INATBA
International Association
for Trusted Blockchain Applications

Response to the EDPB Guidelines 02/2025 on processing of personal data through blockchain technologies

Feedback, June 2025

The International Association for Trusted Blockchain Applications (INATBA) welcomes the opportunity to provide feedback on the EDPB Guidelines 02/2025. INATBA represents a global, cross-sector community of stakeholders—including enterprises, SMEs, academia, civil society, and public authorities—working to advance transparent, inclusive, and accountable development of blockchain and distributed ledger technologies (DLTs) in alignment with European values and regulatory frameworks.

We appreciate the EDPB's efforts to bring long needed clarity and acknowledge areas of alignment, such as:

- Discouraging unnecessary on-chain storage of personal data and clarifying that encryption alone is not sufficient;
- Highlighting the risk of joint controllership for nodes in public networks;
- Requiring DPIAs whenever personal data is placed on-chain;
- Insisting on the rights to erasure and rectification being built into system design;
- Reiterating the need for necessity and proportionality in technology choice.

These alignments confirm INATBA's ongoing efforts to embed privacy, accountability, and regulatory compliance into decentralized systems.

At the same time, we must express our serious concerns about the direction of these Guidelines, which risk hindering innovation, limiting competition, and compromising technological neutrality. In particular, the current document places strong emphasis on permissioned systems, presents a binary view of blockchain architecture, and underemphasizes emerging privacy-enhancing technologies (PETs) such as Zero-Knowledge Proofs (ZKP). In addition, we note the absence of practical tools for small and medium-sized actors, who often lack in-house legal expertise. Without accessible templates, concrete examples, or implementation guidance, legal certainty becomes difficult to achieve in practice.

Additionally, the Guidelines provide minimal consideration of global regulatory interoperability. Blockchain networks are inherently transnational, and failing to reflect this reality risks pushing compliant innovation outside the EU and creating legal fragmentation across jurisdictions.

Taken together, these issues risk not only stalling responsible innovation in Europe but also unintentionally privileging certain architectures over others, thereby distorting competition and undermining the EU's stated commitment to technological neutrality.

The following sections provide constructive feedback and actionable recommendations on how the Guidelines might be further strengthened to better support legal certainty, innovation, and fundamental rights.

#1: Public vs. Permissioned Blockchains

The Guidelines (sections §3.3 and §4.2) express a strong preference for permissioned systems. While INATBA agrees that these offer certain governance advantages, we caution against dismissing public blockchains entirely. In many sectors—such as decentralized finance, identity systems, and cross-border registries—public chains are fundamental to transparency and auditability. A blanket preference for permissioned systems risks stifling innovation and ignoring proven models.

Public blockchains can replace intermediaries, thereby providing a privacy benefit. Provided that the privacy benefits outweigh the remaining privacy risks for a user, the GDPR should not prevent a use case that is net privacy positive. At the same time, users should have the freedom to weigh up the risks and benefits of privacy for themselves. Provided they make an informed choice, they should be free to choose between disclosing personal data to an intermediary or disclosing not completely anonymous data on a public blockchain.

The industry has observed that permissioned ecosystems can struggle due to constrained network effects. Notable examples include the collapse of Corda-based consortia such as B3i[1] and TradeIX[2].

Moreover, when there is sufficient justification for a blockchain to be public, processing in third countries does not have to be prevented and Chapter 5 of GDPR does not apply, per the ECJ Lindqvist (C-101/01) ruling. Otherwise, publication of personal data would not be possible.

Key Recommendation:

- Shift from a blanket discouragement to a **risk-based approach**.

[1] B3i, the Blockchain Insurance Industry initiative, filed for insolvency in July 2022 after failing to secure additional funding and facing challenges in achieving industry-wide adoption. https://www.reinsurancene.ws/b3i-fails-to-raise-new-capital-enters-insolvency.

[2] TradeIX, known for its Marco Polo Network, ceased operations due to difficulties in scaling and attracting sufficient participation: https://www.ledgerinsights.com/marco-polo-blockchain-trade-finance-insolvency/?utm_source=chatgpt.com

- Clarify that public chains may be used responsibly, including nodes in third countries, with adequate safeguards, such as off-chain storage, pseudonymization, PETs, or self-sovereign identity (SSI) models.
- Should the Guidelines continue to discourage public blockchains, it can effectively make it extremely difficult to implement certain important real-world use cases that depend on open, permissionless networks.[3]

#2: Layered Architectures and Data Minimization

Hybrid architectures—where only metadata (e.g., hashes or commitments) is stored on-chain—are commonly used to ensure GDPR compliance. These systems decouple identity and personal data from blockchain records, helping meet storage limitation and minimization requirements.

