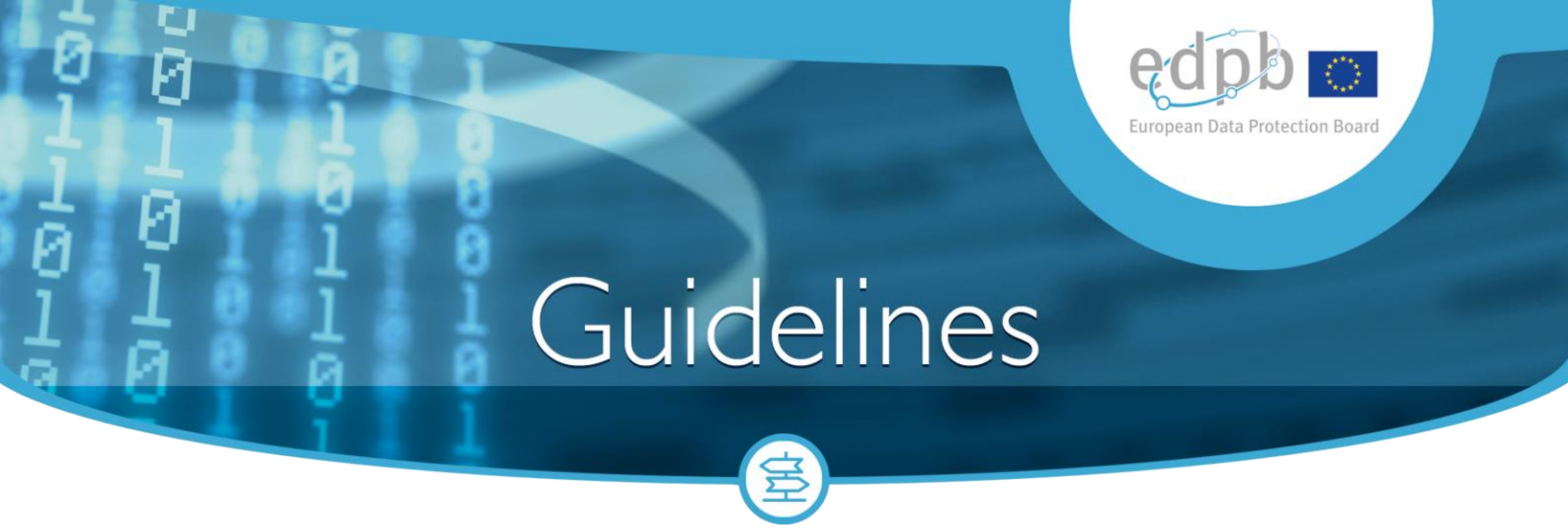

Guidelines 02/2025 on processing of personal data through blockchain technologies

Version 1.1

Adopted on 08 April 2025

Executive Summary

The distributed nature of blockchain and the complex mathematical concepts involved imply a high degree of complexity and uncertainty that leads to specific challenges with respect to the processing of personal data. In this context, in order to ensure that the processing of personal data complies with the GDPR, risks for rights and freedoms of data subjects need to be carefully assessed. Some of these risks can be mitigated through technical measures upfront, while finding a solution for other risks of non-compliance might be more challenging at this stage. Furthermore, blockchains have certain properties that can lead to challenges when dealing with the requirements of the GDPR. Such properties require to reinforce data protection by design measures in order to implement principles and rights, for example/like the principle of storage limitation and data subjects' rights such as the right to rectification and the right to be forgotten. Therefore, the controller should carefully assess the blockchain solution it intends to use to avoid non-compliance risks and specific risks to the rights and freedoms of data subjects.

These guidelines provide a framework for organizations considering the use of blockchain technology, outlining key GDPR compliance considerations for planned processing activities. They provide an overview of the fundamental principles of blockchain technology, assessing the different possible architectures and their implications for the processing of personal data. Furthermore, they clarify that roles and responsibilities of different actors in a blockchain related processing need to be assessed during the design of a processing and what elements need to be considered in this respect.

Depending on the purpose of processing for which blockchain technology is used, different categories of personal data may be processed. The guidelines highlight the need for Data Protection by Design and by Default and adequate organisational and technical measures. They also provide examples of different techniques for data minimisation and for handling and storing personal data.

As a general rule, storing personal data on a blockchain should be avoided, if this conflicts with data protection principles. To assist with the compliance with data protection principles, one of several available advanced techniques, appropriate organisational measures and appropriate data protection policies[1] should be used when considering storage of personal data on-chain. The guidelines detail technical aspects and different ways of implementation for such techniques, highlighting their strengths and weaknesses in order to help organizations on choosing appropriate measures.

Additionally, the guidelines discuss the interplay between the technical aspects of blockchain and the data protection principles of Article 5 GDPR. They emphasize the importance of the rights of data subjects especially regarding transparency, rectification and erasure. The guidelines also highlight the importance of carrying out a Data Protection Impact Assessment (DPIA) prior to implementing a processing using blockchain technology and provide key aspects to be considered in a structured way when conducting a DPIA.

Finally, in Annex A the guidelines provide a set of concise recommendations for organizations planning to set up a blockchain based processing.

[1] GDPR Art 24 (1) and (2)

Table of contents

1 Introduction....................5

2 Context and Scope of Application....................6

3 Description of the technology of blockchains....................6

3.1 Different types of blockchains....................7

3.2 Data inside a blockchain....................8

3.3 Roles and responsibilities....................9

4 Evaluating Blockchain-Based Processing....................10

4.1 Introduction....................10

4.2 Processing of personal data....................11

4.3 Principles of Data Protection....................13

4.4 Lawfulness of processing....................15

4.5 International transfers....................16

4.6 Data protection by design and by default....................16

4.7 Data retention periods....................17

4.8 Security....................17

4.9 Data Protection Impact Assessment....................18

5 Data subject rights....................20

5.1 Information of data subjects, right of access and right to data portability....................20

5.2 Right to erasure and right to object....................20

5.3 Right to rectification....................21

5.4 Right to object to a solely automated decision. 21

ANNEX A – Recommendations....................22

ANNEX B – Glossary....................25

The European Data Protection Board

Having regard to Article 70 (1)(e) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018[2],

Having regard to Article 12 and Article 22 of its Rules of Procedure,

HAS ADOPTED THE FOLLOWING GUIDELINES:

[2] References to "Member States" made throughout this document should be understood as references to "EEA Member States".

1 INTRODUCTION

1. The concept commonly referred to by the term blockchain addresses a technology that implements a distributed and consistent database without centralised management and its coordinated use by an open or predefined set of participants according to an agreed upon set of rules.

2. Blockchain – or, in a more general manner, Distributed Ledger Technologies (hereinafter "DLT") – can replace intermediation-based transactions. For instance, when using blockchains, financial transactions are possible without the intermediation of banks or other financial intermediaries, since the ownership on an asset can be proven without the intermediation of a notary.

3. In practice, blockchains aim to exhibit the following properties:

   - distributed (data is replicated by multiple participants peer-to-peer and so stored in multiple locations)
   - disintermediated (validation of data added to the database does not need the endorsement of a trusted or central party, but rather the agreement of participants in the blockchain)
   - consistent and tamperproof (any update or removal of validated data can be detected)
   - transparent (access to data and its auditing is available to all participants in the blockchain)

4. There is no unique implementation mechanism – an actual blockchain used in a processing could modify, extend, or restrict these general properties in any way, for example, by restraining the public access to the data.

