EDPB Blockchain Guidelines Combined Feedback (Anonymous Submission)

Submitter: Professional working in the life sciences sector and private individual

Date: 9 June 2025

1. Feedback on Clinical Trials and the Life Sciences Sector

The EDPBs Blockchain Guidelines are a welcome step toward legal clarity. However, they lack sufficient specificity for regulated sectors such as clinical research and pharmaceuticals, where blockchain is being cautiously explored to improve compliance and data integrity.

In clinical trials, blockchain is increasingly tested for:

- Verifying and timestamping informed consent events,
- Providing transparent payments to investigators or sites,
- Creating immutable audit trails for monitoring and regulatory purposes.

In these cases, sponsors define the purpose, but CROs or third-party vendors often operate the blockchain infrastructure. This leads to unresolved issues around controllerprocessor relationships, shared responsibility, and data governance.

The guidelines correctly note that hashed data may still qualify as personal data, particularly when it is possible to link a hash to an individual using off-chain data or reference tables. However, they fall short of providing practical guidance on:

- When hashed metadata (e.g., subject IDs, investigator IDs, consent logs) should be considered personal data in a clinical context;
- How to conduct DPIAs for immutable records involving pseudonymized identifiers;
- How joint controllership applies when multiple parties (e.g., sponsor, CRO, blockchain provider) operate or benefit from the ledger.

Recommendation: The final guidelines should include sector-specific annexes or worked examples. What is appropriate in finance or logistics may be unworkable in regulated health research. A clinical trial annex could address:

- Blockchain-based eConsent tracking,
- Site payment auditability,
- On-chain use of hashes or pseudonymized identifiers,
- How to uphold data subject rights in systems designed to be immutable.

This would support privacy-compliant innovation in areas that could directly benefit patient safety, data integrity, and transparency in research.

2. Feedback on Bitcoin and Decentralized Public Blockchains

As a private individual who lawfully uses Bitcoin, I am concerned that the EDPBs guidelines, if interpreted too broadly, could unintentionally impose GDPR obligations on public, decentralized protocols like Bitcoin.

Bitcoin is a decentralized, open-source network with no central controller or processor. It does not process personal data by design. Any link between a public key and an individual is made off-chain, usually by regulated exchanges or custodiansnot by the protocol itself.

The current draft may be misread to:

- Treat Bitcoin infrastructure as subject to GDPR in the same way as enterprise systems;
- Impose legal obligations on protocol-level activity, which is technically and legally inappropriate;
- Discourage the use of privacy-preserving, decentralized infrastructure that supports individual sovereignty and financial inclusion.

Recommendation: The final version should clearly differentiate public permissionless blockchains (e.g., Bitcoin) from private or permissioned enterprise systems, and confirm that:

- GDPR applies to entities that process personal datanot to the neutral infrastructure itself,
- Protocols like Bitcoin should not be viewed as controllers or processors,
- Open networks remain lawful to use and develop without triggering compliance obligations beyond the application layer.

Such clarification would support a balanced framework that upholds privacy while respecting technological realities and decentralization principles.