To whom it may concern,

The draft Guidelines appropriately affirm that Bitcoin addresses may qualify as personal data (§ 3.2) and that the rights to erasure and rectification must remain enforceable (§ 4.2–4.3).

However, the sole technical solution proposed—irreversible anonymisation prior to on-chain recording—is explicitly prohibited or criminalised under the EU's parallel AML framework:

- TFR 2023/1113: mixers, tumblers, or privacy-focused wallets are deemed a "high-risk factor"; complete identification of both originator and beneficiary is required.

- AMLR 2024/1624: CASPs are prohibited from "providing or maintaining accounts or addresses designed to anonymise" crypto-asset transactions.

- French "Narcotrafic" law establishes a presumption of money laundering for operations involving privacy-enhancing techniques.

- Netherlands, Tornado Cash ruling: anonymisation tools are treated as inherently criminal.

As a result, simultaneous compliance with the Guidelines (requiring anonymisation) and the AML framework (prohibiting anonymisation) is unfeasible.

Without further clarification, this creates a regulatory deadlock, rendering any public blockchain inherently unlawful by design.

I respectfully request that the EDPB assess the compatibility of the EU's AML/CFT framework with the GDPR.