Council of the European Union
General Secretariat

Interinstitutional files:
2023/0212 (COD)

Brussels, 23 January 2025

WK 914/2025 INIT

LIMITE

EF
ECOFIN
UEM
CONSOM
CODEC

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	Estonian, Finnish, Latvian and Lithuanian delegations
To:	Working Party on Financial Services and the Banking Union (Digital Euro Package) Financial Services Attachés
Subject:	Digital euro package - WP on 31 January 2025 - Non-paper by Estonia, Finland, Latvia and Lithuania: Strengthening resilience and preparedness of European retail payment landscape by digital euro

Non-paper by Estonia, Finland, Latvia, and Lithuania

Strengthening resilience and preparedness of European retail payment landscape by digital euro

I State of play

The European Union's security environment has changed and worsened significantly in recent years. This is acknowledged by the Russian full-scale invasion of Ukraine in 2022 and by the escalated conflicts in the Middle East. Therefore, the entire world is more dangerous now, the continuation of peace cannot be taken for granted anymore and we all must prepare ourselves for extreme crisis scenarios (The report on Strengthening Europe's Civilian and Military Preparedness, 2024, Niinistö's report[1]). Despite the recent measures taken by the EU (including new EU legal frameworks[2]), they are not compliant with and sufficient to deal with threats and prevent negative consequences stemming from worsened security environment or natural disasters. Enhancing Europe's civilian and military preparedness and readiness is a top priority for our region, which is why we welcome the increased attention brought by the European Commission to this issue and joint policy and coordinated actions to eliminate the potential for security crises within the EU.

While in the beginning, the danger seemed immediate, especially for the northern and eastern parts of Europe, this has now become relevant for the rest of Europe as well. **Key threat related to financial services: state actor sponsored cyber-attacks are trying to penetrate and disable critical infrastructure providers´, payment service providers´, payment scheme operators´ and processors´ IT systems[3].** We are witnessing the explosive growth of cyber-attacks against financial institutions, some of those having been successful in destabilising the provision of individual bank's payment services for relatively long time periods. Unfortunately, there have been successful physical attacks and incidents on critical infrastructure, such as undersea cables in the Gulf of Finland and in Baltic Sea (affected critical undersea infrastructure between Finland and Estonia, Sweden and Estonia, Finland and Germany, Lithuania and Sweden, and Finland and Sweden). In the worst-case scenario, the complete destruction of these infrastructures, which seems unlikely, could leave some countries completely isolated from mainland Europe. Furthermore, there are state actor sponsored (dis/mis)information campaigns ongoing aiming at manipulating the security narrative and trust.

The objective of such hybrid attacks is to destabilize Europe´s financial system and spread fear with disinformation. Such a disinformation campaign towards the reliability and security of a certain bank could lead into a bank run. In another scenario, an operational incident with card payments acquiring may escalate into a systemic risk to financial stability if people panic after a social media campaign claiming to bring further successful hybrid attacks on the financial system.

Therefore, the issues on the agenda of Member States are increasingly national security, the functioning of the economy, reliable payment systems etc. Even a short interruption or breach of confidentiality of financial data would have broad societal and economic consequences. Consequently, along with the evolving technologies and digitalization, Europe becomes more exposed to the consequences of the materialisation of those risks.

Many countries are preparing themselves to secure daily payments if serious disruptions in society or exceptional circumstances prevent the use of normal payment systems[4]. The risk scenarios identified, and the arrangements being prepared are different across countries depending on the payment habits (cash intensive countries versus digitalised countries), their threat perception and the available resources to work on alternative arrangements. Some countries have created backup arrangements to secure daily payments in these events starting from the

[1] https://commission.europa.eu/document/download/5bb2881f-9e29-42f2-8b77-8739b19d047c_en?filename=2024_Niinisto-report_Book_VF.pdf
[2] Such as DORA, NIS and DSA.
[3] Pages 43, 44, 50, 105, 142 of the Niinistö's report.
[4] Some examples:
Continuous operation of banking services (Estonia): https://www.eestipank.ee/en/payment-systems/continuous-operation-banking-services
Descriptions and requirements for continuous operation of payment services and cash circulation (Estonia): https://www.riigiteataja.ee/en/eli/ee/524042019001/consolide/current
Securing daily payments (Finland): https://vm.fi/en/securing-daily-payments
'Home emergency kit' for payments (Finland): https://www.suomenpankki.fi/en/money-and-payments/varautuminen/maksamisen-kotivara/?epslanguage=en
Securing daily payments (Finland): https://www.suomenpankki.fi/en/money-and-payments/varautuminen/paivittaismaksamisen-turvaaminen/

introduction of offline card payments to buy essential goods and ending with standalone state-lead solutions that could be used in crises. However, not all EU Member States have such solutions in place so far.

