Untangling Digital Euro's Personal Data Protection Challenges: An Exploration of Data Processing Activities and Latent Privacy Risks[†§]

Andrés Chomczyk Penedo, Pablo Trigo Kramcsák, Michaël Van den Poel and Alessandro Ortalda[*]

16 October 2024

Abstract

The digital euro is a Central Bank Digital Currency (CBDC) that aims to revolutionise digital payments in the Eurozone by offering a public alternative to private digital payment schemes. The European Commission and the European Central Bank (ECB) have publicly stated their commitment to ensuring high levels of privacy and data protection for Europe's newest form of payment. While the Digital Euro Proposal is already under discussion, this commitment has not been sufficiently examined from a data protection law perspective.

The urgency to bridge the research gap in privacy and data protection standards for the digital euro cannot be overstated. The legislative momentum combined with the intended extensive social usage of this digital currency could seriously impact individuals' lives as their principal means of payment is further digitalised and subject to intensive data-driven processing activities. Financial data, particularly regarding payments, is seen as more sensitive by data subjects, with empirical research establishing that users see privacy as an essential feature of a future digital euro. However, the Proposal presents intricate data-sharing processes that could raise data protection concerns if not adequately addressed.

This paper examines the implications of the Digital Euro Proposal for the right to privacy and data protection, examining the characteristics, architecture, and complex relationships between the ECB, national central banks, service providers and intermediaries. To direct our research, we formulate the following research question: 'How does the digital euro initiative address data protection and privacy issues following the principles, obligations, and rights in the EU data protection framework?'. The paper identifies and examines two principal challenges presented by the proposed digital euro in the context of data protection: unclear allocation of roles and responsibilities, which encompasses the ambiguity surrounding the distribution of duties among the diverse entities engaged in data processing, and balance between data minimisation and availability, i.e., the potential conflict between reducing the amount of data generated by this digital money system while ensuring that seemingly lawful grounds have acess to sufficient data to be fulfiled, such as anti-money laundering, which also includes adhering to the principle of purpose limitation.

Keywords: CBDC, digital euro, privacy, data protection, fundamental rights
JEL classification: K19, K24, K38

[†] A previous version of this paper has been presented at the eLaw Conference 2024 hosted by eLaw Center for Law and Digital Technologies of Leiden University.

[§] The authors are currently being supported by the European Data Protection Supervisor (EDPS) as one of the independent research projects that the EDPS will contribute to as part of its 20th anniversary actions.

[*] All authors are affiliated with the research group Law, Science, Technology and Society (department of Interdisciplinary Study of Law) of the Vrije Universiteit Brussel (VUB) and the Brussels Privacy Hub (BPH).

1 Introduction

1.1 The EU's Digital Finance Strategy: chasing technology with regulation

In an era marked by rapid digital transformation, the European Union's Digital Finance Strategy ('DFS')[1] emerged as a critical policy element to address the changes occurring in the financial services industry. This strategy is not just about leveraging the potential of digital innovation within the financial sector but also about managing the inherent risks that come with such advancements.
Traditionally, introducing new technologies has been subject to supervision by financial services authorities.[2] This has changed as fintech and big tech companies have made their way into the financial services industry[3] through a wide range of business models.[4] Their presence has accelerated innovation in the finance sector,[5] putting pressure on a system previously characterised by a controlled inflow of data-driven solutions.[6] The DFS recognises this change and emphasises the importance of trust and safety in the digital financial landscape, underscoring the need for vigilant data protection and privacy management.[7]

1.2 The current legislative push for the digital euro

Since its publication in 2020, the DFS has slowly produced different regulatory instruments, such as Regulation (EU) 2023/1114 ('MiCA')[8] and Regulation (EU) 2022/2554 ('DORA').[9] In late June 2023, the instruments marking the capstone of the DFS were unveiled.[10] Most notable was the introduction

[1] 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Digital Finance Strategy for the EU' (European Commission 2020) Communication from the Commission (2020) 591.
[2] Technology itself was not regulated by financial supervisors. Instead, as noted by Arner, Barberis and Buckley, supervisors took a reactive approach to the implementation of technologies by financial institutions. This was possible because the entities innovating in the financial industry were financial institutions licensed and subject to existing oversight by regulatory agencies. Douglas W Arner, Janos Barberis and Ross P Buckley, 'The Evolution of FinTech: A New Post-Crisis Paradigm' (2015) 47 Georgetown Journal of International Law 127.
[3] Raihan Zamil and Aidan Lawson, 'Gatekeeping the Gatekeepers: When Big Techs and Fintechs Own Banks – Benefits, Risks and Policy Options' (Bank for International Settlements 2022) FSI Insights on policy implementation 39.
[4] Whilst a discussion on the new business models introduced under the FinTech revolution is a topic on itself (see Douglas W Arner, Janos Barberis and Ross P Buckley, 'The Evolution of FinTech: A New Post-Crisis Paradigm' (2015) 47 Georgetown Journal of International Law 1271), we can briefly mentioned two trends: (i) the creation of new services and products, such as crowdlending and -funding; and (ii) the platformization of financial services, including the consolidation of the Banking-as-a-Service model (see Reijer Hendrikse, David Bassens and Michiel van Meeteren, 'The Appleization of Finance: Charting Incumbent Finance's Embrace of FinTech' (2018) 4 Finance and Society 159; David Bassens and Reijer Hendrikse, 'Asserting Europe's Technological Sovereignty amid American Platform Finance: Countering Financial Sector Dependence on Big Tech?' (2022) 97 Political Geography 102648.)
[5] 'Consumer Risks in Fintech New Manifestations of Consumer Risks and Emerging Regulatory Approaches' (World Bank Group - Ministry of Foreign Affairs of the Netherlands 2021) Policy research paper <https://documents1.worldbank.org/curated/en/515771621921739154/pdf/Consumer-Risks-in-Fintech-New-Manifestations-of-Consumer-Risks-and-Emerging-Regulatory-Approaches-Policy-Research-Paper.pdf> accessed 2 June 2021.
[6] As discussed in footnote [2], by controlled we do not mean slow but rather that the process was mainly conducted by a selected group of gatekeepers, i.e., licensed financial institutions, that were the only ones authorised to conduct this type of activity.
[7] See 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Digital Finance Strategy for the EU' (European Commission 2020) Communication from the Commission (2020) 591 s 4. In this respect, the DFS states that '[f]urther steps towards enhanced data sharing and openness across and within sectors, in compliance with data protection and competition rules, will enable the financial sector to fully embrace data-driven innovation. This will encourage the creation of innovative products for consumers and businesses, and will support broader policy objectives, such as the as the creation of a single market for data.'
[8] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 PE/54/2022/REV/1 OJ L 150, 9.6.2023, p. 40–205.
[9] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 PE/41/2022/INIT OJ L 333, 27.12.2022, p. 1–79
[10] In this respect, we refer to the Proposal for a Regulation of the European Parliament and of the Council on a framework for Financial Data Access and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010, (EU) No 1095/2010 and (EU)

of the digital euro, pushed as a pivotal tool for ushering in the new era for the EU's common currency by the European Central Bank ('ECB').[11] This initiative aims to develop a digital form of the euro, promising to revolutionise the landscape of digital payments and secure the role of the euro within the evolving Digital Single Market and against the advancements by privately issued e-money, particularly stablecoins.[12]

The core objective of the digital euro initiative lies in the creation of an electronic means of payment equivalent yet complementary to the physical banknotes and coins currently in circulation.[13] A successful digital euro would have to feature improved efficiency and inclusivity compared to existing payment systems, while safeguarding the euro's position from competing payment methods and currencies in the swiftly evolving digital economy.[14] At least in the discourse contained in the available policy documents and regulatory proposal, the digital euro is expected to impact the European economy profoundly – it is poised to transform digital commerce, reshape financial services, and redefine monetary transactions.[15] The regulatory proposal for a digital euro (the 'Digital Euro Proposal' or 'Proposal') was published by the European Commission in mid-2023.[16]

In contrast to existing private payment solutions which are dependent on the use of other (financial) services or limited by terms of use, the digital euro accounts should be available to any user.[17] The digital euro thus aims to foster a more competitive and innovative European retail payments market by providing an alternative to the privately offerred status quo.[18]

However, the work conducted by and within the ECB's umbrella, such as for example in the development of the digital euro scheme's Rulebook Development Group,[19] reveals an infrastructure that resembles the current electronic payments system remarkably but also depends extensively on it, as will be discussed later on this article. As such, it is possible to question the very grounds that the digital euro builds upon as it introduces another layer of complexity into an already intricate system

2022/2554 COM/2023/360 final ('FiDA'), Proposal for a Regulation of the European Parliament and of the Council on payment services in the internal market and amending Regulation (EU) No 1093/2010 COM/2023/367 final ('PSR'), and the Proposal for a Directive of the European Parliament and of the Council on payment services and electronic money services in the Internal Market amending Directive 98/26/EC and repealing Directives 2015/2366/EU and 2009/110/EC COM/2023/366 final ('PSD3'). For a preliminary analysis of FiDA, see Andrés Chomczyk Penedo and Pablo Trigo Kramcsák, 'Can the European Financial Data Space Remove Bias in Financial AI Development? Opportunities and Regulatory Challenges' (2023) 31 International Journal of Law and Information Technology 253.

