SLAUGHTER AND MAY/

30 APRIL 2025

WHEN DECENTRALISATION MEETS REGULATION: HOW BLOCKCHAIN AND GDPR CAN COEXIST

The European Data Protection Board (EDPB) has released its long-awaited draft Guidelines on processing of personal data through blockchain technologies.

Back in 2019, we observed that while blockchain emerged as an innovative alternative to traditional databases, it faced significant hurdles under the GDPR — particularly when handling personal data. We argued that, with collaboration between regulators and technologists, privacy-conscious blockchain solutions were within reach. The EDPB's draft guidelines are therefore a welcome step forward, offering some helpful clarity. Their release is especially timely given recent enforcement actions against World Network (originally known as Worldcoin), a crypto project that collects iris scans to authenticate humans, highlighting the legal risks of blockchain systems that lack sufficient data protection safeguards. At the Global Privacy Summit 2025, World Network's Sam Altman emphasised the company's commitment to building privacy-preserving biometric technologies, though how best to achieve this remains a subject of ongoing debate.

While ideally the guidelines would contain some more detail in parts and practical examples, Annex A in particular contains a set of recommendations that serve as a useful checklist for organisations planning to implement blockchain-based personal data processing.

1. Is Blockchain Necessary? Assess First, Build Later

The EDPB begins with a critical reminder: blockchain is not always the appropriate solution for processing personal data. Before deploying blockchain solutions, controllers must carefully assess whether it is truly necessary for their intended purpose. If alternative technologies (e.g. centralised databases) can achieve the same result with fewer data protection risks, they must be preferred in accordance with the necessity principle under the GDPR. To ensure accountability, controllers should document their justification for choosing blockchain.

In addition, and consistent with our 2019 publication, the EDPB advises that private permissioned blockchains, where participation is restricted and roles are clearly defined, should be favoured over public permissionless blockchains (e.g. as Bitcoin or Ethereum), where anyone can participate and transactions are permanently visible to everyone. This is because private permissioned systems offer greater control, clearer role assignment, and improved data governance. The draft guidelines state that public permissionless blockchains may only be considered where there are well-justified, documented reasons and appropriate safeguards in place to mitigate the associated risks. However, they do not give any examples of how public permissionless blockchains could be used in a GDPR compliant way. Indeed, as we concluded in our 2019 publication, it is hard to see how they could unless most or all personal data is stored off-chain.

2. Keep Personal Data Off the Chain Where Possible

As they are immutable by design, blockchains do not allow data deletion or modification in most cases. Once personal data is submitted to a blockchain, it cannot be edited or removed, even if it later proves to be inaccurate, outdated, or no longer necessary for the original processing purpose. The EDPB reiterates in these draft guidelines, as it did in its ChatGPT Taskforce Report, that "technical impossibility" cannot be invoked by controllers or processors to justify a failure to uphold GDPR obligations.

The EDPB outlines several strategies for reducing risks when handling personal data in blockchain systems, along with any associated limitations:

- *Encryption* can restrict access to only those with the decryption key, but the draft guidelines suggest encrypted data still counts as personal data and its long-term security may weaken over time if retained indefinitely.

- *Hashing*, particularly using salted or keyed hashes, can obscure the original data, but still requires secure off-chain storage and the draft guidelines suggest hashes continue to be personal data subject to the GDPR.

- *Cryptographic commitments* offer a way to anchor data on-chain without revealing its content, and once the original data and associated keys are deleted, the commitment can no longer be used to recover or recognise the original personal data.

As a general rule, the EDPB advises that only proof of existence (e.g. cryptographic commitments, hashes derived from a keyed hash function) should be stored on-chain. The actual personal data (e.g. names, email addresses, identity attributes, medical information) should be stored off-chain in a secure environment, such as controller's information system, that complies with GDPR requirements. All sage advice.