In addition, national arrangements do not address Europe-wide preparedness sufficiently. Member States cannot avoid all the risks but can alleviate the social and regional impact by adopting suitable measures, including ensuring the use of retail payments and cash circulation in case of unexpected circumstances**. However, Europe could benefit from the digital euro and its use in exceptional or crisis scenarios to enhance resilience.** The digital euro could enhance resilience in both a going concern and a crisis. For example, given that the digital euro is (i) built with European infrastructure and (ii) based on European standards. It will also help provide an alternative means of payment in Member States that currently rely on few non-European payment options. Therefore, it will empower Europe to independently develop and manage digital payment solutions while strengthening Europe's financial sovereignty and resilience. **This presupposes the widespread adoption and usage of the digital euro under normal circumstances.** To support it a functioning compensation model, easy use, and clear communication about the benefits of the digital euro are again crucial for its widespread adoption. **Access to digital euro and the reliability of the digital euro services** to satisfy the needs of users at all times, in emergencies, crises or any other exceptional situation, is **expected**.

The "preparedness-by-design" principle, outlined in Niinistö's report, for designing new legislation urges us to reflect further on whether the draft Regulation on the establishment of the digital euro (the Regulation) meets these principles and sufficiently addresses the strategic priorities of the new Commission and other EU institutions in the new legislative cycle. We believe the aims of the Regulation should reflect the crucial priorities, including European strategic autonomy and resilience of payments, more clearly and explicitly. Currently, neither the explanatory memorandum nor the articles of the draft Regulation do sufficiently cover these aspects. However, we believe that **ensuring the broad use of the digital euro as a public good and independent rail/infrastructure will not only enhance European resilience but could significantly improve preparedness at the Member State level to ensure continued use of diversified means of payments, inter alia digital euro payments also in case [of an imminent threat that] intermediating banks would be disabled by cyber-attacks or affected by other sorts of operational disruptions**. Therefore, the work should progress on a digital euro to support a competitive and resilient European retail payment landscape and it must be pursued without delay. **This requires open discussions for finding the "boldest common denominator" (as put in Niinistö's report) of Member States' expectations of the digital euro to become the solution for preparedness to continue digital payments, instead of switching necessarily to cash or providing a viable and scalable complementarity to cash payments.**

To sum up, security concerns, natural disasters, and other critical factors serve as catalysts for rethinking the fundamentals of how people pay for goods and services in exceptional circumstances. We believe that the digital euro could serve as a resilient payment instrument. Its offline version could also be used in exceptional circumstances, when online payments are not functioning. Therefore, we see the opportunity to take full advantage of the digital euro to strengthen the resilience and preparedness of the European retail payment landscape since the legal framework of the digital euro and technical features are not set in stone yet. **The main objective of our initiative is to avoid principles and provisions of the legal framework that could prevent or restrict the online or offline use of the digital euro in case of exceptional circumstances.** On the contrary, **it is essential to ensure that the legal framework of the digital euro is contributing to the use of the digital euro as a means of payment in exceptional circumstances.** Based on the legal framework the European Central Bank and the Eurosystem should focus on the technical features and functionalities of the digital euro that are important to ensure resilience in different exceptional and crisis situations.

II Shortcomings in the draft Regulation on the establishment of the digital euro in the current environment

Even though the draft Regulation addresses partly crucial priorities and described aspects (please see Background in the box below), there are a couple of shortcomings and uncertainties. Therefore, **the Regulation should be strengthened** to promote the preparedness-by-design principle and to facilitate the broad use of digital euro and sufficient (by default) offline limit for purchases of necessities during exceptional circumstances. So that the digital euro could be used as an alternative digital means of payment in case private sector payment rails and solutions fail. This may require the use of the digital euro independent from intermediating banks' digital

channels to facilitate better emergency switching (e.g. sovereign payment instruments developed by the market as WERO, Bizum, MB Way, Bancomat Pay or in the future, the European Digital Identity Wallets[5]).

For not restricting use in exceptional circumstances and crises the Regulation would need to better acknowledge that circumstances for activating emergency switching may be different in Member States. Furthermore, the Regulation could foresee the possibility for exemptions in case of extreme scenarios while not compromising on privacy. Where continued use of digital euro would be necessary for essential State functions concerning public security, defence and the safeguarding of national security the Regulation could facilitate the Member States to temporarily allow inter alia (i) online and offline digital euro circulation for all payment service users (up to the predefined limit also for legal entities); (ii) distribute pre-paid digital euro cards/wallets, incl. enable top-up offline digital euro; and if needed (iii) stand in for the systemically important intermediary bank until its recovery or emergency switching without compromising customer privacy; and iv) enable emergency switching of PSPs with the possibility to deviate from the standard KYC and AML/CTF procedures and apply appropriate safeguards to contain ML/TF risks.

Such extreme scenarios would entail hybrid attacks (i) resulting in operational or financial failure of multiple intermediary banks, or (ii) cut-off of the Member State from the Single Euro Payments Area or the International Card Schemes Infrastructure, where currently the only option would be to revert to cash, which may be very complex and costly for the State to arrange without the support of the banks' infrastructure.