[11] In this respect, the ECB's digital euro web resource center contains a detailed timeline of this project. As such, we can highlight that the idea of a digital euro emerged in late 2020, almost 3 years before the European Commission put on the table its proposal (see https://www.ecb.europa.eu/euro/digital_euro/timeline/html/index.en.html, accessed May 28 2024). Moreover, the DFS acknowledges that central banks, including the ECB, had been working around the idea of a CBDC before the DFS was developed and published (see 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Digital Finance Strategy for the EU' (European Commission 2020) Communication from the Commission (2020) 591 s 4.2)

[12] 'Report on a Digital Euro' (European Central Bank 2020). On stablecoins, see infra.

[13] Based on the European Central Bank digital euro resource center, the '(...) digital euro would be a digital form of cash: an electronic means of retail payment issued by us, the European Central Bank. As a form of public money, it would be available free of charge to everyone in the euro area, for any digital payments.' (see European Central Bank, What would a digital euro be?, <https://www.ecb.europa.eu/euro/digital_euro/features/html/index.en.html> accessed 6 June 2024)

[14] Based on the ECB's vision for the digital euro, it is intended to '(...) make our lives easier by giving us the choice to pay with a secure means of payment universally accepted throughout the euro area. Like cash, paying with digital euro would be free of charge for everyone in the euro area.' European Central Bank, 'Why do we need a digital euro?' <https://www.ecb.europa.eu/euro/digital_euro/why-we-need-it/html/index.en.html> accessed 6 June 2024.

[15] Matteo Cotugno and others, 'Ready for a Digital Euro? Insights from a Research Agenda' (2024) 67 Research in International Business and Finance 102117, 10.

[16] Commission, Proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro COM/2023/369 final. As of this date, the Digital Euro Proposal is being considered within the European Parliament and the Council of the European Union after laying dormant during the 2024 EU election period.

[17] According to Recital 18 of the Digital Euro Proposal, '[a]s a new form of the euro available to the general public, the digital euro should have important societal and economic consequences.'

[18] Recital 1 Proposal.

[19] European Central Bank – Eurosystem, '*Update on the work of the digital euro scheme's Rulebook Development Group*', 3 Janaury 2024, < https://www.ecb.europa.eu/euro/digital_euro/timeline/profuse/shared/pdf/ecb.degov240103_RDG_digital_euro_schemes_update.en.pdf?f8e154918d3e5e25736dbf5b3edbaf05> acccessed 16 September 2024.

with several potential points of failure that can prevent from securing an adequate framework for the protection of personal data.

1.3 Structure, research question and methodology of the paper

This contribution will explore the implications of the digital euro for the two distinct rights to privacy and data protection in the EU.[20] It will do so by analysing the characteristics, architecture, and complex relationships between the central banks and intermediaries, with a focus on the roles and responsibilities as data controllers and processors in data protection law. To direct our research, we formulate the following question: 'How does the Digital Euro Proposal address data protection and privacy issues stemming from the principles, obligations and rights in the EU data protection framework?'

The discussion starts by exploring the intrinsic data and privacy challenges of different forms of money with varying levels of digitalization. It then examines the specifics of the Digital Euro Proposal, analysing its objectives, components, and relation with EU data protection law. Next, two key challenges indentified in the allocation of responsibilities and in the interpretation of principles stemming from EU data protection law are identified and discussed. Finally, drawing upon the preceding analysis, the paper concludes by offering insights into the implications of the digital euro for data protection practices.

For this purpose, our research considers literature on the privacy and data protection aspects of digital finance and its legal framework, alongside its interpretation by administrative and judicial bodies.

2 From cash and cards to crypto and CBDCs: a brief history of monetary data protection and privacy challenges

The digital euro initiative belongs to a broader global phenomena that has been denominated as Central Bank Digital Currencies (CBDCs),[21] which are intended as a response to privately issued stablecoins and other cryptocurrencies.[22] These digital assets, each with unique mechanisms and regulatory frameworks, are reshaping the financial landscape, presenting new opportunities and challenges.[23] The meteoric rise of cryptocurrencies (including stablecoins, whose value is pegged to another external traditional asset), especially those with privacy-enhancing (or even anonymity-enhanced) mechanisms built-in,[24] have amplified the public's interest in the right to private digital payments.[25] In this respect, 'CBDCs are not the cause of the need to rethink distribution of traditional competences, but rather a consequence of a redistribution of powers that has already been operating from within the financial system'.[26] In this respect, the purpose of this Section is to briefly explore how we have arrived to this scenario, with a focus on the data protection and privacy issues that arise in each scenario.

[20] Article 7 and 8 CFR.

[21] Raphael Auer, Giulio Cornelli and Jon Frost, 'Rise of the Central Bank Digital Currencies: Drivers, Approaches and Technologies' (Bank for International Settlements (Monetary and Economic Department) 2020) 880.

[22] Dirk Bullmann, Jonas Klemm and Andrea Pinna, 'In Search for Stability in Crypto-Assets: Are Stablecoins the Solution?' (European Central Bank 2019) 230.

[23] Auer, Cornelli and Frost (n 21).

[24] Geoff Goodell and Tomaso Aste, 'Can Cryptocurrencies Preserve Privacy and Comply With Regulations?' (2019) 2 Frontiers in Blockchain 4.

[25] Jerry Brito, 'The Case for Electronic Cash: Why Private Peer-to-Peer Payments are Essential to an Open Society' (CoinCenter 2019) <https://coincenter.org/files/2019-02/the-case-for-electronic-cash-coin-center.pdf> accessed 1 May 2019; Peter Van Valkenburgh, 'Electronic Cash, Decentralized Exchange, and the Constitution' (CoinCenter 2019) <https://coincenter.org/files/e-cash-dex-constitution.pdf>.

[26] Giulio Soana and Thomaz De Arruda, 'Central Bank Digital Currencies and Financial Integrity: Finding a New Trade-off between Privacy and Traceability within a Changing Financial Architecture' [2024] Journal of Banking Regulation p. 3.

2.1 Cash as the paramount of privacy-by-design method of payment

Under its classic definition, money has four functions: a medium of exchange, a unit of account, a means of payment, and a store of value.[27] Prior to the digitalization of finance, the status quo was cash. This form of fiat money is typically government-issued,[28] but is generally seen as easy to use and hard to control and surveil.[29] As transactions leave no trace with the exception of the trade of physical notes or coins, they are seen as anonymous except for those paying and receiving. This makes cash a 'privacy-by-design' means of payment, making it an ideal instrument for exercising fundamental rights without fear for possible consequences due to the difficulty of surveillance. Cash transactions by their nature have mostly remained exempt from Anti-Money Laundering ('AML') and Countering the Financing of Terrorism ('CFT') obligations, as they are peer-to-peer and lack any intermediary. This relative absence of control has been answered by legislators in recent years, which have restricted high denominations and high-value cash transactions.[30] These restrictions aim to decrease cash transactions in favour of more traceable digital transactions susceptible to the forementioned obligations.

2.2 The increased control on digital transactions

Whilst digital transactions are not new, their share in overall payments has been increasing in recent years.[31] This evolution can be traced to government pushes for cashlessness,[32] digitalization of consumer-facing banks, and novel appearances of digital money through non-bank payment service providers.[33] In all forms of digital payments, intermediaries are introduced in the form of banks or service providers, i.e. an intermediary.[34] Compared to cash transactions free from intermediaries, digital transactions create risks for both the privacy of payments and for the right to personal data protection as transaction data is generated in the form of personal identifiers, transactions parties and payment histories.[35]

These risks range from the collection of data considered as sensitive data under data protection law,[36] exposure to enforcement agencies' oversight,[37] potential data breaches[38] as well as general misuse of the collected informaion. Another source of risks is the integration of digital money with cloud

[27] Bill Maurer, How Would You Like to Pay? How Technology Is Changing the Future of Money (Duke University Press 2015) 47. For a full overview of the evolution of money, see Jacob Goldstein, *Money: The True Story of a Made-Up Thing* (Atlantic Books 2020) as well as Maurer's work cited in this footnote.

[28] For an overview of the difference between fiat and commodity money, see Hans-Hermann Hoppe, 'How Is Fiat Money Possible? Or, the Devolution of Money and Credit' (1994) 7 The Review of Austrian Economics 49, 49.

[29] Lana Swartz, New Money: How Payment Became Social Media (Yale University Press 2020). 24.

[30] See for example the Belgian limit of 3 000 euros for cash transactions, article 67§2 Law of 18 September 2017 on Preventing money laundering and terrorist financing and limiting the use of cash, *BS* 6 October 2017. Moreover, see 'ECB Ends Production and Issuance of €500 Banknote' (European Central Bank, 4 May 2016) <https://www.ecb.europa.eu/press/pr/date/2016/html/pr160504.en.html> accessed 2 December 2023.

[31] European Central Bank, 'Study on the Payment Attitudes of Consumers in the Euro Area (SPACE) – 2022' <https://www.ecb.europa.eu/stats/ecb_surveys/space/html/ecb.spacereport202212~783ffdf46e.en.html> accessed 1 October 2024

[32] For example, Sweden has been experimenting with this type of policies for almost 30 years (see Nikola Fabris, 'Cashless Society – The Future of Money or a Utopia?' (2019) 8 Journal of Central Banking Theory and Practice 53).