The draft guidance does not, however, engage with some of the more challenging questions in this area, such as:

- whether there are circumstances in which encryption or hashing could be regarded as effectively achieving anonymisation or deletion (e.g. once all keys, salts etc. are deleted such that there are no "means reasonably likely to be used" to identify any individual to whom relevant information relates); and

- whether information may be personal data in one person's hands (e.g. in the hands of someone with the relevant key), but not another's (e.g. an operator of a node with no access to the relevant key).

3. Clarify Roles: Who's the Controller? Who's the Processor?

Unlike centralised systems, blockchain ecosystems often lack a single entity responsible for decisions related to the processing of personal data. Instead, multiple participants (e.g. node operators, developers, validators) may independently or jointly determine how personal data is processed. This makes it challenging to determine who qualifies as a controller or processor under the GDPR.

The EDPB highlights the importance of the blockchain governance framework (both technical, such as the consensus mechanism, and non-technical, such as any agreement between participants) in answering this question. For private permissioned blockchains, it is possible to establish clear rules, policies, and technical requirements that govern the structure and format of on-chain data, the roles of participants, and the consensus mechanism to validate transactions.

In the case of public permissionless blockchains, where nodes act independently, operators of nodes may influence the processing of personal data, for instance, by making decisions on forking or modifying protocols. In line with the conclusion in our 2019 publication, the EDPB strongly recommends the creation of a consortium or other legal entity to assume the role of controller for such processing activities.

4. Design with Data Minimisation and Storage Limitation in Mind

Under the GDPR, only data necessary for the specified processing purpose must be collected and retained. Blockchain's append-only architecture poses a challenge to this principle, given the technology's features of permanent storage and widespread replication across nodes. According to the EDPB, this tension must be addressed, with key recommendations including the following:

- *Store only what is necessary*: Controllers should ensure that the data recorded on-chain is limited to what is required for the intended purpose.

- *Minimise visibility and publicity*: Personal data should not be made public unless necessary, and privacy-preserving tools like pseudonymisation or zero-knowledge proofs should be considered.

- *Demonstrate proportionality and necessity*: The EDPB expects controllers to justify the use of blockchain and show that their chosen design reflects data minimisation principles, e.g. limiting the amount of personal data processed, restricting access where possible, and avoiding unnecessary retention.

In line with the storage limitation principle, the EDPB advises that personal data should not be written to the blockchain unless the retention period justifies it. If processing does not require data to persist for the blockchain's full lifetime, it should only be recorded in a way that effectively prevents identification. Where lifetime retention is deemed necessary, the controller must justify this as proportionate to the purpose, and document its reasoning.

5. Consider Legal Grounds and Cross-Border Data Transfers

The EDPB highlights the need for blockchain projects to have a valid legal basis for processing personal data. Each processing activity must have a legal basis under Article 6. Where consent is relied on, it must be freely given, specific, informed, and revocable without detriment. If consent is withdrawn, personal data must be deleted or anonymised — a complex issue given blockchain's immutability. In limited cases, restrictions on data subjects' rights may be permitted under Article 23, such as where blockchain is used for anti-money laundering purposes or managing real estate inventories. Depending on the context, other legal bases such as legitimate interests may be more appropriate.

International data transfers also demand attention: public blockchains often distribute data across nodes outside the EEA, requiring compliance with Chapter V GDPR safeguards. The EDPB suggests that controllers could incorporate standard contractual clauses into contracts that node operators must sign before being accepted onto the network.

6. Design for Security from the Start

The EDPB emphasises that blockchain-based processing must meet the GDPR's security requirements, with safeguards tailored to risks such as 51% attacks, compromised wallets, and cryptographic failures. Controllers should implement appropriate technical and organisational measures, including secure key management and contingency plans for algorithm vulnerabilities. The EDPB takes a strict stance in stating that if it is not possible to ensure a level of protection appropriate to the risks involved, blockchain solutions should not be used for processing personal data.

