Deloitte.

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

Deloitte Contribution

Deloitte “Privacy & Digital Regulation” (Italy) welcomes the opportunity to contribute to the public consultation launched by the European Data Protection Board (EDPB) on the draft guidelines addressing the interplay between blockchain technologies and the General Data Protection Regulation (GDPR).

Deloitte supports the EDPB’s efforts to establish legal clarity for blockchain use cases under the GDPR and aligns with the Board’s overarching principle that technological innovation must remain compatible with fundamental rights and freedoms.

In this regard, Deloitte promotes a vision of sustainable innovation, whereby distributed ledger technologies (DLTs) are designed and deployed in ways that respect and operationalise key principles of the GDPR, including:

- Lawfulness, fairness and transparency (Article 5(1)(a),
- Purpose limitation (Article 5(1)(b)),
- Data minimisation (Article 5(1)(c)),
- Storage limitation (Article 5(1)(e)),
- and the principle of accountability (Article 5(2)).

Moreover, Articles 25 (Data protection by design and by default), 32 (Security of processing), and 35 (Data Protection Impact Assessment) are of particular relevance when assessing blockchain-based systems, especially in scenarios where immutability or decentralisation might create tensions with the rights to rectification or erasure (Articles 16 and 17).

Deloitte's contribution to this consultation is grounded in practical experience advising on blockchain governance models, privacy-enhancing technologies (PETs), and GDPR compliance strategies across multiple sectors. We particularly support the EDPB’s emphasis on clear role allocation, necessity assessments, and privacy-by-design mechanisms.

This contribution suggests a number of clarifications and proposed amendments, particularly aimed at:

- Enhancing the technical precision of the document in describing blockchain architectures and consensus mechanisms;
- Reflecting more clearly the diversity of blockchain implementations;
- Emphasising the role of cryptographic techniques and decentralised governance in data integrity, auditability, and transparency.

1. Introduction

Point 1 – Original Text:

The concept commonly referred to by the term blockchain addresses a technology that implements a distributed and consistent database without centralised management and its coordinated use by an open or predefined set of participants according to an agreed upon set of rules.

Comment:

The original sentence implies that blockchain operates only in an "open" environment, excluding permissioned models. Moreover, referring to blockchain as a "database" is reductive and technically inaccurate, as blockchain is better described as a distributed ledger with append-only capabilities and specific consensus logic.

Proposed Revision:

Blockchain refers to a distributed ledger technology (DLT) that enables the secure and immutable recording of transactions across a network of nodes without the need for a central trusted authority. Depending on the implementation, participation may be open (public blockchain) or restricted to authorized entities (permissioned blockchain). Transactions are validated and synchronized across participants through consensus mechanisms and may be governed by predefined logic, such as smart contracts.

Point 3 – Original Text:

disintermediated (validation of data added to the database does not need the endorsement of a trusted or central party, but rather the agreement of participants in the blockchain)

Comment:

The term "disintermediated" is often used in economic literature and may not reflect the technical nature of blockchain systems. "Decentralized" better captures the architectural and governance characteristics. Additionally, "party" is vague, "authority" is more accurate for the context. Lastly, "agreement" simplifies the concept of consensus algorithms, which are fundamental technical components.

Proposed Revision:

decentralized (validation of data added to the ledger does not require endorsement by a central authority, but is based on a consensus mechanism involving independent participants in the blockchain)

Point 3 – Additional Revisions:

consistent and tamperproof (any update or removal of validated data can be detected)

Comment:

This phrase may mislead readers into thinking that blockchain offers strong consistency in a traditional sense. In practice, especially in proof-of-work systems, consistency is eventual: different nodes might temporarily hold diverging versions of the chain. Moreover, "tamperproof" is better described by the term "immutability," which is more accurate. Finally, the current wording underplays the auditability benefit of blockchain[1].

[1] See: Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

Proposed Revision:

immutable and auditable (once transactions are validated and added to the blockchain, they cannot be altered or removed without detection, ensuring integrity and auditability)

Point 3 – Original Text:

transparent (access to data and its auditing is available to all participants in the blockchain)

Comment:

This statement assumes a public blockchain model, while the paper later discusses permissioned blockchains. For accuracy and inclusiveness, the phrase should acknowledge that transparency depends on the blockchain model[2].

Proposed Revision:

Transparent (in public blockchains, all participants have access to data and its auditing; in permissioned systems, transparency is available to authorized parties)

Point 6 – Original Text:

One of the main promises of blockchain technologies is that they can offer strong technical guarantees in terms of integrity and availability due to the cryptographic tools used (hashing and digital signatures) and the decentralised storing system. However, this is a general assumption; in practice, there may not be standardised or formal agreement on the level or quality of service provided.

Comment:

The guarantees should include traceability, which is an inherent property of blockchain's chronological and transparent record structure. The term "decentralised storing system" is vague and should be replaced with "decentralised replication of the ledger across multiple nodes."

Proposed Revision:

One of the main promises of blockchain technologies is that they can offer strong technical guarantees in terms of integrity, availability, and traceability due to the cryptographic tools used (hashing and digital signatures) and the decentralised replication of the ledger across multiple nodes. However, this is a general assumption; in practice, there may not be standardised or formal agreement on the level or quality of service provided.