[33] In this respect, a wide range of examples have emerged in all continents, from e-money providers in the EU, under the the Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC OJ L 267, 10.10.2009, p. 7–17 ('e-Money Directive'), to mobile operators in Africa, such as M-Pesa. For a more detailed analysis, see Tobias Adrian and Tommaso Mancini-Griffoli, 'The Rise of Digital Money' (2021) 13 Annual Review of Financial Economics 57. Moreover, Maurer (n 27) ch 4 provides further examples of these processes.

[34] Swartz (n 29) 84.

[35] Valeria Ferrari, 'Crosshatching Privacy: Financial Intermediaries' Data Practices Between Law Enforcement and Data Economy' (2020) 6 European Data Protection Law Review 522, 524.

[36] Andrés Chomczyk Penedo, 'Ireland · Can a Data Breach Be Caused by Poor Quality Data? An Analysis of a Decision by the Irish Data Protection Commission and Its Potential Influence on Future Financial Data Sharing' (2022) 8 European Data Protection Law Review 278.

[37] Ferrari (n 35).

[38] Chomczyk Penedo (n 36).

computing services, which exposes personal data to multijurisdictional oversight and transfers.[39] Additionally, issues like data security and concentration risks further complicate efforts to protect digital currency systems.[40]

Whilst government interference in the relation between financial institutions, privacy and data protection was initially focussed on client confidentiality and bank secrecy obligations,[41] recent moves to obligatory disclosement for tax reporting, AML and CFT purposes have further increased risks associated with digital banking.[42] As a result, in transactions involving regulated financial institutions, individuals now often anticipate personal data-sharing with government agencies.[43]

2.3 Digital transactions without intermediaries: the rise of cryptocurrencies

Where the financial crisis of 2008/2009 produced a trust crisis regarding incumbent financial institutions,[44] Bitcoin emerged as an alternative digital money system based on cryptographic proof in the blockchain instead of trust in financial institutions.[45] Blockchain technology, as the culmination of several developments in the field of cryptography,[46] eliminates intermediaries, allowing peer-to-peer transactions, aiming to reduce costs and increase efficiency. Blockchain technology creates an immutable ledger of transactions, ensuring that once a transaction is recorded, it cannot be altered or deleted. The elimination of intermediaries is combined with a public and auditable transaction list to reduce risks of fraud and to enhance accountability. From a privacy and data protection perspective,

[39] W. Kuan Hon, Christopher Millard, 'Banking in the cloud: Part 3 – contractual issues' (2018) 34 Computer Law & Security Review 3, 595-614.

[40] Katarzyna Parchimowicz, 'Do not get lost in the cloud: how EU financial institutions could avoid problems with cloud services arising under DORA' (2024) Law, Innovation and Technology, 1–25.

[41] Anatoliy A Lytvynenko, 'Data Privacy and Banking Secrecy: Topical Issues in Commonwealth, Continental Europe and International Jurisprudence' (2019) 5 Athens Journal of Law 303.

[42] In this respect, AML legal rules have compromised bank secrecy and financial privacy since the late 1980 onwards (see He Ping, 'Banking Secrecy and Money Laundering' (2004) 7 Journal of Money Laundering Control 376, 378–379) but also in the quest to address tax evasion this duty has been eroded, particularly in developed economies (see, for example, Niels Johannesen and Gabriel Zucman, 'The End of Bank Secrecy? An Evaluation of the G20 Tax Haven Crackdown' (2014) 6 American Economic Journal: Economic Policy 65)

[43] While limited discussion about this has taken place within the EU context, US-based scholars argue that, while their legal system recognises the right to privacy, their judiciary has eroded this legal protection in the context of financial transactions (see, for example, Janet Dean Gertz, 'The Purloined Personality: Consumer Profiling in Financial Services' (2002) 39 San Diego Law Review 943, 972–976). In this respect, US scholars argue that EU citizens would have a stronger expectation of privacy in the financial transactions thanks to the protection of fundamental rights through the right to personal data protection (see, for example, Virginia Boyd, 'Financial Privacy in the United States and the European Union: A Path to Transatlantic Regulatory Harmonization' (2006) 24 Berkeley Journal of International Law 939)

[44] Bahriye Basaran and Mahmood Bagheri, 'The Relevance of "Trust and Confidence" in Financial Markets to the Information Production Role of Banks' (2020) 11 European Journal of Risk Regulation (EJRR) 650, 663.

[45] Vasilis Kostakis and Chris Giotitsas, 'The (A)Political Economy of Bitcoin' (2014) 12 tripleC: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society 431; Nakamoto S, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (24 March 2009). For an overview in literature about how the blockchain can contribute to confidence in financial transactions, see Primavera De Filippi, Morshed Mannan and Wessel Reijers, 'Blockchain as a Confidence Machine: The Problem of Trust & Challenges of Governance' (2020) 62 Technology in Society 101284.

[46] Alan T Sherman and others, 'On the Origins and Variations of Blockchain Technologies' (2019) 17 IEEE Security & Privacy 72.

this has caused debate within the literature.[47] To respond to many of these claims, privacy-friendly protocols have been developed.[48]

To further compete with digital transactions, stablecoins pegged to traditional currencies have been created, both in a centralized but also in a decentralized manner,[49] offering similar transactions to other cryptocurrencies while aiming to have less fluctuations in their value. This new wave of privately issued currencies outside of the scope of government-regulated financial institutions was received with scepticism and suspicion by regulators.[50]

In those cases where a central intermediary is missing, these regulators would have substantial difficulties enforcing AML and CFT obligations on blockchain transactions. This, in combination with the emergence of stablecoins initiated a push towards a public alternative to cryptocurrencies.

2.4 Central Bank Digital Currencies as a response to cryptocurrencies

This public alternative came in the form of Central Bank Digital Currencies (CBDCs).[51] These forms of money issued by the same central banks responsible for the issuance of traditional cash aim to offer the benefits of government-backed currencies with those of new digital alternatives.[52] They aim to offer similar privacy to cryptocurrency and cash, further amplifying interest in such payments,[53] whilst simultaneously challenging the status quo of banks as data-hungry intermediaries.[54]

As of the time of writing, 134 countries and currency unions, accounting for 98% of global GDP, are prospecting CBDCs. Among them, 19 of the G20 nations are in advanced stages of CBDC development, with eleven already in the pilot phase. These countries include Brazil, Japan, India, Australia, South Korea, South Africa, Russia, and Turkey.[55] China is taking a leading role in developing its CBDC, the digital renminbi, with BRICS countries pushing for a joint 'super-sovereign currency' which aims to challenge the US dollar supremacy in international transactions.[56]

---

[47] In this respect, the debate has focused on which portion of the protocols, if any at all, engaged in the processing of personal data and, consequently, trigger the application of EU data protection law. For example, it has been argued that a public address could constitute a personal data since it is merely a pseudonymous (see Michèle Finck, European Parliament, and Directorate-General for Parliamentary Research Services, 'Blockchain and the General Data Protection Regulation: Can Distributed Ledgers Be Squared with European Data Protection Law?' (European Parliamentary Research Service 2019) PE 634.445 <http://publications.europa.eu/publication/manifestation_identifier/PUB_QA0219516ENN> accessed 25 March 2020). On the other hand, it has been mentioned that truly open protocols behave in a similar manner to the Internet, where the focus to find data controllers is placed on service operators using the protocol rather than focusing on the protocol itself (see Lokke Moerel, 'Blockchain & Data Protection…and Why They Are Not on a Collision Course' (2019) 6 European Review of Private Law 825).

[48] As a response, certain protocols emerged to mitigate the issues discussed in the previous footnote. For example, Monero procures the obfuscation of transactions to ensure fungibility and achieve true anonymity; this, however, comes at the expense of making more difficult the compliance with certain legal framework, such as AML/CFT (see Sara Barj, Aafaf Ouaddah and Abdellatif Mezrioui, 'A Review of Privacy-Preserving Cryptographic Techniques Used in Blockchain Platforms' in Saad Motahhir and Badre Bossoufi (eds), *Digital Technologies and Applications* (Springer Nature Switzerland 2023); Goodell and Aste (n 22)).

[49] In this respect, we have seen both the emergence of centralized stablecoins, such as Diem (formely known as Libra), but also decentralized alternatives, such as DAI (see Alexander Lipton and others, 'Stablecoins' in Alex Pentland, Alexander Lipton and Thomas Hardjono, Building the new economy: data as capital (The MIT Press 2021) 301).

[50] Iris H-Y Chiu, 'A new era in fintech payment innovations? A perspective from the institutions and regulation of payment systems' (2017) 9 Law, Innovation and Technology 2, 190–234, 222.

[51] Auer, Cornelli and Frost (n 21); Dirk Bullmann, Jonas Klemm and Andrea Pinna, 'In Search for Stability in Crypto-Assets: Are Stablecoins the Solution?' (European Central Bank 2019) 230.

[52] Auer, Cornelli and Frost (n 21).

[53] Goodell and Aste (n 24).

[54] Soana and De Arruda (n 26) 3.

