Member State, exempt obliged entities from applying, in full or in part, the customer due diligence measures referred to in Article 20(1), points (a), (b) and to (c), with respect to electronic money on the basis of the proven low risk posed by the nature of the product, where all of the following risk-mitigating conditions are met:*

(a) the payment instrument is not reloadable, and the amount stored electronically does not exceed EUR 150 or the equivalent in national currency

(b) the payment instrument is used exclusively to purchase goods or services provided by the issuer, or within a network of service providers;

(c) the payment instrument is not linked to a payment account and it does not permit any stored amount to be exchanged for cash or for crypto-assets;

(d) *the issuer carries out sufficient monitoring of the transactions or business relationship to enable the detection of unusual or suspicious transactions."*

[21] The AML Regulation (which is to be adopted and published by the end of June 2024) provides for a mandatory threshold of 10,000 EUR for cash payments in exchange for goods or services in all EU member States (which will be able to retain or set a lower limit at the national level). In addition, the AML Regulation provides that obliged entities must identify and verify the identity of any individual seeking to carry out an occasional transaction in cash (amounting to 3,000€ or more).

[22] As it stands, FATF Recommendation 16 states that the message accompanying each transfer of funds (credit transfer, direct debit, transmission, transfer using an electronic money instrument) must

the articulation with Central Bank Digital Currencies. Should a specific work stream be dedicated to CBDC over the next biennium (upon approval of the draft FATF work program), the 14 EU Member States and the Commission (which are members of the FATF) will have to coordinate to argue before other delegations that the current AML-CTF standards need to be adapted to accommodate the specificities of CBDC and, namely, the concept of selective privacy. International works around CBDCs at the FATF will therefore be necessary, regardless of whether the regulation adopts an offline-only approach or whether it provides for an enhanced privacy regime with a proximity-based rationale.

e. Fraud prevention and digital euro user's choice and experience

Building a privacy framework for digital euro transactions, whether offline or online, means that PSPs and other parties to a transaction (Eurosystem, etc.) will access fewer data. However, the mechanisms for preventing and combating fraud, on the one hand, and for reimbursing in the event of fraud, on the other, are based precisely on the use of this data to identify fraud patterns and prevent them both at PSP level and at macro level, in particular at scheme level. In the first case, the introduction of a privacy framework means that the methods used to combat consumer fraud involving personal data will have to be rethought. Above all, national central banks, the ECB, supervisory authorities as well as the private sector will need to give their opinion on the measures to be taken to increase the security of transactions benefiting from privacy. In the second case, it will be necessary to determine how a consumer will be able to request a refund, and whether this would even be possible in practice: without knowledge of the payment data, neither the merchant nor the PSP will be able to issue a refund in the event of fraud. In any event, the relevant rules of the Payment Services Directive (articles 71 to 77) will have to be adapted to the desired privacy for digital euro transactions: it seems imperative that the application of these provisions be clarified in the present text. The Commission's analysis in this area would therefore be welcome, as would the technical analyses of the ECB and national central banks. This applies to both offline and online transactions in digital euros.

In practical and broader terms, choosing to benefit from privacy for a user will present broader trade-offs between:

- On the one hand, not transmitting data to PSPs and the ESY but with less protection against fraud - which will need to be substantiated - and therefore with fewer possibilities for reimbursement, possibly relatively less efficient transactions, possibly with fewer value-added services (subscriptions, commercial use of data, etc.), or a different user experience (we can assume that for a payment benefiting from enhanced privacy, the payer will see less information about his payment history, the identity of the payee, etc.). ;
- On the other hand, a framework with less respect for privacy but with greater security guarantees. This will apply to both offline and online services. In addition, users may wish to select the transactions where they want to benefit from enhanced privacy in cases where a 'privacy quantity' is allocated over a given period.

So, while these trade-offs have yet to be specified, it will be necessary to consider the role of the consumer in choosing the modality with/without enhanced privacy, which could take several forms, such as (i) privacy by default, (ii) consumer's choice to activate enhanced

include a minimum of basic information about the parties to the transaction. There is an exception for the payment of goods or services using payment cards, for which only the card number is required. It is one if the recommendation that would require work to adapt to the emergence of CBCDs.

privacy or deactivate enhanced privacy, etc. The regulation could ultimately include provisions specifying these choices, in order to protect the consumer.

f. Compensation regime

Whatever the legal framework chosen for the digital euro business model, such business model would be based on the determination of transaction fees to be paid by the payee, whether to the payer's PSP, the payee's PSP or both. These fees are usually proportional to the amount of the transaction paid by the payer. In addition, the identification of the payer's PSP by the payee's PSP ensures the compensation that is often necessary to balance the economic model of a payment solution with a 4-corner model.