The Guidelines do not clearly acknowledge that full anonymisation of crypto-asset transfers may be technically or legally impossible, due to obligations under MiCA and AMLR. If anonymisation of transaction data is blocked by other regulation, this should not be treated as a GDPR violation regarding the transaction data that would be otherwise anonymisable.-

Key Recommendations:

- In paragraphs §4.2 and Annex – Recommendations of the guidelines, explicitly endorse **layered design models** as a viable method for achieving data protection by design in decentralized contexts.
- Acknowledge that transaction data on blockchains will not be considered to violate GDPR, if identification is only possible because MiCA or AMLR obligates the identification of transaction metadata or key identifiers.

#3: Functional Erasure and Revocation

Because technical deletion is infeasible due to immutability, privacy can still be protected through mechanisms such as:

- Revoking or invalidating credentials and proofs,
- Removing access to off-chain data or invalidating linkage with external data,
- Expiring authorization keys.

[3] For example decentralized aid disbursement cases**:** Humanitarian organizations use public blockchains to transparently track aid payments in conflict zones (e.g., Ukraine crypto donations, UN's World Food Programme pilot). If public chains are discouraged, such projects can't guarantee transparency or cross-border operability.

Key Recommendations:

In section §4.3 of the guidelines, recognize these **functional erasure mechanisms** as legitimate ways to meet GDPR obligations, when paired with appropriate technical and legal safeguards.

#4: Zero-Knowledge Proofs and Privacy-Enhancing Technologies

ZKPs are not speculative—they are being deployed in self-sovereign identity (e.g., Togggle, Privado), decentralized voting (e.g., Vocdoni, Trevo), and privacy-preserving finance (e.g., Zcash, Nightfall by EY). These systems enable verifiability without exposure of personal data.

Key Recommendations:

In sections §4.3 and §5.2 of the guidelines, encourage the adoption of **ZKPs and other PETs** (with giving examples of real world use cases) by elaborating on their role in data minimization, selective disclosure, and functional compliance. Consider a dedicated future annex or thematic guidance paper on practical implementation of PETs in decentralised systems as well as giving examples of use cases the EDPB considers viable.

#5: Practical Guidance for Developers and SMEs

Legal certainty is only meaningful when it can be implemented. The current Guidelines are difficult for non-legal stakeholders to operationalize.

Key Recommendations:

Include or reference a practical annex featuring:

- GDPR role-mapping templates for blockchain networks,
- DPIA templates with blockchain-specific prompts,
- Visual guidance on off-/on-chain architecture choices,
- Links to PET implementation libraries and standards.

This is especially critical for SMEs, startups, and open-source contributors without in-house legal counsel.

#6: Cross-Border Legal Interoperability

Blockchain networks are inherently transnational. Conflicting interpretations of data protection obligations among Member States—and lack of alignment with non-EU regimes—creates uncertainty and limits innovation.

Key Recommendations:

- We encourage the EDPB to continue their dialogue with standards bodies and regulators inside and outside the EU. A shared understanding of lawful decentralized processing will foster innovation while protecting rights.

#7: Hashes of Personal Data

The guidelines mention that "hashes of personal data will still be considered personal data as will any other identifiers that still might exist". This means that hashes derived from personal data are to be treated as personal data, especially when they are used as identifiers to link additional information to individuals. However, hashes of personal data can also be used in other ways. In the context of blockchain, hashes serve to verify existing information. Automatically classifying all hashes of personal data as personal data would lead to the conclusion that an entire blockchain becomes "personal data" if even a single block contains personal data, since each block is cryptographically linked to the next via hashing.

Key Recommendations:

When hashes of personal data are used, it is recommended that the data protection impact analysis will review whether the hashes in that specific context will be able to act as an identifier and have to be considered personal data as they are used in that specific context.

#8: The Practical Role of Nodes in Public Permissionless Blockchains

The guidelines suggest that nodes in public permissionless blockchains could qualify as controllers or joint controllers under the GDPR. We believe this interpretation misrepresents the technical function of nodes, which operate without discretion and simply validate transactions based on predefined protocols. Nodes do not determine the purpose or means of data processing and function more like Internet routers than data controllers. Treating them as controllers could discourage participation and undermine decentralization, which itself enhances privacy. We urge the EDPB to adopt a case-by-case approach that distinguishes between passive infrastructure and active decision-makers.

