Response to the EDPB on its consultation on its Guidelines 02/2025 on processing of personal data through blockchain technologies

Google welcomes the opportunity to provide feedback on the EDPB's Guidelines 02/2025 on processing of personal data through blockchain technologies (the **Guidelines**). While Google recognises the value of the EDPB's guidelines to encourage further adoption and enable responsible innovation, development and exploration of applications of the technology, it is important that the Guidelines have clear and practicable recommendations that promote privacy protections for individuals.

The Guidelines identify various specific GDPR compliance challenges presented by use of blockchain technologies, including that the:

- permanent availability of data stored on the blockchain presents challenges for complying with the storage limitation principle, as well as with data subjects' rights to erasure, correction, and not to be subject to decisions made solely by automated means;
- decentralised nature of the technology and multiplicity of actors and roles involved in the processing results in a complex controllership analysis; and
- distribution of nodes (which may include nodes outside of the EU) may trigger international transfer rules, but the high number of interconnected nodes and the fact they may not be known to each other, makes compliance with international transfer rules challenging.

Our response to the Guidelines contains some general observations on these challenges and the guidance and recommendations of the EDPB in relation to them. We hope these viewpoints are helpful.

Observation 1: the EDPB strongly encourages use of "off-chain" storage solutions

In the Guidelines, the EDPB strongly discourages the storage of personal data on the blockchain itself ("on-chain").

The Guidelines instead strongly advocate for only storing personal data on-chain which functions as proof of existence (e.g. by use of a pointer, a cryptographic commitment or a hash generated from a keyed hash function), with the data that should be used to verify the proof being kept outside of the blockchain) ("off-chain" storage) (para 54). While we acknowledge the general approach of maintaining personal data off chain where practicable, we suggest that it would be helpful for the EDPB to consider a more flexible, context-based and proportionate approach to how this is addressed (e.g. integrity of the data and transactions on the ledger).

However, the Guidelines reinforce the EDPB's positions on anonymisation and pseudonymisation, including that encrypted data are *in all cases* personal data (para 51). Google refers to its previous responses to the EDPB's Guidelines 01/2025 on Pseudonymisation in this regard. Google also reminds the EDPB of the Opinion of Advocate General Spielman in the case of EDPS v SRB (**AG Opinion**) which contradicts the EDPB's view that pseudonymised data remains personal data *in all cases* when it is in the hands of a third-party recipient (without any reference to whether the receiving third-party can reasonably identify data subjects from the data).

This position also does not allow for or acknowledge possible uses of privacy enhancing technologies (PETs) that could effectively minimise risks to data subjects in future in the context of on-chain storage of personal data other than with only a proof of existence function. As we suggested in our response to the consultation on the EDPB's recent Pseudonymisation guidelines, we encourage the EDPB to delay the finalisation of these Guidelines until after the final judgement of the CJEU is published.

The Guidelines should take the opportunity to promote an approach that creates incentives for the use of PETs and promotes trust and confidence in how personal data is protected.

Observation 2: technical challenges with compliance with data protection principles and data subject rights in the context of blockchain

Encryption and hashing of personal data stored on-chain assists compliance with the integrity and confidentiality principle under GDPR. However, these measures do not resolve the fundamental technical challenges of complying with other data protection principles (including storage limitation) and data subject rights (such as right to rectification and erasure).

The Guidelines are unequivocal in their statement that technical impossibility cannot be invoked to justify non-compliance with GDPR requirements. Google welcomes the helpful statement in the Guidelines that *"Nevertheless, a proactive approach, combining organisational measures, techniques and governance models could transform perceived constraints into opportunities for compliance,"* (para 50). However, when the Guidelines are read as a whole (e.g. with para 103, which simply seems to recommend looking at tools other than blockchain), it is difficult to deduce the EDPB's view as to how organisational measures, techniques and governance models could be employed to ensure that the use of personal data on the blockchain is GDPR compliant. Further guidance on addressing the tension between these points is needed to provide a clearer position on what steps organisations can confidently take.

Observation 3: impracticalities with identifying roles of parties

The current Guidelines appear to place a heavy emphasis on the design choices of the entity initiating a specific blockchain application (the primary controller determining the "why" of processing). However, this focus may not adequately reflect the nuances of responsibility where other entities, such as those providing foundational blockchain infrastructure, platforms, or tools (e.g., cloud service providers offering blockchain-as-a-service or API access), significantly contribute to the non-essential "means" of processing. These entities,

by providing the technical and organizational infrastructure, inherently influence the "how" data is processed on or via the blockchain, even if they do not determine means closely linked to the purpose and the scope of the processing (such as the type of personal data processed or the categories of data subjects), or the ultimate "why" for a specific application built by a third-party controller.

This dynamic is reminiscent of principles articulated in the EDPB's Guidelines 07/2020 on the concepts of controller and processor in the GDPR, which acknowledge that a processor can influence the non-essential means of processing without being considered a controller with respect to that processing. The Blockchain Guidelines could benefit from more explicitly considering how these established principles apply to entities providing the underlying technology and tools. Without such clarity, there is a risk that the significant influence of infrastructure providers on the "means" of processing personal data within blockchain ecosystems is not accurately fully accounted for in the allocation of responsibilities, potentially leading to confusion for data subjects if entities are incorrectly identified as controllers.

In addition, the Guidelines suggest (at para 43) that nodes in a public permissionless blockchain may be *joint controllers*. Indeed, the Guidelines imply (at para 44) that nodes jointly agreeing (or not) on modifications of the protocols and the rules that apply to the blockchain would make them joint controllers, but respectfully, the analysis to support this position is missing. This position implies that any decision by a node to participate in mining and validation activities in a blockchain is a decision with respect to the purpose and/or essential means of processing of personal data, making that node a joint controller with all other nodes in the network. This raises a concern about how this would practically be executed in real life situations, and lack of clarity as to when a node should consider itself an independent controller or a processor.

While the EDPB does state in the Guidelines (at para 44) that it “strongly encourages” the establishment of a consortium or any other type of legal entities among the nodes (to be the controller), this seems like a theoretical approach, more challenging in practice. Further engagement with stakeholders would be needed to test the feasibility of such an approach. Google would therefore welcome more practical guidance and recommendations, particularly on identifying the roles of parties in the blockchain, and documenting and contracting between entities fulfilling those roles.

June 2025