We acknowledge that the Eurosystem will develop the digital euro settlement infrastructure following the highest security and resilience standards in accordance with the European System of Central Banks statutory task of oversight of financial market infrastructures.

Background: As stressed in the explanatory memorandum of the proposal for the Regulation, the digital euro will be offered as a public digital means of payment, alongside the existing private digital means of payment, supporting a stronger and more competitive, efficient, and innovative European retail payments market and digital finance sector, and contributing to further enhance the resilience of the European retail payments market. As such, it should facilitate the development of pan-European and interoperable retail payment solutions, incl. the full roll-out of instant payments.

Furthermore, for this purpose the proposal for the Regulation provides the necessary regulatory framework that should ensure the effective use of the digital euro as a single currency in the euro area, meeting not only the users´ needs and fostering competition and innovation but also improving resilience in the EU´s digitalizing economy.

The digital euro plays an important role in the European Commission's strategy for EU´s strategic autonomy and in its communication on fostering an open, strong and resilient economic and financial system in Europe. Building on the Strategic Agenda 2024-2029 and the European Council conclusions of December 2024, the European Council encourages further work to enhance the EU's and its Member States' resilience, preparedness, crisis-prevention and response capacity in a coherent manner, including with a view to the future preparedness strategy. The digital euro may therefore be one of the actions pursued at EU level to support Member States, taking into account the specificities of different types of crises and respecting Member States' responsibilities and competences.

As underlined in the explanatory memorandum of the proposal, the Regulation needs to make sure that the digital euro can be used in the same way, in accordance with the same rules and conditions without fragmentation, throughout the euro area.

III List of proposals for strengthening the draft Regulation on the establishment of the digital euro (to solve the discrepancies and promote preparedness)

[5] „Ideally, pan-European retail payment solutions for the point of interaction (POI) should be based on a different processing infrastructure from card payments (for example, instant payments), as this would increase the resilience of retail payments. Moreover, the Eurosystem considers that it would be beneficial if solutions were also able to handle the digital euro scheme." (See The Eurosystem's retail payments strategy – priorities for 2024 and beyond, p. 3: https://www.ecb.europa.eu/pub/pdf/other/ecb.eurosystemretailpaymentsstrategy~5a74eb9ac1.en.pdf)

As a starting point, the uniform implementation across the EU should also make sure that the digital euro would provide the same level of resilience, and the digital euro can continue to be used in case of emergency or similar exceptional scenarios[6]. The functioning and design of the digital euro should fully embrace the objectives of improving the strategic autonomy and resilience in payments along with innovation and security. Therefore, we should better exploit the full potential of the digital euro and strengthen its position as a guarantor in accordance with the objectives of fostering resilience and strategic autonomy in Europe. In that respect, we propose several improvements to the proposal of the Regulation to respond to the need to be prepared for potential security threats to infrastructures at the European level by reinforcing the retail payments resilience in Europe and ensuring citizens and businesses safer and secure payments in all circumstances.

Only Recital 76 mentions operational resilience in the context of activities related to ensuring the stability and integrity of the digital euro infrastructure and in the context of processing personal data. Therefore, it is appropriate to draw attention to and stress the importance of the role of the digital euro in achieving greater resilience and autonomy for retail payments also in the recitals of the Regulation. We therefore suggest adding the word "resilient" to the recitals 3, 5 and 16.

Widespread adoption and usage of the digital euro under normal circumstances is a prerequisite for the prompt usage of digital euro in exceptional circumstances. Therefore, we suggest that the recitals 13 and 36 are amended to include the promotion of onboarding of private individuals. Member States could promote the onboarding level through the crisis preparedness narratives, e.g. "keep offline digital euro as well as cash for crisis preparedness"; call for a sufficient (by default) offline limit to cover necessities during exceptional circumstances for assuring that digital euro could be used as alternative digital means of payment in case private sector payment rails and solutions fail.

We also suggest complementing the recital 36 in order to allow the possibility for incoming payments to pile up if the digital euro limit is exceeded and the waterfall account is not reachable in a crisis. The funds beyond the limit shall become available in commercial bank money after the waterfall account has been recovered or after emergency switching.

New Recital (76b) to take a comprehensive approach to features of the digital euro: The design features of the digital euro and limits of its´ store of value should be examined comprehensively in all respects, notably including operational security and cybersecurity risks as well as public security, defence, and national security considerations. This Regulation should be without prejudice to any actions to safeguard essential Member State functions or the possibility to take necessary measures to ensure the protection of essential interests of national security and defence, public policy, and security or to safeguard the interests of users by ensuring the reliability and continuity of retail payments[7].

