The European Decentralisation Institute

Policy Brief: Rethinking Blockchain Regulation under the GDPR: A Call for Technological Alignment

Issued by: European Decentralisation Institute
Date: June 2025

Executive Summary

The European Data Protection Board's (EDPB) "Guidelines 02/2025 on Processing of Personal Data through Blockchain Technologies" aim to align blockchain systems with the GDPR. However, these guidelines risk undermining Europe's digital sovereignty by mischaracterising blockchain as a traditional IT service model rather than a foundational public infrastructure, especially in the case of permissionless blockchains. This brief critiques key assumptions in the EDPB guidelines and provides recommendations for a more accurate and innovation-friendly regulatory approach.

Key Concerns with the EDPB Guidelines

1. **Mischaracterisation of Blockchain as Controllable Infrastructure**

   The EDPB treats blockchain as a technology akin to cloud computing, implying centralised control and deployment decisions. This conflation ignores the nature of permissionless blockchains (e.g., Bitcoin, Ethereum), which are already operational, autonomous infrastructures. Usage occurs by participation, not by deployment choice. This results in impractical assumptions about controllership and privacy-by-design obligations.

2. **Oversimplified Application of GDPR Roles**

   The assumption that entities interacting with blockchains are automatically "controllers" overlooks the distinction between node operation and data determination. On permissionless networks, nodes typically do not determine processing purposes or means; instead, they adhere to software protocols and act similarly to Internet routers or telecommunications relays.

3. **Overly Broad Interpretation of Personal Data**

   The guidelines regard metadata (e.g., public keys, hashes) as personal data, even in the absence of feasible re-identification. This presumption creates legal uncertainty for developers and users and could criminalise the use of privacy-preserving technologies that operate pseudonymously by design and in consequence, effectively driving decentralised innovation out of Europe.

4. **Infeasible Erasure and Rectification Expectations**

   Imposing expectations like the right to erase on immutable infrastructures ignores both technical constraints and the public utility logic of blockchain. The focus should

be on minimising personal data on-chain (data scarcity) and enabling privacy-preserving architectures, rather than forcing technical features that contradict the nature of permissionless blockchain.

5. **Inadequate Distinction Between Blockchain Types**

   The guidelines fail to sufficiently distinguish between permissionless/public and permissioned/private blockchains, as defined in ISO/TS 23635:2022 **"**Blockchain and distributed ledger technologies - Guidelines for governance", adopted as European standard by CEN-CLC/JTC 19 "Blockchain and Distributed Ledger Technologies". Regulatory expectations must reflect these structural differences defined in international standards, especially regarding controllership, accessibility, and data governance.

Strategic Recommendations

1. **Anchor GDPR Interpretation in Blockchain Purpose**

   Recognise the purpose and architecture of blockchain applications, particularly those aligned with permissionless public utility models (e.g. Bitcoin, Ethereum). Regulation must be rooted in the governance intention behind the technology, not merely its technical components.

2. **Redefine Controllers by Use, Not Infrastructure**

   Shift from a provider-centric model of liability to a user-centric one. Entities that initiate state changes (e.g. submit transactions) should bear responsibility where appropriate, while passive participants like nodes should not be held liable by default.

3. **Refine Definition of Personal Data**

   Limit the classification of metadata (e.g., hashes, public keys) as personal data to contexts where re-identification is reasonably likely. Technical and legal standards should prohibit malicious triangulation, rather than prohibit the use of pseudonymous identifiers.

4. **Support Standardisation and International Coordination**

   Acknowledge existing standardisation efforts (e.g. ISO TC 307, CEN-CLC/JTC 19) and the role of decentralised ledgers in frameworks such as eIDAS. Promote a coordinated approach to blockchain regulation under the UN or OECD to ensure global interoperability and compliance. Avoid developing European norms that contradict international legal and technical standards.

5. **Encourage Decentralisation-Aware Policy Design**

Recognise that blockchain operates more like a public utility than a private service. Adapt governance models to reflect decentralised coordination, where participants operate based on mutual protocol rather than contractual arrangements.

Conclusion

Europe's strategic opportunity lies in embracing decentralised technologies that align with its democratic and sovereignty principles. The EDPB's approach, while grounded in valid concerns, risks deterring innovation in Europe if not recalibrated. A more informed, differentiated, and decentralisation-aware regulatory stance will empower Europe to lead in responsible digital infrastructure.

The European Decentralisation Institute is ready to collaborate on this critical agenda.

Contact: Roman Beck | European Decentralisation Institute