Point 7 – Original Text:

it cannot individually be altered or removed without being detected as an inconsistency in the chain.

Comment:

This formulation may erroneously imply that alteration is technically possible but merely results in detection. However, due to the cryptographic linking of blocks and the distributed consensus model, any unilateral alteration is computationally infeasible in practice. Therefore, a more accurate formulation should emphasise the effective impossibility of alteration, grounded in the blockchain's immutable design.

ISO/TR 23244:2020 – Blockchain and distributed ledger technologies — Privacy and personally identifiable information protection considerations.

[2] See: https://eprint.iacr.org/2022/1440.pdf

Proposed Revision:

it cannot be individually altered or removed, due to the immutable structure of the blockchain, which is underpinned by cryptographic linking and consensus mechanisms. Any unilateral modification would not only break the chain's integrity but also be computationally infeasible without control over a majority of the network's nodes (e.g., a so-called "51% attack"), which is highly improbable in well-distributed networks. Furthermore, proposed changes to blockchain protocols or ledgers typically require a collective agreement among participants, often realised through mechanisms such as hard forks, rather than unilateral edits.

Point 9 – Original Text:

In particular, regarding the application of the principles of minization and storage limitation, and the effective exercise of rights like erasure and rectification

Comment:

There is a spelling error: "minization" should be corrected to "minimization" to align with the terminology in Article 5(1)(c) GDPR.

Proposed Revision:

In particular, regarding the application of the principles of minimization and storage limitation, and the effective exercise of rights like erasure and rectification

3. DESCRIPTION OF THE TECHNOLOGY OF BLOCKCHAINS

Point 15 – Original Text:

Blockchains provide a distributed database consisting of a public ledger of use-case specific transactions.

Comment: Referring to blockchains as a "database" is inaccurate and reductive. Technically, they are distributed ledgers specifically designed to ensure immutability and transparency, not general-purpose databases.

Proposed Revision:

Blockchains implement a distributed ledger that records use-case-specific transactions in a transparent and immutable manner.

Point 15 – Original Text:

Participants can use their own node(s) with a copy of the ledger or rely on the ledger of other nodes. The consistency and integrity of all ledgers is crucial for achieving a consensus and realised by two core principles:

Comment:

The phrase "a copy of the ledger" may suggest multiple inconsistent versions. It is more accurate to describe participants as maintaining a local copy of the same ledger. Also, consensus is defined in the white paper of each blockchain.

Proposed Revision:

Participants may operate their own node(s), maintaining a local copy of the distributed ledger, or rely on copies maintained by other nodes in the network. Ensuring the consistency and integrity of these copies is crucial for achieving consensus, which is governed by the blockchain's protocol.

Point 15 – Original Text:

First, sets of transactions are denoted as blocks. Each block is always cryptographically linked to its previous block, so that all blocks form a chain.

Comment:

"Denoted" could be inaccurate. Transactions are grouped into blocks. It's important to mention that each block includes the hash of the previous one.

Proposed Revision:

First, sets of transactions are grouped into structures called blocks. Each block is cryptographically linked to its previous block by including its hash, forming a continuous chain.

Point 15 – Original Text:

Second, a consensus algorithm is used to agree on the one valid block that will be appended to the chain.

Comment:

The sentence could be made clearer by emphasizing the consensus among participants.

Proposed Revision:

Second, a consensus algorithm ensures agreement among participants on the one valid block to be appended to the chain.

Point 16 – Original Text:

Nodes communicate with each other and use a consensus mechanism to ensure the consistency of the blockchain.

Comment:

Blockchains provide eventual consistency, not immediate consistency.

Proposed Revision:

Nodes communicate with each other and use a consensus mechanism to reach agreement on the state of the blockchain, thereby ensuring eventual consistency.

Point 17 – Original Text:

The proof of work mechanism implies that the new block includes the solution of a resource-intensive mathematical puzzle, while the proof of stake mechanism implies that the node that generates the next block is chosen via various combinations of random selection and token of implication in the blockchain (like for example account balance or account age).

Comment:

"Token of implication" is technically incorrect. The proper term is "staking" which involves locking tokens as collateral.

Proposed Revision:

The proof of work mechanism requires that the new block includes the solution to a resource-intensive mathematical puzzle. In contrast, the proof of stake mechanism selects the node that generates the next block based on a combination of random selection and the staking of tokens, which may depend on parameters such as account balance or account age.

Point 24 – Original Text:

The initial concept of blockchain includes transactions where the identities of the parties involved are visible to all.

Comment:

Identities are not directly visible; public keys or wallet addresses are pseudonyms. This should be clarified.

Proposed Revision:

In the original concept of blockchain, transaction data are publicly visible, including pseudonymous identifiers (such as wallet addresses) of the parties involved.

4. EVALUATING BLOCKCHAIN-BASED PROCESSING

Point 45 – Original Text:

Some of these non-compliance risks can be easily mitigated through technical measures upfront, while finding a solution for other risk might may be challenging at this stage.

Comment:

There is a spelling error: "might may" should be corrected to "might".

Proposed Revision:

Some of these non-compliance risks can be easily mitigated through technical measures upfront, while finding a solution for other risk might be challenging at this stage.