Formal Objection to EDPB Guidelines 02/2025

Guidelines 02/2025 on the Processing of Personal Data in Relation to Blockchain Technology

To the European Data Protection Board,

I am writing to express significant concerns regarding the recently published Guidelines 02/2025 on the processing of personal data in blockchain technologies. After careful review, I believe these guidelines, as currently drafted, pose an existential threat to public blockchain infrastructure and innovation within the European Union, while failing to achieve an appropriate balance between personal data protection and technological advancement.

Key Areas of Concern

1. Disproportionate Remedies and the "Blockchain Kill Switch"

The proposal that an entire blockchain may need to be deleted when the erasure of individual personal data is impossible represents a fundamentally disproportionate approach. This is akin to suggesting the deletion of the internet to address specific privacy concerns—a remedy that vastly exceeds the scope of the problem it seeks to address.

Public blockchains represent critical digital infrastructure supporting significant economic and social activity. The suggested remedy fails to recognize the widespread collateral damage such actions would cause to legitimate users, services, and systems dependent on this infrastructure.

2. Structural Bias Against Public Blockchains

The guidelines demonstrate a clear preference for permissioned blockchains over public, decentralized networks. This preference appears to arise from applying centralized data protection frameworks to decentralized systems without sufficient adaptation.

Public blockchains provide unique benefits—including censorship resistance, transparency, and trustless operation—that permissioned systems cannot replicate. By creating regulatory frameworks that systematically

disadvantage public blockchains, the guidelines threaten to eliminate these distinctive advantages rather than finding ways to preserve them while addressing legitimate privacy concerns.

3. Incompatibility with Decentralized Governance Models

Requiring blockchain systems to establish a "data controller" fundamentally misunderstands the nature of decentralized networks. True public blockchains operate without centralized authorities—a feature, not a defect, of their design.

Forcing the designation of controllers would necessitate the introduction of centralized control points, undermining the core value proposition of decentralization and potentially creating new security vulnerabilities and single points of failure.

4. Cross-Border Data Transfer Complications

The global distribution of nodes in public blockchains creates unreasonable complexity under the proposed guidelines' approach to cross-border data transfers. The practical reality of globally distributed validation makes compliance with territorially bound data transfer mechanisms exceedingly difficult without fundamentally altering blockchain architecture.

5. Failure to Recognize Technological Solutions

Perhaps most concerning is the guidelines' apparent dismissal of Privacy-Enhancing Technologies (PETs) such as zero-knowledge proofs and homomorphic encryption. These technologies represent sophisticated approaches to reconciling privacy with blockchain transparency, yet receive insufficient recognition as valid compliance tools.

By ignoring these technological advances, the guidelines miss the opportunity to encourage privacy-by-design approaches that could address many of the identified concerns without destroying the underlying technology.

Impact on Innovation and European Competitiveness

Should these guidelines be implemented as written, Europe risks:

- Driving blockchain innovation offshore to more accommodating jurisdictions
- Preventing European citizens and businesses from participating in global blockchain ecosystems

- Creating a two-tier system where European users are restricted to less capable, permissioned solutions
- Undermining European digital sovereignty by ceding leadership in this critical technology

Proposed Alternatives

I urge the Board to consider the following alternatives:

1. Develop a proportionate, risk-based approach that distinguishes between different types of personal data on blockchains and their associated privacy implications

2. Explicitly recognize privacy-enhancing technologies as valid compliance mechanisms

3. Create blockchain-specific guidance that acknowledges and accommodates the unique architectural characteristics of decentralized systems

4. Establish a technical working group including blockchain developers, privacy experts, and regulators to develop practical, technology-aware standards

5. Implement a regulatory sandbox approach that allows for continued innovation while protecting

fundamental rights

Conclusion

While I fully support the EDPB's mission to protect personal data and privacy, I believe the current draft guidelines fail to strike an appropriate balance between protection and innovation. Public blockchains represent an important technological and social innovation with significant potential benefits for European citizens and businesses.

I respectfully request that the Board reconsider these guidelines with greater attention to technological realities and proportionate regulation that protects privacy without eliminating entire classes of beneficial technology.

Thank you for the opportunity to provide feedback during this consultation period. I look forward to a revised approach that protects privacy while enabling responsible innovation.

Respectfully submitted,

Adam Sobotka
adam.sobotka@duck.com