To whom it may concern,

The draft Guidelines appropriately acknowledge that Bitcoin addresses may qualify as personal data (§ 3.2), and that rights such as erasure and rectification must remain enforceable (§ 4.2-4.3).

Nonetheless, the sole technical safeguard suggested—irreversible anonymisation prior to recording on-chain—is explicitly restricted or criminalised under the EU's concurrent AML legislative framework:

- TFR 2023/1113 designates the use of mixers, tumblers, or privacy wallets as "high-risk factors" and mandates full identification of both originator and beneficiary.
- AMLR 2024/1624 prohibits CASPs from "providing or maintaining accounts or addresses intended to anonymise" crypto-asset transfers.
- French "Narcotrafic" law presumes money laundering for any transaction involving privacy-enhancing technologies.
- In the Netherlands, the Tornado Cash ruling considers anonymisation tools inherently illicit.

This creates a clear contradiction: compliance with the Guidelines (which require anonymisation) appears incompatible with the AML framework (which forbids it).

Absent further clarification, this conflict could result in a regulatory deadlock, effectively rendering any public blockchain illegal by design.

I respectfully urge the EDPB to examine the coherence of the EU's AML/CFT regime with the obligations under the GDPR.