MAY 2025

GDPR & Blockchain: Navigating Legal Compliance in Decentralised Systems.

PATSALIDES.COM.CY

31 EVAGORAS AVENUE,
EVAGORAS BUILDING,
4TH FLOOR, NICOSIA

INDEX

Table of Contents

Executive Summary

Blockchain technology has introduced new opportunities for innovation, decentralisation, and transparency across sectors. However, its distinguishing features—particularly immutability, decentralised control, and cross-border data flow—pose significant challenges to compliance with the General Data Protection Regulation (GDPR). This booklet provides a structured overview of the legal issues that emerge when blockchain-based solutions intersect with data protection law.

It begins with a concise introduction to blockchain technology and the core principles of the GDPR. It then explains how personal data may be processed within such systems. Furthermore, it explores how blockchain's technical architecture may affect GDPR compliance, by identifying and analysing six critical questions, namely:

1. How can data subject rights, such as the "right to be forgotten," be respected in immutable ledgers?
2. Who qualifies as the data controller in decentralised networks?
3. What are the lawful bases for processing personal data in blockchain contexts?
4. How can purpose limitation and data minimisation be achieved?
5. How can compliance with international data transfer rules be ensured?
6. How can the right to object to solely automated decisions, including profiling, be achieved?

The booklet also highlights the recent guidance issued by the European Data Protection Board (EDPB) in Guidelines 02/2025, which offers practical suggestions for reconciling GDPR compliance with decentralised design.

This resource is addressed to developers, businesses, legal practitioners, and policymakers involved in blockchain initiatives that process personal data. It aims to support responsible innovation by identifying regulatory risks and outlining practical steps toward compliance.

Blockchain & GDPR

Blockchain Technology

Blockchain is a type of distributed ledger technology that allows data to be recorded across a network of computers in a secure, transparent, and immutable way. It is the underlying technology behind cryptocurrencies like Bitcoin and Ethereum, but its applications extend far beyond digital currencies, including smart contracts, Decentralised Finance (DeFi) and Decentralised Autonomous Organisations (DAOs).

As its name suggests, data in a blockchain is stored in blocks that are digitally connected to one another, forming a chronological chain. Unlike traditional databases maintained by a central authority, blockchain relies on a decentralised network of participants (or "nodes") who work together to verify and store information in blocks. In blockchain, every node in the network gets a copy of the ledger and can view all transactions, enhancing trust across the network.

Nodes within a blockchain network may perform various functions depending on the governance structure of the blockchain, ranging from validating transactions to maintaining the network's state. Nodes use consensus mechanisms to establish the validity of transactions, with mechanisms such as Proof of Work (PoW) and Proof of Stake (PoS) being among the most common. The choice of consensus mechanism varies depending on the specific blockchain employed, influencing the network's efficiency, security, and energy consumption.

Blockchain technology implements hashing to ensure the immutability of data. Specifically, each block contains a code known as a hash digest—a unique, cryptographically encrypted fingerprint that cannot be altered unless the data within the block is changed. Each block contains both its own hash value and the hash value of the previous block. If someone attempts to tamper with a block's data, the hash value will change, thereby invalidating not only that block but also all the subsequent blocks linked to it. To reverse this, one would need to re-mine that block and every block that follows, a process that demands immense computational power, making such tampering virtually impossible.

Moreover, blockchains use public/private key cryptography to secure transactions and establish ownership. The private key is a randomly generated number that must be kept secret. The public key, which is derived from the private key, is visible to all the nodes.

Blockchain & GDPR

Smart Contracts

Smart Contracts refer to computer code and are essentially an application of blockchain technology. Smart contracts were initially facilitated by Ethereum. However, nowadays, many other blockchain networks, such as Solana, can support their application.

Smart contracts enable the automatic execution of transactions once predefined conditions are met, using a simple if-this-then-that logic. A helpful analogy is the vending machine: when a coin is inserted, the machine automatically dispenses a product (e.g., a bottle of water). Similarly, when the specified conditions are fulfilled, a smart contract self-executes according to the coded instructions embedded in the blockchain.

