Fireblocks

Feedback

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

Summary

About us

Fireblocks provides its clients with access to a proprietary software-as-a-service ("SaaS") platform that enables its clients to securely store, manage, and administer their own holdings of digital assets on various blockchains using a combination of encrypted public and private keys and self-created wallets without the assistance or intervention of Fireblocks (the "SaaS Platform").

Fireblocks is a third-party technology vendor founded in 2019. We provide access to and usage of our SaaS platform for enterprise customers globally. Clients enter into agreements with Fireblocks to use the SaaS platform. Fireblocks has a registered office in the UK, and clients throughout the EU. Fireblocks entities are wholly owned by Fireblocks Ltd., an Israeli company and the developer of the SaaS platform. Fireblocks is registered in the EU Transparency Register with number 336761697446-09.

Our views

We welcome the initiative by the European Data Protection Board (EDPB) to issue guidelines on how data privacy requirements could be met when blockchain technology is used. We believe distributed ledger technologies do create new requirements for technology risk management, including in safeguarding privacy. We urge further assessment and nuance in seven key areas:

1. In our view, **classifying blockchain node operators as data controllers** is inconsistent with GDPR expectations that data controllers have clear knowledge of the purposes and means of PII being processed.

2. We are concerned that the proposed **methods to address data subject rights are technology prohibitive**, rather than technology neutral, and we propose alternative approaches to reaching the GDPR privacy objectives.

3. We suggest the development of further guidelines for data minimization and off-chain storage

4. We suggest a clearer role for the concept of linkability in the identification of personal data in the contex of blockchain transactions.

5. We recommend a greater role is given to Data Protection Impact Assessments.

6. We suggest further clarity on how international transfer rules apply to decentralised networks.

7. We discourage language in the Guidelines that creates a preference for the technology choice of permissioned ledgers over permissionless ledgers, and we suggest adequate risk mitigation is outlined for both technology sub-categories.

1. De-classifing node operators as controllers

The Guidelines rightly emphasise the necessity of delineating roles and responsibilities in data processing, including those of controllers, joint controllers, and processors within blockchain ecosystems.

However, further clarity can be introduced in mapping these roles and responsibilities onto decentralised ledger technologies (DLTs), especially public permissionless ones.

Specifically, the Guidelines propose that nodes operating on public, permissionless blockchains could be considered controllers or joint controllers under the GDPR.

We respectfully submit that defining node operators as data controllers under GDPR does not accurately reflect the technical function of nodes in a DLT.

Nodes passively validate transactions according to predefined consensus protocols and do not exercise discretion or determine the purposes or means of data processing. Functionally, they are more comparable to network routers than data controllers.

Even if node operators process personal data, they do so without a clear understanding of the purposes and means of the processing. Therefore, they do not align with the definition of data controllers under the GDPR.

Classifying node operators as controllers is thus disproportionate. It risks deterring participation in decentralised systems. It seems to run counter to the EU broader objectives of regulatory simplification as well as innovation. It could inadvertently undermine the privacy benefits that decentralisation itself provides.

We encourage the EDPB to adopt a more proportionate approach that differentiates between passive infrastructure participants and entities with meaningful decision-making authority over personal data processing.

Recommendation: The guidelines should make clear that operating a node, in itself, does not equate to controllership. The assignment of GDPR roles should be based on an entity's actual influence and involvement in determining the purposes and means of processing. This can be determined by performing a comprehensive Data Protection Impact Assessment.

2. Addressing the trade-off between immutability and data subject rights with technological neutrality

We appreciate the EDPB's recognition of the tension between DLT's architecture-critical aspect of immutability and the exercise of data subject rights under the GDPR, particularly the rights to rectification (Article 16) and erasure (Article 17). While the Guidelines rightly advocate for off-chain storage of personal data as a practical mitigation measure, further clarity is needed on how to address residual risks and exceptions, especially when personal data may be written on-chain inadvertently or through user actions beyond the service provider's control.

In public and permissionless blockchain environments, where any participant can write to the ledger, preventing the inclusion of personal data altogether is technically challenging. For example:

- Metadata embedded in transactions (e.g., public wallet addresses, IP-related data, or user-generated content) may contain or infer personal data.
- Smart contracts may encode user-specific terms or identifiers that become permanently etched into the chain.