[55] 'Central Bank Digital Currency Tracker' (*Atlantic Council*) <https://www.atlanticcouncil.org/cbdctracker/> accessed 1 October 2024

[56] Zhixuan Ren, 'The Impact of Central Bank Digital Currency Issuance on the International Monetary System - Taking China and Other Countries as Examples' (2024) 181 SHS Web of Conferences 02007. It should be noted that the digital renminbi has been linked with cybersecurity, data protection and espionage links, see Thai-Binh Elston, 'China Is Doubling Down on Its Digital Currency - Foreign Policy Research Institute' <https://www.fpri.org/article/2023/06/china-is-doubling-down-on-its-digital-currency/> accessed 5 June 2024.

CBDCs can be organised in different ways, primarily using a token-based or account-based approach.[57] Account-based CBDCs, of which the digital euro is an example, involve a model similar to that of electronic money, as defined under the e-Money Directive, with a central authority controlling balances, ownership, and the transfer of funds. Token-based CBDCs, like the Bahamian Sand Dollar, imply a model resembling cryptocurrencies, where these operations are usually conducted on a peer-to-peer basis after the initial issuance of money.[58] Other possible classifications divide CBDCs in wholesale or retail, direct or indirect forms, centralised or decentralised, and whether they are used for domestic or cross-border use.[59]

2.5 A brief overview of the data protection challenges for CBDCs in contrast to other forms of digital money

Protecting privacy and personal data is thus seen as imperative in digital finance. Besides the legal requirement to protect data and respect privacy of users,[60] privacy protections are also considered necessary by users, with 43 per cent of respondents to an ECB public consultation marking privacy as the most important aspect of a digital euro.[61] Transaction data can reveal a lot about a person, including special categories of personal data,[62] requiring safeguards to ensure that those categories are not used in manner than compromises fundamental rights.[63] Protecting these data is thus not just about meeting regulatory requirements; it's about maintaining consumers' and users' trust and the integrity of the entire financial system. Therefore, stringent data protection measures are key, not only to safeguard individual privacy and ensure secure financial transactions but also to empower individuals with a sense of autonomy and control over their personal financial data.

Before moving to analyzing the core challenges for the digital euro, it is possible to briefly reflect on the issues that CBDCs have to overcome when it comes to respecting the rights to privacy and personal data protection. We can identify three main issues: (i) the consequences from having a centralised infrastructure; (ii) the problems with making money programmable; and (iii) how the final settlement of transactions should take place. In this sense, From a very conceptual perspective, it is possible to trace some points of convergence and departure between the forms of money discussed previously in this section.

As a starting point, cash constitutes the ultimate form of a privacy-friendly form of money that collects the minimum amount of data by itself.[64] In contrast to intrinsically hard-to-trace cash payments, e-money and other forms of bank digital money involve the intermediation of, at least, a third party that

[57] Michalopoulos and others, '*Compliance Design Options for Offline CBDCs: Balancing Privacy and AML/CFT*', (2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), IEEE, 2024), p 2.

[58] Frédéric Tronnier, 'Privacy in Payment in the Age of Central Bank Digital Currency' in Michael Friedewald, Stefan Schiffner and Stephan Krenn (eds), Privacy and Identity Management (Springer International Publishing 2021).

[59] In this respect, a wholesale CBDC is distributed to intermediaries to streamline settlement processes, whereas a retail CBDC is distributed directly to the public for everyday transactions, making it more comparable to traditional fiat currency. There are three main models for distribution. In a direct CBDC model, the Central Bank manages everything, and users transact directly with one another in a peer-to-peer system. In an indirect model, intermediaries handle all user-related activities while the Central Bank oversees the underlying network, similar to traditional financial markets. The hybrid model combines these approaches, allowing peer-to-peer transactions for smaller amounts while requiring intermediaries for larger ones. CBDCs can be implemented using either centralized or decentralized technology, though they typically use a permissioned blockchain to maintain control. The design of a CBDC can also vary in terms of its geographic scope—it can be used domestically, for cross-border transactions, or be indifferent to location, depending on whether it is accepted by the payee. For further analysis, see Soana and De Arruda (n 21) 7.

[60] This legal requirement stems from both primary (article 7 and 8 of the Charter of Fundamental Rights of the EU and article 16 of the Treaty on the Functioning of the EU) and secondary (GDPR) EU law.

[61] 'Eurosystem Report on the Public Consultation on a Digital Euro' (European Central Bank 2021) 10–11.

[62] See Chomczyk Penedo (n 36).

[63] Swartz (n 29).

[64] In this sense, we acknowledge that the involved parties can record, outside of the scope of the instrument itself, other details related to the transaction where certain amount of cash was involved. For example, in Argentina during certain time, it is common practice to record in public deeds the serial number of US dollars involved in transactions to avoid possible counterfeits and, if they were involved, have a robust proof of where they came from.

records a considerable amount of information regarding one transaction. In this sense, '[t]he transition from cash (token-based and peer to peer) to digital transactions (account-based and necessarily intermediated) makes any transaction routed through such networks traceable and the connected metadata available to the private and public eye'.[65] However, given the decentralized nature of these forms of money, data minimization still is allowed to survive. However, when moving up to CBDCs, a public single solution system for electronic payments, while beneficial in several domains, introduces a high-risk of data breach given both the number of involved parties with potential access to data, but also the creation of new necessary mechanism that further expose personal data, such as the single access point in the digital euro ecosystem. In particular, and concerning the digital euro, In this sense, the decision to adopt an account-based approach, which according to the literature would be the predominant criteria for CBDCs projects, including the digital euro, exposes transactions to potential analysis by the wide range of intermediaries responsible for managing the corresponding ledger. As will be explored in the following Section, this would be the case with the digital euro, according to its current design .

Connected to how a CBDC operates, we can also briefly discuss and compare the programmable capabilities between these and other forms of digital money. In this respect, by programmable money we mean the technical possibility embedded within the system itself which would enable certain entities with key operational powers to limit the use of the currency through the very same technical means.[66] Considering that financial data, particularly that regarding payments, can be considered as personal data, the processing of such information and running it through the parameters set beforehand, can constitute a severe limitation to the exercise of certain rights.

In this respect, each form of digital money can have a very different approach to this issue. For example, in truly decentralized cryptocurrencies, such as Bitcoin, it might be harder to implement but also enforce this type of measures given the lack of a central authority and the need to find consensus to put in place this kind of limitation, not even discussing about defining the criteria for those limites. On the other hand, centralized e-money systems might have an 'easier' time doing so as it would be possible to have an authority putting in place these conditions as well as setting the parameters for their ocurrance. In other words, '(…) a CBDC would reunite all the, currently fragmented, ledgers into a single currency-wide ledger'.[67]

When turning particularly to field of CBDCs, the introduction of programmable money characteristics is a highly discussed topic among regulators and policymakers. In the case of the digital euro, making it programmable money was ruled out by the ECB and Commission, ensuring its unrestricted use.[68]

On a final note, it is possible to discuss the implications, as with any other financial transaction, related to the final settlement, i.e., the conciliation of accounts between different system parties, from a data protection perspective. In this regards, this set operations is necessary to minimise unnecessary movement of funds between the operators, therefore making it more efficent in its process. Cash-based transactions, on the one side of the spectrum, constitute the most data protection friendly solution as the final settlement takes place within the very same transaction between the parties involved; on the other hand, digital money systems with a wide range of intermediaries, demand settlement layers that expose transaction data to other parties. For example, credit card purchases involve a common third party between the acquirer, the issuer, the merchant and the account holder itself; this means that for the transaction between the last two, three parties know, at least, some details regarding the operation, if not all transaction information. When turning to CBCDs, the discussion about its infraestructure comes to the foreground. In this respect, in the case of the digital euro for example, settlement between

[65] Soana and De Arruda (n 21) 13

[66] Alexander Lee, 'What Is Programmable Money?' (Board of Governors of the Federal Reserve System, 2021) FEDS Notes <https://doi.org/10.17016/2380-7172.2915> accessed 5 December 2023.

[67] Soana and De Arruda (n 21) 13

[68] Article 24(2) Proposal.

financial institutions will be handled within the Eurosystem for online payments,[69] while offline transactions will be settled locally.[70] While the online euro would suffer and be exposed to equivalent issues as e-money, the arena can look promising for the offline variant, as long as certain issues are adequately addressed in the regulatory framework under discussion.

Ultimately, it is possible to argue that the proposed web of intermediaries to be found in CBDCs projects, including the digital euro, runs counter to the principle of proportionality found in GDPR, particularly to justify the creation of a parallel infrastructure that fall in the same problem as current digital money solutions, given the mimic to the very same organizational structure. From a the point view of the analysis of information flows, as a starting point for a data protection perspective, and despite its complex architecture, the digital euro in its current configuration and design is nothing more than a dataset that will keep track of account balances assigned to given (natural) persons, like many other forms of digital money.[71] If an entity can potentially trace one or more transactions to a specific individual, personal data protection rules will apply, making it necessary, for example, to reflect on aspects such as data controllership.[72]

3 The Digital Euro Proposal and the role of EU Data Protection Law

So far, and despite the intention to implement the digital euro as a form of digital cash-alternative, various organisations have raised concerns about this currency being potentially problematic for privacy and data protection; central to these concerns is the digital euro's unnecessary complexity.[73] While digital assets like cryptocurrencies demonstrate the possibility of direct end-user acquisition from the source, the proposed structure for the digital euro introduces a complex web of intermediaries, which some argue is not fundamentally different from existing digital payment solutions.[74] These concerns become even more prevalent when considering the potential interaction of the proposed digital euro with other structures and tools, such as the European Union Digital Wallet, recently introduced by the newly revised eIDAS Regulation, and other digital wallet solutions already existing on the market.[75] In order to consider that the digital euro process personal data in a proportionate matter, it requires that it maintains a considerable degree of anonymity, particularly guaranteeing non-traceability for lower-value transactions that would typically be associated with traditional cash-based transactions. In this line, the ECB, in its Opinion on the Digital Euro, 'suggests considering the possibility of offering increased privacy for certain low-risk, low-amount payments in digital euro'.[76] Sufficient safeguards for these transactions are crucial, as low-value transactions should offer 'cash-like privacy', bringing into the table something is not to be found in existing centralized digital money systems.