It should be noted that smart contracts may be programmed to execute based on the occurrence of off-chain events. In such cases, they rely on oracles, external service providers that verify and transmit real-world data to the blockchain, enabling the contract to function as intended.

Key features of smart contracts include:

- **Eliminating intermediaries:** Transactions are executed automatically, reducing reliance on third parties.
- **Increased efficiency:** Transactions are processed faster and at lower cost.
- **Immutability:** Once deployed, smart contracts cannot be altered, ensuring the integrity of the process.
- **Reliability:** Transactions are executed in a consistent and predictable manner according to pre-agreed rules.

In fact, smart contracts form the backbone of many blockchain-based business models. For instance, DAOs are created and governed through smart contract interactions. Similarly, DeFi relies on smart contracts to develop protocols that replicate traditional financial services in a more open and transparent manner.

Blockchain & GDPR

The General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is a comprehensive data protection law that took effect on 25 May 2018, replacing the previous Data Protection Directive 95/46/EC. It was designed to harmonise data privacy laws across the European Union (EU), protect and empower all EU citizens' data privacy, and reshape how organisations approach data privacy. The GDPR applies to the processing of personal data, either entirely or partially, through automated means, as well as to non-automated processing of personal data that is part of, or intended to be part of, a structured filing system.

Notably, although the GDPR was drafted and passed by the EU, it imposes obligations on organisations worldwide, as long as they target or collect data related to people in the EU.

The GDPR imposes hefty fines for violations of its privacy and security standards. Specifically, the regulation can impose fines of up to €20 million or 4% of the annual global turnover of the preceding financial year, whichever is higher, for serious infringements. **However, given blockchain's decentralised nature, imposing GDPR enforcement provisions on public blockchains seems challenging.**

Additionally, the persons whose data is illegally processed have the right to seek compensation for damages. Beyond compensation, data subjects are granted several rights, including the right of access, the right to data portability, the right to rectification, the right to erasure, the right to object, the right to object to a solely automated decision-making, including profiling, the right of non-discrimination of data subjects in such processes and the right to information.

GDPR's Key Principles: GDPR establishes seven protection and accountability principles, as outlined in Article 5.1-2, applicable when personal data is being processed:

1) Lawfulness, Fairness, and Transparency
2) Purpose Limitation
3) Data Minimisation
4) Accuracy
5) Storage Limitation
6) Integrity and Confidentiality
7) Accountability

Blockchain & GDPR

Processing of Persona Data in Blockchain

According to Article 4 of the GDPR, *personal data* refers to any information relating to a natural person who is, or can be, identified directly or indirectly (the data subject), particularly by reference to an identifier such as a name, identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person. The same article defines *processing of personal data* as any operation or set of operations performed on personal data, including collection, storage, and dissemination.

To determine whether data protection rules apply in blockchain networks, it is necessary to assess whether personal data is being processed through the use of blockchain technology. As previously explained, blockchain functions as a ledger for recording data and transactions; therefore, it can be argued that processing does, in fact, occur.

Blockchain networks store transaction metadata combined with a payload.

Metadata includes essential information for identifying and verifying transactions, such as user identifiers. In traditional blockchain systems, where the public key is publicly visible, these identifiers may include the public key itself. In this context, the distinction between anonymised and pseudonymised data becomes relevant. Anonymised data refers to information that cannot be linked to any identifiable individual, while pseudonymised data allows for a user's transactions to be linked to one another through an identifier without revealing the user's actual identity. **The GDPR does not apply to anonymised data, as per Recital 26 GDPR; however, it must be emphasised that the threshold for data to be considered truly anonymised is very high.**

