DIGITALEUROPE

23 OCTOBER 2023

DIGITALEUROPE position on the Digital Euro

Executive summary

The draft Digital Euro proposal provides an important first step towards developing the basis of a public-private partnership to deliver public money for a new digital age. If well designed, the Digital Euro has the potential to drive further innovation, competition, and choice for consumers in Europe, and to strengthen the single market. To achieve success, the Digital Euro must deliver clear benefits to end users and maintain financial stability. **To meet this goal, the EU must:**

1. **Articulate a clear compelling customer value proposition by defining a set of key desired end-user benefits** which should be mapped to specified design choices. Benefit to consumers is an important and necessary condition to being widely used and successful (today, customers already have access to competitive digital payment solutions, with new ones being developed frequently).

2. **Conduct a cost-benefit analysis on the Digital Euro** relative to alternative approaches that aim to modernise the payment system. The Digital Euro should contribute to making payments, and ultimately Europe, more competitive.

3. **Conduct an evidence-based study of the potential risks to financial stability.** Potential negative impacts on financial stability and banks' capacity to fund the economy, and therefore economic growth, should be avoided by design.

4. **Acknowledge the technical and operational complexities of a Digital Euro roll-out** and allow for a two-phased approach to its implementation.

We understand that considerations such as monetary sovereignty and open strategic autonomy provide the rationale behind the EU exploring

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

the potential launch of a digital euro. For a successful roll-out, policymakers should introduce guidelines and institutional safeguards within this project, all while indeed preserving central banking independence in Europe.

Table of contents

Distribution (Chapter IV)

A two-phased approach (Art. 13.7)

We believe a two-phased approach to implementation is needed, purely to technically facilitate the initial rollout of the digital euro. In Phase 1, PSPs should provide a single digital euro account per citizen to avoid system technical complexities that would halt the digital euro implementation. At the same time though, the European Central Bank (ECB) through the Scheme Rulebook should actively lay the groundwork for operationalising multiple account functionalities to be made available in a subsequent Phase 2. This preparatory work will embrace the promise of innovation and consumer choice that multiple account functionalities can bring. As the groundwork matures and the system demonstrates operational resilience, Phase 2 can commence, phasing in multiple accounts. This implementation approach will be key to provide technical robustness while capturing inherent innovation possibilities, also taking the opportunity to learn from end users to identify areas for improvement.

We also welcome the ECB's approach to enable merchants to have multiple wallets.

- Although the initial release focuses on retail users (P2P and B2C-use-cases), a digital euro can also be a significant contributor to digital, automatized business processes. To not create significant complexities for the development of a digital euro and future releases, it is important to consider the needs of corporates today as well as not to discourage future innovation.
- Merchants (as points of acceptance for payments) have the need for multiple wallets and multiple wallets can also make sense for businesses in the case of some use-cases and innovative business models, that might be for example based on cutting-edge technologies. Restrictions such as intra-day holding limits have to be viewed and decided on taking this perspective into consideration.

This brings up several questions that have not yet been considered or answered. For instance, the criteria to differentiate legal entities and which restrictions apply to whom. We believe that for a successful digital euro it is crucial to also consider these aspects and to not overly restrict corporate usage, discouraging possible future innovation.

Distribution Points (Art. 14.3)

Whilst we support the use of public resources (e.g. postal offices) as an option for digital euro distribution, the rules governing public facilities operating as distribution points should operate under the principal of "same risk, same regulation" in order to avoid creating an unbalanced playing field.

This provision addresses issues of financial inclusion for those who do not wish to open accounts at credit institutions, as well as increases the number of potential distribution points to facilitate adoption.

Legal Tender (Chapter III)

The Digital Euro Regulation proposal for legal tender and mandatory acceptance could result in a significant burden for merchants across the euro area. This is especially true given that the digital euro design process is still underway, and it is unclear what additional upgrades merchants will need to implement (e.g., if QR codes will be the initial point-of-sale (POS) solution).

- **Market integrity:** Mandatory acceptance could distort competition among digital payment providers and crowd out innovation. Fostering competition is the most fundamental principle to protect and for consumers: robust competition pushes service providers to bring their best capabilities and drive innovation. The best way to encourage competition for the Digital Euro is to leverage the existing and widely used acceptance infrastructure for digital payments. By creating an open platform built on existing acceptance infrastructure, policymakers can tap into the already very competitive, innovative, and secure payment system.