7. Evaluate Risks with a DPIA

Conducting a DPIA is mandatory under the GDPR when processing is likely to result in a high risk to the rights and freedoms of individuals—and blockchain-based processing often meets this threshold. The DPIA must assess the entire processing ecosystem, not just the blockchain component, taking into account both on-chain and off-chain data flows, governance models, and potential vulnerabilities.

When carrying out a DPIA for blockchain processing, aspects that need to be addressed include: (i) a clear description of the processing operations and blockchain model, governance mechanisms and data lifecycle, (ii) an assessment of the necessity and proportionality of using blockchain, and (iii) identification and mitigation of risks, including an assessment of the risks and safeguards in case of international transfers.

8. Embed Data Subject Rights into Your Design

- *Right to Information, Access & Data Portability*: Controllers must provide clear and accessible, information to data subjects before submitting personal data for blockchain validation. The rights of access and portability can be compatible with blockchain, provided that the controller ensures compliance with relevant GDPR provisions (e.g. data format, access method).

- *Right to Erasure & Right to Object*: These rights must be considered and built into the design phase of any blockchain-based system. Because blockchain is immutable, actual deletion is often technically infeasible. To comply, personal data should either not be stored on-chain or be structured in a way that allows for effective anonymisation upon request.

- *Right to Rectification*: This right must be addressed by design. The EDPB notes that in some cases, rectification may be fulfilled by submitting a new transaction to correct or override an earlier one (even though the earlier transaction remains on the chain). However, the EDPB suggests that in some cases, rectification may require erasure of the incorrect information, in which case the same means should be used as those for achieving compliance with the right to erasure.

- *Right to Object to Automated Decision-Making*: If smart contracts constitute automated decisions, controllers must ensure compliance with safeguards under Article 22.

As far as we are aware, this is the first time the EDPB has expressed a view on the vexed question of whether the right to rectification may require erasure of the erroneous data. As we noted in our 2019 publication, there are some significant challenges if this is the case, and it is not always possible to achieve rectification by appending a subsequent correction. For example, erasure is problematic and may be illegal where the erroneous data could be used as evidence in legal proceedings. Some of these challenges are recognised in Articles 17(2) and 17(3) in respect of the right to erasure, but similar provisions do not apply to the right to rectification. In our opinion, this issue would benefit from additional EDPB guidance, particularly considering the potentially conflicting decisions/guidance by European authorities on the issue.

Final Thoughts: Aligning Blockchain Innovation with Data Protection

The EDPB does not preclude the use of blockchain technology, but it sets a clear expectation that its use must be measured, well-justified, and privacy-aware. While blockchain offers exciting opportunities for security and decentralisation, its design and use must align with GDPR obligations.

Organisations must carefully assess whether blockchain is necessary for their processing needs, whether personal data can be kept off-chain, and whether the chosen architecture and governance model can support GDPR compliance.

The EDPB's guidance makes clear: GDPR and blockchain can coexist — but only when privacy is built in from the beginning.

The full text of the draft guidelines can be found here.

Our 2019 publication, which takes a detailed look at the GDPR challenges faced by blockchain solutions and considers them in the context of a real-world use-case, can be found here.

Please feel free to reach out to any of the authors below or your usual Slaughter and May contact if you would like to discuss anything in this briefing note or any matters relating to GDPR and regulatory compliance and emerging technology.

This article was written by Rob Sumroy, Ian Ranson and Hilal Temel. Rob, Ian and Hilal are part of Slaughter and May's Tech, Digital and Data Team. For further insights on tech, digital and data, see our Lens blog or Tech and Digital page.

CONTACT

ROB SUMROY
PARTNER
T: +44 (0)20 7090 4032
E: Rob.Sumroy@SlaughterandMay.com

IAN RANSON
SENIOR ASSOCIATE
T: +44 (0)20 7090 3932
E: Ian.Ranson@SlaughterandMay.com

HILAL TEMEL
ASSOCIATE
T: +44 (0)20 7090 3524
E: Hilal.Temel@SlaughterandMay.com

Published to provide general information and not as legal advice.
For further information, please speak to your usual Slaughter and May contact.