The public key is considered pseudonymous rather than anonymous, as its visibility could enable the gathering of information that leads to the identification of an individual—either because a service provider holds additional data or because a third party is able to link the public key to an individual or organisation (for example, through an IP address). Additionally, if nodes consistently use the same public key for their transactions, it may be possible to single out an individual based on their transaction patterns, even if their identity is not directly revealed. Recital 26 of the GDPR clarifies that pseudonymised personal data, which can be attributed to a natural person through the use of additional information, falls within the scope of the Regulation. **As a result, a public key that can be associated with an individual will likely qualify as personal data for GDPR purposes.**

Notably, newer blockchain technologies offer a higher degree of anonymity. However, whether this level of anonymity satisfies European data protection standards remains uncertain. For instance, newer technologies based on zero-knowledge proofs enable transaction verification without revealing the underlying details. Despite their privacy advantages, these methods involve complex cryptographic processes and high computational costs, which pose scalability challenges.

An alternative approach could involve generating a new public key for each transaction while using the same private key. However, this technique requires careful implementation and is only feasible for certain types of public keys. It may also necessitate the involvement of a key issuing authority—a centralised body (or potentially several authorities)—which derives unique public keys from a core private key for individual transactions.

Additionally, it should be noted that when interacting with a blockchain, other personal data, though not stored on the blockchain itself, may still be processed or made available. For example, when accessing a blockchain wallet, an individual's IP address may be collected by the service provider.

Furthermore, the payload represents the actual content or data being stored. This can include amounts of cryptocurrency, smart contract executions, document links, purchased items, or other transaction-specific data. The payload may also contain personal data related to the users involved or other individuals, which is stored on-chain within the blocks themselves. Depending on the use case of blockchain, different personal data may be included, particularly in the payload. For instance, in specialised blockchain systems, the payload might contain sensitive personal information, such as financial statements or medical records. **Notably, hashing is considered a pseudonymisation technique. Thus, even when payload data is hashed, it may still be possible to trace it back to an individual, hence still constitutes personal data under GDPR.**

SUMMARY OF THE

Key Legal Implications Of Blockchain Under the Lens of GDPR

A

How can an individual's "right to be forgotten" and "right to rectification" be respected?
(Articles 16 and 17 GDPR)

B

Who qualifies as the data controller?
(Articles 4(7) and 24 GDPR)

C

How can the lawfulness of the processing of personal data be determined?
(Article 6 GDPR)

D

How can Purpose Limitation and Data Minimisation be achieved?
(Articles 5(1)(b) and 5(1)(c) GDPR)

E

How can compliance with international data transfer rules be ensured?
(Chapter V, Articles 44-50 GDPR)

G

How can the right to object to solely automated decisions, including profiling, be achieved?
(Article 22 GDPR)

Legal Implications of Blockchain Under the Lens of GDPR

A How can an individual's "right to rectification" and "right to erasure" be respected? (Articles 16 and 17 GDPR)

The integration of blockchain technology with GDPR presents a significant challenge, particularly concerning the "right to rectification" and the "right to erasure" (articles 16 and 17 GDPR). This is due to blockchain's defining feature, i.e., its immutability. As explained in the introductory section, once data is recorded on the ledger, there is typically no practical way to delete or modify it.

The technical possibility of modifying a blockchain through a "soft" or "hard" fork exists, but this approach does not provide a viable solution for GDPR compliance. **Even when a hard fork occurs, the original transaction history is generally preserved in the initial ledger.** Furthermore, the concept of forking a blockchain raises concerns about its immutability, as the potential to alter the ledger, even in principle, may undermine trust in the technology and negatively affect its reputation.

As a result, blockchain environments present a significant challenge in ensuring compliance with these two vital rights of data subjects.

Legal Implications of Blockchain Under the Lens of GDPR

B

Who qualifies as the data controller? (Articles 4(7) and 24)

A data controller determines the purposes and means of processing personal data. The data controller is responsible for ensuring that personal data is processed lawfully and transparently, safeguarding the rights of data subjects, and implementing appropriate technical and organisational measures. In the event of a data protection breach, the controller is the main entity held accountable for addressing the breach and mitigating its impact.

