Cardano Foundation

09 June 2025

Submitted via online form on the EDPB website
(https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/reply-form_en?node=8743)

Re: Public consultation on EDPB Guidelines 02/2025 on processing of personal data through blockchain technologies

To whom it may concern

We appreciate the European Data Protection Board's (EDPB) openness and welcome the opportunity to provide comments in this public consultation.

The Cardano Foundation is an independent Swiss not-for-profit organization that oversees and supervises the advancement of the public, permissionless blockchain protocol Cardano and its ecosystem. As an important contributor to the blockchain and the owner of the Cardano brand, the Foundation works to drive adoption and partnerships, grow the wider blockchain community, shape relevant legislation, and commercial standards, and ensure stakeholder accountability.

Kindly find our comments below. We focus our efforts on the three most material issues we identify with the consultation. We further support the more extensive feedback provided by INATBA under separate cover. We gladly address any follow-up questions and would be happy to contribute to further discussions with the EDPB.

Yours sincerely,

Nicolas Jacquemart

Chief Legal Officer, Dr. iur.
Cardano Foundation
nicolas.jacquemart@cardanofoundation.org

1 Introduction

A central element of the Cardano Foundation's mission is to support the development of regulatory frameworks that are proportionate, technologically neutral, and non-discriminatory towards open, permissionless systems such as the Cardano blockchain protocol.

The Cardano blockchain is a public, permissionless 'Layer 1' blockchain protocol based on academic research and built on open-source architecture. Since its launch in 2017, it has maintained ongoing operation and is supported by a globally distributed set of maintainers and participants, such as stake pool operators, developers, and users. Its core design principles—resilience, transparency, decentralization, and adaptability—position Cardano as a form of digital public infrastructure capable of underpinning a wide range of use cases and applications.

We share the EDPB's view that privacy, accountability, and regulatory compliance are critical components of a trustworthy digital environment. We appreciate the overarching aim of the proposed Guidelines 02/2025 (hereinafter "Guidelines") to provide practical and actionable guidance on the application of the EU General Data Protection Regulation (GDPR) in the context of blockchain technologies. However, the current proposal does not sufficiently reflect the defining characteristics of public, permissionless blockchains and lacks relevant differentiation between the infrastructure and application layer. As a result, certain proposed requirements appear misaligned with the technical and economic realities of such systems and risk unduly limiting their lawful use within the EU. Given the EU's tendency to err on the side of more rather than less regulation, the guidance accompanying such regulation should at least endeavour to be as permissive as possible under applicable law.

In the following, we will lay out (i) why distinguishing between blockchain as infrastructure and its application is critical for assigning responsibility under the GDPR, (ii) how an overly broad interpretation of personal data—particularly regarding hashed data—risks misapplying compliance obligations, and (iii) the importance of an open, technologically neutral and innovation-enabling approach towards public, permissionless blockchains.

2 Blockchain as public infrastructure

We believe the Guidelines fall short in appropriately distinguishing between the technical operation of a public, permissionless infrastructure and its use, leading to inadequate role assessment and misattribution of GDPR obligations. In particular, they too broadly assume that node operators act as controllers, without sufficiently considering their limited and protocol-bound function.

At its core, blockchain is a base-layer technology that combines a distributed database with a protocol for network coordination. It is inherently general-purpose and agnostic to the type of data it records. As such, a blockchain should be understood as a neutral infrastructure—comparable to the internet protocol suite TCP/IP or an open-source operating system.

In the case of public, permissionless blockchains such as Cardano, anyone can read from or write data to the ledger in accordance with predefined rules. Likewise, anyone may contribute to the network's operation by running a node, ensuring the updating of the ledger and maintaining consensus on the system's current state. Nodes are merely validating data according to set technical rules and do not have operating discretion. Node operators are redundant components of a distributed system acting in accordance with the defined parameters of the protocol.

The act of using a blockchain—by reading from it or writing data by submitting transactions—must be clearly distinguished from the function of operating the infrastructure itself. The infrastructure functions as an open and neutral platform. Neither the protocol itself nor the nodes determine or have any influence over the purpose or content of the processed data . Control over how the infrastructure and, in particular, what data is recorded on-chain, rests entirely with the individual users implementing blockchain as a back-end technology in their applications. Nodes of public, permissionless blockchains should not be made GDPR subjects just by the mere potential that such infrastructure might be used for processing personal data. Assuming that the purposes and means of the processing of personal data can be determined by the underlying infrastructure is neither expedient nor proportionate to protect and enforce data subjects' rights. By similar logic, operators of switching infrastructure could be argued to be responsible for all data routed and thereby "processed" in their data centres. This is obviously not compatible with the neutral base functions of the internet.

We believe the Guidance lacks sufficient distinction and risks conflating the neutral operation of a base-layer infrastructure with the use of it. Further guidance should be provided, including the clarification that running a node for a public, permissionless infrastructure does not imply control over the purpose and means of data processing.