The digital euro legal framework and technical implementation would support national frameworks and measures introduced for improving the operational resilience of essential services and the continuity of payment services in case of crisis or emergencies. In conformity with the Regulation there should not be any position to oppose the use of digital euro under exceptional circumstances should the need arise, nor to the conditions thereof.

Therefore, we suggest that to reflect the efficient functioning of the digital euro in emergencies of Member States the Regulation should provide a sufficient level of flexibility for Member States to determine the exceptional circumstances as a trigger for emergency switching. Therefore, we suggest **reconsidering the proposal of the Belgian Presidency (Art 31 (4)) for adopting a Commission delegated act** to supplement the Regulation by identifying the circumstances under which the authorisation of switching digital euro payment accounts as a minimum be observed, would not be appropriate to address the concern as it would not provide the level of scrutiny for Member States.

We need to acknowledge that circumstances and preconditions for activating emergency switching may be different in Member States stemming from regulation regarding essential State functions. Therefore, the identified circumstances under which the Eurosystem may authorise switching of digital euro payment accounts, as well as the procedural requirements that should as a minimum be observed emergency switching should ensure application of national regulation regarding essential State functions concerning public security, defence and national security. Emergency switching should apply equally to private individuals and to legal entities, to

[6] As run on an independent infrastructure, contributing to the level of assurance, incl. in case other (private) payment methods become unavailable to citizens.

[7] In accordance with Article 4(2) of the Treaty on European Union and without prejudice to the judicial review by the Court of Justice.

ensure smooth business activity in exceptional circumstances. For example, in case of merchants, the rules for emergency switching would need to ensure timely access to offline digital euro stored on POS terminals. Consequently, **we suggest adjusting the recital 67a.**

New Recital (76c) to outline preparedness by design and the boldest common denominator: while acknowledging the initial scope of the digital euro the Member States shall have the possibility of exemptions in case of extreme scenarios while not compromising the privacy; this shall apply where continued use of digital euro would be necessary for essential State functions concerning public security, defence and the safeguarding of national security enabling the Member States temporarily to (i) allow online and offline digital euro circulation for all payment service users (up to the predefined limit also for legal entities); (ii) distribute pre-paid digital euro cards/wallets, incl. enable top-up offline digital euro; and if needed (iii) stand in for the systemically important intermediary bank until its recovery or emergency switching without compromising customer privacy, which may require applying transaction limits to apply ad-hoc rules on KYC, AML, CTF, and sanctions screening[8]. Switching PSPs would entail KYC procedures under applicable law, which sets the requirements PSPs must comply with. In case of emergency switching, numerous consumers and businesses would need to become clients of other PSP(s) during a short period. To ensure a smooth change, PSPs may need the possibility to deviate from the standard KYC procedures (e.g. ex-post due diligence, risk assessment, profiling). At the same time, the proper safeguards should be applied to minimize the ML/TF risk, acknowledging the need to ensure payments for essential goods - food, medicine, and fuel. The measures for risk management could include the restriction to transfer to and from offline holdings for individuals until the full KYC is performed and, the limitation to transfer digital euro holdings for businesses.

IV Identified list of Articles of the draft Regulation on the establishment of the digital euro to be reassessed and streamlined to ensure comprehensive approach to features of the digital euro, and preparedness

In addition to the further work on the recitals, we have identified the following Articles that have required a fresh look and adjustment:

Article 2: Definitions

Article 9: Exceptions to the obligation to accept the digital euro

Article 14: Access to the digital euro in Member States whose currency is the euro

Article 16: Limits to the use of the digital euro as a store of value

Article 25: European Digital Identity Wallets

Article 28: Front-end services to access and use the digital euro

Article 31: Switching of digital euro payment accounts

Article 37: Anti-money laundering rules applying to offline digital euro payment transactions

The following drafting suggestions (in Annex) are based on the Belgian Presidency drafting suggestions circulated on the 27th of June 2024.

[8] Still under scrutiny and to be discussed further in the negotiations. The exemption for the use of digital euro in exceptional circumstances could be written in a similar way as art 19 (7) of AMLR.

Annex

Proposal for a
REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
on the establishment of the digital euro

(3) Central bank money in the form of banknotes and coins cannot be used for online payments. Today, online payments rely entirely on commercial bank money. The acceptability and fungibility of commercial bank money rely on its convertibility on a one-to-one basis to central bank money with legal tender, which serves as a monetary anchor. That monetary anchor is at the core of the functioning of monetary and financial systems. It underpins users' confidence in commercial bank money and in the euro as a currency and is therefore essential to safeguard the stability of the monetary system in a digitalised economy and society. As central bank money in physical form alone cannot address the needs of a rapidly digitalising economy, this could gradually remove the monetary anchor for commercial bank money. It is therefore necessary to introduce a new form of official currency with legal tender which is risk free**, resilient,** and helps visualise the convertibility at par of the money issued by various commercial banks.