5. These guidelines concern the processing of personal data in connection with the use of the blockchain technology and use the term to refer to technologies with the above properties.

6. One of the main promises of blockchain technologies is that they can offer strong technical guarantees in terms of integrity and availability due to the cryptographic tools used (hashing and digital signatures) and the decentralised storing system. However, this is a general assumption; in practice, there may not be standardised or formal agreement on the level or quality of service provided.

7. Blockchains show a number of properties, that create specific non-compliance risks and risks for the rights and freedoms of natural persons[3] when dealing with personal data. For example, once a transaction is recorded on the chain, it cannot individually be altered or removed without being detected as an inconsistency in the chain.

8. In addition, blockchains do not allow for a gradual adoption. Once introduced, they offer very limited possibilities to step back as they do not have a default process to support the deletion of transactions.

9. There can be issues for the implementation of the data protection principles under Article 5 GDPR and data protection by design and default pursuant to Article 25 GDPR, as is discussed in section 4 of these guidelines. The controller should analyse thoroughly whether the use of a blockchain will allow them to comply with data protection law. In particular, regarding the application of the principles of minization and storage limitation, and the effective exercise of rights like erasure and rectification

10. Moreover, the use of decentralized technologies may trigger different compliance risks and risks to individuals' rights and freedoms due potential international transfers, multiple stakeholders, new

[3] e.g. a paradox: While the intention behind using blockchain is often to give users more control over their data, users may end up losing control over their data, owing to the permanent availability of data stored on the blockchain.

processing operations for maintenance of blockchain system[4], allocation of responsibilities, and governance and management issues.

2 CONTEXT AND SCOPE OF APPLICATION

11. Blockchain is a technology that can be used in various ways and for very different types and purposes of processing of personal data. Therefore, these guidelines will not study blockchain as a processing of personal data, but will rather analyse the interplay of the technical characteristics of this technology with the data protection principles. These guidelines aim to provide practical guidance to controllers planning to use blockchain technology.

12. Many uses of blockchain technology will involve international transfers and the use of cloud computing or alike. This is especially true if a blockchain includes nodes that are based outside of the EU, and controllers should be especially aware of their legal obligations when using blockchain technologies in such circumstances. Issues arising from those circumstances are not specific to blockchains. The reader is referred to other guidelines and statements on those subjects published by the EDPB.

13. Blockchains generated and controlled by and for a single entity are out of scope for part of these guidelines. However, the evaluation of the necessity of such blockchains should still be carried out when personal data are processed, and mitigation measures found in this document could prove useful for any blockchain processing personal data.

14. The choice of the components that constitute a specific blockchain determines its inherent technical properties. For the purposes of the following analysis, the EDPB considers the following blockchain components:

- the block data structure describing the data fields retained in blocks and any other data on-chain storage (accounts, smart contract storage, receipt logs, etc);
- roles and responsibilities of different stakeholders;
- the consensus algorithm describing the conditions to append and verify blocks;
- the governance mechanism;
- communication networks for an exchange of information among users;
- ecosystem to interact with the blockchain, like user access tools (e.g. wallets), exchange offices, chain exploration tools, identification protocols, or local storage in databases;
- off-chain storage.

3 DESCRIPTION OF THE TECHNOLOGY OF BLOCKCHAINS

15. Blockchains provide a distributed database consisting of a public ledger of use-case specific transactions. Participants can use their own node(s) with a copy of the ledger or rely on the ledger of other nodes. The consistency and integrity of all ledgers is crucial for achieving a consensus and realised by two core principles:

- First, sets of transactions are denoted as blocks. Each block is always cryptographically linked to its previous block, so that all blocks form a chain.
- Second, a consensus algorithm is used to agree on the one valid block that will be appended to the chain.

[4] ISO 22739:2024: system that implements a blockchain.

16. Each node is interconnected with other nodes and together they form the blockchain network. A node contributes to different tasks, e.g., validating transactions or maintaining the state of the blockchain network. Nodes communicate with each other and use a consensus mechanism to ensure the consistency of the blockchain. This helps to prevent any single point of failure or manipulation of the data. As more nodes join the network, the blockchain network's size grows, making it harder for an attacker to alter the data. Different types of nodes can exist depending on the specific architecture of the blockchain network. Overall, the interconnected nature of nodes in a blockchain network is essential for maintaining the desired properties of the blockchain.

17. Common consensus algorithms rely on the proof of work or the proof of stake mechanism, but other consensus mechanisms also exist. The proof of work mechanism implies that the new block includes the solution of a resource-intensive mathematical puzzle, while the proof of stake mechanism implies that the node that generates the next block is chosen via various combinations of random selection and token of implication in the blockchain (like for example account balance or account age). For example, the Bitcoin blockchain uses a proof of work mechanism through a mathematical puzzle that many nodes try to solve in parallel, while Ethereum uses a proof of stake mechanism.

18. The verification of the validity of the transactions to be added in the new block is made by the nodes depending on the underlying consensus algorithm. The consensus algorithm ensures that no conflicting transactions are contained in the entire chain of blocks. In case of two valid, but conflicting, successor blocks, usually the longer chain is considered valid and as the chain to build upon. This last point usually implies that a transaction is considered as definitive only when a few blocks have been subsequently added.

19. Once a transaction is definitive, it usually cannot be removed from the blockchain, as the inconsistency would be detected. A full verification of the blockchain requires access to all of its blocks.

20. A lot of blockchains allow for so-called smart contracts[5], which allow for programmable transactions or even more generic programs. The results of transactions involving them are reflected in changes to the state of the information stored on the blockchain, among which is the smart contract storage. The smart contract is automatically recorded on the blockchain itself when created.

3.1 Different types of blockchains

21. Blockchains can be categorised according to their policies for access, participation and control of the infrastructure. This often breaks down into two elements: (1) whether the chain is public or private and (2) whether it is a permissioned or permissionless blockchain. The most commonly used ones are public permissionless blockchains (e.g. Bitcoin and Ethereum) and private permissioned blockchains (common choice within companies).

22. Permissionless blockchains provide for participants with equal rights and capacities: anyone can read, write, or create blocks. Those blockchains are decentralised.

23. Permissioned blockchains diverge from the original concepts and include an authority that must give permission to participate: only selected nodes can read, write, or create blocks, depending on the rules that apply to the blockchain. Depending on the particular design, the authority can be a single entity or a group of entities sharing a common interest on the blockchain. Participants are not always equal (although this is also true in permissionless public blockchains). The power of each participant depends on the governance system and its level of participation.

[5] The EDPB notes that this term is not unique to the blockchain environments. Article 2(39), Regulation 2023/2854 ('the Data Act') defines a smart contract as "*a computer program used for the automated execution of an agreement or part thereof, using a sequence of electronic data records and ensuring their integrity and the accuracy of their chronological ordering*".

24. The initial concept of blockchain includes transactions where the identities of the parties involved are visible to all. Some blockchains provide ways of hiding those identities to most people reading the chain using advanced cryptographic tools. While zero knowledge proofs are only one of the cryptographic solutions used for this, the blockchains using such tools are often called "zero knowledge blockchains".

3.2 Data inside a blockchain

25. Blockchains store metadata of the transaction combined with a payload.

26. Metadata of transactions includes both identifiers of the users who are participants of the transactions and other metadata. Each user participating in a transaction may, for instance, be associated with an identifier comprised of a series of alphanumeric characters which looks random, and which constitutes a public key derived from a private key known to the user. If the user is a natural person and those public keys can be used to identify the individuals by means reasonably likely to be used, for example in case of a data breach[6], then those identifiers qualify as personal data.

