bitkom

Position Paper

June 2025

Bitkom on the EDPB's »Guidelines 02/2025 on processing of personal data through blockchain technologies«

Summary

Bitkom welcomes the initiative of the European Data Protection Board (EDPB) to provide clarity through specific guidelines on the application of the GDPR to blockchain technologies. The draft provides a sound basis for discussion, but at the same time raises questions in several areas – particularly with regard to technical feasibility, innovation-friendliness and legal enforceability in decentralised infrastructures.

Blockchain technology offers a wide range of opportunities for trustworthy digital infrastructures. Data protection and innovation are not mutually exclusive – they must be considered together and interlinked in a technically and legally sound manner.

1. Ensuring Technological Neutrality and Practical Applicability

We support the EDPB's objective of strengthening data protection in the development and operation of blockchain applications. However, the proposed measures should be formulated in a technology-neutral and practical manner. In particular, the immutability of data should not be viewed as an obstacle across the board, but must be taken into account appropriately in combination with encryption, pseudonymisation and off-chain storage.

In certain contexts – such as for evidence management, documentation of rights or in digital evidence systems – the immutability of data can create considerable added

value in terms of transparency and trust. These characteristics should not be considered a general shortcoming in the context of data protection.

The blanket classification of blockchain addresses or public keys as personal data should also be viewed in a differentiated manner. The decisive factor is whether it is actually possible to draw conclusions about a natural person. Separating identity data from information stored on-chain and using pseudonymised address structures can contribute to GDPR compliance.

The guidelines should also recognise that the decision for or against the use of a particular technology – such as blockchain – also has implications for innovation and trust. The blanket recommendation to resort to alternative technologies in cases of doubt can have an inhibiting effect on innovation. It should be sufficient to demonstrate that data protection requirements are met in technical and organisational terms, regardless of the chosen technology stack.

2. Purpose Limitation & Justification of Technology Use

The guidelines suggest that the use of blockchain technology itself must also be documented and justified. For example, in the sense of strict purpose limitation or as part of a data protection impact assessment. This requirement should be framed with a sense of proportion. As long as data protection obligations are fulfilled, the question of whether blockchain is appropriate for a particular application should be left to the technical and regulatory discretion of those responsible.

3. Data Protection by Design and by Default

The requirement to integrate GDPR requirements as early as the design phase is crucial. At the same time, the guidelines should recognise that many applications already rely on proven protective measures such as:

- off-chain-storage of sensitive data,
- cryptographic hashing and commitments,
- homomorphic encryption,
- selective disclosure through verifiable credentials to mitigate data protection risks.

These approaches should be recognised as compatible with the GDPR and thus actively promoted.

Practical example: Qualified Electronic Ledger (QEL) as a «Data Protection by Design and by Default» infrastructure

One example of privacy-friendly design in ledger-based infrastructures is the Qualified Electronic Ledger (QEL) in accordance with Art. 45i eIDAS 2.0. This enables immutable, auditable proof of digital events without storing personal data directly on-chain. Data

protection is ensured by measures such as hashing with Salt, off-chain referencing and revocation of decryption keys.

As a qualified trust service, the QEL is subject to a conformity assessment and meets strict requirements from the GDPR, NIS2 and other security standards. It thus exemplifies how data protection and immutability can be combined technically and organisationally.

In addition, QEL or similarly structured DLT infrastructures enable privacy-preserving verification mechanisms, for example in the context of verifiable credentials, trust lists or revocation mechanisms. The EDPB guidelines should take up such positive practical examples and present the possibilities of technology-based data protection in a differentiated and future-oriented manner.

4. Right to Erasure and Data Minimisation

We support the principle of not storing personal data on-chain at all, or only in minimised form, wherever possible. At the same time, the guidelines should clarify:

- That the right to erasure can be fulfilled by revocation or destruction of decryption keys or deleting the off-chain component,
- that pseudonymised on-chain data that is not reasonably likely to be re-identified is not considered personal data per se.

For off-chain data stored in connection with blockchain systems, it should also be ensured that deletion is technically feasible. The use of automated deletion mechanisms, as well as sharded or distributed data storage, can contribute to GDPR compliance in this regard.

Within the framework of the GDPR, different interpretations and technical implementations of the right to erasure are being discussed. The EDPB guidelines on blockchain technologies provide initial indications of how this right can be implemented technically – for example, by separating on-chain and off-chain data or by anonymisation.

However, key questions remain unanswered:

- Can the EDPB clarify whether and when encryption combined with key destruction is considered effective deletion within the meaning of Art. 17 GDPR? (para. 51)
- What standards apply to anonymisation or pseudonymisation, in particular with regard to «means reasonably likely to be used» as referenced in Recital 26 GDPR?
- The guidelines include: «[...] this may require deleting the whole blockchain». How is this statement to be understood in the context of decentralised infrastructures – in particular permissionless blockchains without a central control authority? (para. 62)

European case law (including Google Spain, C-131/12; Nowak, C-434/16) shows that deletion can be understood in a context-dependent manner – for example, as access restriction, rendering unusable or actual destruction. The EDPB should therefore clarify

which measures – depending on the blockchain architecture – are considered compliant with Article 17 GDPR.

5. Responsibilities and Governance

The assessment that decentralisation does not constitute an exception to the GDPR is understandable.