(5) In a context where cash alone cannot answer the needs of a digitalised economy, it is essential to support financial inclusion by ensuring universal, affordable**, resilient,** and easy access to the digital euro to individuals in the euro area, as well as its wide acceptance in payments. Financial exclusion in the digitalised economy may increase as private digital means of payments may not specifically cater for vulnerable groups of the society or may not be suitable in some rural or remote areas without a (stable) communication network. According to the World Bank and the Bank for International Settlements, "efficient, accessible and safe retail payment systems and services are critical for greater financial inclusion". That finding was further substantiated by the study on new Digital Payment Methods commissioned by the European Central Bank, which concluded that for the unbanked/underbanked/offline population, the most important features of a new payment method are easiness of use, not requiring technological skills, and to be secure and free of charge. A digital euro would offer a public alternative to private digital means of payments and support financial inclusion as it would be designed along these objectives, thus catering for free access, easiness of use and wide accessibility and acceptance.

(13) Member States, their relevant authorities and payment service providers should deploy information and educational measures to ensure the necessary level of awareness and knowledge of the different aspects of the digital euro **to promote broad adoption and wide use by onboarding of private individuals**.

(16) The digital euro, as a digital currency with the status of legal tender denominated in euro issued by the European Central Bank and national central banks of the Member States whose currency is the euro, as part of the Eurosystem, should be widely accessible, usable**, resilient,** and accepted as a means of payment. Granting legal tender status to the digital euro should support its usability in payments across the euro area and thus also support the efforts to ensure the continued availability and accessibility of central bank money in its role of monetary anchor, as cash alone cannot address the needs of a rapidly digitalising economy. In addition, the mandatory acceptance of payments in digital euro as one of the main conditions of the legal tender status ensures that people and businesses benefit from a wide acceptance and have a real choice to pay with central bank money in a digital way and in a uniform manner throughout the euro area.

(36) The digital euro should allow for a smooth payment experience **also in circumstances where the online digital euro system is unavailable, whether in normal times or under exceptional circumstances, by enabling by default offline payments to cater for critical day-to-day payments**. Any instruments that the European Central Bank might employ to limit the digital euro's store of value function should take this objective into account. Automated mechanisms that link a digital euro payment

account with a non-digital euro payment account should allow for an uninhibited payment functionality of the digital euro, by ensuring that transactions are successfully executed in the presence of individual digital euro holding limits that may become binding on the payer's or payee's side. In particular, digital euro users should be able to initiate a digital euro payment transaction even though the amount of their digital euro holdings is inferior to the amount of the transaction, by automatically mobilising funds from a non-digital euro payment account to complement the transaction amount ('reverse waterfall functionality'). Conversely, digital euro users should be able to receive digital euro payment transactions even though the amount of the transaction exceeds the limit set on their digital euro holdings, by automatically transferring funds in excess of the limit to a non-digital euro payment account ('waterfall functionality') **or in exceptional circumstances in case waterfall functionality is unavailable by queuing incoming payments until functionality becomes available or in case the emergency switching is performed**. Such payment functionalities should be expressly authorized by digital euro users. Where digital euro payment account held by one payment service provider is linked with non-digital euro payment account held by another payment service provider, they should enter into an arrangement specifying their respective roles and responsibilities under data protection rules, as well as agree on the security measures necessary to ensure secure transmission of personal data between the two payment service providers.

(67a) Where a payment service provider is operationally unable to perform switching for a prolonged period of time, or where it is likely that it will operationally be unable to perform switching for a prolonged period of time, including due to having lost the relevant data related to the digital euro payment account, the European Central Bank should be able to authorise the switching of the digital euro payment accounts concerned so that the receiving payment service provider is able to retrieve the information about the digital euro holdings of the digital euro user and perform the switching without the need to exchange information with the unavailable payment service provider. This process should allow a digital euro user to continue accessing its digital euro holdings via the receiving payment service provider. In this case, the switching does not extend to other digital euro payment services that were offered by the unavailable payment service provider, including conditional payments. The provision of those digital euro payment services will therefore have to be re-established, if appropriate, with the receiving payment service provider. The European Central Bank and the national central banks should not be operationally involved in the switching of digital euro payment accounts between unavailable and receiving payment service providers. To support receiving payment service providers in the process of switching digital euro payment accounts from unavailable payment service providers, the Eurosystem may establish a single access point. ~~The Commission should be empowered to adopt delegated acts to supplement this Regulation by specifying what is understood under a prolonged period of time and by identifying the circumstances under which the Eurosystem may authorise switching of digital euro payment accounts, as well as the procedural requirements that should as a minimum be observed.~~ Given, on the one hand, their importance for safeguarding essential State functions, the circumstances for activating emergency switching stemming from national law are at the same time different in the Member States, therefore, the Eurosystem should support switching of digital euro payment accounts in accordance with national regulation regarding essential State functions concerning public security, defence and national security.

