



IOTA Stiftung, Pappelallee 78/79, 10437 Berlin, Germany


Berlin, June 5, 2025

Dear Chair of the European Data Protection Board,

The IOTA Foundation welcomes the opportunity to provide comments on the EDPB's Guidelines on the interplay between the General Data Protection Regulation and blockchain technology. Drawing on our technical expertise and regulatory experience, we offer the following feedback to support the development of a balanced, technology-neutral, and future-proof approach to data protection in permissionless blockchains. Please reach out to us at [legal@iota.org](mailto:legal@iota.org), if you wish to discuss any of the topics mentioned below in more detail with us.

Sincerely,

DocuSigned by:

  
C11470B4DA0E453...  
Dr. Anja Raden  
Board Member

---

IOTA Stiftung  
[www.iota.org](http://www.iota.org)

[legal@iota.org](mailto:legal@iota.org)

Pappelallee 78/79  
10437 Berlin  
Germany



## **Comment on the fundamental thesis that blockchain data are not personal data**

We support the position that blockchain data, by their nature, should not be considered personal data under the GDPR or similar data protection regimes, for the following reasons:

1. *Structural Design of Blockchain Protocols*  
Most public permissionless blockchains are explicitly designed to avoid direct identification of natural persons. They operate using pseudonymous addresses (public keys), which, without additional external information, do not allow for the identification of a specific individual. The data stored on-chain—such as transaction records or smart contract interactions—are linked to these addresses rather than to real-world identities.
2. *Pseudonomized Data on the Blockchain as personal Data*  
The broad classification of blockchain data as 'pseudonymized' assumes a level of identifiability that often does not exist. Without additional off-chain information, blockchain addresses are typically not attributable to individuals, which significantly limit related data protection concerns.
3. *Contextual Identification Requirement*  
According to established legal interpretation (e.g., Recital 26 of the GDPR), data qualifies as personal data only if a natural person can be identified directly or indirectly, considering all means reasonably likely to be used. In the case of blockchain, the process of identifying a user from an address often requires disproportionate effort, off-chain data, and contextual knowledge that is not accessible or available to the vast majority of participants. Therefore, in most cases, the threshold of identifiability is not met.
4. *Decentralization and Data Control*  
Public blockchains lack a centralized controller or processor who determines how and why data is processed. Node operators in permissionless networks do not process data on behalf of a controller, nor do they independently define the purposes or means of processing. Their role is purely technical: validating transactions based on pre-established consensus rules, without discretion or direct access to identifiable personal data. This absence of a legally meaningful controller–processor relationship calls into question whether the GDPR should apply at all to such decentralized infrastructures. Rather than assuming the presence of personal data by default, regulators should carefully assess whether any entity within a permissionless blockchain actually qualifies as a controller under Article 4(7) GDPR. In many cases, no such actor exists — and thus, the premise of GDPR applicability should be reconsidered accordingly.
5. *Privacy-Preserving Technologies Are Inherent to Many Protocols*  
Emerging privacy-enhancing technologies such as zero-knowledge proofs further obfuscate any potential link between blockchain data and real-world identities. These mechanisms reinforce the idea that blockchain networks can function in a privacy-preserving way without handling identifiable personal data.
6. *Functional and Legal Interpretation*  
The purpose of storing information on a blockchain is typically to establish transparency, auditability, and security—not to track or identify individuals. Treating all blockchain data as

personal data would not only be legally overreaching but also risk undermining the innovation and utility of decentralized technologies.

### **Comment on technological neutrality**

We are concerned that the current draft of the guidelines appears to favor permissioned blockchain architectures over permissionless ones. While it is true that permissioned systems may allow for more straightforward governance and clearer allocation of roles and responsibilities, this architectural preference risks marginalizing an entire class of open, decentralized technologies that offer critical societal and technical value.

Public permissionless blockchains provide unique advantages—such as transparency, immutability, censorship resistance, and open participation—that are foundational to a growing number of use cases in the public interest. These include decentralized finance, self-sovereign identity, open scientific collaboration, and global supply chain accountability. Dismissing or sidelining these architectures in regulatory guidance may inadvertently stifle innovation, hinder user empowerment, and discourage the development of privacy-preserving applications that operate without reliance on centralized intermediaries.

Importantly, GDPR compliance should not hinge on the type of infrastructure used, but rather on the implementation of appropriate technical and organizational safeguards that reflect the nature, scope, context, and purpose of the processing activity. A permissionless system can be designed to align with data protection principles such as purpose limitation, data minimization, and accountability. Through tools such as hashed identifiers, off-chain data management, and zero-knowledge proofs, developers and controllers can achieve meaningful compliance even in decentralized environments.

A technology-neutral regulatory approach is essential to ensure fairness, legal certainty, and continued innovation. By focusing on the risks and responsibilities tied to specific processing operations—rather than the architecture on which they are built—regulators can support more effective and future-proof compliance strategies. Encouraging such flexibility would also help align the guidelines with the broader principles of innovation-friendly regulation that the European Union continues to endorse.