However, a payment with enhanced privacy will not enable either the payer's or the payee's PSP to identify the exact amount of the transaction, or the other payment service provider who is involved in the transaction.

This intrinsic difficulty can nevertheless be overcome by the private sector to build a viable economic model, through several options:

- depending on the use case, the beneficiary could be charged a fixed fee for a transaction benefiting from a privacy framework. While it is true that these fees could not be adapted according to the amount of the transaction, this would present a lesser difficulty insofar as the transactions benefiting from privacy could only be for small amounts.
- Charging merchants for defunding offline could be another option, providing a good proxy for targeting merchants collecting digital euro transactions without compromising privacy.

These options may be specified as and when the Eurosystem further develops technical payment solutions benefiting from privacy. In particular, the choice will be clearer once the co-legislators have a clear knowledge of the costs involved for PSPs and merchants and of the technical possibilities offered by these solutions. The objectives of this choice should be (i) to align offline pricing and online pricing as far as possible, (ii) not to lower the privacy requirements to make a given business model workable.

g. Level playing field issues

As regards the level-playing field with other payment solutions, including private payment solutions, it should first be noted that the framework proposed by the Commission, which provides selective privacy for offline transactions, already introduces a difference between private solutions and the digital euro in that the digital euro would benefit from an ad hoc framework.

Above all, the co-legislator is faced here with a choice in terms of balancing different public policies, and in particular between level-playing field and respect for a privacy framework offered by a public solution. This choice already exists for public money in that cash already benefits from an ad hoc privacy framework relating to its historical use. In this sense, the European co-legislator is once again faced with this choice.

4. Timetable considerations

It is essential for the Eurosystem to begin to work now - particularly during the preparation phase - on the technical characteristics of a digital euro with greater privacy for proximity transactions, online and offline, the technological needs it entails, and what it would mean for PSP distributing digital euros**.** Designating an online digital euro from the outset with limited privacy poses a real risk to the very possibility of modifying this privacy framework at a later date: the path effects on the design of the digital euro could prevent in the future, even at a later stage, the introduction of a framework more protective of civil liberties for transactions in public money.

It is therefore essential that the ECB and national central banks further explore selective privacy for online transactions as long as they are performed in physical proximity. Such analytical and technical work would in particular inform the co-legislators of any unidentified difficulties and ensure the technical feasibility in detail, insofar as it appears promising today.

Also, it seems advisable that special care should be taken in consulting *ex ante* on this specific issue on all stakeholders, namely PSPs and the whole payments industry, along with merchants, regarding the technical requirements and the impact on their capacity to deliver smooth transactions operations and user experience, but also consumers' representatives. The Commission could conduct dedicated consultations in parallel to the technical work by the ECB and national central banks.

5. Way forward

The framework initially proposed by the Commission needs to be adapted.

Firstly, the draft regulation shall reflect the absence of a direct link between offline/online and local/remote transactions so that there is a clear difference between the two concepts (although offline naturally implies proximity).

Above all, the core of the regulation must ensure equal treatment of online and offline digital euro transactions from a privacy perspective. Since the construction of an ad hoc privacy framework for the digital euro requires the establishment of a new balance between several public policies, this highly political balance must also enjoy significant democratic support and therefore be determined by the co-legislators, without delegation to other institutions. In this sense, Member States shall determine the appropriate limit under which transactions of a lower amount will benefit from increased privacy, and other protective measures to avoid any loopholes. In order to ensure close monitoring of this framework and to provide for adaptations, if necessary, a report from the Commission, based on the consultation of the AMLA and the EDPB one year after the issuance of the digital euro, should make it possible to carry out an initial assessment, accompanied by a legislative proposal if the Commission deems this necessary.

In addition, as indicated above, this framework will have to be based on the identification of the proximity realisation of a transaction. The private sector will therefore need to be guided in identifying this character for a variety of initiation channels, including private ones. It is therefore proposed that the ESAs and the ECB put in place a precise level 2 framework specifying how to recognise a transaction carried out in close proximity, in a robust and secure manner, to the extent possible[23].

6. Proposal for changes

Therefore, as a way forward,

[23] However, for some form factor (e.g. pay by link, alias, static QR codes), it may not be possible to determine whether the transaction is initiated remotely or in proximity. These transactions could therefore not benefit from selective privacy. Such situations will need careful technical assessment.

