

To whom it may concern,

The draft guidelines acknowledge that blockchain identifiers—such as those used in widely adopted decentralized networks—can constitute personal data, and reaffirm that data subjects must retain their rights to erasure and rectification, even when data is recorded on a public ledger. In principle, these protections are welcome and necessary. However, the only technical measure proposed to reconcile blockchain architecture with these rights—irreversible anonymisation before on-chain publication—is fundamentally at odds with the European Union's anti-money laundering and counter-terrorism financing regulations.

Under the EU's AML framework, tools and methods designed to obscure transaction details are treated not as privacy measures, but as threats. Regulations such as the Transfer of Funds Regulation (TFR) 2023/1113 identify mixers, tumblers, and privacy wallets as high-risk instruments and require full identification of all transacting parties. The AML Regulation (AMLR) 2024/1624 prohibits crypto-asset service providers from offering or maintaining addresses or accounts that facilitate anonymised transfers. In France, recent legislation associated with anti-drug trafficking policies presumes money laundering when privacy-enhancing technologies are used in crypto operations. In the Netherlands, judicial decisions have treated anonymisation protocols themselves as inherently criminal.

This situation creates a structural conflict: the GDPR implies that anonymity may be essential to safeguard personal data, while AML/CFT rules effectively ban any technical approach that allows for it. As it stands, it is not possible to comply with both regimes simultaneously. Attempting to do so places developers, service providers, and users in a regulatory trap, where fulfilling one legal obligation means violating another.

Unless this contradiction is addressed, the logical consequence is that public blockchains—by design transparent and immutable—could become legally incompatible with the European regulatory environment. This would not only undermine innovation but also erode legal certainty for all participants in the digital asset ecosystem.

For this reason, I respectfully urge the European Data Protection Board to assess the underlying incompatibility between current AML/CFT instruments and the fundamental rights framework established by the GDPR.