27. In many blockchains, these identifiers are always visible to all participants in order for transactions to be fulfilled and verified. Some approaches may provide ways of hiding identifiers using advanced cryptographic tools, but the data which replaces those identifiers may still constitute personal data.

28. Further, additional data can be processed or made available when interacting with a blockchain (e.g. through a decentralised application (i.e. dApp), blockchain wallet, third party, intermediaries, etc.), such as IP addresses, which can constitute personal data but are not stored on the blockchain.

29. Transactions on a blockchain are generally associated with content data (also called the "payload" of a transaction). This can be an amount of cryptocurrency, a link to a document, an item purchased, a smart contract procedure call, etc. This payload can also include personal data, related either to the users involved in the transaction or to other natural persons.

30. The transaction payload is stored on-chain, meaning that the data will be stored inside the blocks themselves. However, the EDPB also emphasises that on-chain data (including on-chain personal data) is not limited to the transaction data; rather, it may include other data structures stored on the chain, and that these other data structures may also contain personal data. Alternatively, off-chain storage can be used, meaning that the data will, at least partially, be stored outside the blockchain, with a link or reference to the data stored in the transaction payload to address scalability or confidentiality needs.

31. When the controller decides to store additional personal data on-chain beyond the identifiers already present in transaction metadata, different approaches may be used to mitigate the data protection compliance risks associated with on-chain storage or to allow data subjects to exercise their rights. However, they all come with some drawbacks discussed in section 4.2 of these guidelines.

32. Encryption algorithms can be used for on-chain storage as a security measure. This can mean that only encrypted payload data is stored in the blockchain. This is intended to limit access to those with the corresponding encryption key, although the possibility of data breaches cannot be entirely ruled out.

33. It is also possible to use other security measures[7], such as key derivation functions, hash-based message authentication codes (HMACs), other cryptographic one-way functions or other schemes. These can also be used to protect the confidentiality of the original data by putting only the function

[6] Multiple hacks and data breaches on blockchain, see for example https://defillama.com/hacks

[7] Security measures are technical and organisational protections, but not fully guarantees for data protection.

values obtained with a given secret key on-chain, while storing the original data off-chain. If needed, the integrity of the data can be checked by applying the function again using the same secret key.

34. Cryptographic commitments can likewise be used as a measure to protect the confidentiality of the original data by putting only the commitment on-chain, while storing the original data off-chain. This will allow the use of the blockchain for proving the integrity of the commitment. Such commitments, in theory and when applied correctly, can allow users to bind themselves to a value (i.e. a piece of information) in such a way that (i) they cannot change their mind afterward and (ii) no information can be learned on the value committed just by seeing the commitment. If needed, the commitment can be used to verify the validity of a value the user reveals as the data they committed to.

35. It should be noted that the storage of personal data as plain text data could conflict with various data protection principles under Article 5 GDPR as discussed further below and therefore, is strongly discouraged.

3.3 Roles and responsibilities

36. The decentralised governance model used by blockchain leads to a multiplicity of actors and roles involved in the processing[8]. However, neither this fact nor the selection of a particular technical infrastructure can be used as a reason not to comply with the GDPR. There must, therefore, be a careful assessment of the roles and responsibilities for each processing activity carried out in and over the blockchain.

37. The EDPB has already issued comprehensive guidelines on the concepts of controller and processor in the GDPR[9].

38. The GDPR defines the data controller as the entity “which, alone or jointly with others, determines the purposes and means of the processing of personal data”[10], while the processor is defined as “a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller”[11]. Blockchain is a technology on which different data processing activities can be built in addition to those that exist by design. In practice, there are various blockchain systems, so it is important to take into account the different elements of the respective blockchain system. In line with the accountability principle[12], where responsibilities are not already assigned by law, a factual assessment, that takes into account different elements to properly allocate the responsibilities under the GDPR, is needed. Such elements may include the nature of the service provided, the governance mechanism of the blockchain, the technical and organisational features of the blockchain, the relationships between the different actors involved, etc.

39. The governance mechanism is often of key importance for the determination of roles and responsibilities under the GDPR as it defines the design of the model that could be centralised or distributed, registered on the blockchain or agreed upon separately. The governance framework often defines a set of policies, technologically-enforced or not, as well as technical requirements (such as formats, protocols, algorithms, implementations, updates, etc.) and organisational and legal requirements (such as the accountability requirements, contractual obligations among participants, management of inconsistencies and violations, data protection by design approaches, among others).

[8] See AEPD technical note: Proof of concept Blockchain and the right of erasure https://www.aepd.es/guias/Tech-note-blockchain.pdf .

[9] See EDPB guidelines on the concepts of controller and processor in the GDPR, V2.0, adopted on 7 July 2021.

[10] Article 4(7) GDPR.

[11] Article 4(8) GDPR.

[12] Article 5(2) GDPR.

40. **Permissioned blockchains** require someone, acting as an authority[13], to give permission to participate: only selected participants can read, write or create blocks, depending on the rules that apply to the blockchain and defined by the authority. Depending on the particular design, the authority can be a single entity or a group of entities sharing a common interest on the blockchain. This option offers a clearer allocation of responsibilities, which is a key element for the protection of data subjects, and organisations should favour permissioned blockchains. Organisations should only explore different blockchain governance alternatives if well-justified and documented reasons hinder this preference. 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.

41. Participants are not always equal, even in permissionless public blockchains: the role and responsibilities of each participant depends on the elements recalled above and in particular on the governance system. This can be more straightforward in the case of a permissioned blockchain.

42. In some blockchain systems, nodes have only a limited decision-making power as the validation of transactions involves only the preparation of transactions to include in the next block without particular interest or benefit resulting from choosing specific transactions, and a simple verification that (i) transactions meet technical criteria (e.g. a maximum format and size), and (ii) each issuer is able to carry out its transaction vis-à-vis the chain. In such circumstances, nodes would not determine the purposes and means of the processing itself, and therefore might not be considered as controllers. The EDPB recalls that processors process personal data on behalf of a controller and need to comply with Article 28 GDPR, otherwise they would act as controllers.

43. Conversely, nodes in **public permissionless blockchain** may carry out various processing activities to offer blockchain services, and the role of nodes may differ depending on the circumstances and processing at stake. There may be cases where nodes should be qualified as controllers or joint controllers when nodes would exercise a decisive influence on the determination of purposes and essential means of the processing activity.

44. In certain cases of public and permissionless blockchains, nodes do not act "on behalf of the controller" and they do not take any instructions from any controller; on the contrary, they may, in some cases, meaningfully decide to modify purposes and/or essential means to pursue their own objectives (e.g. decision on forking) in relation to mining and validation activities. In that sense, nodes may either individually exercise a decisive influence on the subset of transactions to be added to the next block they mine, or as a group by jointly agreeing (or not) on modifications of the protocols and the rules to apply. In this case, the EDPB strongly encourages the establishment of a consortium or any other type of legal entities among the nodes. This entity, when it exists, would then be controller of this processing.

