European Data Protection Board (EDPB)
Rue Wiertz 60, B-1047 Brussels, Belgium

SUBJECT: Critical Statement on the GDPR Interpretation Regarding Decentralized Blockchain Technologies

Dear Members of the EDPB,

In light of ongoing discussions regarding the data protection assessment of public blockchain protocols such as Bitcoin, Ethereum, and similar technologies, we would like to express a number of technical, legal, and ethical concerns arising from the current interpretation of the GDPR and related positions of the EDPB. We submit these concerns in the spirit of democratic engagement and to support the constructive evolution of data protection law.

1. Technical Concerns
- The immutability of blockchain conflicts with the GDPR rights to erasure and rectification (Art. 16/17 GDPR), which are technically unfeasible in this context.
- The absence of a central “data controller” in decentralized networks is incompatible with the requirement set forth in Art. 4(7) GDPR.
- Although the GDPR claims technological neutrality, in practice it disadvantages privacy-preserving and tamper-resistant technologies.

2. Legal Concerns
- The global applicability of the GDPR (Art. 3) is practically unenforceable in the context of decentralized and globally operated protocols, creating legal uncertainty.
- Treating pseudonymous data equivalently to personal data hinders the implementation of effective technical privacy architectures.
- An overly expansive interpretation of the “right to be forgotten” poses risks of de facto censorship and stifling innovation.

3. Ethical and Moral Concerns
- The GDPR emphasizes central control over individual responsibility, potentially undermining citizen-centered data sovereignty.
- Crypto technologies that provide protection from state or corporate surveillance are unjustly cast under general suspicion.
- The focus on blockchain as a “problem” distracts from addressing truly high-risk centralized data processors.

4. Particular Concern Regarding KYC Obligations
- Regulatory KYC (Know Your Customer) requirements compel crypto exchanges to collect extensive personal data and link it to pseudonymous wallet addresses.
- This linkage enables deep profiling and violates the principle of data minimization.
- The compulsory disclosure of such data to state authorities (often without a concrete suspicion) contradicts the fundamental aims of data protection.

CONCLUSION:
We urge the EDPB to reassess the interpretation of the GDPR in the context of decentralized technologies, considering not only legal dimensions but also broader societal and innovation-related implications. A regulation adapted to technological realities is essential for harmonizing privacy rights with digital freedom.

Sincerely,

A. Mutz