- **Driving out the use of cash:** Mandatory acceptance may in practice further drive out the use and acceptance of cash. Article 5 of the Proposal on the Legal Tender of Euro Banknotes and Coins allows merchants to decline cash "in good faith". If all merchants – small, medium, large – are required to invest in digital euro acceptance infrastructure, they will be incentivised to focus on digital means of payment as handling cash will become another operational burden.

- **Compatibility:** We welcome the proposal's recommendation in Recital 59 that the ECB *"should seek to ensure that the digital euro is compatible with private digital payment solutions at the point of interaction, and in person-to-person payments"* as well as the *"use of open standards, common rules and processes, and possibly shared* *infrastructures.*"[1] This language should be incorporated into the Regulation itself. We believe this will encourage greater interoperability in the payment system and reduce merchant acceptance burdens.

- **Interoperability:** To further ensure interoperability and reduce merchant acceptance burdens, we recommend that the Commission explores further exemptions for merchants, such as prohibiting mandates that merchants adopt new payment terminals, especially for those already accepting a comparable means of payment. On a more technical level, we encourage the Commission to leverage on the existing payment solutions to route messages between user accounts as part of the core infrastructure.
- **Small businesses:** To further limit the burden on small businesses, we recommend expanding the exemption to accept the digital euro from businesses with 10 employees to those with 50, in line with EU small business definitions.[2]

Use of the Digital Euro as a Store of Value and as a Means of Payment (Chapter V)

Holding Limits (Art. 16)

- **Holding limits set by the ECB:** We welcome the mandate to the ECB to establish holding limits since the ECB will always take into consideration and safeguard financial stability. Excluding the holding limits from the regulation will make it easier to adapt to the reality surrounding the use of cash across Europe at any given time and to maintain financial stability.
- **A low holding limit in the first phase:** Such a limit should be low, in a first phase, to avoid a dramatical impact in liquidity ratios and leakages of banking deposits in a scenario of total adoption of the digital euro. The limit can be tested before final roll-out to avoid financial instability.
- **Fair and evidence-based process:** To uphold the objective of financial stability, the ECB should be subject to a statutory due process when changing the holding limits. Such an evidence-based

---

[1] Recital 59, Proposal for a regulation of the European Parliament and of the Council on the Establishment of the Digital Euro (2023/0212).

[2] Small and medium-sized enterprises (SMEs) are defined in the EU recommendation 2003/361, Article 2(2), here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32003H0361

approach would at minimum include a consultative process where all relevant industry stakeholders are consulted. This approach should be supported by a specific and detailed impact assessment – drawing on bank level data through a Qualitative Impact Study (QIS) – that has been undertaken by the Eurosystem, providing a full picture of the consequences for banks' balance sheet and liquidity management. To safeguard both micro- and macro- financial stability, the SSM arm of the ECB should be given the authority to review holding limits on a continuous basis.

- **Justified reasoning:** The ECB should justify their reasoning before issuing the digital euro together with the analysis mentioned in Article 16(2) about how potential risks for financial stability will be mitigated and have the support of the co-legislators. If legally possible, the regulation could include for example certain triggers that would have to happen to enable the ECB to take the decision.

Fees on Digital Euro Payment Services (Art. 17)

The Digital Euro's remuneration model is a critical component to enable its optimal functionality (and thus benefit to users) as investments in technical infrastructure will be required to enable the Digital Euro to function.

Stakeholders involved in the development, integration and subsequent provision of Digital Euro services must be compensated in a manner that enables them to cover all relevant costs incurred and not only the transaction fee (besides the initial cost of deploying the digital euro ecosystem, the provision of digital euros will have recurring costs for its distribution and intermediation, such as those related to the identification (KYC) of users and the funding and defunding of digital euros, custody and maintenance of accounts/wallets, payment initiation, post-settlement services (including dispute management and fraud with merchants), customer service (offices, complaints at call centres)).

PSPs and banks should also have the option, and be incentivised to, offer innovative value-added Digital Euro services to customers. The digital euro infrastructure should allow for these services to be open to innovation for the clear benefit of customers and merchants. To promote innovation and ensure a competitive pricing environment, the fees of these additional services should be left to the market to decide.