These realities present an operational dilemma: once personal data is on-chain, it cannot be modified or deleted without undermining the fundamental structure and trust model of the blockchain.

Recommendations such as “deleting the entire blockchain” undermine the fundamental principle of immutability on which DLTs operate. This leads to significant technology neutrality concerns: if the operation of DLTs is impossible and highly unlikely without the immutability principle being observed, the recommendation to “delete entire blockchains” is technology-prohibitive; it is not neutral.

To avoid propagating technology-prohibitive policies, the following areas can be addressed:

- Clarification on “Effective Erasure” in Blockchain Contexts: The Guidelines could expand on how “effective erasure” may be interpreted where deletion is technically infeasible. For example, could rendering data inaccessible (via key deletion or cryptographic obfuscation) fulfil the intent of Article 17 in certain contexts? A more definitive position would assist controllers in developing compliant blockchain architectures.

- Encouraging the Use of Privacy-Preserving Technologies: Emerging technical solutions—such as chameleon hashes, zk-SNARKs, and commit-reveal schemes—offer promising ways to reconcile blockchain’s immutability with GDPR requirements. While these tools are not yet mainstream, the EDPB’s endorsement or recognition of their potential could incentivise innovation and accelerate adoption.

- Differentiating Between Personal Data and Metadata: The Guidelines should further address whether all on-chain information, such as pseudonymous addresses, transaction hashes, or smart contract identifiers, should be treated as personal data per se, or whether context and re-identifiability thresholds should apply. A more nuanced treatment of these borderline cases would help stakeholders assess risk proportionately.

Recommendation: We urge the EDPB to provide additional interpretive guidance on how data subject rights, particularly erasure and rectification, can be respected in immutable environments, including through alternative technical means. Additionally, we recommend that the Guidelines promote a technology-neutral approach.

3. Data Minimisation and Off-Chain Storage

We support the Guidance advocating for data minimisation and the avoidance of storing personal data directly on a blockchain. This principle is particularly vital given the immutability of DLTs, which can render any inclusion of personal data effectively permanent and inaccessible to modification or deletion.

Many service providers utilise off-chain storage solutions to house any data that could be linked to identifiable individuals, storing only hashed pointers or identifiers on-chain to maintain the necessary functionality without compromising privacy.

To this end, further elaboration in the Guidelines would be helpful in the standardisation of off-chain architectures. While many blockchain service providers adopt off-chain storage to remain GDPR-compliant, the lack of harmonised standards leads to inconsistent implementations and potential security risks.

Recommendation: More concrete guidance or alignment with existing frameworks (e.g., ISO/IEC 27001, NIST) would be valuable to ensure that off-chain environments meet an appropriate threshold for data protection and security.

4. Identifying and Protecting “Personal Data” based on Linkability

We believe the Guidelines would benefit from a more in-depth treatment of the question: what constitutes personal data in blockchain contexts?

While the GDPR defines personal data broadly as “any information relating to an identified or identifiable natural person,” its application to pseudonymous identifiers, public keys, hashes, and metadata in blockchain systems requires nuanced interpretation.

Blockchain systems, especially public permissionless ones, often rely on cryptographic identifiers (e.g., public wallet addresses, transaction hashes, or smart contract interactions) that may not directly identify individuals but could be linked to them through auxiliary data. The

threshold for identifiability and thus the determination of whether data is “personal”, is context-dependent and can vary widely based on available datasets, analytical tools, and the actor’s capabilities.

Areas for Clarification:

- Risk-Based Assessment of Identifiability: The Guidelines could explicitly encourage a risk-based, contextual analysis of whether data is “personal” in a given scenario. For example, a public key may be considered personal data in a retail DeFi application with persistent identifiers, but not in a purely technical infrastructure layer where keys are rotated frequently and no external profiling occurs.

- Linkability and the Role of Pseudonymisation: The potential for linking on-chain data to off-chain identities is a critical vector of risk. Even when only hashed or pseudonymised data is stored on-chain, re-identification may still be possible through external data correlation or behavioural pattern analysis. We recommend that the Guidelines provide concrete examples of what constitutes sufficient pseudonymisation in blockchain settings and differentiate it from anonymisation, which is rarely achievable on-chain.