Consequently, the following two sections will explore (i) how the EU data protection framework is applicable to the digital euro, and (ii) two basic issues emerging from regarding the allocation of responsibilities and the underlying tension between principles using fraud detection as an example.

---

[69] Article 30.2 Proposal.
[70] Article 30.3 Proposal.
[71] Lee (n 66).
[72] Gloria González Fuster, 'EU Data Protection and Future Payment Services', in Gabriela Gimigliano (ed.), *Bitcoin and Mobile Payments: Constructing a European Union Framework*, Palgrave Macmillan, Palgrave Studies in Financial Services Technology, 2016.
[73] 'BEUC's Recommendations on the Legislative Framework for the Digital Euro' (BEUC - The European Consumer Organization 2023); 'Digital euro and Right to Cash Policy Analysis from a Human Rights Perspective' (epicenter.works – for digital rights 2023); 'ESBG Response to the European Commission Call for Feedback on the Proposed Regulation on the Establishment of the Digital Euro' (ESBG (European Savings and Retail Banking Group) 2023).
[74] 'Digital euro and Right to Cash Policy Analysis from a Human Rights Perspective' (epicenter.works – for digital rights 2023).
[75] 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 PE/68/2023/REV/1 OJ L, 2024/1183, 30.4.2024
[76] 'Opinion of the European Central Bank of 31 October 2023 on the Digital Euro Proposal (CON/2023/34)'.

3.1 The digital euro architecture

Turning back to the Digital Euro Proposal, Article 133 TFEU serves as its primary law basis.[77] This avoids fragmentation by establishing the digital euro as a single currency across the euro area. The ECB, along with national central banks, will thus be responsible for issuing the digital euro.[78] The distribution of the digital euro will occur through payment service providers (PSPs), credit institutions, and other entities.[79] Operating the digital euro will require a public interface, which can be developed by either PSPs or the ECB, giving users the freedom to choose between them.[80] Moreover, the Proposal prescribes the interoperability or integration of the European Digital Identity Wallet as a possible interface.[81] This would allow users to link digital euro accounts to their European Digital Identity platform. When such a link is created with the offline digital euro, every transaction will inherently be linked and traceable to an individual, compromising cash-like privacy. The design of the digital euro conditions how the rights to privacy and data protection will be safeguarded. The Proposal is based on an account-based approach, which exposes personal data to trusted intermediaries. Alternatives taking a token-based approach could be more privacy-friendly, but are outside of the scope of our analysis.

3.2 Applicable data protection requirements

Monetary transactions are data.[82] When this data relates to an identified or identifiable natural person, the GDPR rules regarding personal data processing become applicable.[83] More importantly, monetary transactions can reveal other types of data, including special categories of personal data.[84] Whether directly or indirectly,[85] the digital euro will process personal data. Even when the personal data processed does not fall under the defined special categories of the GDPR,[86] it might still be deemed as sensitive by data subjects due to the higher risks involved in processing financial information. Examples include the inference of behavioural data from financial transactions by individuals. As potential high-risk data processing will take place to implement the digital euro, data protection rules, including the GDPR, should be complied with in full. The current safeguards offered in the Proposal seem weak in this regard.

As the European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS) note in their Joint Opinion, the importance of privacy and data protection in implementing the digital euro should mean that ‘data protection by design and by default should be embedded in the design of the digital euro from the outset’.[87] As the Commission proposal is still vague on many technical

[77] Article 133 TFEU requires the Council and Parliament to ‘lay down the measures necessary for the use of the euro as the single currency’ and already serves as the legal basis for the establishment of the present euro.
[78] Article 4 Proposal.
[79] Articles 13 and 14 Proposal.
[80] Article 28 Proposal.
[81] Article 25 Proposal.
[82] For example, Westermeier argues that money is data as banks and other entities involved in financial transactions have acknowledged ‘(...) the increasing relevance of transactional data is tightly bound to the potentiality of information stored within money streams.’ (see Carola Westermeier, ‘Money Is Data – the Platformization of Financial Transactions’ [2020] Information, Communication & Society 1).
[83] Article 4(1) GDPR
[84] Chomczyk Penedo (n 36). In this regard, it is relevant to highlight that monetary transactions can both constitute a special category of personal data (for example, a payment to a political party will meet the legal requirements laid out in GDPR) but also these transactions, when used to form profiles, can reveal them (for example, having a record of numerous payments to a pharmacy might reveal an underlying medical condition, therefore triggering the existence of a special category of personal data).
[85] This refers to personal information related to an individual who is not the primary user of a particular digital currency or its associated services/infrastructure. This is considered as the processing of 'silent party data' (see ‘Guidelines 06/2020 on the Interplay of the Second Payment Services Directive and the GDPR’ (European Data Protection Board 2020) 1.0.
[86] Article 9 and 10 GDPR.
[87] ‘Joint Opinion 02/2023 on the Proposal for a Regulation of the European Parliament and of the Council on the Establishment of the Digital Euro’ (European Data Protection Board - European Data Protection Supervisor 2023).

details, the ECB is tasked with implementing 'detailed measures, rules and standards'.[88] These delegated responsibilities require careful consideration of fundamental rights by the ECB, a body with substantially less democratic legitimacy than the co-legislators, given that EU citizens do not directly elect their bodies.[89] The fundamental rights to privacy and data protection lay thus in the hands of the ECB in the current version of the Proposal.

As a safeguard, the parties involved will not only have to consider data protection legislation but will also be subject to supervision by data protection authorities. The EDPS retains its full competencies under the EUDPR, which applies to the ECB.[90] This includes Article 40 of the EUDPR, which mandates prior consultation with the EDPS for high-risk processing, when 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. Additionally, the supervision of national central banks and PSPs will be scrutinised to ensure their compliance with data protection regulations. As important players defining technical and operational details not covered by the Proposal as co-designers and distributors of the digital euro, respectively, they are subject to the GDPR. This includes supervision by national supervisory authorities in the member states where these actors are established.[91]

To include the views of data protection authorities, Article 5(2) of the Proposal requires the ECB to 'consult' the EDPS when adopting these measures affecting data protection.[92] Although the EDPB and EDPS have welcomed this provision,[93] its wording appears limited given the extensive responsibilities that data protection authorities will and should have in implementing the digital euro under the current EU data protection framework.

Regarding AML rules for offline digital euro transactions, Article 37(6) of the proposal allows the Commission to request the European Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA) to issue an opinion on 'assessing the level of money laundering and terrorist financing threats associated with the offline digital euro and its vulnerabilities'. The Commission may also consult the EDPB on this matter. However, the EDPB and EDPS, highlight that the consultation process is unclear. They recommend the co-legislators establish a formal and structured mechanism for this consultation rather than leaving it optional.[94]

4 Two key challenges that the digital euro poses for the rights to privacy and personal data protection

[88] Article 5(2) Proposal.

[89] In this respect, we can refer to the work of Manger-Nestler and Gentzsch on the delicate balance that the ECB encounters between democratic legitimation and its independence (see Cornelia Manger-Nestler and Markus Gentzsch, Democratic Legitimation of Central Bank Independence in the European Union (Springer International Publishing 2021) <https://link.springer.com/10.1007/978-3-030-75115-9> accessed 6 June 2024.)

[90] See Annelieke Mooij, 'Digital euro's Legal Framework' (Economic Governance and EMU Scrutiny Unit - European Parliament 2023) PE 747.840 23-25, referencing Case C-11/00 *Commission v European Central* [2003], ECLI:EU:C:2003:395.

[91] The role and supervision of the national central banks should be nuanced, as when acting together as part of the European System of Central Banks, they might be considered as an institution for the purpose of data protection supervision, placing them under scrutiny of the EDPS applying the EUDPR. See Annelieke Mooij, 'Digital euro's Legal Framework' (Economic Governance and EMU Scrutiny Unit - European Parliament 2023) PE 747.840 23-25.

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

[93] 'Joint Opinion 02/2023 on the Proposal for a Regulation of the European Parliament and of the Council on the Establishment of the Digital Euro' (n 87).

[94] 'Joint Opinion 02/2023 on the Proposal for a Regulation of the European Parliament and of the Council on the Establishment of the Digital Euro' (n 87) para 96.