Technical Features (Chapter VII)

Accessibility and Use (Art. 22)

- **We support Art.13(4) that states that PSPs may only link each digital euro payment account to a single non-digital euro payment account** to allow for the reverse waterfall mechanism. **In addition, we also support Art.22(4)** allowing users to link multiple non-digital euro payment accounts to grant them the freedom to switch their funding mechanism at any given time. This will reduce friction on the usability of the digital euro by European citizens.
- **In addition, the linking of a digital euro account with the non-digital euro account (payment account) of another citizen should not be allowed.** This would introduce substantial additional complexity, with multiple balance checks and (de)funding transactions needed with said 'other citizen' for each digital euro transaction (and all within the constraint of the entire transaction being instant).

Offline and Online Digital Euro Payment Transactions (Art. 23)

Given the technical complexities related to settlement/holding limit enforcement in offline wallets as well as the difficulty to articulate offline wallets as a clear customer benefit, we suggest as a possible option to explore that the digital euro allows for self-custody wallets to be offered by PSPs as an option.

A defining characteristic of a digital currency is determining who will be the entity holding the private keys, which are required to sign a transaction. In a custodial wallet there is a custodian (intermediary) who holds the customer´s key and can sign transaction on their behalf. Custodial wallets are similar to bank accounts where intermediaries have oversight of all transactions but also hold liability in case the funds are lost. In a self-custody wallet, the user directly holds the key to sign a transaction. This means that the transaction remains private between the parties completing the transaction as there is no intermediary with oversight. Self-custody wallets are closer to physical cash in design, which also means that in the event of loss there is no immediate recovery mechanism (in the same way that customers are not currently able to recover a physical bank note if it gets lost from their wallet). **We invite authorities to explore this alternative model in which customers can choose between custodial and self-custody wallets, in the same way they can currently choose between using cash and bank accounts.** As it is proposed for the offline digital euro, any holding limits on digital euro payment accounts would also apply to self-custody wallets. In addition, intermediaries should have access to all transaction data required to comply with its legal obligations, as well as to provide digital euro services based on the self-custody wallet. Self-custody wallets should be subject to specific transaction and holding limits to prevent money laundering and terrorist financing in accordance with Article 37, as well as to mitigate fraud risk.

Due to the operational complexity of enabling digital euro, PSPs should be given the option, to choose whether they will be offering custodial and/or self-custody wallets to customers.

Conditional Payments (Art. 24)

We support the proposed Article 24.1 wording in support of conditional payments. Programmability could be a key factor that allows PSPs to offer value added services to customers and merchants, as well as to create entirely new use cases that enhance innovation and broader economic efficiency. Conditional payments can make it easier to deliver existing payments use cases (such as Preauthorization, Account on File and Recurring Payments), and allow for the creation of entirely new ones (such as automating machine-to-machine payments or supporting contingent “delivery vs. payment” transactions). New services based on conditional payments can become a new revenue stream for intermediaries to compensate the costs of enabling digital euro.

Interoperability (Art. 26)

We consider that the legal framework should mandate the private sector to establish pan-eurozone interoperability rules for digital euro payment solution on the basis of a jointly governed digital euro scheme rulebook. This is because, after the creation of a digital euro, it will be necessary to support transactions via establishing interoperability both between other currencies within Europe but also establish interoperability beyond the European region. The ECB must ensure that development is in line with global standards and initiatives.

Front-end Services to Access and Use the Digital Euro (Art. 28)

In order to avoid unintended consequences in terms of competition and financial stability, we propose that rather than PSPs being obliged to offer the ECB front-end app (as per the current Proposal) on top of their own app, PSPs should instead have the option of also offering the ECB app. We note that this **option**, also as per the Proposal, should remain as being developed by the ECB but provided and used by the PSP to ensure no overlap and competition with private solutions and avoiding a situation where users would have direct communication with the ECB.

In addition, the EU co-legislators, in the legal framework, should allow credit institutions to have the option to distribute the digital euro either via existing payment solutions or via the ECB-built front-end.

Privacy, Data Protection and Anti-Money Laundering (Chapter VIII and IX)

A Privacy-Friendly Model for the Digital Euro

DIGITALEUROPE members firmly believe that strong privacy safeguards for digital euro users are a paramount condition for the successful implementation and uptake of the digital euro. Considered as the most important feature by both citizens and professionals, privacy is a fundamental right that should be upheld in the design of the digital euro, alongside the security and legitimacy of transactions.

Preserving Financial Stability without Compromising Privacy (Art. 34-36)

Throughout the text, DIGITALEUROPE identified a number of discrepancies between the Commission's aim to provide a high level of privacy while ensuring that the digital euro distribution model preserves financial stability and fosters digital innovation.