- Functional vs. Legal Identifiers: In many cases, blockchain systems use identifiers (like wallet addresses) that are essential for system functionality but were not originally intended as personal identifiers. The Guidelines should recognise the distinction between “functional identifiers” and traditional personal identifiers, and suggest appropriate design measures to minimise identifiability risk, such as address rotation, mixers, zero-knowledge proofs, or confidential transactions.

- Over-Classification and Regulatory Chilling Effects:
  If the definition of personal data is applied too broadly and without proportionality, even non-intrusive or privacy-preserving blockchain uses may be captured unnecessarily under GDPR obligations. This risks stifling innovation and discouraging the adoption of

beneficial decentralization practices. A balanced interpretation, grounded in technical realities and actual re-identification risk, would support more pragmatic compliance.

- Forward-looking risk management: Once the risk of re-identification of pseudonymous data stored on chain is assessed via an assessment of linkability, proportionate safeguards, such as cryptographic commitments or zero-knowledge proofs, can be recommended or required.

Recommendation: We recommend that the EDPB provide additional guidance on assessing identifiability in blockchain contexts, including a spectrum of examples ranging from clear cases of personal data to borderline pseudonymous or hashed data. This will help developers, privacy professionals, and regulators alike apply GDPR requirements more consistently and proportionately.

5. Data Protection Impact Assessments (DPIAs)

We strongly support the EDPB's emphasis on conducting Data Protection Impact Assessments (DPIAs) for blockchain-based processing activities. Given the innovative and often complex nature of blockchain systems, DPIAs serve as an essential tool to identify, assess, and mitigate data protection risks early in the design process, aligning with the principles of privacy by design and by default (Article 25 GDPR).

However, we believe the Guidelines would benefit from additional specificity regarding how DPIAs should be tailored to blockchain contexts, particularly where the conventional assumptions of controllership, centralisation, and data lifecycle management do not hold.

Key Areas for Clarification and Support:

- Blockchain-Specific Risk Scenarios: Many of the risks associated with blockchain technologies, such as the irreversibility of data recording, lack of central governance, and potential for linkability or re-identification of pseudonymous data, are not adequately covered by existing DPIA templates or risk libraries. The EDPB could enhance practical compliance by identifying common blockchain-specific risk scenarios (e.g., the use of

smart contracts for automated decision-making, on-chain storage of metadata, or node replication across jurisdictions) and proposing typical risk ratings and mitigation options.

- Decentralised Governance Models and Residual Risk Ownership: In permissionless or consortium-led blockchain networks, no single entity may fully control or influence the data processing operation, which complicates the attribution of responsibility and the implementation of mitigation measures. DPIAs in such environments must account for shared governance models and recognise that residual risks may not always be controllable by a single actor. The Guidelines should provide direction on how to document such scenarios transparently and how to collaborate across entities (e.g., through joint DPIAs or cooperative governance models).

- Pre-DPIA Screening Criteria: Given the unique technical features of blockchain, the Guidelines could recommend screening questions specific to DLT systems to help determine whether a DPIA is required in the first place. For example:

    - Is any personal data being written to the blockchain, either directly or indirectly?

    - Are smart contracts used to trigger automated actions with legal or significant effects?

    - Are nodes or participants located in third countries without adequacy decisions? These criteria would help streamline the risk assessment process for organizations at an early stage of design.

- Collaboration with Developers and Architects: DPIAs for blockchain projects must be cross-functional by nature. Privacy professionals need to work closely with system architects, smart contract developers, and network designers to ensure that privacy risks are correctly understood and appropriately mitigated. The Guidelines should encourage the embedding of DPIA processes into agile and DevOps cycles, particularly in fast-evolving Web3 environments.

Recommendation: We urge the EDPB to develop or endorse DPIA guidance and templates specifically tailored for blockchain applications. These should address the unique technical and governance challenges of decentralized systems, promote standardized risk identification, and provide practical advice on documenting mitigation strategies even in the absence of full control over the processing ecosystem.

6. International Data Transfers

We welcome the EDPB's inclusion of international data transfer considerations in the context of blockchain networks, where nodes may be geographically dispersed and the flow of data often transcends jurisdictional boundaries.