However, identifying the data controller in decentralised blockchain networks is challenging due to the varied roles participants may assume, complicating the allocation of GDPR compliance obligations and accountability in the event of a data protection breach. In some cases, a node might function as a data controller if it has the authority to determine the purposes and means of processing personal data. For example, a node that initiates transactions or sets specific processing rules might be considered a controller for those particular activities. Conversely, nodes that merely validate transactions or maintain the ledger without influencing the processing decisions might not qualify as data controllers. Instead, they may act as data processors, executing tasks on behalf of the controller without determining the processing's overarching objectives. This distinction is critical because it affects the allocation of GDPR compliance obligations and accountability.

In permissioned blockchains, where participation is restricted and requires prior authorisation, governance and accountability structures can be clearer, potentially facilitating the identification of a data controller or joint controllers. For example, the consortium or organisation that establishes and operates the blockchain could act as the data controller. Conversely, permissionless blockchains, which are open to anyone without identification requirements, present greater challenges in attributing legal responsibility. The role of nodes may vary depending on the processing context, further complicating the identification of a controller.

Legal Implications of Blockchain Under the Lens of GDPR

C How can the lawfulness of the processing of personal data be determined? (Article 6)

Under the GDPR, all personal data processing must rely on a valid legal basis. This principle applies equally to blockchain-based processing. However, due to the wide variety of blockchain use cases and their technical characteristics, there is no one-size-fits-all legal basis. Each processing activity must be assessed individually to determine which legal ground under Article 6 GDPR is most appropriate.

In some cases, organisations may seek to rely on consent as their legal basis. **In such cases, data processing must meet the high threshold of being *freely given, specific, informed, unambiguous* and *revocable*.** Importantly, if a data subject withdraws consent, the organisation must be able to delete or anonymise the personal data without causing detriment to the data subject. This presents a clear tension with blockchain's immutability. Additionally, obtaining valid consent in a decentralised network can be challenging, as it requires clear communication and agreement from all data subjects involved.

Other potential legal bases include compliance with a legal obligation under Article 6(1)(c) GDPR or the pursuit of a legitimate interest of the controller or third party under Article 6(1)(f) GDPR. However, the latter requires a careful balancing test: where the data subject's fundamental rights and freedoms override the controller's interest, such processing is not permitted. This balancing exercise can be particularly complex in blockchain environments, where multiple parties may pursue diverging interests.

It should be noted that, in specific contexts, such as when blockchain solutions are implemented to facilitate anti-money laundering, Member States may legitimately restrict data subject rights, including those related to the lawfulness of processing. **Such restrictions are only permitted under Article 23 GDPR if they are *legally justified, proportionate,* and *necessary* in a democratic society.**

Legal Implications of Blockchain Under the Lens of GDPR

D How can Purpose Limitation and Data Minimisation be achieved? (Articles 5(1)(b) and 5(1)(c))

Under the GDPR, personal data must be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes"—a principle known as purpose limitation. In addition, the processing of personal data must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed," a requirement referred to as data minimisation.

However, given that blockchain data is replicated across all nodes and stored immutably, any data added to the chain remains permanently accessible, even if it is no longer necessary for the original purpose. This permanence poses a significant challenge to both purpose limitation and data minimisation, as it prevents the removal or alteration of data that may become irrelevant or excessive over time.

Moreover, once data is placed on-chain, it may be reused or accessed for unforeseen purposes, challenging the requirement to limit processing to the original specified purpose. This potential for data to be repurposed without the data subject's consent or awareness raises concerns about compliance with GDPR principles.

Additionally, the decentralised nature of blockchain networks complicates the ability to control and restrict access to data, as multiple nodes may have differing interpretations of the data's intended use.

Legal Implications of Blockchain Under the Lens of GDPR

E How can compliance with international data transfer rules be ensured? (Chapter V, Articles 44-50)

Under Chapter V of the GDPR, any transfer of personal data to a third country or international organisation must comply with the Regulation and ensure a level of protection that is essentially equivalent to that within the EU. The data controller must be aware of these obligations, identify when such transfers occur, and implement appropriate mechanisms to facilitate these data flows. This requirement aims to safeguard personal data transferred outside the EU, thereby maintaining the high standards of protection established by the GDPR.