- Article 2 shall reflect the distinction between online/offline and remote/proximity.
- The provisions laid down in article 37 should be applicable to proximity payments regardless of whether they are performed online or offline.
- Article 37 shall also cater for regulatory technical standards to be developed by ESAs and the ECB.

The proposed approach suggested are the following ones:

	Drafting suggestion
Article 2 – paragraph 15 15. ‘offline digital euro payment transaction’ means a digital euro payment transaction, made in physical proximity, where authorisation and settlement take place in the local storage devices of both payer and payee;	Article 2 – paragraph 15 15. ‘offline digital euro payment transaction’ means a digital euro payment transaction, **~~made in physical proximity~~**, where authorisation and settlement take place in the local storage devices of both payer and payee;
Article 2 – new paragraph 15a	**15a. ‘offline digital euro’ means a digital euro recorded in the local storage device of the digital euro user;**
Article 37 – title Anti-money laundering rules applying to offline digital euro payment transactions	Article 37 – title **Privacy and a~~n~~**te-money laundering rules applying to offline digital euro payment transactions and online digital euro payment transactions **below a certain threshold**
Article 37 – paragraph 1 1. Payment services providers shall apply paragraphs 2 to 6 to offline digital euro payment transactions.	Article 37 – paragraph 1 1. Payment services providers shall apply paragraphs 2 to 6 to **~~offline~~** digital euro payment transactions, **made in physical proximity, either offline or online below the amount of EUR [XXX] whether the transaction is carried out in a single operation [or in several operations which appear to be linked].** *The amount below which digital euro transactions will benefit from enhanced privacy will be specified at a later date.*
Article 37 – new paragraph 1a	Article 37 – new paragraph 1a **1a. EBA, in close cooperation with AMLA and the ECB, shall develop draft regulatory technical standards to specify the methodology to be used by PSPs to identify when a transaction is made in physical proximity.** **EBA shall submit the draft regulatory technical standards referred to in the first subparagraph to the Commission by [12**

	months after the entry into force of this Regulation]. **Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in the first subparagraph of this paragraph in accordance with Articles 10 to 14 of Regulation (EU) No 1093/2010.**
Article 37 – paragraph 2	Transaction data shall not be [**retained/processed]** by payment service providers or by the European central bank~~s~~ and the national central banks. *Possible clarification of this provision subject to technical work by the Eurosystem - see above.*
Article 37 – paragraph 5 5. The Commission is empowered to adopt implementing acts setting offline digital euro payment transaction limits and holding limits. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39.	Article 37 – paragraph 5 ~~**5. The Commission is empowered to adopt implementing acts setting offline digital euro payment transaction limits and holding limits. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39.**~~
Article 37 – paragraph 6 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; (c) the objective of ensuring the usability and acceptance of the digital euro as a legal tender instrument. For the purposes of point (a), the Commission may request AMLA to adopt an opinion assessing the level of money	Article 37 – paragraph 6 ~~**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:**~~ ~~**(d) an assessment of the money laundering and terrorist financing threats, vulnerabilities and risks of the digital euro when funding and defunding their payment instrument;**~~ ~~**(e) 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;**~~ ~~**(f) the objective of ensuring the usability and acceptance of the digital euro as a legal tender instrument.**~~ ~~**For the purposes of point (a), the Commission may request AMLA to adopt an opinion assessing the level of money**~~

laundering and terrorist financing threats associated with the offline digital euro and its vulnerabilities. The Commission may consult the European Data Protection Board.	~~**laundering and terrorist financing threats associated with the offline digital euro and its vulnerabilities. The Commission may consult the European Data Protection Board.**~~
Article 37 – new paragraph 6a	Article 37 – new paragraph 6a **6a. By one year after the first issuance of the digital euro and after consulting the AMLA and the EDPB, the Commission shall present a report to the European Parliament and the Council on the application of this article and on the money laundering and terrorist financing vulnerabilities and risks of the digital euro transactions, accompanied, where appropriate, by a legislative proposal. The report shall contain at least the following:** **(a) an assessment of the money laundering and terrorist financing remaining vulnerabilities and risks associated with digital euro transactions benefitting from enhanced privacy;** **(b) an assessment of the money laundering and terrorist financing remaining vulnerabilities and risks of the digital euro when funding and defunding their payment instrument;** **(c) an assessment of the usability and acceptance of the digital euro as a legal tender instrument.**