Response to EDPB Draft Guidelines 02/2025 on processing of personal data through blockchain technologies

KEY POINTS

We welcome EDPB's focus on providing clarity as regards blockchain and data protection law. Overall, however, we have concerns that the guidelines are based on a misunderstanding of public blockchain technology and will give rise to problems if implemented. Our general feedback is that the guidelines would benefit from further consideration.

In particular, the guidelines mischaracterise the role of nodes in permissionless blockchains, which do not determine the purposes or means of processing and are not able to exercise control over data. A suggestion that nodes should form formal consortia is impractical and inconsistent with the open participation and lack of central coordination that are essential features of decentralised networks.

The guidelines appear contrary to EU policy generally in respect of decentralised technology and are problematic for organisations who wish to build products and services on permissionless blockchains, who might be fixed with very difficult compliance obligations affecting the application layer, due to the interpretation of settlement layer obligations.

In particular, but non-exhaustively, the following points are of concern:

- broad and unsupported statements in the guidelines appear to be unduly negative towards blockchain technology in general, going beyond EDPB's remit without grounding in legal or technical reasoning. This includes, in particular, statements in section 40 that organisations should generally only use permissioned blockchains, and should consider whether it is appropriate to use blockchain at all;
- guidance suggests that public keys, transaction data and hashes are all personal data and therefore should not be made generally available in an unencrypted format. This transparency is, however, is a core feature of how public blockchains work. It is not clear how this requirement could be met by a public blockchain;
- the suggestion that nodes are data controllers or processors is based on an inaccurate understanding of how nodes process transactions, as required by the blockchain protocol. Nodes do not decide what data is captured or have the ability to influence purposes or means of processing. Nodes do not act jointly, and a decentralised blockchain has no controller on behalf of whom nodes process data;
- the suggestion that non-compliant blockchains should be deleted as a remedy for non-compliance is technically unworkable and would compromise legitimate third-party rights recorded on the ledger;
- nodes in proof-of-work systems are in competition with each other for transaction fees and to win blocks (for example, by creating more effective mining software). Some alignment on standards might be possible, but it is hard to envisage how this would work in respect of anonymous node parties who might join and leave a blockchain at will. We do not think that forming a consortium is a feasible solution;
- we do not consider that it is workable to suggest that Article 22 GDPR automated decision-making rules apply to autonomous smart contracts, which are not controlled by any person to whom this obligation could attach.

DETAILED COMMENTS

Controller and processor responsibilities

The guidance suggests that a factual assessment must be carried out to understand GDPR controller and processor responsibilities in respect of blockchains.

The governance mechanism is suggested to be of key importance for determining GDPR roles and responsibilities (s.41). It is not clear what EDPB means by governance mechanism, as blockchains can employ a variety of technical, practical and legal governance arrangements. EDPB refers to a broad list of arrangements, including 'management of inconsistencies and violations', not all of which are generally considered to be part of a blockchain's governance arrangements.

We are also unclear what EDPB means when suggesting that a data protection by design approach can be relevant to the factual assessment of GDPR responsibilities: data protection by design is an obligation under GDPR, not a gateway to defining scope, application and compliance responsibilities?

Governance and decentralisation

s.36 says that decentralised governance cannot be used as a reason not to comply with GDPR.

Does EDPB here suggest that regulation applies to decentralised, permissionless technology? If so, we note this is at odds with the approach taken in most jurisdictions in respect of financial services law, including as set out by IOSCO.[1]

Nodes as data controllers / processors

The intended effect of s.42 is unclear. This section suggests that nodes might in some circumstances be considered to be data controllers or processors but acknowledges that a node that only: (i) prepares blocks; and (ii) validates transactions, *might* not be considered to be a controller.