(76b) The digital euro should be designed to ensure the stability and integrity of the digital euro infrastructure to ensure the role of the digital euro in achieving the best possible resilience in retail payments. To ensure the preparedness by design of the digital euro, the design features of the digital euro shall include operational security and cybersecurity as well as public security, defence, and national security considerations. This Regulation should be without prejudice to any actions to safeguard essential Member State functions or the possibility to take necessary measures to ensure the protection of essential interests of national security and defence, public policy, and

security or to safeguard the interests of users by ensuring the reliability and continuity of retail payments[9].

(76c) Member States shall have the possibility in case of exceptional circumstances while not compromising the privacy by design principle to temporarily (i) allow online and offline digital euro circulation for all payment service users (up to the predefined limit also for legal entities); (ii) distribute pre-paid digital euro cards/wallets, including enable top-up offline digital euro; and if needed (iii) stand in for the systemically important intermediary bank until its recovery or emergency switching without compromising customer privacy, which may require applying transaction limits to apply ad-hoc rules on KYC, AML, CTF, and sanctions screening. Switching PSPs would entail KYC procedures under applicable law, which sets the requirements PSPs must comply with. In case of emergency switching, numerous consumers and businesses would need to become clients of other PSP(s) during a short period. To ensure a smooth change, PSPs may need the possibility to deviate from the standard KYC procedures (e.g. ex-post due diligence, risk assessment, profiling). At the same time, the proper safeguards should be applied to minimize the ML/TF risk, acknowledging the need to ensure payments for essential goods - food, medicine, and fuel. The Member States should have the possibility for continued use of digital euro for essential State functions concerning public security, defence and the safeguarding the national security of the Member States.

Article 2

Definitions

For the purpose of this Regulation, the following definitions shall apply:

37. (new) 'exceptional circumstances' means situations, limited in time, that can cause serious and extensive disruptions in the essential state functions and functioning of society, in particular disruption of payment services, or cause great property, economic or environmental damage, including a natural disaster, a major cybersecurity incident or other attack, negatively affecting the population of the Union or the whole or part of a Member State, and which is determined or officially declared in accordance with the relevant procedures under Union or national law;

Article 9

Exceptions to the obligation to accept the digital euro

By way of derogation from Article 7(3) and Article 8, a payee shall be entitled to refuse digital euro in any of the following cases:

(a) where the payee is an enterprise **or a self-employed person** which employs fewer than 10 persons or whose annual turnover or annual balance sheet total does not exceed EUR 2 million, or a non-profit legal entity as defined in in Article 2, point (18), of Regulation (EU) 2021/695, unless it accepts comparable digital means of payment **initiated at the point of interaction**;

[9] In accordance with Article 4(2) of the Treaty on European Union and without prejudice to the judicial review by the Court of Justice.

(b) where a refusal is made in good faith and where such refusal is based on legitimate and temporary grounds in line with the principle of proportionality in view of concrete circumstances beyond the control of the payee;

(c) where the payee is a natural person acting in the course of a purely personal or household activity;

(d) where, prior to the payment, the payee has agreed with the payer on a different means of payment, subject to Article 10.

For the purposes of point (b), the burden of proof to establish that legitimate and temporary grounds existed in a particular case and that the refusal was proportionate shall be on the payee.

This Article is without prejudice to the responsibility of Member States' regarding essential State functions concerning public security, defence and national security in accordance with Union law. Exceptions to the obligation to accept the digital euro could be limited by Member States, for duly justified reasons, especially for the purpose of continuous operation of payment services in exceptional circumstances.

Article 14

Access to the digital euro in Member States whose currency is the euro

1. For the purpose of distributing the digital euro to natural persons referred to in Article **12a** (a) **where these persons are acting as consumers**, credit institutions that provide payment services as referred to in points (1), (2) or (3) of Annex I to Directive (EU) 2015/2366 shall, upon request of their clients, **for whom they already provide payment services on a contractual basis**, provide those persons with all basic digital euro payment services as referred to in Annex II.

2. For natural persons referred to in Article **12a** (a), **who are acting as consumers, and who** do not hold a non-digital euro **payment** account, Chapter IV of Directive (EU) 2014/92 shall apply, **as transposed into national law by the respective Member State**, with the exception of Articles 17 and 18, to the **provision of basic digital euro payment services as referred to in Annex II**.

3. Member States **may** designate the authorities referred to in Article 1, point**s (e) and** (f), of the Directive (EU) 2015/2366, or post office giro institutions referred to in Article 1, point (c), of the Directive (EU) 2015/2366 to:

(a) provide basic digital euro payment services to natural persons referred to in Article **12a** (a), that do not hold a non-digital euro payment account;

(b) provide digital inclusion support provided face-to-face in physical proximity to persons with disabilities, functional limitations or limited digital skills, and elderly people**;**

(c) provide temporarily digital euro payment services and payment instruments to persons referred to in Article 12a (a) in their territory for duly justified reasons in order to ensure essential State functions concerning public security, defence and national security in accordance with Union

law, especially for the purpose of continuous operation of payment services in exceptional circumstances.