4 EVALUATING BLOCKCHAIN-BASED PROCESSING

4.1 Introduction

45. Blockchain is only a technology, as cloud computing or peer-to-peer networks, and it is not a processing of personal data as such. Nevertheless, the choice of technology does affect the processing activity and its compliance with GDPR (Article 24 GDPR). Blockchains are not an exception in this matter,

[13] Governance involves exercising authority and control to decide the objectives of an organisation, making decisions, based on assets, resources, context and risk management, to achieve those objectives in a prioritised and balanced way, and continuously monitoring that the progress of each of the actions taken is on track. Governance has to be implemented by defining roles, policies, procedures, plans, organisational, legal and technical measures to manage the organisation.

therefore risks for rights and freedoms of data subjects need to be evaluated and assessed when it comes to processing personal data in a GDPR-compliant manner. Some of these non-compliance risks can be easily mitigated through technical measures upfront, while finding a solution for other risk might may be challenging at this stage. It is therefore of the utmost importance that controllers make a proper evaluation for their own processing before implementing a blockchain – and that this evaluation is used to ensure that blockchains are only deployed in a way which is compliant with the GDPR and provides the proper protections for data subject rights. This evaluation needs to be included in the formal Data Protection Impact Assessment (hereinafter "DPIA") whenever it exists (see section 4.9 of these guidelines).

46. The evaluation should answer to the following questions:

i. Will the data on the blockchain contain personal data? (See section 3.2 of these guidelines)

ii. If so, why is a blockchain necessary for this processing? (What is the rationale for this choice? What are the alternatives?)

iii. What type of blockchain should be used? (Is a private blockchain sufficient? Can a permissioned blockchain be used? Is a "zero-knowledge" architecture possible?)

iv. What technical and organisational measures are used? (Will personal data be stored on or off-chain? Are any privacy-enhancing technologies being used – if not, why?)

47. In order to evaluate the risks for rights and freedoms of individuals raised by the processing and to implement the technical and organisational measures appropriate for those risks[14], controllers should assess the blockchain technology and model that answers their needs. Blockchain technology reduces some risks and raises others. The choice of this technology among others has to comply with the necessity principle enshrined in GDPR[15]. It is thus important to document why this has been chosen.

48. Controllers should also evaluate the level of publicity required for their processing and the personal data involved (user's identifiers, payload data, etc.) to choose the appropriate blockchain architecture. The first part of the evaluation should consider the impact of the (relative) publicity of who sends transactions to whom, which will affect the choice of the blockchain to use. The second part should evaluate the publicity of the data involved[16]. In general, it is not advisable to store personal data on the blockchain, and it should not be stored in the content of transactions. When needed, personal data could be represented inside a blockchain transaction in various ways described in the next section.

4.2 Processing of personal data

49. Controllers are reminded that, according to Article 25(2) GDPR, technical and organisational measures shall ensure "(…) that by default personal data are not made accessible without [the data subject's] intervention to an indefinite number of natural persons." This requirement applies to the storing of personal data on both public and non-public blockchains, and public blockchains should only be employed if public access to the blockchain is necessary for at least one of the purposes of the processing. If the blockchain is not public then, pursuant to Article 5(1)(f), 25(2) and 32 GDPR, measures should be taken to limit the accessibility of personal data stored on the blockchain to what

[14] Article 25 GDPR.

[15] European Court of Human Rights (6538/74) - Court (Plenary) - Judgment (Merits) - case of the Sunday Times v. the United Kingdom: 86.96.: *The Court has noted that, whilst the adjective "necessary", within the meaning of Article 10 (2) (art. 10-2), is not synonymous with "indispensable", neither has it the flexibility of such expressions as "admissible", "ordinary", "useful", "reasonable" or "desirable" and that it implies the existence of a "pressing social need".*

[16] All existing data has to be taken into account: all data structures (not only transaction data) stored on Blockchain and all data that is not stored on the Blockchain (off-chain data).

is necessary for each specific purpose of the processing and to protect the data against unauthorised processing.

50. Storing personal data in a directly identifying form on a blockchain has several implications. First of all, once stored on a blockchain, the data will stay on the blockchain with no practical possibility of deletion or modification in most cases. Even though it is technically possible to modify a blockchain, such modifications are very hard to put in place as it requires that all nodes update their copy of the chain (or to delete their copy) and agree upon the change. This undermines the principles of consistency and tamperproof processing, which are the core of most blockchains design. In practice, such modification may not even impact all copies of the original block, meaning that the original data might still be available. The EDPB emphasises that technical impossibility cannot be invoked to justify non-compliance with GDPR requirements[17]. Nevertheless, a proactive approach, combining organisational measures, techniques and governance models could transform perceived constraints into opportunities for compliance.

51. **Encryption of personal data:** To address this issue, one way is to encrypt personal data before storing it on a blockchain. Using state-of-the-art encryption algorithms and keys, the data will be accessible in clear text only to those knowing the appropriate key. This also means that upon deletion of this decryption key, the encrypted data will be unintelligible, at least until the algorithm is broken, the decryption techniques advance sufficiently to allow the decryption of the cipher text, or if the key had already been compromised or leaked. The EDPB recalls that encrypted personal data is still personal data and encryption does not remove the need for GDPR compliance. Further, even state-of-the-art encryption perfectly implemented will be overtaken by time if the blockchain is retained indefinitely. This needs to be taken into consideration by the controller when deciding whether to store encrypted personal data on the chain.

52. **Hashing of personal data:** Another measure is to store only a salted or keyed hash of the personal data on the blockchain. The unhashed data itself, as well as the secret key or the long random salt used, are stored confidentially off the chain. Although this may be referred to as “off chain” storage, it is important to recall that, the GDPR will still apply to that processing activity and that the hash will also be considered personal data, as will any other identifiers that might exist. The advantage of this architecture is that the original data (i.e. the argument of the hash function) cannot easily be recovered from the hash. Indeed, a hash obtained through a state-of-the-art hash function and a randomly generated secret key or salt of a sufficient size, will, in theory, be verifiable only by people having access to the original data and the given associated key or salt. This also means that, after deletion of the secret key or salt, the hash should not be linkable to the original data, provided that the algorithm has not been broken, the keys have not been compromised or leaked, and the salt was not leaked or poorly chosen. However, this architecture requires the use of another system in order to store the data itself, therefore creating a personal data processing in another component of the infrastructure, which bears its own risk. It should also be noted that the use of unsalted or unkeyed hashes should, in general, not be considered sufficient to guarantee the necessary level of confidentiality protection for storing personal data on a public blockchain.

53. **Cryptographic commitments:** the third measure to avoid storing personal data in a directly identifying form on the chain consists in storing a cryptographic commitment on the blockchain instead. If the commitment has been computed using a perfectly hiding state-of-the art scheme, then once the

[17] EDPB, Report of the work undertaken by the ChatGPT Taskforce, May 2024, para. 7: “*In particular, technical impossibility cannot be invoked to justify non-compliance with these requirements, especially considering that the principle of data protection by design set out in Article 25(1) GDPR shall be taken into account at the time of the determination of the means for processing and at the time of the processing itself*”.

original data and its witness are deleted, the commitment persisting in the blockchain is useless. It will be neither possible to recover nor to recognise the original personal data.

54. Whenever it is necessary to store personal data on the blockchain, it is better to store the data in a form which is primarily intended to function as a **proof of existence**[18] (e.g. by use of a pointer, a cryptographic commitment or a hash generated from a keyed hash function, etc.) on the blockchain, with the data that should be used to verify the proof being kept outside of the blockchain (such as, for example, on the data controller's information system). This must be done ensuring a high level of confidentiality.