However, the decentralised nature of blockchain—which permits global participation and data replication across borders—poses significant challenges to meeting these requirements. **By design, blockchain networks allow data to be stored and accessed by nodes situated in multiple jurisdictions worldwide, thereby complicating efforts to control or restrict international data transfers.**

Ensuring compliance with the GDPR's rules on international transfers in such a distributed environment is highly complex, and in some instances, may prove practically impossible. The absence of a central authority responsible for managing or overseeing data transfers further exacerbates these difficulties, as it is often unclear which entity bears responsibility for ensuring compliance (i.e. identifying the controller, as discussed in Part [B]).

Moreover, blockchain networks may not readily accommodate traditional safeguards such as Standard Contractual Clauses or Binding Corporate Rules, given their decentralised and open architecture. This raises important questions about how to effectively implement protective mechanisms that satisfy the GDPR's international transfer requirements.

ANALYSIS OF THE

Legal Implications of Blockchain Under the Lens of GDPR

How can the right to object to solely automated decisions, including profiling, be achieved? (Article 22 GDPR)

Under Article 22 of the GDPR, individuals have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or similarly significant consequences.

However, smart contracts, as explained in the introductory part of this booklet, enable the automatic execution of transactions once the pre-defined conditions have been fulfilled. Specifically, the whole idea of smart contracts is to eliminate third-party intervention, thus enabling data subjects to object to such automatic transactions in an ecosystem of smart contracts, such as a DAO, could severely hinder the operability of such systems and may ultimately defeat their purpose.

That being said, the 02/2025 Guidelines clarify that the execution of a smart contract may, in certain cases, constitute an automated decision within the meaning of Article 22 GDPR. **However, whether the execution of a smart contract, that relies on off-chain events, qualifies as a solely automated decision under Article 22 remains an open question.**

Overview of EDPB Guidelines 02/2025

To provide greater legal clarity, the European Data Protection Board (EDPB) published Guidelines 02/2025 in April 2025, which are now open for public consultation until 9 June 2025. These guidelines aim to clarify how blockchain-based solutions can comply with GDPR, given the inherent challenges posed by blockchain's decentralised and immutable nature.

KEY TAKEAWAYS:

A

Identification of Roles:

- The EDPB emphasises the need to clearly identify data controllers and processors in blockchain networks. This will be achieved through the implementation of clear governance structures.

B

Data Minimisation and Purpose Limitation:

- The EDPB emphasises the need to adhere to GDPR principles of data minimisation and purpose limitation. Organisations should evaluate whether personal data needs to be stored on the blockchain and consider alternatives, such as off-chain storage, to minimise the amount of personal data recorded on the blockchain.
- The EDPB reiterates that information such as encrypted identifiers or hash values may still qualify as personal data if it can be linked back to an individual; thus, simply "disguising" data may not always be enough (as discussed on pages 7 and 8 of this booklet).

C

International Data Transfers:

- The EDPB emphasises that any transfer of personal data outside the EU must comply with the provisions of Chapter V of the GDPR, and that appropriate mechanisms should be integrated into the design of the blockchain to facilitate such transfers.

Overview of EDPB Guidelines 02/2025

KEY TAKEAWAYS:

D

Technical and Organisational Procedures:

- The EDPB recommends establishing technical and organisational procedures to disclose vulnerabilities to blockchain users.
- Inter alia, an emergency plan should be in place to enable modifications to the underlying code where a vulnerability is identified.
- The relevant Supervisory Authority, along with the affected data subjects, must be notified in the event of security incidents or personal data breaches.

E

Ensure safeguards with provisions of Article 22:

- When a business operating on blockchain is facilitated through the interaction of smart contracts, such as a DAO or a DeFi system, the data controller must ensure that the rights, freedoms and fundamental interests of the data subject are safeguarded, at least ensuring that human intervention is possible, and that the data subject has the ability to express their views or contest the decision, even if the smart contract has already been executed.

