Feedback submission to the European Data Protection Board on Guidelines 2025/02 (Blockchain and GDPR)

Submitted by: Fabrizio Degni, Chief AI – AI Ethics and Governance Researcher

GSOM – Politecnico di Milano (Italy)

Date:15-05-2025

Executive Summary

The EDPB's draft Guidelines 2025/02 is a great initiative to define a clear interplay between blockchain technology and the GDPR. However, then I would suggest several changes and improvements to operationalize GDPR principles in blockchain environments related to:

1. Role allocation and legal responsibility in decentralized settings.
2. Ambiguities on data minimisation and "off-chain vs. on-chain" data strategies.
3. Unclear guidance on the right to rectification and erasure ("right to be forgotten").
4. Insufficient practical direction on Data Protection Impact Assessments (DPIAs).
5. Lack of prioritization between permissioned and permissionless blockchains.
6. Overlooked transparency requirements and algorithmic accountability.

---

1. Roles and responsibilities (Section 3.3)

Issue: The current draft lacks a taxonomy for the various actors involved (e.g., miners, validators, smart contract developers, dApp providers) and does not propose a mechanism for joint controllership or governance delegation in decentralized environments.

Recommendation:

- Propose a **role-based risk matrix** outlining the likely obligations and responsibilities of typical actors.
- Introduce a **template governance model** for private-permissioned blockchains to promote accountability.
- Clarify the applicability of *joint controllership* under Article 26 GDPR for DAO-style implementations.

Legal Basis: Article 4(7) and 5(2) GDPR on controller responsibilities; EDPB Guidelines on Controller and Processor Definitions.

---

2. Data minimisation and storage limitation (Section 4.3, 4.6, and 6)

Issue: The Guidelines acknowledge the tension between blockchain's immutability and data minimisation but fall short of providing concrete technical strategies to reconcile this.

Recommendation:

- Encourage the use of **zero-knowledge proofs (ZKPs)**, **selective disclosure credentials**, and **data hashes** instead of storing personal data on-chain.
- Strongly promote a **"hybrid" data storage model** (personal data off-chain, reference data on-chain) with encrypted off-chain vaults.
- Require a demonstrable **"data minimisation audit trail"** to prove efforts made to comply with Article 5(1)(c).

Legal Basis: GDPR Article 5(1)(c) & (e) on data minimisation and storage limitation.

---

3. Right to erasure and rectification (Sections 5.2 and 5.3)

Issue: The document explains the challenge of modifying data on a blockchain but offers no operational solution for reconciling immutability with GDPR rights.

Recommendation:

- Offer **design patterns** for implementing functional erasure via **revocable encryption**, **access token invalidation**, or **tombstoning hashes**.
- Develop a protocol for **"logical rectification"** (e.g., writing a correction transaction that nullifies the previous incorrect entry).
- Introduce a **"state transition ledger" model**, where newer data layers supersede previous erroneous entries.

Legal Basis: Articles 16 and 17 GDPR on the right to rectification and erasure.

---

4. Data Protection Impact Assessment (DPIA) (Section 4.9)

Issue: While the Guidelines recommend DPIAs, they lack an actionable checklist or methodology tailored to blockchain projects.

Recommendation:

- Include a **blockchain-specific DPIA template** as an annex, addressing:
    - Chain governance (public/private)
    - Nature and sensitivity of on-chain data
    - Risk of re-identification
    - Off-chain storage vulnerabilities
- Require explicit assessment of **consensus protocols and key management** as sources of risk.

Legal Basis: Article 35 GDPR; Working Party 29 Guidelines on DPIA.

---

5. Right to transparency and access (Section 5.1)

Issue: The guidelines overlook challenges in identifying the data controller and accessing one's data in pseudonymous blockchain contexts.

Recommendation:

- Encourage **self-sovereign identity (SSI)** frameworks to support data subject access requests.
- Suggest **decentralized identifiers (DIDs)** as a basis for linking identity to transactions while preserving privacy.

Legal Basis: Articles 12–15 GDPR on transparency and access.

---

6. On preference for permissioned blockchains

Issue: While the Guidelines suggest that permissioned chains offer better accountability, they fail to set a clear preference or threshold for adopting them.

Recommendation:

- Clearly recommend **permissioned blockchains** as the default for processing personal data, unless a necessity justification is provided.

- Define **risk criteria** for when permissionless chains might be allowed, subject to enhanced safeguards.

Legal Basis: Recital 39 and Article 24 GDPR on accountability and risk management.

---

7. Practical implementation annex (Missing)

Issue: The document lacks a practical "how-to" annex for compliance teams or developers.

Recommendation:

- Add **Annex C**: "Practical Implementation Guide" with:
    - Risk-based flowcharts
    - Sample consent mechanisms for blockchain apps
    - Case study comparisons (public vs. consortium blockchains)
    - Decision-tree for "on-chain vs off-chain" data mapping

Conclusion

I believe what you did is a pioneering work in addressing the complex interaction between blockchain and data protection law. However, the Guidelines would significantly benefit from more granular, technically informed, and risk-based guidance tailored to real-world blockchain deployments.

Should the EDPB require assistance in further developing these proposals, I am available and honored to participate in working groups.

Respectfully submitted,

Fabrizio Degni

AI Ethics and Governance – GSOM Politecnico di Milano

Fabrizio.degni@gsom.polimi.it

+39 3458810815