
# EDPB letter to the European institutions on the privacy and data protection aspects of a possible digital euro

Slovenian Presidency of the Council
***Sent by e-mail only***

Brussels, the 18 June 2021
REF: OUT2021-0113

Dear Sir/Madam,

In October 2020, the European Central Bank (ECB) issued the **Report on a digital euro**[1] aiming at consulting stakeholders, including the general public, on its project of a central bank digital currency (CBDC) in the Euro zone, which is expected to be available for retail payments ('digital euro'). In response to a significant decline in the role of cash as a means of payment, the digital euro would be an alternative to physical cash, not a substitute. As a digital form of the euro currency, the ECB want to "ensure that it was trusted from its inception and that this trust was maintained over time"[1].

In April 2021, the ECB published a **feedback of the public consultation**[2]. The main finding was the very predominantly expressed preference by the stakeholders and the public for privacy[3] (43% as the most important feature)[4]. This result can be observed throughout the EU, population characteristics and in all categories of respondents (citizens, payment industry, merchants, NGOs, academics…). The majority of citizens declared they wanted "a digital euro focused on privacy and the protection of personal data, which can be used offline" (53%).

In this context, the European Data Protection Board acknowledges that decisions regarding the launch of the project starting with a two-year exploratory phase will be held by mid-2021. The EDPB takes this opportunity to proactively advise the competent EU institutions on the privacy and personal data

[1] https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf.
[2] https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210414~ca3013c852.en.html.
[3] "the privacy of payment data is considered the most important feature, ranging from full privacy of transactions to the possibility that only low-risk small transactions are private", feedback document, page 3.
[4] Although not representative of the EU population from a statistical point of view, the views collected nevertheless indicate issues that are important to the public.

protection aspects of a digital euro, and inform the public debate in that regard, from the very early stage of decision making.

## 1. Background of the digital euro project and key data protection principles

In the light of the views expressed by the citizens during the public consultation, the EDPB stresses that a very high standard of privacy and data protection is **crucial to reinforce the trust** of end users and shall be considered as a distinctive element in the offering of digital euro, representing a key factor of success of the project.

The EDPB acknowledges that the main architectural and design choices of a digital euro are not yet defined, while the ECB documents offer options between different features and modalities. In any chosen circumstance, the EDPB recalls the importance of taking in due account the compliance with the European data protection applicable framework[5] at an early stage of the project, pursuant to the key principle of data protection "**by design and by default**", privacy and data protection principles should not be considered *a posteriori*, as a pure compliance exercise[6]. It shall be wired within core decisions on the outcome of the project, constituting a cornerstone of the final goal that the Eurosystem wants to achieve with respect to fundamental values of the European Union.

The EDPB recalls that the rights to privacy and to the protection of personal data are **fundamental rights** enshrined in the articles 7 and 8 of the Charter of Fundamental Rights of the European Union. They shall not be considered as absolute values, but carefully balanced with other rights at stake. The Court of Justice of the European Union has developed case law on the principles of necessity in a democratic society and proportionality of limitations to fundamental rights and principles, ensuring their appropriate protection[7] .

Under this light, the Report published by the European Central Bank offered a comprehensive overview of different interests at stake in relation to different design choices (innovation, privacy, financial stability, monetary policy, financial inclusion, etc.). However, new risks for rights and freedoms of individuals might arise from this project, while others already identified risks might be amplified (see part 2 below). Balance among these interests on one hand, and between them and privacy and personal data protection on the other hand, should be cautiously assessed in order to validate or adapt existing approaches in an innovative manner, with the final aim of minimising these risks.

---

[5] According to decision taken on personal data controllership, different legal instruments might come into play, mainly the Regulation (EU) no. 2016/679, General Data Protection Regulation, and/or the Regulation (EU) no. 2018/1725, on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data.

[6] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en and https://edps.europa.eu/data-protection/our-work/publications/opinions/privacy-design_en.

[7] See for example: C-511/18 - La Quadrature du Net and Others, 6 Oct 2020; Tele2 Sverige AB (CJEU, C-203/15, ECLI:EU:C:2016:970); Ministerio Fiscal (CJEU, C-207/16, ECLI:EU:C:2018:788).
See also: EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, at: 19-12-19_edps_proportionality_guidelines2_en.pdf (europa.eu).

Moreover, in the context of the digital euro initiative, the EDPB points out in particular to the **principle of data minimization**, according to which personal data shall be limited to what is necessary in relation to the purposes for which they are processed. **Purpose limitation,** according to which personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes, shall also be complied with in the context of a digital euro.

The EDPB wants to underline the **clear distinction** between an anonymous use of the digital euro[8] and the case where a natural person is identified or identifiable during its use, including if the data are pseudonymised, which requires the full compliance with GDPR. The choices made in that regard will of course also depend on the policy objectives pursued and on a number of public interests to be balanced. In any case, the architecture of the digital euro shall be designed to allow a privacy feature ranging from anonymisation, at least on part of the transactions, to a high level of pseudonymisation of the data[9]. The WP29 guidelines on anonymisation[10] are currently reviewed and the EDPB will be in a position to give more detailed advice on the subject matter from a technical point of view in the future[11].

The EDPB considers that **a holistic assessment** of different aspects and fundamental rights at stake (financial and digital inclusion, privacy and data protection, freedom of movement, security) should be made to ensure that the digital euro project is in line with the values of the European Union and, in particular, with the protection of privacy and personal data.

## 2. Relevant privacy and data protection issues regarding the 'architecture' of the project

The EDPB welcomes the overall objective of the project, namely increasing access to central bank currency in digital transactions enhancing innovation and pursing public interest in a well-functioning economy.