- **ECB central repository of data:** **For example, PSPs are expected to enforce holding limits across multiple wallets, based on the ECB's central repository of data (a single access point of digital euro user identifiers).** This implies that the PSPs will have to disclose to the ECB data about a user's identity and the number of accounts they hold, consequently being able to refuse their requests to open new accounts if they reach their holding limits. In comparison with the offline world, users are not asked nowadays if they hold other bank accounts with other credit institutions or to disclose their transaction history as a condition of account opening. At the same time, the ECB will need access to certain data to identify trends and monitor the digital euro in circulation, notably to be able to adjust holding limits in the future – but the proposal does not foresee access to data for the purpose of maintaining the financial stability.

- **Alignment with the GDPR:** The GDPR already regulates access to private data by private intermediaries and should fully apply to the digital euro. Whilst recitals 12, 70, 72 and 73 clarify that the GDPR will apply, the provisions included in Art. 34(1) and (2) and Annex III seem to limit the applications to specific purposes for data processing by intermediaries, and the specific data that will be accessible. If the objective of Article 34 is to clarify what happens when the data is not used for the purposes listed in this paragraph, it **should be explicit that all data that is not processed for those purposes will be treated in accordance with GDPR regulation.** The Regulation could explicitly state that the PSPs may process other alternative data for other purposes e.g. to provide value-added services, on the basis of the remaining legitimate grounds under the GDPR (e.g. consent of the data subject or performance of the contract).

- **Joint controllership:** The reference to joint controllership in Art.34(3) is concerning and we recommend deleting the last sentence *'these payment service providers shall be joint controllers'*. Each PSP should act as an **independent data controller** and be responsible separately according to the personal handling data contracts agreed with the user and under the prevailing law. Although the processing by each PSP would be linked by means of a contractual relationship, both PSPs would not make converging decisions.

- **Technical measures referred to in Art.34(4) to ensure that any data communicated do not directly identify individual Digital Euro users should be clearly defined by means of guidance,** that allow for technology neutrality, taking into account that (i) the use of additional information can lead to the identification of the individuals (it would be pseudonymous personal data); and (ii) the integration of different indirect identifiers to a dataset (i.e. the ECB) increases the risk of identification (which is a risk that should not be assumed by the PSP);. This should also be extended to payment support services (PSSs), that have a similar obligation under Art.36(4).

  Article 34(4) places the responsibility on the PSP to establish such technical measures and there is therefore a need for clear and harmonised standards.

- **Know Your Customer (KYC):** To safeguard privacy in the digital euro, we would welcome the legislation to enable PSPs and intermediaries offering digital euro wallets to leverage the European Digital Identity Wallets (art 25) for KYC customer verification (as referred to in Recitals 57 and 58). This would offer greater customer privacy and would enable intermediaries to save costs and duplicative efforts.

  The legislation could also allow for a tiered approach to KYC which would apply different levels of scrutiny to transactions according to risk. Such a concept of "tiered KYC/AML," which would provide the end user the option to obtain one of multiple "tiers" of e-KYC credential, where higher tiers correspond to increased verification and transaction tracking and allow for increased transaction values. This would allow for increased levels of scrutiny to be applied to higher risk transactions, focusing resources where risks are highest. It could also be used to facilitate an allowance for certain low value transactions to operate with a privacy similar to cash.

- **International Level:** The proposal also requires intermediaries established or operating in third countries to implement the holding limits set by the ECB. **This raises two questions, namely the ability for these intermediaries to access the ECB's central repository and fund/defund euro holdings, and the ECB's ability to force these provisions in third countries where it has no means or jurisdiction.** Additionally, the Commission's ambition to enable the use of offline digital euro cross-border raises privacy concerns, especially for countries with strict data localisation requirements.

- **Data Processing by Different Parties: In the same vein, the proposal needs clarifications with regards to conditions related to the processing of personal data by the different parties.** Article 35 para 4 requires *"clear segregation of personal data to ensure that the European Central Bank and the national central banks cannot directly identify individual digital euro users".* However, if in practice PSPs must report personal identifiers and transaction data to the ECB's single access point, it is not clear how a central repository that resides with the ECB and where the ECB acts as "controller" of this data can be segregated between the ECB and intermediaries.

The proposal requires important adjustments to ensure the digital euro's long-term viability and success without compromising on the level of privacy nor the stability of this new payment instrument and by extension the economy as a whole.