4. Payment service providers referred to in paragraphs 1 to 3 shall provide digital inclusion support to persons with disabilities, functional limitations or limited digital skills, and elderly persons. Digital inclusion support shall comprise, **but not be restricted to**, a dedicated assistance for onboarding to a digital euro **payment** account and using all basic digital euro **payment** services.

5. The Authority for Anti-Money Laundering and Countering the Financing of Terrorism and the European Banking Authority shall jointly issue guidelines specifying the interaction between AML/CFT requirements and the provision of basic digital euro payment services:

(a) with a particular focus on financial inclusion of vulnerable groups including asylum seekers or beneficiaries of international protection, individuals with no fixed address or third country nationals who are not granted a residence permit but whose expulsion is impossible for legal or factual reasons;

(b) in exceptional circumstances and in the event of emergency switching in order to ensure essential State functions relating to public security, defence and national security in accordance with Union law, especially for the purpose of continuous operation of payment services in exceptional circumstances.

Article 15

Principles

1. With a view to enabling natural and legal persons to access and use digital euro, to defining and implementing monetary policy and to contributing to the stability of the financial system, the use of the digital euro as a store of value **shall** be subject to limits.

(1a) With a view to improving the operational resilience of essential services and the continuity of payment services in exceptional circumstances, the limits to the use of the digital euro as a store of value shall not restrict the online and offline use of the digital euro in exceptional circumstances in the Member States whose currency is the euro.

(1b) The limits as referred to in paragraphs 1 and 1a are without prejudice to the responsibility of Member States' regarding essential State functions concerning public security, defence and national security in accordance with Union law.

2. With a view to ensuring an effective use of the digital euro as a legal tender means of payment, and to avoiding excessive charges for **payees** subject to the obligation to accept the digital euro under Chapter III while providing compensation for the relevant costs incurred by payment services providers for the provision of digital euro payment **services**, the level of charges or fees to be paid by **digital euro users** to payment service providers, or between payment service providers, shall be subject to limits.

Article 16

Limits to the use of the digital euro as a store of value

1. For the purpose of **paragraphs (1), (1a) and (1b) in** Article 15~~(1)~~, the European Central Bank shall develop instruments to limit the use of the digital euro as a store of value and shall decide on their parameters and use, in accordance with the framework set out in this Article. PSPs providing account servicing payment services within the meaning of Directive 2015/2366 to natural and legal persons referred to in Article 12(1) shall apply these limits to digital euro payment accounts.

2. The parameters and use of the instruments referred to in paragraph 1 shall:

(a) safeguard the objectives set out in Article 15(1), in particular financial stability;

(b) ensure the usability and acceptance of the digital euro as a legal tender instrument;

(c) **ensure the flexibility to temporarily increase the limits and online use of the digital euro services by persons referred to in Article 12a (a) and in accordance with Article 14 in exceptional circumstances;**

(d) respect the principle of proportionality.

3. The parameters and use of the instruments referred to in paragraph 1 shall be applied in a non-discriminatory manner and uniformly across the euro area.

4. Any holding limits on digital euro payment accounts adopted pursuant to paragraph 1 shall apply to both offline and online holdings. Where a digital euro user uses both an offline and online digital euro, the limit that applies to online digital euro shall equal the overall limit determined by the European Central Bank minus the holding limit for offline digital euro set by digital euro users. A digital euro user may set its offline holding limit at any amount between zero and the holding limit set in accordance with Article 37.

5. Visitors to the euro area as referred to in Article **12a**(1), point (c), and natural and legal persons as referred to in Article **12a**(1), points (b), (d), (e) **and (f)**, shall be subject to limits as regards the use of the euro as a store of value that are not higher than the ones effectively implemented in the euro area for natural and legal persons residing or established in Member States whose currency is the euro. The parameters and use of the instruments shall be applied in a non-discriminatory manner and uniformly across Member States whose currency is not the euro. When deciding on the use of the instruments in those Member States and setting the parameters, the European Central Bank shall consult national central banks of Member States whose currency is not the euro.

6. In case a digital euro user has multiple digital euro payment accounts, the digital euro user shall specify to the payment service providers with which the digital euro payment accounts are held how the individual holding limit is to be allocated between the different digital euro payment accounts **and local storage devices**.

7. Where a digital euro payment account is **jointly** held by more than one digital euro user, any holding limit on **this** digital euro payment account shall **be equal** to the sum of the individual holding limits allocated to **it by each** of its users.

(7a) For the purpose of supporting the task of payment service providers to implement and enforce the instruments referred to in paragraph 1, the ECB may alone or jointly with national central banks establish a single access point.