55. In some cases, data controllers may need to make some information public and accessible with a retention period equal to the life of the blockchain. In these particular cases, it may be appropriate to store personal data on a public blockchain in a directly identifying form, but only if it is justified by the purpose of the processing and a DPIA has been conducted and concluded that the risks for data subjects have been properly addressed and mitigated.

56. The measures presented above can be helpful for reducing risks to data subjects. Nevertheless, they will also need to be accompanied by other appropriate technical and organisational measures to ensure that the processing meets all applicable GDPR requirements and grants the data subject rights.

4.3 Principles of Data Protection

57. The data protection principles are those enshrined in Article 5 GDPR. Controllers are responsible for their implementation in an accountable way and in an effective manner[19]. The EDPB emphasises that data protection principles are not negotiable, although their implementation may vary according to the context and the level of risks. Below, the EDPB presents some issues in a non-exhaustive manner that should be taken into account by data controllers when evaluating their processing of personal data with regard to the data protection principles.

58. Fairness principle[20] requires that personal data should not be processed in a way that is unjustifiably detrimental, unlawful, discriminatory, unexpected or misleading to the data subject. Measures and safeguards implementing the principle of fairness also support the rights and freedoms of data subjects, specifically the right to information (transparency), the right to intervene (access, erasure, data portability, rectify) and the right to limit the processing (right not to be subject to automated individual decision-making and non-discrimination of data subjects in such processes)

59. When considering the transparency principle[21], the controller must be clear and open with the data subject about how they will collect, use and share personal data. Transparency is about enabling data subjects to understand, and if necessary, make use of their rights in GDPR Articles 15 to 22. The principle is embedded in GDPR Articles 12, 13, 14 and 34. Measures and safeguards put in place to support the principle of transparency should also support the implementation of these Articles.

60. Pursuant to the **principle of purpose limitation**, data shall be processed for a specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with these purposes. However, blockchain technology, by design, is disintermediated[22] in nature and the relationships between participants cannot always be governed by contracts or other legal acts that bind them to

[18] Bunch of data that links or references to existing data stored off-chain

[19] Article 5(2) and Article 25 GDPR.

[20] See EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, V2.0, adopted on 20 October 2020, chapter 3.3.

[21] See EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, V2.0, adopted on 20 October 2020, chapter 3.1.

[22] See Annex B Glossary: disintermediation means that transactions can be conducted directly between parties without the need for a central authority or intermediary.

implement appropriate technical and organisational measures to ensure compliance[23]. Controllers should therefore be very careful to understand their particular role while also ensuring their purposes of processing personal data is clear and unambiguous to all stakeholders. Once those purposes has been achieved, data should either be deleted or rendered anonymous in line with the storage limitation principle (which will be discussed in more detail below).

61. The append-only and ever-growing nature of a blockchain challenges the **data minimisation principle**, which is exacerbated by the potential for unlimited persistence and manifold replication. This tension needs to be reconciled and controllers must ensure that they have appropriate measures in place for doing so. Data minimisation, in connection with the purpose and storage limitation principles, is crucial and only data which is necessary data to achieve the purpose may be processed in a blockchain. Finally, the data minimisation principle should also include a reflection on the level of publicity applicable for any personal data involved. Seen through this lens, the data minimisation principle is an obligation for controllers to demonstrate that the technique chosen is the one assuring that only the minimum of information necessary for the processing is used and with the minimum level of publicity.

62. The **principle of accuracy** requires that personal data is accurate, and where necessary kept up to date. This principle, as with all of the others, is not restricted to particular technological implementations and applies equally to processing activities which include blockchain. Due to the limited margins for intervention once data has been submitted to a blockchain, a heavy emphasis should be put on the preliminary phases of the processing and controllers should pay the utmost care during the initial selection of data to ensure accuracy, this forms part of the governance. Due to the rigidity of the blockchain, the accuracy question can also be seen as a data minimisation question about the risks for data subjects stemming from out-of-date data still existing on the blockchain.

63. Personal data must be erased once the purposes of the processing has been achieved and any regulatory periods for retention have expired in order to conform to the **principle of storage limitation**. Data deletion at the individual level in a blockchain can be challenging and requires ad-hoc engineered architectures. When deletion has not been taken into account by design, this may require deleting the whole blockchain. If the combination of on-chain and off-chain data compliance with data protection has been taken into account by design, it may be possible to prevent the future identification of a data subject through erasure of off-chain data, depending on the exact method chosen and the specific facts in question. Whichever approach to storage limitation is chosen, it must be effective. Where this would require the deletion of part of the blockchain, including the deletion of any copies held by nodes or other parties, controllers should ensure that sufficient technical and organisational measures are in place for doing so[24].

64. If the future identification of a data subject is to be prevented, it should be possible to prevent the linking, with means reasonably likely to be used, of an existing transaction involving a particular data subject with a future transaction involving that same person. It might be possible, depending on the type of blockchain and the way transactions are recorded, to modify off-chain data so that the data subjects involved in the transaction are no longer identifiable with reference to data remaining on the chain. Such modification will likely preclude any use of the data stored on the chain for the original specified purposes beyond the maintenance of the block chain structure. This means that the "anonymised transaction" would have lost all its semantics, but still exists to allow the verification of integrity for other, remaining transactions.

65. A core essence of a blockchain is disintermediation, which is achieved by broadcasting every internal transaction and allowing many-to-many cross checks. Therefore, confidentiality of metadata depends on the type of blockchain chosen (e.g. public vs permissioned). The focus should be on confining the

[23] e.g. storage limitation

[24] Deletion requires governance and traceability measures. See GDPR Recital 66 and AEPD Technical note: Proof of concept Blockchain and the right to erasure (https://www.aepd.es/guias/Tech-note-blockchain.pdf).

processing of broadcasted information only to the relevant blockchain actors and preventing it from being unduly processed by any other non-blockchain-related parties. The content confidentiality would rely on the mechanisms used (encryption, commitment, etc.) and on classical measures assuring the security of any off-chain data.

66. If a law were to mandate the use of a blockchain, among other elements[25], legislators should include provisions regarding the acceptable level of publicity and discourage any breach of confidentiality.

67. The **integrity principle** in a blockchain is assured by its protocol and relies on trust in the consensus mechanism and nodes. Trust cannot be enforced but can only be incentivised, e.g. by the use of certified software for interacting with the blockchain, by ensuring a way to identify nodes and if necessary and by using permissioned blockchain. The **confidentiality principle** should be implemented by measures applied to all instances of the blockchain, and by measures (possibly including the measures listed in section 4.2) applied to transaction data stored on- and off-chain.

68. Additional measures to reinforce security in the context of blockchain technologies consist in continuous checks on the trustworthiness of the actors participating in the blockchain.

69. To limit the impact that a potential algorithm failure may have on the security of personal data, technical and organisational procedures should be put in place. This may include means to disclose software vulnerabilities to all affected stakeholders, an emergency plan that allows algorithms to be changed when a vulnerability is identified, and ways to notify security incidents and personal data breaches to the relevant SAs and to communicate the incident to the involved data subjects. Furthermore, the governance of changes should be documented in a way to reduce the risk of misalignment between the specification and its implementation.

4.4 Lawfulness of processing

70. Given the fact that a Blockchain infrastructure allows certain data processing to be implemented on it, there is no one legal basis for all processing activities using blockchains. For each processing of personal data, the legal basis specific most appropriate for the processing's purpose has to be determined. The legal basis for the processing of personal data must be one of those set out in Article 6 GDPR. Further, if data relevant for Article 9(1) GDPR is processed, then one of the exceptions mentioned in Article 9(2) GDPR apply. Several alternatives may exist permitting such processing, the assessment if there is a valid legal basis should be based on the specific context of the processing at stake.

