Comment on EDPB Guidelines 02/2025 on the Interplay Between the Use of Blockchain Technology and the GDPR

Submitted by: Dennis Pasveer

Date: 9 June 2025

Contact email: dennis.pasveer@gmail.com

Affiliation: Independent software developer, The Netherlands

Document type: Formal comment on draft guidelines

To the Members of the European Data Protection Board,

In response to the public consultation on Guidelines 02/2025, I submit the following remarks addressing potential inconsistencies and implementation challenges raised by the current draft.

I am submitting this comment as an individual developer active in the European digital economy.

My perspective is grounded in practical experience implementing privacy-respecting tools within EU-based systems. I have a strong interest in ensuring that the European regulatory environment remains both rights-based and technologically workable. I am not representing a particular company or trade association, but I write as an informed practitioner concerned with legal coherence and proportionality.

The draft Guidelines, as currently formulated, raise several legal and technical concerns that I believe warrant reconsideration.

1. Public keys are not always personal data

Recital 26 GDPR says identifiability turns on what is "reasonably likely" given cost, time and technology[1]. The draft presumes that *any* public key can identify a natural person, yet modern blockchain analytics still need substantial off-chain data and specialised tools. A blanket rule therefore exceeds the factual test Recital 26 requires.

2. Proportionality and "state-of-the-art" duty

Article 25(1) GDPR and Recital 78 require controllers to apply measures that are *appropriate* in light of the state of the art and the cost of implementation[2]. Deleting or rewriting a global, permissionless ledger that resides on millions of nodes lies far beyond what is technically or economically feasible. The EDPB proposal disregards the proportionality built into the Regulation itself.

[1] https://www.privacy-regulation.eu/en/recital-26-GDPR.htm
[2] https://gdpr-info.eu/recitals/no-78/

3. Erasure is not absolute

Article 17(3)(b) GDPR exempts data that must be kept for compliance with other legal obligations, and Article 89 allows retention for archiving in the public interest. Blockchains serve auditability, fraud-prevention and, increasingly, financial-market supervision under MiCA. Treating erasure as unconditional ignores these statutory derogations.

4. Controller concept is unworkable for Bitcoin

The draft suggests nodes or a "consortium" should act as joint controllers[3]. In Bitcoin no governance body exists, miners are outside EU jurisdiction and node operators are pseudonymous. Imposing controller duties on unidentified actors contravenes the very definition in Article 4(7) GDPR and cannot be enforced.

5. Direct collision with AML/CTF law

- 2023/1113 Transfer-of-Funds Regulation flags mixers, tumblers and privacy wallets as *high-risk* anonymity tools[4].
- 2024/1624 AML Regulation Recital 160 prohibits EU service providers from offering "accounts allowing for anonymisation"[5].

The draft tells controllers to anonymise data before writing on-chain, yet AML law bans or disincentivises the very techniques that would satisfy the EDPB. The two rule-sets cannot both be met.

6. EU digital-finance policy pulls the other way

MiCA Recital 6 states that a "harmonised framework … should support innovation and fair competition" and must avoid *"unnecessary and disproportionate regulatory burden on the use of technology"* [6]. The draft guidelines, by making ordinary Bitcoin use impossible, contradict the goals of MiCA and the Commission's Digital Finance Strategy[7].

7. Undermining fundamental rights and the Single Market

Forcing destruction of valid ledger entries interferes with the freedom to conduct a business and the right to property under Articles 16 and 17 of the EU Charter. It would also push EU users to non-EU intermediaries, fragmenting the Single Market that MiCA and the Digital Finance Package aim to strengthen.

8. International enforceability is nil

Nodes in the US, Asia or Latin America will not honour EU erasure orders. The draft therefore risks a purely symbolic compliance duty on EU-based actors, creating legal uncertainty without delivering effective protection.

---

[3] https://www.edpb.europa.eu/system/files/2025-04/edpb_guidelines_202502_blockchain_en.pdf
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32023R1113
[5] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32024R1624
[6] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32023R1114
[7] https://finance.ec.europa.eu/news/digital-finance-2024-12-19_en

9. Contradicts recent jurisprudence on privacy tools

The 2024 Dutch *Tornado Cash* judgment treated a mixer as "not a legitimate tool … it is specifically intended for criminals" [8]. The EDPB's own "solution" relies on the same privacy technology the courts and AML regulators have just condemned.

10. Less intrusive alternatives exist

Controllers can already:

- keep personal data off-chain and store only salted hashes;
- rely on key destruction as functional erasure where balances are zero;
- use permissioned sidechains or roll-ups for EU users while leaving the base layer untouched.

These layered approaches align with Recital 78's risk-based, cost-aware standard and avoid the need to "delete the whole blockchain" as envisaged in the draft[9].

I respectfully urge the European Data Protection Board to revise the draft guidelines in light of the technical realities and legal constraints highlighted above. Specifically, I ask the Board to:

a) clarify that blockchain public keys are not inherently personal data, but only potentially so when combined with additional identifiable context, in line with Recital 26 GDPR;
b) address the conflict with AML/CTF regulations by ensuring that recommended privacy measures do not compel actors to breach other binding EU law; and
c) introduce a proportionality-based safe harbour for decentralised and immutable ledger systems, where full GDPR compliance is not technically or legally attainable despite good-faith efforts.

These changes would help preserve the integrity of EU data protection law while maintaining consistency with the Union's broader commitments to digital innovation, regulatory coherence, and the functioning of the Single Market.

Respectfully submitted,

Dennis Pasveer
Nijmegen, The Netherlands

[8] https://www.asisonline.org/security-management-magazine/articles/2024/06/legal-report/
[9] https://www.edpb.europa.eu/system/files/2025-04/edpb_guidelines_202502_blockchain_en.pdf