- Firstly, it is problematic overall that nodes in permissionless systems could be considered data controllers. In a decentralised system, nodes perform a series of pre-defined actions by running protocol-aligned software. Nodes are anonymous parties who leave and join the network at will for the sole purpose of processing transactions, and do not define the data structure of a network, nor exercise any control over data added to the network by independent third parties. In addition, the core activities of nodes when securing blockchain transactions might generally go beyond the functions listed by EDPB in s.42 and include, for example, selecting and ordering transactions. This is not, however, an action that amounts to a determination of the purposes or means of processing data, but rather performance of an activity predetermined by the blockchain protocol.
- s.44 suggests that exercising a 'decisive influence' on the next subset of transactions to be added to a block mined is indicative that nodes should form a consortium. In a proof of work system, nodes compete with each other to win a block, like participants in a race. Transactions attract fees, and certain transactions might offer a higher

[1] https://www.iosco.org/news/pdf/IOSCONEWS720.pdf

payment to nodes, and consequently be picked up faster from a mempool and processed more quickly.

Nodes are in essence independent actors and in competition with each other, including in respect of transaction processing fees and investment in faster transaction processing software. Whilst some discussion between nodes on technical questions is likely permissible (as in an industry working group between competitors), it is unlikely to be feasible for nodes to create a formal consortium, as suggested by s.44. s.44 also misunderstands the influence nodes are able to exert, which does not relate to the data included in transactions, but is rather just a mechanical activity of processing performed in return for reward.

In addition, references to 'block' in this section make it unclear how this is intended to apply to nodes on other forms of distributed ledger network, in particular proof of stake blockchains.

In a permissionless blockchain, there is no link between nodes and any controller, and therefore we note that nodes will not generally be processing on behalf of a controller.

s.45 acknowledges that 'blockchain is only a technology, as cloud computing or peer-to-peer networks, and it is not a processing of personal data as such'. A blockchain comprises software, including a consensus mechanism and other protocol features, run by nodes – the blockchain includes and cannot be distinguished from the activities of the nodes. Without nodes, there is no blockchain. Nodes are part of the functioning of the technology.

Permissionless Blockchains

s.40 suggests that permissioned blockchains are preferable to permissionless blockchains and: *"offer a clearer allocation of responsibilities, which is a key element of the protection of data subjects, and organisations should favour permissioned blockchains. Organisations should explore different blockchain governance alternatives only if well-justified and documented reasons hinder this preference."*

We find this is contrary to the principle of technology-neutral regulation and is out of alignment with broader EU legal policy on decentralised systems. It also goes beyond the data protection regulator's remit.

In particular, complexity in respect of legal reasoning is not a relevant reason to ground a finding that all use of permissionless blockchains should in general be avoided.

s.40 further says: *'where such reasons exist, organisations should also consider whether it is actually appropriate to use blockchain technologies at all, and should carefully consider whether other technologies would be suitable for their purposes.'*

This statement reads as a general opinion, rather than objective legal guidance and we do not see a basis for its inclusion.

Non-compliant blockchains should be deleted

s.63 says: *"when deletion has not been taken into account by design [of a blockchain], this may require deleting the whole blockchain."*

In the case of permissionless blockchains:

- this is technically unworkable;
- deletion of a blockchain would also compromise the legitimate property rights of third parties in assets recorded on the ledger.

Processing unrelated personal data

s.95 says that: *"in some blockchain models, and particularly due to their distributed nature, personal data not related with the primary processing purposes could be processed in the blockchain ecosystem by third parties, like communication metadata or encryption management metadata. The controller should assess the data involved in such processing and take measures to guarantee the application of GDPR principles, in particular minimising such data, controlling the access to and storage of such data and making such processing transparent to the data subject."*

We note that application and product developers are not able to exert any influence over content that is already embedded in a blockchain and should not be controller nor processor in such circumstances. It is likely not to be practically or economically feasible for third party developers to bring incidental processing to the attention of unknown data subjects, nor are such notifications likely to be helpful or welcome to the data subjects concerned.

Smart contracts

s.107 says that the execution of a smart contract may, in some cases, constitute automated decision-making within the scope of Article 22 GDPR.

In the case of decentralised smart contracts, we note that it is not clear who would be subject to these duties, which would potentially execute autonomously, and that this guidance will likely give rise to practical and interpretive issues.

9 June 2025

Charles Kerrigan, Lisa McClory and Tom Marshall