However, an inappropriate design of the forthcoming digital euro would bring **significant risks** under the data protection perspective. Relevant safeguards shall be put in place in order to avoid, for example, generalised tracking of user transactions throughout the payment system and to address and mitigate the risk of excessive interference in privacy of the persons concerned by both centralized entities and market operators.

In order to reach this objective, the identification of the end users should remain limited to what is necessary to the performance of regulatory obligations by obliged entities. Collection and access to personal data should be minimized to what is necessary to transfer the funds[12], and security risks should be identified and mitigated.

[8] As it is the case for physical cash.
[9] A thresholded approach could be based on the monetary value of the transaction. For example, low value transaction of less than €1000 could enjoy full privacy as they are unlikely to entail AML high risks. Another possible limitation could cover use outside the Euro area.
[10] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf
[11] See EDPB Work Program: https://edpb.europa.eu/system/files/2021-03/edpb_workprogramme_2021-2022_en.pdf
[12] According to article 4 of the PSD2 directive, 'payment transaction' means an act, initiated by the payer or on his behalf or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee.

Moreover, the EDPB understands that the digital euro **will have legal tender status** in the EU at the time of its issuance, which means, in regulatory terms, that it will be assimilated to euro banknotes within the meaning of Article 128 TFEU. Those are the only ones "to have the status of legal tender within the Union". This means that a digital euro would be, in legal terms, an equivalent to cash. In this context, the EDPB considers that a digital euro shall have as far as possible 'cash-like features', in particular regarding the data protection aspects.

Concerning the 'AML/CFT status' of the new currency, the EDPB notes that regulators in this field assimilate central bank digital currencies to cash, considering it in this respect equivalent to any form of fiat currency issued by a central bank. Since both AML/CFT and data protection and privacy concerns are important concerns to be balanced in the design of the architecture of a digital euro, it follows that **physical cash is the relevant benchmark** to strike such a balance, for example by using a threshold-based approach, allowing full privacy for daily life transactions.

From an operational point of view, research conducted by the ECB shows that ensuring the adoption of appropriate pseudonymisation techniques in the use of digital cash under a certain threshold, while still ensuring that higher-value transactions are subject to mandatory AML/CFT checks, is technically challenging but could be considered[13].

In this context, it seems to the EDPB that a modality offering **off-line transactions** (without internet connection to be accessible everywhere in the EU) anonymously or, in the lack of it, at least with a high level of pseudonymisation, is necessary to mitigate risks for rights and freedoms of data subjects.

Moreover, to the EDPB highlights that if a 'decentralized approach' were to be followed in that regard, the data should be tokenized[14] in order to avoid central monitoring of transactions, a good practice to consider would be to **store tokens locally** on an end-user device or digital wallet (like a smartphone or card to reach all types of public, and meeting the necessary software and hardware security conditions).

This token-based feature is compatible with interconnections to an **intermediary** distributing the digital euro, in order to refill the amounts of digital euro in the device or wallet, as it is currently the case for ATMs for example. During the interconnection, the transaction data would not be reported to the intermediary unless it reaches a given threshold. Moreover, the transactions that would be reported to the intermediary in charge of conducting AML/CFT due diligence and reporting have to be configured in at the minimum possible. Under such a framework, the on-boarding of end-users and monitoring of transactions by the ECB would not be necessary.

The technological and organisational features of the aforementioned token-based, decentralised approach should allow only and not prevent targeted identification of the parties, notably for AML/CFT purposes, avoiding any complete obfuscation of transactions, as it can be the case for some cryptocurrencies.

[13] https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.mipinfocus191217.en.pdf?3824c3f26ad2f928ceea370393cce785.

[14] In other words, substitute a randomly generated identifier for a sensitive piece of data in order to prevent unauthorized access.

The EDPB considers that the **simplicity of the design**, its easy access and the use of current infrastructures (if an assessment shows that this does not come at the cost of privacy and data protection) of the new digital currency is also important in terms of financial inclusiveness.

## 3. Next steps on privacy and data protection

While data protection and privacy aspects need to be carefully evaluated within legislative processes, the EDPB notes that the digital euro project will entail an obligation to carry out a data protection impact assessment (DPIA) by the relevant controllers[15]. Any data controller involved in personal data processing operations shall then perform the assessment before the beginning of its operations and evaluate the need to consult the competent supervisory authority prior to processing if necessary[16].

However, performing this analysis, as a high-level assessment on the overall project, would be of major help in correctly assessing and mitigating risks for rights and freedoms of data subjects and would provide key elements to be considered when deciding on the possible design and architectural scenarios.

In this context, we recommend that the EU body in charge of the design of the project performs such a **high-level impact assessment** on privacy and data protection during the exploratory phase.

Due to the importance of the initiative, the EDPB stands ready to **provide advice** upon formal or informal consultations by the ECB or by other EU institutions with the aim of ensuring at the same time the effectiveness and the less privacy-intrusive configuration, right after a decision to launch the project is taken, in order to provide a more granular compliance advice on the options considered.

Besides of the formal involvement of the EDPS, the EDPB would also like to express availability to **work at expert level** with the competent EU institutions from the early stage of development of the project, as well as during the exploratory phase.

For the European Data Protection Board,

The Chair

(Andrea Jelinek)

[15] See WP29, Guidance and https://edps.europa.eu/data-protection/our-work/publications/guidelines/accountability-ground-provisional-guidance_en.

[16] That is, if the DPIA indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in view of the available technologies and costs of implementation.