Key Recommendations:

The guidelines should clarify that node operation alone does not imply controllership, and emphasize that GDPR roles must be assessed based on actual influence over data processing activities.

#9: The Combined Effect of Financial Regulations and GDPR

While financial regulations require the identification of the natural persons behind a transaction, GDPR requires only to put information on public blockchains where the identity behind those transactions is protected against being discovered. On public blockchains this can be achieved using privacy enhancing technology like ZKP, one-time blockchain addresses or ring signatures. However, e.g. Art 76.3 MICAR, prevents exchanges from listing privacy coins that use PET that the EDPB recommends in their proposed guidelines. This could lead to a situation where assets based on public blockchains not employing PET can no longer be traded by natural persons due to GDPR and, conversely, assets based on public blockchains employing PET can no longer be traded due to financial regulation.

Key Recommendations:

The guidelines should clarify that transaction data that can be identified with natural persons only due to financial regulation can be kept on public blockchains as long as the identifiability is limited to the requirements of financial regulation.

Conclusion

INATBA stands ready to collaborate with the EDPB and other regulators to ensure these Guidelines continue to evolve alongside innovation, in a manner that upholds fundamental rights while enabling the full potential of decentralized technologies.

We are concerned, however, that the current approach does not sufficiently reflect the technological advancements and operational realities of decentralized systems. Modern blockchain architectures differ fundamentally from legacy digital infrastructures in how they distribute responsibility, manage data flows, and embed transparency and privacy at the protocol level. Public, permissionless blockchains provide benefits in terms of digital self-determination and privacy by removing the need for intermediaries. These benefits need to be considered when determining the level of acceptable privacy risks in public blockchains. Applying conventional, centralized compliance models to these decentralized environments risks creating not only legal uncertainty but also a chilling effect on innovation in Europe.

Rather than issuing guidance that appears to prohibit by default, the EDPB should encourage the creation of a dedicated framework that actively explores how decentralised technologies can meet high data protection standards through privacy-enhancing technologies, technical safeguards, and system-level accountability. Such an approach would better align with the unique properties of permissionless blockchains, as well as it would be understood as complementary for permissioned blockchain, and support innovation without compromising fundamental rights.

If implemented in their current form, these Guidelines would significantly impact the viability of permissionless blockchain networks and their use across multiple sectors—from finance and digital identity to climate reporting and supply chain traceability. The potential market impact includes: limiting the EU's global competitiveness in blockchain innovation, reducing investment certainty, and discouraging the development of open-source and community-driven infrastructure.

We also recommend removing or reformulating language around "blockchain deletion," which is technically and conceptually misleading. Instead, the Guidelines should focus on data protection measures appropriate to immutable systems—such as access removal, encryption, and off-chain data control—without invoking imagery that suggests destroying parts of a blockchain network.

This feedback is supported by the following signatories:

Niko Demchuk, AMLBot AMLBot	Benjamin Bürgi, Senior Legal Counsel, Cardano Foundation Cardano Foundation	Dr. Jörn Erbguth, President, Geneva Macro Labs, EUBOF Expert
Harris Niavis, Inlecom Innovation inlecom	Natalie Avram and Giannis Rousopoulos, IOTA Foundation IOTA FOUNDATION	Sebastian Becker, thebrainbehind GmbH [tbb*]
Eugenio Reggianini, Independent, ISO TC 307 accredited expert, EUBOF Expert	Daniel Szego, Independent DLT Architect, EUBOF Expert	Dr. Luis Carro, INATBA Academic Advisory Board
Urko Larrañaga Piedra, Independent, Digital Identity and DLT Architect, EUBOF Expert	Francesco Bruschi, Head of Blockchain and Web3 Observatory, Politecnico di Milano, INATBA Academic Advisory Board	Jim Mason, Independent, Identity and Trust Architect, EUBOF Expert

Ingrid Vasiliu-Feltes MD MBA, Institute for Science, Entrepreneurship and Investments, EUBOF Expert	Dr. Joachim Schwerin, Principal Economist, European Commission, in my personal capacity within the INATBA Governmental Advisory Board	Fabio Budris. VP Cognite La. Director ID LATAM, Board SAIA, Chair Blockchain-AI TF INATBA