The GDPR – in particular Article 26 GDPR – offers a suitable set of instruments with the concept of joint responsibility. The European Court of Justice has clarified in several rulings (Wirtschaftsakademie (C 210/2016), Fashion ID (C 40/2017)) that even actors with limited influence on processing can be considered joint controllers if they jointly decide on the purpose and means or enable data processing.

The EDPB guidelines emphasise that, in order to clarify responsibilities, particularly in the case of public, permissionless blockchains, it makes sense to form consortia or legal entities that can act as joint controllers. This creates legal certainty and enables clear governance structures, which are essential for compliance with the GDPR.

It is crucial to clearly distinguish between infrastructure operators (e.g. validators, miners) and application operators (e.g. DApps, smart contracts). Responsibility for data protection-compliant processing lies primarily with those actors who decide on the purposes and means of processing – usually at the application level. This role model can be usefully compared to the established relationship between cloud providers and cloud users: there, too, data protection responsibility lies with the application operator, not with the cloud infrastructure provider, who merely provides the technical basis.

This analogy underscores the relevance of a functional view of responsibility. Just as cloud providers are not held responsible for all data processing carried out via their infrastructure, infrastructure actors in blockchain systems should not automatically be classified as data protection controllers – neither in permissionless nor in permissioned networks. Instead, risk-based and purpose-related criteria are decisive, such as whether an actor has actual influence on data processing or merely enables it technically.

A blanket assignment of data protection responsibility should therefore be avoided and replaced by differentiated, functionally justified criteria. In this way, the governance of blockchain systems can be designed to be GDPR-compliant without ignoring the technological peculiarities and decentralised nature of the infrastructure.

Furthermore, differentiated criteria are needed to properly determine responsibilities in decentralised structures. The guidelines should:

- promote clearly defined governance structures.
- establish realistic guidelines for dividing roles between controllers and processors.
- recognise role concepts and technical access restrictions (e.g. Layer 2 or permissioned subsystems) as a means of sharing responsibility in accordance with the GDPR.

- Identify specific examples or case groups for joint responsibility in the blockchain context (e.g. for smart contract platforms, multi-signature wallets or operator roles in DApps) in order to make the application of Art. 26 GDPR more tangible in practice.

At the same time, the transparency of blockchain in areas such as audit trails, supply chain transparency or identity management can be a means of strengthening accountability and traceability within the meaning of the GDPR.

6. International Data Transfers

The blanket classification of public blockchains as potential third-country transfers is insufficient. It should be recognised that purely technical references (hashes, links) **do not constitute a «transfer» of personal data** within the meaning of Chapter V of the GDPR – especially if there is no additional identifiability.

In addition, the risks posed by indirect identifiability via off-chain metadata, e.g. IP addresses or wallet links at exchanges, should be addressed. From a data protection perspective, the minimisation of metadata and the targeted use of aggregation or obfuscation techniques should be supported.

7. Recommendation on Standardisation, Security & DPIAs

We support the proposal to conduct data protection impact assessments (DPIAs) for sensitive blockchain applications. At the same time, the development of technical standards for data protection-compliant blockchain solutions (e.g. within the framework of ISO, ETSI, W3C) should be actively supported and listed in the guidelines as a sensible measure.

Security aspects should also be taken into account: the protection of private keys – e.g. through HSMs – as well as protection against 51% attacks or potential risks from future technological developments (e.g. quantum computing) are essential in order to consider data protection and system security together.

Concluding Remarks

Bitkom is all for actively utilising and further developing the potential of blockchain technology – in line with effective and responsible data protection.

Regulatory guidelines should not hamper the technology with rigid requirements, but rather open up ways in which «data protection by design and by default» can be implemented intelligently.

The guidelines should explicitly clarify that existing blockchain systems – including those that are publicly accessible and decentralised – can continue to be operated and used in accordance with the principles of the GDPR. Unduly restricting such

technologies through overly narrow interpretations of specific provisions would not only weaken European innovation, but also jeopardise Europe's ability to keep pace with global technological developments.

Bitkom represents more than 2,200 companies from the digital economy. They generate an annual turnover of 200 billion euros in Germany and employ more than 2 million people. Among the members are 1,000 small and medium-sized businesses, over 500 start-ups and almost all global players. These companies provide services in software, IT, telecommunications or the internet, produce hardware and consumer electronics, work in digital media, create content, operate platforms or are in other ways affiliated with the digital economy. 82 percent of the members' headquarters are in Germany, 8 percent in the rest of the EU and 7 percent in the US. 3 percent are from other regions of the world. Bitkom promotes and drives the digital transformation of the German economy and advocates for citizens to participate in and benefit from digitalisation. At the heart of Bitkom's concerns are ensuring a strong European digital policy and a fully integrated digital single market, as well as making Germany a key driver of digital change in Europe and the world.

Published by

Bitkom e.V.

Albrechtstr. 10 | 10117 Berlin

Contact persons

Frederic Meyer | Policy Officer Blockchain

T +49 30 27576-161 | f.meyer@bitkom.org

Elena Kouremenou | Policy Officer Data Protection

T +49 30 27576-425 | e. kouremenou@bitkom.org

Responsible Bitkom Committee

WG Blockchain

WG Data Protection