However, the practical application of Chapter V of the GDPR to decentralised blockchain environments remains ambiguous and presents substantial compliance challenges.

In traditional architectures, data exporters can identify recipients, assess the legal environment of the third country, and implement appropriate safeguards such as Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs). In contrast, blockchain participants, particularly in public, permissionless networks, cannot easily identify where nodes are located, nor who controls them, making it nearly impossible to determine if a transfer has occurred, let alone establish a lawful mechanism for it.

Key Challenges and Areas Needing Clarification:

- Definition of "Transfer" in Decentralised Systems:
  The Guidelines would benefit from a more precise definition of what constitutes a "transfer" in blockchain settings. For instance, is it a transfer when a transaction is validated by a node located in a third country, even if the transaction was initiated within the EEA? More clarity on when and how blockchain activity triggers the transfer regime would support consistent application of GDPR obligations.

- Applicability of Transfer Mechanisms (e.g., SCCs, BCRs):
  Current mechanisms for international data transfers were designed with centralised data exchanges in mind. Their application in open networks, where data may be propagated to unknown entities in unknown jurisdictions, is highly impractical. The Guidelines should acknowledge this gap and provide interim solutions or endorse alternative approaches (e.g., contractual obligations at the application layer, technical access restrictions, or architectural segregation between EEA and non-EEA nodes).

- Risk-Based Approach to Global Validation: In many blockchain use cases, the on-chain data is either pseudonymised or rendered non-personal via robust design strategies (e.g., storing only hashes or encrypted values). In such contexts, the risks traditionally associated with international transfers are significantly reduced. We encourage the EDPB to adopt a proportional, risk-based perspective when considering enforcement of transfer rules for blockchain systems.

- Support for Privacy-Enhancing Network Designs: Emerging blockchain designs, such as permissioned networks with geographic node controls or consortium chains with enforced jurisdictional restrictions, offer practical avenues for transfer compliance. The Guidelines could highlight these as examples of best practice, encouraging privacy-aware architecture design.

Recommendation: We recommend that the EDPB provide greater clarity on how international transfer rules apply to decentralised networks, and explore the development of transfer-compliance frameworks specifically tailored for blockchain systems. Additionally, the EDPB should consider recognising the value of technical and organisational measures that reduce re-identification and cross-border exposure as part of a proportionate risk-based assessment.

7. Refrain from creating policy preferences for permissioned DLTs

The Guidelines state that “Permissioned blockchains [...] offer a clearer allocation of responsibilities, which is a key element for the protection of data subjects, and organisations should favour permissioned blockchains.”

We submit to the Board that the allocation of responsibilities, in terms of system architecture, is as clear in permissioned as it is in permissionless DLTs. However, we acknowledge that permissioned DLTs typically allocate responsibilities to fewer and more clearly identifiable persons.

The presence of identifiable legal entities in the maintenance of a data network is one approach to privacy-preserving governance. Avoidance of centralized data monopolies is an alternative privacy-preserving governance approach, as it typically performs stronger in terms of resilience, censorship resistance, collusion resistance, and user data ownership.

We encourage, once again, the EDPB to adopt a technology-neutral approach to its Guidelines, refraining from creating a regulatory advantage for developers of permissioned DLTs.

The choice of DLT model, as stated elsewhere in the Guidelines, should be a function of its need, use, design, and governance. Permissionless DLTs do offer privacy disadvantages, which the Guidelines explicitly assess, Yet, permissionless DLTs also offer privacy advantages, which the EDBP does not explicitly asses. Thus, we encourage a more balanced exploration of both aspects. This would allow industry participants to assess each DLT on its unique merits, of which the permissioning model is just one.

Finally, we urge the EDPB to focus on achievable data protection outcomes rather than strict structural alignment.

Recommendation: We recommend that, in order to uphold the principle of technological neutrality and adopt a risk-based, architecture-sensitive approach to blockchain privacy, EDPB assess how decentralization can contribute to privacy protection outcomes.

Conclusion

The EDPB's Guidelines 02/2025 provide a foundational framework for aligning blockchain technologies with GDPR requirements. By addressing the nuances highlighted above, the Guidelines can offer more comprehensive support to organisations striving for compliance in this evolving landscape.