To strike this crucial balance from the beginning, DIGITALEUROPE recommends EU policymakers to require users' digital euro accounts to be only linked to one nominated PSP during the first phase of the digital euro rollout to reduce financial and data risks, operational complexity, and deposit substitution. Further, consumers and businesses see benefits from value-added services, which are not essential services but can significantly enhance the core product improving the end user's experience or providing more effective fraud prevention tools. The proposal should clarify that, for such purposes, intermediaries should be able to access customers' payment data, with their consent.

Further, DIGITALEUROPE calls on EU policymakers to adopt a technology-neutral approach to PETs and remain supportive of their usage without constraining it to enable their development. DIGITALEUROPE recognises the Commission's efforts to encourage the development of state-of-the-art security and privacy preserving measures, such as pseudonymization and cryptography techniques, to preserve users' privacy. While we are seeing significant developments in this area and believe in the great promise they hold, privacy-enhancing technologies (PETs) are still in their early stage of development and roll out.

Reconciling Privacy with the EU's AML/CFT Requirements (Art. 37)

DIGITALEUROPE calls for additional guidance to be developed by the European Banking Authority and the Anti-Money Laundering Authority to provide financial entities with more legal certainty and information on how to adjust European AML/CFT requirements to offline digital transactions.

There is an evident but not irreconcilable tension in the proposal between the Commission's objective to provide a "higher degree of privacy" to users of offline digital euro and the need for involved parties to access data to comply with relevant European anti-money laundering (AML) and counter-terrorist finance (CFT) requirements.

From an AML compliance perspective, it seems problematic that the text does not take into consideration that users could conceivably open multiple offline accounts with different PSPs, inside and outside the eurozone. According to the proposal, PSPs would only be aware of the amounts that are being funded or defunded from their linked offline accounts and are not even required to report the funding and defunding data to the ECB for monitoring of digital euro in circulation. There is also the issue of real-time monitoring of double spend if users can have both online and offline wallets with no ability for PSPs to track offline transactions. PSPs will also have no visibility of suspected AML if they do not have transaction data and have no network view of multiple offline usage. In order to effectively fight money laundering and terrorism financing, it is undeniable that access to certain data is necessary, in full compliance with the GDPR.

FOR MORE INFORMATION, PLEASE CONTACT:

Vincenzo Renda

Associate Director for Digital Transformation Policy

vincenzo.renda@digitaleurope.org / +32 490 11 42 15

Laura Chaney

Officer for Digital Transformation Policy

laura.chaney@digitaleurope.org / +32 493 09 87 42

About DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory environment that enables European businesses and citizens to prosper from digital technologies. We wish Europe to grow, attract, and sustain the world's best digital talents and technology companies. Together with our members, we shape the industry policy positions on all relevant legislative matters and contribute to the development and implementation of relevant EU policies, as well as international policies that have an impact on Europe's digital economy. Our membership represents over 45,000 businesses who operate and invest in Europe. It includes 105 corporations which are global leaders in their field of activity, as well as 41 national trade associations from across Europe.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Applied Materials, Amazon, AMD, Apple, Arçelik, Arm, Assent, Autodesk, Avery Dennison, Banco Santander, Bayer, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, CaixaBank, Cisco, CyberArk, Danfoss, Dassault Systèmes, DATEV, Dell, Eaton, Epson, Ericsson, ESET, EY, Fujitsu, GlaxoSmithKline, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, Honeywell, HP Inc., Huawei, ING, Intel, Johnson & Johnson, Johnson Controls International, Konica Minolta, Kry, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Meta, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe, NEC, Nemetschek, NetApp, Nintendo, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Pearson, Philips, Pioneer, Qualcomm, Red Hat, RELX, ResMed, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Energy, Siemens Healthineers, Skillsoft, Sky CP, Sony, Sopra Steria, Swatch Group, Technicolor, Tesla, Texas Instruments, TikTok, Toshiba, TP Vision, UnitedHealth Group, Visa, Vivo, VMware, Waymo, Workday, Xerox, Xiaomi, Zoom.

National Trade Associations

Austria: IOÖ
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Czech Republic: AAVIT
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, SECIMAVI, numeum
Germany: bitkom, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: Infobalt
Luxembourg: APSI
Moldova: ATIC
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, Digital Poland Association
Portugal: AGEFE
Romania: ANIS
Slovakia: ITAS
Slovenia: ICT Association of Slovenia at CCIS
Spain: Adigital, AMETIC
Sweden: TechSverige, Teknikföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT Ukraine
United Kingdom: techUK