We therefore strongly recommend that the guidelines avoid expressing explicit or implicit preferences for particular blockchain architectures. Instead, they should promote adaptable, risk-based compliance approaches that can be applied across both permissioned and permissionless systems, while recognizing the specific context and challenges each model presents.

### **Comment on the practical role of nodes in public permissionless blockchains**

The guidelines appear to suggest that nodes operating in public permissionless blockchains could, in many cases, qualify as controllers or joint controllers under the GDPR. We believe this interpretation risks mischaracterizing the practical role and technical function of nodes within decentralized networks, and may lead to overly broad and burdensome compliance expectations.

In most public blockchains, nodes participate by validating and propagating transactions according to pre-defined, consensus-based protocols. They do not determine the purposes or essential means of

processing, nor do they have access to user identities or the ability to alter transaction content. Their function is mechanistic and rule-bound, not discretionary. In this sense, nodes act more like Internet routers than data controllers, as they merely facilitate the operation of a decentralized system without shaping its data processing activities.

If the mere operation of a node were to be interpreted as an act of controllership, it could have significant unintended consequences. Such an approach risks deterring participation in open blockchain networks—particularly by individuals or small entities who lack the resources to assume complex legal responsibilities—thereby undermining decentralization. This would be especially counterproductive given that decentralization itself can serve as a privacy-enhancing mechanism by eliminating single points of failure, limiting access to personal data, and distributing trust.

We therefore urge the EDPB to adopt a more nuanced, context-sensitive approach. **Rather than applying a blanket assumption of controllership based on technical participation**, the guidelines should reflect the GDPR's foundational principle that controllership is a factual, case-by-case determination based on actual influence over the purposes and means of processing. Distinguishing between passive technical validation and purposeful data processing is crucial to avoid conflating infrastructure providers with decision-makers.

A more precise assessment of node roles—grounded in functionality and legal precedent—will help ensure that regulatory obligations are proportionate and aligned with the realities of decentralized technologies. This would also support legal certainty and reduce the risk of regulatory overreach in this emerging domain.

### **Comment on the use of off-chain storage as a sufficient safeguard for GDPR compliance**

The guidelines rightly emphasize the importance of data minimization and storage limitation in the context of blockchain technology. However, they could more explicitly acknowledge that well-designed off-chain storage solutions, when paired with cryptographic techniques such as commitments or hashes, can serve as effective and GDPR-compliant safeguards in decentralized environments.

A growing number of blockchain applications—particularly in public permissionless networks—already implement architectures where only non-personal and non-identifying data is recorded on-chain. Instead of storing personal data directly on the ledger, these systems use the blockchain to anchor cryptographic proofs of existence or integrity, while the actual personal data remains securely stored off-chain under the control of the data subject or a designated controller. This architectural separation enables greater flexibility in managing data protection obligations, without compromising the immutability or transparency of the underlying ledger. Such on-chain data should not be considered personal data where identification of a natural person is only possible with disproportionate effort or unlikely in practice.

We therefore encourage the EDPB to explicitly recognize responsible off-chain storage strategies as a valid and effective mechanism for achieving compliance with GDPR, particularly when combined with robust governance and user-centric design. Clear regulatory affirmation of these models would support innovation, provide legal certainty to developers and data controllers, and help ensure that the guidelines remain both practical and forward-looking.

## **Comment on the Evolution of Governance Structures in Public Blockchains**

The guidelines raise legitimate concerns regarding the allocation of roles and responsibilities in decentralized blockchain environments. While this remains a complex issue, it is important to recognize that public blockchain ecosystems are not governance-free zones. They are rapidly developing and experimenting with a variety of governance models aimed at enhancing accountability, transparency, and regulatory responsiveness.

Many of these ecosystems already feature evolving governance frameworks that include foundations, core development teams, technical committees, and increasingly, decentralized autonomous organizations (DAOs). These structures, while still maturing, are beginning to provide mechanisms for collective decision-making, protocol upgrades, and in some cases, active regulatory engagement. Rather than viewing decentralization as a regulatory gap, we believe it should be seen as an area of ongoing innovation, one that is capable of aligning with legal norms through the development of more formalized and transparent processes.

Discouraging the use of public blockchains on the basis of their current governance diversity risks undermining the very innovation that is essential to making these systems more compliant over time. Instead, the guidelines should explicitly recognize and support the positive trajectory of governance development within decentralized networks. Encouraging experimentation with novel governance models—provided they aim to clarify roles, ensure accountability, and respect user rights—will help foster a new generation of GDPR-aligned public blockchain ecosystems without sacrificing the resilience, inclusiveness, and openness that decentralization enables.

We therefore recommend that the guidelines adopt a forward-looking stance that encourages the evolution of governance in public blockchains. By doing so, regulators can support a more constructive dialogue with the ecosystem and help shape governance innovations that are both effective and legally sound.