To: European Data Protection Board (EDPB)

From: Bitpanda Legal Privacy Team

Date: June 2, 2025

Subject: Concerns Regarding EDPB Guidelines on Blockchain and Personal Data

This memorandum sets out to address critical issues entailed in the European Data Protection Board (EDPB) guidelines on processing personal data through blockchains.

General observations:

A Regulatory Compliance and Security First approach has been fundamental to our operations since the outset of our presence in the market.This position always requires specific focus, dedication, close cooperation with relevant authorities and willingness to take the "extra mile", especially in view of the new technology that provides unorthodox solutions, approach and innovation to the established financial legacy system or data protection laws. We are strong believers in ensuring compliance and security while maintaining a reasonable, proportionate and tech-agnostic position on a given technology. Such an approach will lead to proper regulatory approach, stronger innovation and overall growth of the single market and now, the Saving and Investment Union.

It should not be attempted to fit new technologies and its distinctive characteristics into an existing regulatory framework that is not designed to accommodate them. The risk is that the current approach fails to recognise the inherent protection of privacy while providing an unseen before level of financial transparency and traceability (the principle of treating different things differently). Unfortunately, **we fear** that this is the case with the proposed Guidelines by EDPB **due to the fact that** they highlight **alleged incompatibilities** between blockchain key technical features and data protection rules. Should the guidelines remain unchanged, there is a real and tangible risk that the blockchain and decentralisation will simply vanish in the EU and we will experience stifling of innovation and outflow of capital and users to jurisdictions with lower level of protection and standards.

Consequently, we strongly encourage you to revisit and adjust the current proposal in order to avoid damaging impact and ultimately "closure" of the industry in the EU and properly reflect the nature and architecture of this technology. Below, we provide our recommendation and approach to mitigate the concerns about data protection principles.

Problematic points in general:

The guidelines as they are, conflict with the following unique attributes of blockchain technology

1. **Conflict with the Principle of Immutability and non-recognition of pseudoanonymity** - one of the key attributes of blockchain is its "**immutability**" - once data is recorded, it cannot be altered or deleted. Importantly, on-chain data storage is not a common practice. The system is in itself "pseudoanonymous" which is a compromise between privacy and transparency for an open, decentralised financial system without the need of intermediary and central supervision.
2. **Defining a Data Controller in Decentralized Networks** - another feature is decentralisation

and lack of single point of contact (also failure). It is at the same time permissionless, meaning inclusionary. The rules on “data controller” should they recognise this without compromising blockchain functionality.

The guidelines collide with the fundamental architecture of blockchain - decentralised, immutable, transparent and pseudonymous access - whose objective is to strike a fair balance, especially in financial terms, between different objectives and interests. Therefore, data protection is by default an inherent objective of blockchain.

Specific issue:

The guidelines' assertion in paragraph 63, that "**if personal data recorded on a blockchain cannot be deleted individually, it may be necessary to delete the entire blockchain**," **is deeply problematic**. This stance **presents significant technical and legal hurdles**, potentially rendering the deployment of public permissionless blockchains within the EU practically impossible. This outcome would undermine European competitiveness, innovation, and individual privacy rights.

The interpretation fails to acknowledge the technical realities of public permissionless networks, where data is replicated across numerous nodes globally, often beyond any jurisdictional reach. Deleting an entire blockchain is, in most cases, technically infeasible. Moreover, such a requirement could result in the irreversible loss of valuable data and assets, disrupt critical financial infrastructure, and erode trust in the stability and reliability of blockchain-based systems. The risk of forced deletion could also deter investment and participation in EU-based blockchain projects, driving talent and capital to more technologically accommodating jurisdictions.

Solutions:

The proposed recommendation by EDPB, unfortunately, does not ease the friction. We do not see that they recognise the inherent difficulty to be compliant (ex. Conducting Data Protection Impact Assessments or Clarifying Roles and Responsibilities). The solution needs to adjust to the new reality. Once again, blockchain is not an adversary of data protection but a proponent. The current features should not be seen as a bug but as an added-value feature based on its objectives. Therefore, in our view, alternative solutions that align with both the General Data Protection Regulation (GDPR) and blockchain technology's operational realities must be considered. **Some of the solutions might entail the following:**

1. **Key Deletion (Crypto-shredding):** Deleting the encryption key effectively renders the underlying data permanently inaccessible, achieving the functional equivalent of deletion.
2. **Off-chain Storage with Revocation Capabilities:** Storing sensitive data off-chain and posting only hashes or proofs on-chain, coupled with revocation mechanisms via smart contracts or access controls, offers a viable alternative.
3. **Zero-Knowledge Rollups:** Employing zero-knowledge rollups enables verifiable state transitions without revealing the underlying data, thus safeguarding privacy.

It is imperative to interpret the GDPR in light of its purpose, which is to protect personal data, while also acknowledging the technical limitations and unique characteristics of blockchain technology. A strictly literal interpretation that mandates the deletion of an entire blockchain is not only impractical but also counterproductive to the GDPR's aims and the EU's broader digital strategy.

In conclusion, we strongly urge the EDPB to reconsider its stance and adopt a more pragmatic approach that recognizes the technical realities of blockchain while upholding the principles of data protection.