May 22, 2025

Processing of Personal Data through Blockchain Technologies – EDPB Draft Guidelines

Client Updates

Recently, the European Data Protection Board (EDPB) published a draft of Guidelines 02/2025 on the processing of personal data through blockchain technologies ("**Draft**"), for public consultation.

The Draft outlines the intersection between blockchain technologies and personal data and addresses the challenges relating to the application of the General Data Protection Regulation (GDPR) to that intersection.

Drawing on the principle of "Data Protection by Design and by Default", the EDPB provides practical recommendations on how data controllers can safeguard personal data in light of blockchain's unique characteristics.

Unique Characteristics of Blockchain

Blockchain is a type of Distributed Ledger Technology (DLT) that maintains a shared and consistent database across multiple participants without centralized control. It enables transactions without intermediaries by relying on participant consensus rather than a trusted central authority. Blockchain ensures transparency and while data is resistant to unauthorized changes, once it is recorded, it cannot easily be altered or removed.

Blockchains may process and store various types of personal data, including pseudonymous identifiers (e.g., wallet addresses) and transaction payloads containing identifiable information. Frequently, additional data is stored off-chain to address concerns about data minimization and confidentiality, while only references or hashed values are kept on-chain. However, blockchain's immutable nature can still create risks for data subjects' rights and freedoms.

Key Challenges of Personal Data Processing on Blockchain under the GDPR

- Since blockchain technology supports various forms of data processing, there is no single lawful basis under the GDPR that applies to all blockchain-related activities. Each processing purpose must be assessed independently to determine the appropriate legal basis.
- The immutability of blockchain presents a key challenge when processing personal data. Once data is recorded, it is difficult to alter or remove, which conflicts with GDPR requirements such as data accuracy, data minimization, and the rights of data subjects, specifically the rights of a data

subject to demand rectification or erasure of his/her personal data. It may also contravene the purpose limitation principle if the data is retained beyond its intended use.

- Blockchain's global nature raises additional concerns. Data is often transferred across borders, particularly in public blockchains, where nodes may be located outside the EU and are neither selected nor monitored. This raises questions about international data transfers and the level of protection applied to such data.

Practical Measures to Protect Personal Data in Blockchain Systems

In general, it is not advisable to store personal data directly on the blockchain, and such data should not be embedded in the content of transactions. Where necessary, personal data may be represented within a blockchain transaction through various technical means (such as hashing).

The Draft offers several practical measures to protect personal data, including:

- **Cryptography and Off-Chain Storage of Personal Data -** where possible, personal data should be encrypted, hashed or included as a cryptographic commitment. Nevertheless, the use of such techniques does not eliminate the requirement to comply with the GDPR.
- **Establish a Valid Legal Basis -** processing of personal data must be based on a valid legal ground. Where consent is used as the basis, it must comply with the GDPR requirements and be freely given, specific, informed, and unambiguous.
- **Ensure Transparency to Data Subjects -** data subjects must receive all necessary information to understand how their personal data is collected, used, and with whom it is shared.
- **Enable the Exercise of Data Subject Rights -** controllers must ensure that data subjects can exercise their rights under the GDPR — namely, the rights of access, rectification, erasure, restriction, and portability. These rights must be addressed from the outset, during the design of the processing. For example, preparation for handling erasure requests can be addressed by storing personal data off-chain and implementing anonymization techniques to on-chain data.
- **Define Clear and Lawful Purposes for Processing -** personal data must be processed only for specific, explicit, and legitimate purposes. Controllers should also define appropriate data retention periods, which may differ from the operational lifespan of the blockchain.
- **Implement Technical and Organizational Safeguards -** robust security and confidentiality measures must be embedded into the blockchain infrastructure. This may include emergency protocols or mechanisms for updating consensus algorithms in the event of a vulnerability.
- **Address International Data Transfers -** where personal data is transferred outside the European Union, such transfers must comply with the requirements set out in Chapter V of the GDPR. In the context of blockchain, this can be challenging due to the decentralized and global nature of the technology. To address this, organizations can implement measures such as entering into

standard contractual clauses (SCCs) to ensure adequate protection of personal data.

- **Conduct a Data Protection Impact Assessment (DPIA) -** Where a processing activity is likely to result in a high risk to the rights and freedoms of natural persons, a DPIA should be conducted to assess and appropriately mitigate risks associated with the processing of personal data on the blockchain.

The Draft has faced significant criticism from the Blockchain industry. However, the GDPR fundamental principles remain applicable to decentralized systems, requiring organizations to incorporate data protection considerations from the earliest stages of blockchain architecture design. Therefore, it is important for companies operating in this space to take appropriate steps to comply with the applicable data protection regulatory requirements.

The Draft Opinion is open for public comment until June 9, 2025.

Should you have any questions regarding digital assets, blockchain activities, or related privacy considerations, our firm's specialists are available to provide expert guidance on privacy and regulatory compliance.

This client update is designed to provide general information only, is not a full or complete analysis of the matters presented, and may not be relied upon as legal advice.

* This client update was prepared with the assistance of Ella Schreck.

Key Contacts

Assaf Harel
Partner

Avital Haitovich
Senior Associate