4.1 The unclear allocation of roles and responsibilities among the various actors involved in data processing

As noted by Recital 79 GDPR, '[t]he protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors, also in relation to the monitoring by and measures of supervisory authorities, requires a clear allocation of the responsibilities under this Regulation, including where a controller determines the purposes and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller'. In this sense, a fundamental starting point is determining 'who is who' and 'who does want' within the digital euro framework. In this sense, and while the Proposal tackles this topic, its current wording gives considerable margin for interpretation by both the participants as well as the supervisory authorities. As such, the purpose of this section is to explore the Proposal's current text and determine whether this allocation is clear enough or if further legislative amendments could be necessary given the current state of the legislative process.

4.1.1 Processing of personal data by Payment Service Providers

Article 34 of the Proposal highlights several crucial aspects concerning processing personal data by PSPs, key stakeholders in the digital euro infrastructure. The article addresses various elements, including (i) the legal basis for data processing of certain activities, (ii) a group of critical activities that PSPs will carry out, (iii) types of personal data that can be processed concerning these activities; (iv) the capacity in which the PSPs will engage with regards to personal data involved in these activities; and (v) the adoption of safeguards to avoid the communication of personal data to the ECB. As for the first element contained in Article 34 Proposal, and in contrast to other EU regulations and directives dealing with the Digital Finance Strategy,[95] the text clearly indicates the legal basis that should be used for certain processing activities when personal data is involved in the PSPs' activities with regard to the digital euro: public interest.

However, there exists a potential conflict regarding applicable legal bases. In this sense, Article 34 Proposal refers to 'public interest', including the provision of the offline digital euro capabilities; as noted by EDPB and EDPS, the selection of this legal basis might not be the most suitable since the Proposal would be imposing an obligation on PSPs to engage in the distribution and operation of the digital euro rather than extending an invitation to the system. At the same time, Article 13(6) Proposal suggests that the legal basis for the digital euro services would be a contractual arrangement between the digital currency user and the PSP. In the same vein, EDPB and EDPS have pointed out that Recital 73 would also follow this approach on a contractual basis, particularly for additional services built on top of the digital euro.[96]

Regarding the second element identified (the activities to be carried out by PSPs), questions can be raised about whether other tasks not included in Article 34 Proposal can be performed or if the list provided should be understood as a closed repertory. In this sense, if other activities can be performed, they would need to be structured around a different legal basis, such as consent or the performance of a contract.[97] In a similar sense, as the EDPB and EDPS note, the presence of the word 'including' in Article 34(1)(a) and (c) is not appropriate, as it leaves legal uncertainty regarding the exact tasks for which PSPs can process personal data.[98]

[95] For example, the FiDA proposal and, previously, PSD2.

[96] 'Joint Opinion 02/2023 on the Proposal for a Regulation of the European Parliament and of the Council on the Establishment of the Digital Euro' (n 87) 24.

[97] In this respect, the reliance on these legal bases can be troublesome as they have been interpreted very particularly in the context of financial services. As such, we can briefly mention the issue of consent within the Payment Service Directive 2 and how the EDPB interpreted the provisions in that legal rule (see 'Guidelines 06/2020 on the Interplay of the Second Payment Services Directive and the GDPR' (European Data Protection Board 2020) 1.0.)

[98] Ibid 24.

Another concern relates to the registration and deregistration by PSPs of local offline clients provided for in Article 34(1)(c) Proposal. In this respect, Recitals 34 and 35 indicate that PSPs 'should' perform these activities. Recital 73 would also seem to tie this activity, alongside others, to compliance with AML/CFT legal obligations, just like using an ATM. However, in contrast to ATMs and cash, the offline digital euro would be hosted in local storage that, at some point, would have to (re-)connect with PSPs for funding or de-funding. This situation exemplifies how adopting an account-based approach places additional pressure on ensuring the protection of personal data rights. As AML/CFT activities are data-intensive and they have been criticised for their lack of success in achieving their objectives,[99] it is possible to wonder if stricter measures, such as limiting the activities related to these objectives to merely the registration and de-registration of devices to block balances in case of, for example, theft, should be adopted in the proposed text to protect end-users from undue intrusions and potential unlawful uses of their personal data.

The Proposal also provides extensive powers to the Commission to determine the categories of personal data that can be processed to provide the abovementioned services.[100] These powers present a challenge due to the uncertainty surrounding the scope of activities and services that will fall under the digital euro framework. While, on the one hand, this possibility under Article 34(3) Proposal allows room for the improvement of the digital euro, it does so at the expense of legal certainty to the digital euro users. Yet again, the digital euro proves to be a field of uncertainty compared to the cash it tries to emulate, with details such as specific safeguards being able to be defined down the line.

Turning to the capacity in which PSPs will engage within the digital euro framework, we can identify a notorious tension between the definition of controller under GDPR and the actual activities that PSPs perform. Under the GDPR, a controller defines the means and purposes for processing personal data. This includes deciding all matters pertaining to personal data lifecycle for a given activity.[101] Within the digital euro framework, PSPs are designated as the primary channels for distribution, but they have limited discretion over how personal data processing will be conducted. As noted above, the ECB and national central banks retain a considerable margin for determining how the digital euro operates. Therefore, it is, at least, questionable that these entities do not share any responsibility over how personal data is processed. Moreover, the safeguards mentioned in Article 34 are ambiguous,[102] giving what appears to be a broad discretion to the ECB.

4.1.2 Processing of Personal Data by the European Central Bank and the National Central Banks

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

---

[99] Ronald F Pol, 'Anti-Money Laundering: The World's Least Effective Policy Experiment? Together, We Can Fix It' (2020) 3 Policy Design and Practice 73.

[100] Article 34(3) Proposal allows the Commission to adopt delegated acts changing the categories of personal data processed for the tasks described in article 34(1) Proposal.

[101] 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR' (European Data Protection Board 2021) Guidelines 07/2020 <https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf> accessed 28 July 2021.

[102] The wording employed is as follows' Payment service providers shall implement appropriate technical and organisational measures including state-of-the-art security and privacy-preserving measures to ensure that any data communicated to the European Central Bank and the national central banks or to providers of support services do not directly identify individual digital euro users.'. While the wording used would seem to match the application of the accountability principle under GDPR, the powers vested in the ECB to determine how the digital euro operates would condition the safeguards that can be adopted on the ground.

The Proposal is reasonably clear in the legal basis used by the ECB and national central banks when processing personal data according to Article 35 Proposal.[103] The text mentions that these central banks 'perform a task in the public interest or exercise official authority where they process personal data' for the listed purposes but does not explicitly refer to processing on the ground contained in Article 6(1)(e) GDPR and Article 5(1)(a) EUDPR. This leads the EDPB and EDPS to call for the inclusion of an explicit reference in Recital 76 Proposal.[104]

As with PSPs, the Proposal lists a number of processing activities in Article 35(1)(a) through (e), which leads to the same consideration of whether this is an exhaustive list or not. If not, the same question regarding the applicable legal basis for other processing activities comes to the foreground. Besides this, there are concerns over the key activities. In this respect, 'safeguarding the security and integrity of the digital euro settlement infrastructure and of local storage devices' (Article 35(1)(c) Proposal) poses a challenge to ensure that the offline digital euro acts like cash, as supposedly intended by the Proposal.[105]

In connection with this, Article 35(4) Proposal presents a significant challenge in the digital euro logic. Its latter part states that for the performance of the tasks indicated in Article 35(1), the measures to be adopted concerning personal data '(…) shall include the clear segregation of personal data to ensure that the European Central Bank and the national central banks cannot directly identify individual digital euro users'. As it will be further elaborated, the supposed 'artificial walls' that certain scholars argued the ECB would put in place,[106] are absent in the Proposal. Even if implemented, the Proposal contains elements that suggest the possibility of breaching these 'artificial walls'.[107]

Article 35 Proposal brings to light two additional concerns for the digital euro system under Article 35(7) and (8), each with a corresponding risk data protection: (i) the potential re-centralization of its infrastructure, and (ii) the creation of a single access point for the digital euro.

Regarding the first issue, article 35(7) allows the ECB to provide directly a dispute mechanism as well as a general fraud detection and prevention mechanism. Therefore, there is a risk of consolidating control and data processing in a smaller number of entities, potentially undermining the decentralised nature that digital currencies typically aspire to achieve and, thus, increasing the impact that a single data breach can have.

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

As such, if the ECB and the national central banks have such vast powers to determine the means and purposes for which personal data can be processed within the digital euro framework, then they meet the definition of controller, with the PSPs acting as their processors. The ECB is designated data controller for the purposes outlined in paragraphs 1 and 8 of Article 35. When the ECB carries out a task referred to in those paragraphs jointly with national central banks, they will act as joint controllers for those tasks. In this sense, Recital 25 points out that '[w]hen the European Central Bank establishes

[103] Which refers to Annex IV Proposal for a list of types of personal data, which can be updated by the Commission through the adoption of delegated acts. See article 35(2) and (3) Proposal.

[104] Joint Opinion 02/2023 on the Proposal for a Regulation of the European Parliament and of the Council on the Establishment of the Digital Euro' (n 87) 27.

[105] As discussed previously, the current structure of the offline digital euro incorporates the idea that it can (and requires at some point) a connection towards PSPs, that exposes natural persons' data, leading up to their complete identification. This could impact the ECB's and national central banks' obligations to safeguard the security and integrity of local storage devices.

[106] Mooij (n 90).