71. If consent is the legal basis for the processing under Article 6(1)(a) GDPR, it must comply with all the requirements laid down in Articles 4(11) and 7 GDPR. This includes that it must be a freely given, specific, informed and unambiguous indication of the data subject's wishes. Furthermore, consent can only be considered as freely given if the data subject has a genuine and free choice and is able to refuse or withdraw consent without detriment[26]. Importantly, where the storing of personal data is justified on the basis of consent, the personal data must be deleted or rendered anonymous if that consent is withdrawn[27].

72. Restrictions on data subjects' rights are possible only to the extent described in Article 23 GDPR. Examples may include cases where blockchain solutions are implemented for anti-money-laundering requirements or for certain asset (e.g. real estate) inventories, which can be imposed by Union or Member State law. In those circumstances, as required by Article 23 GDPR[28], restrictions on individuals'

[25] Article 6(3) GDPR.

[26] See EDPB Guidelines on consent under Regulation 2016/679, V1.1, adopted on 4 May 2020, p. 7.

[27] Consent does not override GDPR compliance.

[28] See EDPB Guidelines 10/2020 on restrictions under Article 23 GDPR, V2.1, adopted on 13 October 2021.

rights must be proportionate, strictly defined in the law and respond to the specific requirement of necessity in a democratic society.

73. A blockchain might also be used where the processing operation is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject to whom the personal data refer in line with Article 6(1)(f) GDPR[29] [30] [31]. .

4.5 International transfers

74. Chapter V GDPR lays down the rules under which transfer of personal data outside the EEA make take place. Blockchain technology will often involve international data transfer, in particular when information are shared across nodes that are based outside of the UE. These nodes are neither necessarily chosen or vetted, such as in public blockchains[32] which may raise compliance concerns. Nevertheless, any transfer of personal data outside of the EU has to comply with the provisions of Chapter V GDPR[33]. Controller should be aware of these obligations and identify transfers as well as relevant mechanisms to facilitate these data flows. As an example, controller could incorporate standards contractual clauses in any existing contract that should be signed before being accepted as a node.

75. In any case, ensuring a proper application of the data transfers requirements should be addressed from the design of blockchain activities[34]. A privacy by design architecture may help assess compliance obligations.

4.6 Data protection by design and by default

76. As clarified by the EDPB in its Guidelines 4/2019 on Data Protection by Design and by Default, effectiveness is at the heart of this concept[35]. This means that controllers should be able to demonstrate that they have applied context-specific measures to implement data protection principles, and that they have integrated specific safeguards that are necessary to secure the rights and freedoms of data subjects, including in contexts where a traditional implementation would have not been equally effective. Data protection by design and by default also emphasises that the effect of the measures matters; it is not enough to implement generic measures solely to document a formal compliance to the GDPR.

77. This data protection by design and by default approach is very important in the context of blockchain as the technology is particularly challenged by data protection principles. This may therefore require a combination of different privacy enhancing technologies to provide sufficient levels of data protection for data subjects.

[29] See EDPB Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR.

[30] This processing ground has been discussed in detail in EDPB Guidelines 1/2024 on Article 6(1)(f) GDPR. any processing based on a legitimate interest pursued by the controller must also be necessary and balanced against the interests or fundamental rights and freedoms of the data subjects.

[31] EDPB Opinion 11/2024 on the use of facial recognition to streamline airport passengers' flow (compatibility with Articles 5(1)(e) and(f), 25 and 32 GDPR par. 32: *assess whether the negative impact on the data subjects' fundamental rights and freedoms is proportional to any anticipated benefit. If the benefit is relatively minor, then such impact might not be proportionate.*

[32] e.g. Bitcoin

[33] Further guidance can also be found in the EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

[34] See Article 25 GDPR.

[35] EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, V2.0, adopted on 20 October 2020, paragraph 13.

4.7 Data retention periods

78. Controllers should consider each piece of data according to the purpose of its processing, when specifying the retention period. It is one of the characteristics of blockchains that the data registered on a blockchain is tamper-proof and that, once a block in which a transaction is recorded has been accepted by the majority of nodes, alterations to that transaction would be detected. However, this is not a reason to assume that the lifetime of the blockchain is an appropriate data retention period; rather, data should be deleted when the end of the processing activity is reached and in line with the data processing principles discussed above.

79. Controllers should evaluate, among other things, the techniques laid out in section 4.2, which can, in some cases, mitigate the consequences according to their risk assessment.

80. As described in section 3.2 of these guidelines, a blockchain can contain different categories of personal data, including metadata, such as the users' identifiers, and the payload. For the majority of blockchains, these identifiers are always visible as they are essential for its proper functioning. It is important to recall that the data retention period also applies to these identifiers and, if the identifiers take the form of public signature verification keys, the transactions signed by the corresponding private signing keys. The payload data stored on the blockchain can also contain personal data which relates to both the blockchain users and nodes, and also to other individuals. A retention period should be determined depending on the processing and at the end of the retention period data must be deleted or rendered anonymous.

81. The EDPB considers that, in cases where processing does not require a retention period equal to, or longer than, the lifetime of the blockchain, personal data should not be written to the blockchain unless it is done in a way that allows for the effective prevention of identification of the data subjects with reference to that data employing means reasonably likely to be used. If the data retention period is the lifetime of the blockchain, the controller should be able to justify that such retention period is necessary and proportional in relation to the purpose and the analysis that led to this conclusion should be properly documented.

4.8 Security

82. The different properties of a blockchain – being distributed, disintermediated, consistent, tamperproof and transparent –rely on three factors: the behaviour of participants, the number of nodes and a set of cryptographic mechanisms.

83. The EDPB recommends carrying out an evaluation of the necessary safeguards to reduce, or prevent, misuse by a group of participants of the blockchain, such as the so-called 51%-attacks. For permissioned blockchains, depending on the potential divergence or convergence of participating actors' interests, these safeguards may be included in the contractual relationship between participants and may be enforced by the creation of administrative privileges for a controller to oversee the use of the blockchain. The process surrounding the granting and maintenance of permissions should be closely governed.

84. There should also be appropriate safeguards in place to protect against unintended or unauthorized transactions by participants who may have had their wallets compromised or have a rogue employee. This also implies an obligation for participants to implement corresponding technical and organisational safeguards on their sides.

85. The EDPB also recommends setting out technical and organisational procedures to limit the impact of potential algorithm failures. Such failures could arise from, for example, the publication of a vulnerability on a cryptographic mechanism, or due to implementation issues. Measures to address potential algorithm failures could include, for example, the implementation of an emergency plan which allows algorithms to be changed or fixed if a vulnerability is identified. Since the operation of a blockchain-based processing relies strongly on its cryptographic mechanisms, the risk of a potential compromise of such mechanisms regarding the expected lifespan of the blockchain must be assessed.

86. Furthermore, the governance of changes to the software or protocols used in or by the blockchain should be documented, and technical and organisational procedures should be set out to ensure an alignment between planned permissions and practical application.

87. Particular attention should be granted to the measures implemented to ensure the blockchain's confidentiality if it is not public. Any data controller carrying out processing through transactions on a blockchain should ensure the security of the secret keys used, for example by ensuring that they are stored on secure media. Further, as data breaches can result from vulnerabilities in the infrastructure used to interact with the blockchain, such as stolen identities, the security of the blockchain processing should be assessed as a whole, including when personal data is stored off-chain.

