To whom it may concern,

The draft Guidelines rightly acknowledge that Bitcoin addresses can constitute personal data (§ 3.2) and affirm the importance of ensuring that the rights to erasure and rectification remain effective (§ 4.2–4.3).

However, the only technical mitigation suggested—irreversible anonymisation before recording data on-chain—is explicitly restricted or criminalised under the EU's parallel AML framework:

- **TFR 2023/1113**: Mixers, tumblers, and privacy wallets are classified as high-risk; full identification of both originator and beneficiary is required.
- **AMLR 2024/1624**: CASPs are prohibited from offering or maintaining accounts or addresses intended to anonymise crypto-asset transfers.
- **French "Narcotrafic" law**: Presumes money laundering in any transaction using privacy-enhancing technologies.
- **Netherlands, Tornado Cash ruling**: Treats the use of anonymisation tools as inherently criminal.

As a result, it is currently impossible to comply simultaneously with the GDPR Guidelines (which encourage anonymisation) and the AML regulations (which prohibit it). This contradiction risks creating a regulatory deadlock in which the use of public blockchains becomes effectively unlawful by design.

I respectfully urge the EDPB to examine the compatibility of the EU's AML/CFT framework with the GDPR, and to provide clear guidance to resolve this conflict.