F

Privacy by Design and Default:

- The EDPB encourages organisations to embed data protection into blockchain design from the outset. This may require using a combination of Privacy-Enhancing Technologies (PETs) to ensure adequate protection for data subjects.

CONTINUATION...

Overview of EDPB Guidelines 02/2025

KEY TAKEAWAYS:

G

Data Protection Impact Assessments (DPIA) as a Mandatory Step in specific cases:

- A DPIA should be conducted prior to processing personal data using blockchain technology if the processing meets the criteria indicating a high risk to the rights and freedoms of individuals.
  - Specialised blockchain systems aiming to process personal data, should likely conduct a DPIA.
- A DPIA must include:
  a. Examination of Personal Data Involvement: Determine whether personal data will be processed within the blockchain system, considering the implications for data protection compliance.
  b. Assessment of Blockchain Necessity: Evaluate the rationale for using blockchain technology and consider less privacy-intrusive and less risky methods for individuals' rights and freedoms.
  c. Evaluation of Blockchain Network Suitability: Assess the most appropriate blockchain network to use, taking into account the effectiveness of PETs, such as zero-knowledge proofs and encryption, in mitigating risks. Consider the possibility of implementing private or permissioned blockchains.
  d. Consideration of Technical and Organisational Measures: Identify the technical and organisational measures in place, such as whether personal data will be stored on-chain or off-chain, and whether PETs are being used. If not, provide justification for their absence.
  e. Evaluating Data Subject Risks: Assess the risks to data subjects' rights and freedoms from processing, including blockchain-specific risks, potential data breaches, the extent and scale of processing and infrastructure, and risks regarding data protection rights in international transfers.
  f. Precise Identification and Assessment of Specific Measures: Evaluate measures to address blockchain-related risks, including accountability, data protection by design and default, data minimisation, accuracy strategies, cryptographic guarantees, and security issues.

What does this mean for blockchain businesses?

As the public consultation period for EDPB Guidelines 02/2025 progresses, it is increasingly clear that the fundamental tensions between blockchain design and GDPR obligations will persist. The decentralised and immutable nature of blockchain offers unique benefits—but also presents regulatory uncertainties that cannot be ignored.

Organisations involved in blockchain development and deployment must therefore take a proactive approach to GDPR compliance. This includes assessing whether personal data is being processed, identifying roles and responsibilities, selecting suitable legal bases, and considering privacy-enhancing technologies.

In particular, businesses should, amongst other things:

- Conduct Compliance Readiness Assessments to identify legal and technical gaps;
- Implement Privacy by Design and Default, integrating data protection into technical architectures from the outset;
- Explore Off-Chain Alternatives where appropriate to minimise risks; and
- Engage with Regulatory Developments, including public consultations and guidance issued by supervisory authorities.

By understanding the evolving legal landscape and aligning their practices accordingly, blockchain businesses can pursue innovation responsibly while upholding the fundamental rights of data subjects.

HOW WE CAN ASSIST:

At Christos Patsalides LLC, we offer targeted legal guidance to organisations navigating the evolving intersection of blockchain technology and data protection law. Our team supports clients in aligning their blockchain initiatives with the requirements of the General Data Protection Regulation (GDPR), from initial design to ongoing compliance.

We assist in identifying legal responsibilities within decentralised ecosystems and assessing the suitability of technical solutions such as off-chain storage and privacy-enhancing technologies. Moreover, we provide tailored advice to determine whether a DPIA is required, conduct in-depth risk assessments, and prepare detailed reports that evaluate the potential impact on data subjects' rights and freedoms.

By partnering with us, organisations can confidently navigate the complexities of data protection compliance while harnessing the full potential of blockchain technology.

AUTHORS:

Varteni Kasapian

Partner
Data Protection Expert
varteni.kasapian@patsalides.com.cy

Ioanna Patsalidou

Associate
PhD Candidate at King's College London
ioanna.patsalidou@patsalides.com.cy

Thank You