8. The digital euro shall not bear interest.

Article 25

European Digital Identity Wallets

1. Front-end **solutions** shall be interoperable with or integrated in the European Digital Identity Wallets**, in particular, in order to onboard digital euro users, store digital euros in the payment instrument and facilitate offline proximity payments in digital euro.**

2. On request by digital euro users, payment service providers distributing the digital euro shall ensure that those users can rely on the functionalities of their European Digital Identity Wallets in accordance with Article **5a** of **Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework**;

Article 28

Front-end **solutions** to access and use the digital euro

1. Payment service providers distributing the digital euro shall provide digital euro users with the choice of using the following digital front-end **solutions** to allow digital euro users to access and use digital euro payment services:

(a) front-end **solutions** developed by payment service providers; ~~**and**~~

(b) **sovereign payment instruments developed by market;**

(c) in the medium-term the European Digital Identity Wallets; and

(d) a front-end **solution** developed by the European Central Bank **and the national central banks**.

Where a payment service provider does not offer a digital euro front-end **solution, it shall use the front-end solution developed by the** European Central Bank **and the national central banks**.

2. **The European central bank and the national central banks shall ensure that the** front-end **solution** referred to in paragraph 1, point (~~b~~d):

(a) supports the provision of all the basic digital euro payment services as referred to in Annex II;

(b) uses the logo of the payment service provider **who offers** digital euro payment **services through the front-end solution**.

The European Central Bank shall not have access to any personal data in relation to the front-end solution developed by the European Central Bank and used by the payment services providers. The front-end solution referred to in the first subparagraph shall not entail the establishment of any customer relationship between the European Central Bank and the national central banks on the one hand and digital euro users on the other hand.

3. Payment service providers distributing the digital euro shall ensure that:

(a) digital euro payment services use the official digital euro logo;

(b) digital euro payment accounts can be quickly and easily accessed and used by digital euro users;

(c) digital euro users can easily distinguish online and offline digital euro holdings.

Article 31

Switching of digital euro payment accounts

1. **At the request of digital euro users,** payment service providers shall **without undue delay** switch **these users'** digital euro payment accounts to other payment service providers.

(1a) When switching digital euro payment accounts in accordance with this Article, it shall be ensured that:

(a) the digital euro payment account number is maintained;

(b) all the relevant information for providing access to the switched digital euro payment account is transferred to the receiving payment service provider.

2. In exceptional circumstances where a payment service provider is operationally not in a position to **switch** digital euro payment **accounts** for a prolonged period of time, **or where it is likely that a payment service provider will not be in a position to offer this service for a prolonged period of time**, the European Central Bank or national central banks may authorise the switching of digital euro payment accounts held with that payment service provider to another payment service provider designated by the digital euro user. **Based on this authorisation**, the **receiving** payment service provider **shall perform** the switching **upon the digital euro user's request**, without **the need to exchange information with** the unavailable payment service provider.

(3) For the purpose of ensuring switching in accordance with paragraph 2, the ECB may alone or jointly with national central banks establish a single access point.

~~**(4) The Commission is empowered to adopt delegated acts in accordance with Article 38 in order to supplement this Regulation by specifying the prolonged period of time and identifying the**~~

(4) The circumstances under which the European Central Bank and national central banks may authorise the switching of digital euro payment accounts in accordance with paragraph 2, as well as the procedural requirements ~~**that must as a minimum be observed. When preparing those delegated acts, the Commission shall consult the European Central Bank.**~~ **shall in exceptional**

circumstances respect the responsibility of Member States' regarding essential State functions concerning public security, defence and national security in accordance with Union law. In exceptional circumstances, Member State may request the European Central Bank or national central bank to activate emergency switching in case this is warranted for public security, defence and national security.

Article 37

Anti-money laundering rules applying to offline digital euro payment transactions

1. Payment services providers shall apply paragraphs 2 to 6 to offline digital euro payment transactions.

2. Transaction data shall not be retained by payment service providers or by the European central banks and the national central banks.

3. Payment service providers shall retain data of funding and defunding for storing digital euros on payment instruments in accordance with Article 40 of Directive (EU) 2015/849 and national provisions transposing that Article. Payment service providers shall, upon request, make those data available to the Financial Intelligence Unit and other competent authorities as referred in Article 2(**4**) of Regulation **(EU) 2024/1624**.

4. For the purposes of paragraph 3, the funding and defunding data means the following:

(a) the amount funded or defunded;

(b) the identifier of the local storage device for offline digital euro payment;

(c) the date and hour of the funding and defunding transaction;

(d) the accounts numbers used for funding and defunding.

5. The Commission **shall** adopt implementing acts setting offline digital euro payment transaction limits**, offline digital euro** holding limits **or both**. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39. **Offline digital euro holding limits shall respect the limits established in accordance with Article 16.**

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**;**

(d) the limits are sufficiently high for purchases of necessities during exceptional circumstances.

For the purposes of point (a) **and (b)**, the Commission **shall** request **the Authority for Anti-Money Laundering and Countering the Financing of Terrorism** 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 **shall** consult the European Data Protection Board.