[107] As we will discuss briefly below, while a considerable number of operations to be conducted by the ECB and the Member State national central banks will rely on pseudonyms, for example for the settlement phase, this presents two issues: (i) a pseudonym still remains personal data (see for example Case C-604/22 IAB Europe v Gegevensbeschermingsautoriteit. [2024] ECLI:EU:C:2024:214); and (ii) as such, this still causes having to comply with GDPR and solving issues such as joint controllership.

the single access point together with the national central banks, they should be joint controllers.' Based on the existing case law around the notion of joint control,[108] in the current configuration, the ECB and national central banks[109] should be joint controllers together with other digital euro operators in light of the extensive definition of joint controllership in the case law of the European Union Court of Justice,[110] even more so considering the absence of respective responsibilities in the context of the Proposal, as noted by EDPB and EDPS in their Joint Opinion.

Based on the analysis conducted by Soana and de Arruda, who discuss the balance between securing privacy in the digital euro while also trying to promote financial integrity,[111] both of these issues would be at odds with the intention to deploy a digital equivalent to cash.[112] While international organizations, when discussing about CBDCs in general, but also the ECB, when justifying the very essence of the digital euro, argue that certain measures can be adopted to ensure this balance, we share the concerns that the literature has over the fact that this scheme would create an infrastructure that leaves the door open for unrestricted data processing and possible privacy violations.[113]

4.1.3 Processing by providers of support services

Article 36 Proposal introduces rules on the processing by providers of support services. These support services include (i) the provision of fraud prevention and detection capabilities and (ii) the provision of message exchange capabilities for the settlement of disputes.

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

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

Regarding the selected legal basis for these activities, and in contrast to the activities operated by PSPs under Article 34 Proposal, which have a contractual relationship with data subjects, the use of public

---

[108] Paul De Hert and Georgios Bouchagiar, 'Fashion ID and Decisively Influencing Facebook Plugins: A Fair Approach to Single and Joint Controllership or the Introduction of Unbearable Burdens in the Name of Illusory User-Control?' (2021) 7 Brussels Privacy Hub Working Paper series; René Mahieu, Joris van Hoboken and Hadi Asghari, 'Responsibility for Data Protection in a Networked World: On the Question of the Controller, "Effective and Complete Protection" and Its Application to Data Access Rights in Europe' (2019) 10 Journal of Intellectual Property, Information Technology and E-Commerce Law 85.

[109] Either seperatly or as part of the ESCB. See Mooij (n 90) 24-25.

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

[111] Soana and de Arruda (n 21).

[112] It is relevant to discuss that the whole digital euro project presents different semantics, and subsequent implications, depending on which document is consulted. For example, the Proposal presents the digital euro as a digital form of cash rather than a pure equivalent with the same cash-like properties. In this regard, Recital 5 is particularly illustrating of this approach as it presents the digital euro as 'public alternative to private digital means of payments'.

At the same time, and particularly Member States national central banks, seem to have developed a different narrative that presents the digital euro as an equivalent, such as for example in the case of France (see https://www.banque-france.fr/en/monetary-strategy/means-payment/digital-euro, accessed 30 September 2024), Ireland (see https://www.centralbank.ie/financial-system/a-digital-euro, accessed 30 September 2024), the Netherlands (see https://www.dnb.nl/en/innovations-in-payments-and-banking/digital-euro-what-why-and-how/, accessed 30 September 2024) or Spain (see https://www.bde.es/wbe/en/areas-actuacion/sistemas-pago/euro-digital/, acccessed 30 September 2024).

Ultimately, consumers' expectations might play a crucial role in this regard. Individuals will be presented with an instrument that has the same legal tender as cash, will be branded as such but will not have the same privacy-related characteristics.

[113] Soana and de Arruda (n 21) 17.

interest is reasonable, particularly considering that these activities are intended to ensure a healthy and sound financial system. However, simultaneously, it is possible to repeat the same arguments to analyse the PSPs' legal basis and consider that compliance with an obligation would be more fitting.
Regarding scenarios outside the tasks outlined in Article 34 that could involve joint controllership situations, where PSPs with the European Central Bank (ECB) and, eventually, other national central banks jointly determine the purposes and means of processing, the legal bases for data processing present significant challenges.[114] The ability of PSPs to rely on performing a task in the public interest as a legal ground for data processing should be restricted to the purposes listed in Article 34(1). The legal bases for processing personal data vary between the public and private sectors, reflecting their distinct roles, objectives, and purposes. The Article 29 Working Party's Guidelines on Consent under Regulation 2016/679 (GDPR) provide some clarity on the use of multiple legal bases for data processing activities. According to section 5.2 of these guidelines, it is not permissible to rely on multiple legal bases for a single purpose. Once a legal basis for processing has been established, it cannot be changed or interchanged with another. This rule ensures consistency and clarity in data processing activities. On the other hand, regarding the relationship among joint controllers, the EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, note that each joint controller must ensure that they have a legal basis for the processing. Then, in footnote 56, the Guidelines mention that "[a]lthough the GDPR does not preclude joint controllers to use different legal basis for different processing operations they carry out, it is recommended to use, whenever possible, the same legal basis for a particular purpose'. However, the possibility that the joint controllers may base data processing operations aimed at fulfilling the same purpose on various lawful grounds is far from unproblematic. Transparency concerns and the legal basis for data processing are crucial for the rights of data subjects. For instance, when data is processed based on consent, subjects can revoke this consent, obligating the data controller to stop processing the data collected.
Turning to the activities, the dispute mechanism will only concern activities pertaining to the operation of the digital euro, which, as noted by Recital 60, refers to controversies over '(...) situations where the transaction amount differs, where there are duplicates, or where there is no authorization or pre-validation (...) [as well as] situations of identity theft, merchant identity fraud, counterfeit goods.' Considering that monetary transactions can by themselves be considered personal data, these disputes also deal with personal data.

4.1.4 Exercising Data Subject Rights

In the digital euro framework, the lack of clearly defined responsibilities among data processing stakeholders—especially in joint and separate controllership scenarios—may impede data subjects' ability to exercise their rights effectively. This ambiguity also challenges fulfilling the GDPR's information provisions and transparency rules. Notwithstanding that the EDPS and EDPB have highlighted in their Joint Opinion that the proposed decentralised model could enhance the enforcement of data subject rights, with each financial intermediary acting as a controller, any shift towards re-centralization of the digital euro's infrastructure risks negating these benefits, complicating the process for data subjects to exercise their rights and for controllers to adhere to GDPR provisions.

4.2 The potential tension between data minimisation, purpose limitation, and data availability. The cases of fraud detection and AML/KYC

Besides the challenge of allocating responsibilities based on who is a controller and who is a processor, the application and interpretation of certain key principles, mainly data minisation and

[114] EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR point out that joint participation in data processing can occur through a common decision by multiple entities or through complementary, converging decisions. An essential criterion is that the processing must rely on joint controllers' participation, making their roles inseparable and inextricably linked to the determination of the purposes and means of the processing.

purpose limitation, might come across the wide range of data generated as a result of the digital euro's operation. As such, a final point of criticism on the Digital Euro Proposal pertains to potential concerns regarding the application of the data minimisation principle in data protection law.[115] Closely linked to provisions on data protection by design and by default, this principle is traceable to the general requirement of necessity in Article 52(1) of the Charter of Fundamental Rights of the EU ('CFR'). In this respect, we have selected two key activities where this tension might surface: fraud detection and AML/KYC.

4.2.1 Fraud detection

One of the primary digital services for natural persons, according to Annex II of the Proposal, is the '(…) initiation and reception of digital euro payment transactions (...) in the following use cases: (…) point-of-interaction digital euro payment transactions, including point-of-sale and e-commerce'.[116] As such, the digital euro is intended to facilitate both offline and online payments. Particularly in the online Digital Market, fraudulent transactions can be a concrete and tangible barrier to the effective development of e-commerce. To counter fraud using the digital euro, the Proposal incorporates fraud detection and prevention mechanisms.

The Proposal would introduce a broad mandate for the ECB to establish a 'general fraud detection and prevention mechanism'.[117] According to its provisions, the ECB would be free to choose whether it operates this mechanism itself or delegates this responsibility to designated 'providers of support services'.[118] PSPs would provide this mechanism with personal account and transaction data.[119] The involvement of PSPs builds upon previous legislation, [120] which is used as an argument for its transposition to the digital euro.[121] A blind copy-paste of fraud mitigation measures from other regimes would neglect data protection law considerations, which is even more relevant due to the data-driven solutions used.[122] In this sense, the necessity of the proposed measures and the existence of appropriate privacy safeguards should be scrutinised.