3 Hashes and an overly extensive scope for 'personal data'

A central concern in the application of the GDPR to blockchain infrastructure lies in the interpretation of what constitutes personal data. The Guidelines adopt an overly broad stance, stating that "hashes of personal data will still be considered personal data, as will any other identifiers that still might exist." While this may be correct in certain contexts—particularly where hashes serve as persistent identifiers linked to individuals—this determination is inherently fact and circumstance bound. The current Guidelines risk significant overreach and ultimately the stifling of innovation by applying such a principle without regard to function or context.

In blockchains, hashes are an essential component used to link blocks together and to cryptographically verify data integrity. Automatically classifying all hashes as personal data if a single

block contains an identifier derived from or linked to an individual could lead to the conclusion that an entire blockchain qualifies as personal data. This would effectively extend GDPR obligations to all infrastructure participants—even those with no access to or control over the data in question, such as nodes (see above) or other users of the infrastructure—based solely on the presence of these cryptographic links.

This problem reflects a broader uncertainty around the interpretation of personal data. As per the Guidelines, the EDPB seems to lean towards an absolute interpretation, where personal data is any information that could allow anyone, with any available means, to identify a natural person—even if such identification potential is highly improbable. While this view offers a uniform and straightforward standard, it applies the GDPR to situations where no meaningful risk to data subjects exists and creates misaligned obligations. We advocate for a more moderate approach ('relative approach'), that considers whether a specific actor has the actual means, knowledge, or legal authority to identify an individual based on the data in question, without disproportionate effort. We refer to the related European Court of Justice (ECJ) jurisprudence regarding dynamic IP addresses and similar cases[1] that supports a less absolute approach whereby the identifiability should be assessed in light of whether the controller has legal means to obtain additional identifying information from a third party.

Applied to blockchain, the scope of what qualifies as personal data is particularly important. On-chain hashes may originate from personal data, but if they are mathematically irreversible, not used as permanent identifiers, and not combined with re-identifiable information, treating them as personal data would be disproportionate. Such an interpretation creates legal uncertainty for infrastructure operators who, by design, have no access to application-layer data or insight into its origin, as demonstrated in section 2 above. The Guidelines should therefore avoid absolute classifications for personal data and instead promote a contextual assessment based on whether the party processing the data can reasonably identify a natural person. This would uphold the GDPR's principle of proportionality and prevent an overreaching application.

4 Implied bias against public, permissionless blockchains

The Guidelines reflect a discernible preference for permissioned blockchain systems, framing them as more readily aligned with the structure and requirements of the GDPR. While permissioned systems may offer simpler solutions in terms of defined governance and identifiable data controllers, this implicit preference undermines the principle of technological neutrality and fails to recognize the benefits of decentralized and open-access infrastructures such as public, permissionless blockchains.

Public, permissionless blockchains offer unique structural benefits that can directly support data protection objectives. By design, they eliminate the reliance on centralized intermediaries, thereby reducing single points of failure, limiting opportunities for data misuse, and enhancing user control and

[1] ECJ, judgment of 19 October 2016 – C-582/14; European General Court (EGC), judgment of 26 April 2023 – T-557/20; ECJ, judgment of 9 November 2023 – C-319/22.

digital self-sovereignity. Their transparency and immutability provide auditability, enabling verifiable records without reliance on proprietary infrastructure. These properties are particularly valuable in contexts such as decentralized identity, digital registries, and cross-border services, where trust can only be truly established without centralized oversight. The openness and inherent transparency of these systems also offers a meaningful alternative to the challenges posed by monopolistic platforms, where a small number of dominant actors amass vast amounts of personal data and concentrate informational power (e.g. social media networks or search engine providers), gatekeeping major parts of the digital sphere.

Additionally, as public, permissionless blockchains provide an open and neutral infrastructure, they can also indirectly enable new privacy-enhancing solutions, such as for instance the Veridian[2] platform using Cardano. Veridian is an open-source, self-sovereign identity (SSI) suite that enables the issuance and verification of decentralized identifiers (DIDs) and credentials using secure, interoperable protocols like KERI and ACDC. It leverages the Cardano blockchain to anchor cryptographic commitments, ensuring data integrity, auditability, and trustless verification without relying on centralized authorities.

If the EDPB aims to support digital self-sovereignty and does not want to unduly stifle innovation in Europe, they must avoid defaulting to centralized and control-based architectures and instead promote a level regulatory playing field inclusive of public, permissionless infrastructure. The Guidelines should adopt a risk-based approach that recognizes open systems not as a threat, but as viable, rights-preserving alternatives. Advancing the GDPR's objectives in a technologically neutral manner requires acknowledging that public, permissionless infrastructure, when used correctly, can enhance data protection.

[2] https://www.veridian.id/