88. Thus, including for security reasons, the data uploaded to the blockchain and processed by nodes should be assessed to only include minimized personal data as set out in the data protection context.

89. The EDPB recalls that security of processing is a requirement under the GDPR[36] . Nevertheless, while the specific measures may vary from case to case, they have to ensure a level of security appropriate to the risks for the rights and freedoms of natural persons when personal data is being processed; if it is not possible to achieve the necessary level of security that is appropriate to the risk while using blockchain solutions, controllers should not utilise blockchain solutions as part of their personal data processing activities.

4.9 Data Protection Impact Assessment

90. As described above, the use of blockchain can add some sources of risk to the rights and freedoms of individuals when used as part of the processing. The risk assessment and management should consider the processing as a whole, including the blockchain-related risks.

91. Where a processing activity is likely to result in a high risk to the rights and freedoms of natural persons, it is mandatory to conduct a Data Protection Impact Assessment (DPIA) to appropriately evaluate and mitigate the risk presented by the processing of personal data appropriately. The Working Party 29 has already clarified the criteria that should be followed to determine if a processing operation requires a DPIA[37].

92. If the use of a specific model of blockchain in a processing activity creates risk to the rights and freedoms of individuals that cannot be mitigate with appropriate technical and organisational measures, the controller always has the option to instead use a different model of blockchain or another technology that reduces, or does not introduce, such risks.

93. Sources of risk in a blockchain-based processing come not only from the storage of data in the blockchain, but also from other operations inherent to the blockchain model. Some elements that might introduce such risks include the communication of transactions and blocks among different stakeholders, the gathering and storage of transactions awaiting validation for block creation, the management of blocks in dead-end branches, the off-chain storage of personal data related to in-chain identifiers or hashes, the generation and storage of communication metadata, and the management of cryptographic information (keys, seeds, salts and so on), among others. All such related risks, as well as any others which are identified, should be managed.

94. As part of their analysis, the controller should assess if the accountability and governance mechanisms implemented in the blockchain allows it to handle the processing risks. This could include, for example,

[36] Article 32 GDPR.

[37] See Working Party 29 "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679", endorsed by the EDPB, (hereinafter, "DPIA Guidelines").

mechanisms for access control, access record, traceability and audit, data breach management among others.

95. 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 data. The controller should assess the data involved in such related 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.

96. Privacy on the blockchain can be supported by the robustness of its encryption mechanisms. However, all encryption systems have an undetermined, but limited, life span. Therefore, it is necessary to manage obsolescence and the possibility of encryption algorithms being broken. The computational effort needed to break encryption systems, and the possibility of technical advances such as cryptanalytically-relevant quantum computers, should be balanced with regard to the sensitivity and value of the data, and the risks to the data subject, not for the processing itself. Such risk should be assessed in the design phase of the processing and should be part of the risk management process along the life cycle of the processing, including with periodic reassessment. Depending on the risk, measures to enhance the encryption system or port the processing to other technologies, including other blockchain-models should be planned in advance.

97. In order to comply with the GDPR, the exercise of data subject's rights must be guaranteed. These rights are technology neutral and therefore apply regardless of whether or not blockchain is involved in the processing activities. In some cases, it may be possible for blockchain solutions to implement innovative measures for the exercise of these rights, although these measures should be in line with the more general guidance and should never lead to a lower level of protection for data subjects. Those ways could rely on new technical and organisational measures. The risk of such measures should be assessed regarding its effectiveness in the actual processing. It should be considered in the risk management with regards new vulnerabilities, malfunctions or updates in the nature, scope, context and purpose of the processing.

98. When conducting a DPIA for a blockchain-related processing, there are additional aspects that should be specifically addressed:

- A systematic description of the blockchain processing operations, including, for example, the processing purposes, the specific use case, the identification of the blockchain infrastructure, the blockchain model, the definition of roles and responsibilities, the categories and (where appropriate) identities of data recipients and other potential third parties, the data governance model, the type of operations carried out over the life cycle of the processing, the data sensitivity, whether there is any on/off-chain processing, whether there are any smart contracts and means of automatic personal data inference, the implementation of the exercise of rights, any data protection by design and by default measures, to the existence of any international transfers and related safeguards, any data communications, and any other processing activities supported in the same blockchain infrastructure.
- An assessment of the necessity and proportionality of the processing operations that are carried out depend on the blockchain. In particular, the DPIA should explain if the use of blockchain is considered necessary and why the objective cannot reasonably be as effectively achieved in a way that is less invasive of privacy and carries less risk for the rights and freedoms of natural persons.
- An assessment of the risks to the rights and freedoms of data subjects of the processing as a whole, including the risks that are specific of the use of blockchain such as those described in previous sections, an assessment of possible data breaches, an estimation of the extend and

scale of processing and the blockchain infrastructure, and an assessment of the risks for data protection rights and safeguards in case of international transfers among others.

- A precise identification and assessment of the specific measures to address the risks stemming from the use of blockchain technology. This could include accountability measures, data protection by design and by default measures, data minimisation and guarantee of data accuracy strategies, cryptography guarantees and other security issues, PETs used in the blockchain itself and its ecosystem, and personal data breach management measures, among others. That effectiveness of the blockchain specific measures must be assessed considering all the other measures implemented in the processing.

99. The DPIA Guidelines state that, in some cases, the DPIA could or should be an on-going process[38]. This may apply, in particular, if the processing is implemented in blockchain infrastructures that are not under the control of the data controller, is permissionless, includes international transfers or could be used to implement other processing activities that, due to the kind of stakeholders, data, scale or purposes, could increase the overall risk.

5 DATA SUBJECT RIGHTS

5.1 Information of data subjects, right of access and right to data portability

100. The data controller must provide concise information that is easily accessible and formulated in clear terms to the data subject before submitting personal data to nodes for validation (see section 4.3 for possible points in time to provide such information).

101. The same applies for the right of access and the right to portability: the EDPB considers that the exercise of these rights can be compatible with blockchains' technical properties as long as the controller fulfils all GDPR requirements concerning the exercise of those rights[39].

5.2 Right to erasure and right to object

102. The rights to erasure and to object[40] must be complied with by design.

103. The EDPB observes that it might be technically impracticable to grant the request for actual deletion[41] made by a data subject when personal data is stored directly on a blockchain. The principal property of a blockchain is the strong integrity of its chain assured by cryptographic and consensus tools. Since the full blockchain or information stored on it might not be easily deleted, controllers should consider this requirement early in the design phase and make sure that any personal data stored on the blockchain can be effectively rendered anonymous if an erasure request or objection is received. This presupposes that the relevant transaction data stored on the blockchain does not allow the direct identification of the data subject and that any additional (off-chain) data which would, with means reasonably likely to be used, allow for indirect identification is erased. Considering the difficulty of achieving this in practice, the EDPB recommends looking at other tools if the strong integrity property of blockchains is not needed. The facilitation of data subject rights should be considered at the design phase of the processing, in line with Article 25.

104. It is technically demanding and often difficult to grant the request for rectification or for erasure made by a data subject when clear text, encrypted or hashed data is recorded on a blockchain. It is therefore

[38] See DPIA Guidelines, Section III D, p.14.

[39] For example, see Articles 12, 15, 16 GDPR.

[40] See Articles 17 and 21 GDPR respectively.