Detecting and preventing fraud implies a potential compromise on the fundamental right to data protection, subject to Article 52(1) CFR requirements. The Proposal, as discussed before, intends to create a digital equivalent to cash to meet the needs of the digital economy.[123] However, due to its anti-fraud measures, the text significantly differs from the privacy standards provided by cash. Reviewing transactions, particularly ex-ante, to detect patterns that might give away suspicion involves processing the personal data of the parties to such transactions. This is particularly far-reaching when compared to cash operations, whose features either provide effective anonymity or enable enhanced data subjects' privacy.[124] It should be noted that the added value of the digital euro in terms of data protection compared to commercial payment service providers will depend on its design, with payment anonymity being crucial.[125] The awareness of implementing an ex-ante control system could create a chilling effect that runs counter to the freedom that cash and its digital counterpart should

[115] Article in GDPR, EUDPR and LED. Article 5(1)(c) of the GDPR and Article 4(1)(c) of Regulation (EU) 2018/1725
[116] Annex II Proposal.
[117] Article 32 Proposal.
[118] Article 32(1) Proposal.
[119] Article 32(4) and Annex 5 Proposal.
[120] Recital 5 Proposal.
[121] Under the current e-payments landscape, detecting and preventing fraud falls upon trusted third parties. PSD2 obligates the collection of consent for the execution of transactions on their behalf. See Article 5(i) and (j) PSD2.
[122] Yang Bao, Gilles Hilary and Bin Ke, 'Artificial Intelligence and Fraud Detection' in Volodymyr Babich, John R Birge and Gilles Hilary (eds), Innovative Technology at the Interface of Finance and Operations, vol 11 (Springer International Publishing 2022).
[123] Recital 5 Proposal.
[124]Rodney J Garratt and Maarten RC van Oordt, 'Privacy as a Public Good: A Case for Electronic Cash' (2021) 129 Journal of Political Economy 2157.
[125] Ralf Grötker, Bürgergutachten digitaler Euro. Demokratiefragen einer öffentlich zugänglichen digitalen Zentralbankwährung (Darmstadt: Zentrum verantwortungsbewusste Digitalisierung (ZEVEDI), 2024), 25.

provide. This effect should thus be weighted with the necessity of the measures imposed in the Proposal.

As the EDPB and EDPS note in their Joint Opinion, the provisions relating to the general fraud detection and prevention mechanism contained in Article 32 of the Proposal "lacks foreseeability, undermining legal certainty and the ability to assess the necessity of establishing such measure, which is a necessary requirement for every limitation to the fundamental right to data protection under Article 52(1) of the Charter".[126]The Joint Opinion also points out that the proposal does not demonstrate sufficiently the necessity to establish a general fraud detection and prevention mechanism operated by the ECB "and of providing the appropriate safeguards necessary to make the processing compliant with the principle of proportionality. The EDPB and the EDPS thus invite the co-legislators to further demonstrate such necessity or, should such necessity not be demonstrated, consider less intrusive measures from a data protection perspective".[127] Finally, necessity requires a careful analysis of less intrusive measures. It should be noted, for example, that if algorithmic profiling is used for this purpose, it does not go without risk, as illustrated by past instances like the SyRI case in the Netherlands, where AI-based systems demonstrated the potential adverse impacts of such technology.[128]

Adopting a balanced approach, including necessity and proportionality criteria, involves establishing specific thresholds to differentiate between high-risk and low-risk cases. This assessment considers the severity and scope of the infringement, ensuring a nuanced response tailored to the level of risk involved. More importantly, given the rapid development of this field, these measures should follow international trends and developments on privacy-enhancing technologies and safeguards.[129]

Then, in formulating the operational framework for the fraud detection and prevention mechanism to be adopted, the selection of methods should prioritise those that involve the minimal processing of personal data, in accordance with the principles of necessity and proportionality, taking due count of the guidance and opinions of data protection supervisory authorities. If there is a foreseeable risk that these measures might exclude vulnerable populations from utilising the digital euro, then such mechanisms should not be implemented.

4.2.2 AML/KYC

Both the available literature and policy documents around CBDCs dedicate a considerable amount of attention to the issue of how to integrate the AML legal regime into the operation of these. In this respect, the Digital Euro Proposal is no stranger to this situation, with several provisions dealing with this issue. For example, its Recital 78 indicates that the online digital euro should be subject to AML regulations and, considering that it can enable transactions beyond the proximity that cash requires, Recital 80 furthers confirms this. On the other hand, the offline digital euro, given its intended similiraty to cash, it should be treated on equal terms to it, based on Recital 82.

Beyond the Recitals, and without prejudice to the application of the relevant AML legal rule, Article 37 deals with a set of minimum requirements specific for the digital euro. As discussed in the before, the Proposal envisages a twofold scheme for the digital euro: an online and an offline system. The adoption of an account-based system facilitates the implementation of AML/CFT measures to comply with relevant provisions on the matter. However, as a general, it prohibits the collection of transaction data, In this respect, the Proposal states in its Article 37(2) that '[t]ransaction data shall not be retained

[126] 'Joint Opinion 02/2023 on the Proposal for a Regulation of the European Parliament and of the Council on the Establishment of the Digital euro' (n 87) 21.

[127] Ibidem.

[128] Marvin Van Bekkum and Frederik Zuiderveen Borgesius, 'Digital Welfare Fraud Detection and the Dutch SyRI Judgment' (2021) 23 European Journal of Social Security 323.

[129] For example, see Project Tourbillon for pro-payer privacy CBDC design, https://www.bis.org/about/bisih/topics/cbdc/tourbillon.htm, accessed 5 December 2023.

by payment service providers or by the European central banks and the national central banks.' While the provision is adequate, it has several shortcomings.

First, the Proposal currently lacks a proper definition of what constitutes transactional data within the operation of the digital euro. As noted by EDPS and EDPB,[130] the lack of such a definition further increases the uncertainty over the operation of the digital euro. As such, it is highly difficult to determine whether the principle of data minimisation is adequately complied with as there is no objective point to assess the extent of the data collected during transactions.

Moreover, Article 37 mandates that payment services providers retain funding and defunding data, which includes: '(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.'

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

As noted in different EDPS opinions,[131] finding a balance between AML/CFT and data protection is considerably difficult. This balance should take into account the value citizens pay to privacy in their euro payments.[132] Promoting an offline digital euro as identical to cash when its functionality does not align with cash, apart from ethical concerns, amounts to misrepresentation and a failure to meet the transparency obligations expected from the responsible data controllers involved. However, if the offline digital euro is intended to operate as a cash equivalent, then this design decision brings along the necessity to adopt further safeguards to ensure its privacy-equivalence.

5 Conclusion

The exploration of the digital euro and its implications for data protection reveals several critical challenges and considerations. While it promises enhanced convenience and integration within the digital economy, the proposed currency also introduces significant privacy and data protection concerns. Central to these concerns are the ambiguous allocation of roles and responsibilities among the various actors involved in data processing, as well as the potential conflict between data minimisation and access to data for different purposes. These issues raise risks related to behaviour tracking, profiling, and data security.

Firstly, the unclear distribution of data processing responsibilities among the ECB, national central banks, PSPs, and support service providers creates a complex regulatory landscape. This ambiguity can lead to gaps in accountability, making it difficult to enforce data protection standards effectively.

Secondly, the balance between data minimisation and data availability, particularly for fraud detection, poses another significant challenge. While it is essential to collect sufficient data to prevent fraud and ensure the security of the digital euro, excessive data collection could infringe on individuals' privacy and data protection rights. The current proposal's provisions for fraud detection mechanisms necessitate scrutiny to ensure that they do not lead to disproportionate data processing or create a chilling effect on users' willingness to engage with the digital euro.

Given these challenges, the digital euro framework must incorporate robust data protection measures. This includes establishing clear and precise rules governing data processing activities, ensuring transparency in allocating roles and responsibilities, and adopting data minimisation practices that align with the principles of necessity and proportionality. Furthermore, continuous engagement with

[130] Joint Opinion 02/2023 on the Proposal for a Regulation of the European Parliament and of the Council on the Establishment of the Digital Euro' (n X) 27.

[131] For example, Opinion 12/2021 on the anti-money laundering and countering the financing of terrorism (AML/CFT) package of legislative proposals, European Data Protection Supervisor, 24/9/2021

[132] See the ECB survey referenced in Section 2.5.

data protection supervisory authorities will be essential to effectively address the evolving privacy landscape. Incorporating privacy-enhancing technologies will also play a critical role in mitigating privacy risks and ensuring compliance with data protection standards as new challenges emerge.

From a practical standpoint, the realisation of a privacy-friendly CBDC is contingent upon a design that prioritises data protection by design and by default. A digital euro that fails to ensure privacy protections equivalent to, or exceeding, those provided by physical currency risks undermining public trust in the system. Public trust is essential to the successful adoption and functioning of any CBDC, and legal safeguards must ensure that individuals' rights to privacy and data protection are rigorously upheld.

In conclusion, while the digital euro represents a transformative innovation for the Eurozone's digital economy, its success will depend on the effective integration of comprehensive data protection measures within its legal and technical infrastructure. Privacy and data protection considerations must be given primacy throughout the design and operational stages, with continuous engagement with supervisory authorities to adapt to emerging challenges. Only through such a holistic and rights-based approach can the digital euro achieve both the economic benefits it promises and the necessary trust of its users, securing its role in the future digital economy.

However, to do so, the current regulatory and policy framework around the digital euro needs to be sincere to the public regarding what we can expect from it in clear terms. As noted previously, the very conflicted nature of whether the digital euro will be equivalent to cash or some form of digital money operated by public bodies rather than a private entity needs to be addressed so that the privacy and data protection challenges can be properly identified and tackled. In other words, the digital euro still needs to ask and answer the question of what it wants to be and the public should be made aware of this in a clear and direct manner to avoid failing to meet their expectations, particularly when privacy and data protection have been ranked among the main concerns.