Response to the EDPB Public Consultation on Guidelines 02/2025 on processing of personal data through blockchain technologies Version 1.1

Bilgesu Sumer,
Doctoral Researcher, *KU Leuven, CiTiP*
Contact: bilgesu.sumer@kuleuven.be
Bilgesu Sumer — CITIP
Bilgesu Sumer - Google Scholar

1. General Comments

The EDBP's guidelines for processing personal data through blockchain are long-awaited and necessary and include significant information. However, they remain highly general; some parts do not even go further than summarising the GDPR provisions. While the guidelines seem to align with the most scientific and legal proposals in the literature, no credit is given to this research.

Furthermore, the guidelines lack a detailed analysis of the case law regarding personal data and controllership, thus risking divergent interpretation as explained in detail below, e.g., factual influence (Case C-40/17 Fashion ID), relative approach (Breyer Case) doctrines.

2. Specific Comments

2.1. Personal data processing

The Guidelines provide information about the data inside a blockchain in paragraphs 25-35, and processing of personal data as a follow-up to this initial section in Section 4.2 (p.11). It is particularly appreciated that the Guidelines acknowledge that there is no black-and-white threshold regarding personal data and identifiability—it is ultimately a matter of risk.

Moreover, the Guidelines have established the importance of off-chain storage to prevent the storage of personal data directly in an immutable and public ledger of blockchains. In this approach, personal data is retained solely in separate storage connected to the blockchain via hash pointers. In most instances, transactional data is essential for the network's operation, as it verifies the integrity of the data through hash values and timestamps in the transactions.

Nonetheless, the following points should be taken into account when providing guidelines on personal data processing via blockchains:

It should be noted that identifiability is not given an absolute meaning in the GDPR (Recital 26) or in the CJEU case law.[1] This means that not all pseudonymised data is personal data (Also see AG Spielmann's Opinion in EDPS v SRB). Per the relative approach, some actors are usually in a position to combine such data. This analysis is indispensable when assessing the existence of personal data.

As explained aptly in paragraph 28 of the Guidelines, additional data can be processed or made available by third-party service providers, e.g., wallets. While these data are not stored in blockchain, the logic of blockchain only makes sense when there is a link with on-chain data and off-chain (identifiable) data. Thus, again, a relative approach analysis is a must when it comes to different storages that are linked to each other. While off-chain storage is mentioned in the context and scope of application of the guidelines (Section 2, p.6), this aspect is not clear in the Guidelines.

In the same vein, *cryptographic commitments*' legal status is unclear. In **para 53**, it is said that when original data is deleted, the commitment on the blockchain is useless. However, as explained,

[1] Breyer Case

blockchains are used to preserve and prove the link between the original identifiable data and the proof on-chain. Thus, this recommendation makes sense with regard to erasure, but does not change the fact that for some actors, the processing includes personal data.

Such an analysis is essential for the clarity of the roles and responsibilities and is unfortunately missing from the current guidelines.

2.2. Roles and responsibilities:

Between paragraphs 36 and 44, the Guidelines explain roles and responsibilities under the GDPR. It is highly appreciated that the connection between the principle of accountability and the roles is made.

Throughout the document, the EDBP repeatedly points to the controllers regarding their obligations under the GDPR. However, as the connection between personal data and controllership has not been made clearly based on the legal doctrines, neither for the academics nor for the stakeholders, who could be the controller, is clear.

In paragraph 42, nodes with limited decision-making powers are discussed and connected to the role of the processors. This is partly due to the absence of concrete examples, a pattern that appears throughout the document.

Different consensus models have different implications for the roles and responsibilities. Today, the most common protocol is Proof-of-Stake, and it should be given extra attention when discussing these roles and responsibilities.

Referring back to my note in Section 2.1, off-chain data and governance should be considered when discussing controllership and the responsibilities of the core developers (in line with Article 25 of the GDPR), and applying the factual influence doctrine in the recent case law of the CJEU.

In paragraph 44, and in general, centralisation within the network is suggested. This approach might not only conflict with the CJEU's factual influence doctrine (formal arrangements do not affect the real factual influence over the processing and thus the responsibility as a controller) but also undermine the potential of decentralised and distributed technologies to provide more control to the data subjects. In other words, centralisation-leaning approaches risk stifling innovation in truly decentralised technologies.

3. Concluding remarks

While the EDBP guidelines address some ambiguities, there is still a need for clarity on how the current case law applies to blockchains; the EDBP has overlooked the detailed assessment of the roles and responsibilities. A more thorough and updated analysis based on the upcoming case law is necessary.

Moreover, sectoral examples are needed as the GDPR is not a legal vacuum even when it comes to data protection.

Last but not least, sensitive, particularly biometric data processing through blockchains, e.g., proof of personhood, remains a crucial topic and should be addressed by the EDBP.

09.06.2025

Leuven