[41] Developments are possible with appropriate governance and design measures. See AEPD Technical note: Proof of concept Blockchain and the right to erasure (https://www.aepd.es/guias/Tech-note-blockchain.pdf).

not advisable to register personal data in those forms on a blockchain. Instead, personal data in those forms should be stored off-chain.

5.3 Right to rectification

105. As with the rights to erasure and to object, the right to rectification must be complied with by design.

106. In some cases, the right to rectification can be met by a subsequent transaction, which announces the cancellation of an earlier transaction, even though the first transaction will still appear in the chain. In other cases, where the right to rectification requires the erasure of the data, the same solutions as those applied following a request for deletion of personal data could be applied to erroneous data.

5.4 Right to object to a solely automated decision.

107. The execution of a smart contract may, in some cases, constitute an automated decision. When these automated decisions fall into the scope of Article 22, the data controller should ensure that the safeguards in that provision are satisfied, including the possibility of human intervention, and allowing the data subject to contest the decision, even if the smart contract has already been performed and regardless of what is registered on the blockchain.

For the European Data Protection Board

The Chair

Anu Talus

ANNEX A – RECOMMENDATIONS

Recommendation 1. Architecture – Documentation

108. The EDPB recommends to controller and processors to document:

i. Will the data on the blockchain contain personal data?

ii. If so, why is a blockchain a necessary and proportionate means for this processing? (i.e. What is the rationale for this choice? What were the eventual alternatives?)

iii. What type of blockchain should be used? (i.e. Is a private blockchain sufficient? Can a permissioned blockchain be used? Is a "zero-knowledge" architecture possible?)

iv. What technical and organisational measures are used? (i.e. Will personal data be stored off-chain? Which privacy-preserving technologies are used?)

Recommendation 2. Architecture – Off-chain storage

109. The EDPB recommends controllers to store any additional personal data off-chain, beyond the identifiers already present on-chain in transaction metadata, to mitigate data protection risks.

Recommendation 3. Information

110. Data controllers must inform data subjects in clear terms on the rationale of the processing, the existence of their rights and the modalities to exercise them. Suitable times to provide such information are when a data subject is about to commit data to the blockchain and on creation of the blockchain itself. The information should also be available for data subjects to find at other times, e.g. on the controller's website.

Recommendation 4. Minimisation

111. Controllers should assure that only data that is relevant and limited to what is necessary in relation to the purposes are processed. The amount of personal data stored on- and off-chain, the period of their storage and their accessibility should be minimised. Assessment in this regard should be documented for the metadata as well as for the payload of the transactions.

Recommendation 5. Trust

112. The choices of implementation should include mechanisms for assuring trust including in software and nodes' identities. It might be done, for example, through certification by international standards and independent third parties.

Recommendation 6. Legal provisions if use of blockchain is mandated by law

113. Where the use of a blockchain is mandated by Union or Member State law, legislators should include provisions regarding the acceptable level of publicity and discourage any breach of confidentiality.

Recommendation 7. Software Vulnerabilities

114. The EDPB recommends setting out technical and organisational procedures to disclose software vulnerabilities to all participants, including an emergency plan that allows algorithms to be changed when a vulnerability is identified and to notify security incidents and personal data breaches to the relevant SAs, and to communicate the incident to the involved data subjects

Recommendation 8. Governance

115. The governance of changes to the software used to create transactions and to create and validate blocks should be documented and technical and organisational procedures should be set out to ensure an alignment between specification and implementation.

Recommendation 9. Consent

116. If any use of the consent legal basis is made, it must be ensured that it is freely given and that the data subject is able to refuse or withdraw consent without detriment. Technical choices for the implementation of the processing should ensure these two points. In particular, this requires that no personal data is stored on the blockchain that cannot be rendered anonymous by the erasure of off-chain data and an effective procedure for assuring such erasure in the case of withdrawal of consent is implemented. Consent should not be used for a processing which requires transactions with individuals if the blockchain architecture does not provide a way to delete the personal data regarding the parties in a transaction.

Recommendation 10. Data protection by design and by default

117. All data protection principles should be included by design and by default in any processing from the outset and throughout the processing life cycle. All processing operations need to be necessary and proportionate in relation to the purposes of processing.

118. By default, personal data should not be made accessible on a public blockchain without the data subject’s intervention.

Recommendation 11. Data retention – duration

119. The data retention period of metadata, such as users’ identifiers, and payload should be established pursuant to Art. 17 in conjunction with Art. 25(1) GDPR and taken into account when deciding which kind of blockchain and which format to store those data to use.

120. In cases where a data retention period is not as long as the lifetime of the blockchain, a technical solution should guarantee the appropriate data retention period. At the end of the retention period for personal data stored on the blockchain, this solution should either allow for data deletion or, if applicable, render the data anonymous. If such solution does not exist, then no personal data should be stored on the chain.

Recommendation 12. Security – Evaluation

121. Carry out an evaluation of the security safeguards necessary to assure the security of the blockchain appropriate to the risks.

Recommendation 13. Security – Limit the impact of algorithm failure

122. Set out technical and organisational procedures to limit the impact of a potential algorithm failure (as an attack on one of the cryptographic primitives used in the blockchain).

Recommendation 14. Security – Governance of evolution

123. The governance of software and protocol evolution should be documented.

Recommendation 15. Security – Confidentiality

124. Whenever it is not necessary for the purposes of the processing, that a public blockchain is used for, then the measures need to be implemented to limit accessibility of the blockchain and ensure the blockchain’s confidentiality. Those measures should be documented and verified.

Recommendation 16. Data subjects’ rights

125. Data subjects’ rights cannot be restricted – neither by choice of technical implementation nor by the data subjects’ consent. They must be fulfilled in accordance with the GDPR. Technical choices for the

implementation of the processing should ensure this. In particular, personal data needs to be erased or rendered anonymous in the event of an objection to processing pursuant to Art. 21 GDPR or a request for erasure pursuant to Art. 17 GDPR.

ANNEX B – GLOSSARY

126. **Disintermediated**
Refers to the removal of intermediaries or middlemen in a transaction or process. In the context of blockchain, disintermediation means that transactions can be conducted directly between parties without the need for a central authority or intermediary, such as a bank. It should be noted, however, that even though a transaction on a blockchain does not require a central authority, it will in general still need other blockchain participants (such as miners, validators or others, depending on the particular blockchain implementation) to be carried out.

127. **Fork**
A fork occurs when a blockchain splits into two separate chains, often as a result of a change to the underlying protocol or a disagreement among network participants. This can result in the creation of a new blockchain or the continuation of the original chain.

128. **Ledger**
A ledger is a record of transactions that have taken place on a blockchain. It is a decentralized and distributed, digital bookkeeping system that allows multiple parties to agree on the state of a transaction without the need for a central authority.

129. **Mining/Validating**
The process of verifying and adding new transactions to a blockchain. Nodes use a consensus mechanism, such as proof of stake or proof of work, which helps to secure the network and validate transactions. In return, nodes are often rewarded with cryptocurrency or other incentives.

130. **Node**
A node is a computer that connects to each other and form the blockchain network. Nodes can help to validate and relay transactions. They can be thought of as individual points on the network that work together to maintain the properties of the blockchain. A node is operated by a natural or legal person. While the node itself is a technical component, when these guidelines refer to the actions and responsibilities of a node, these are attributed to the natural or legal person that operates or controls the node.

131. **Proof of existence**
A method of proving that a particular piece of data or asset exists without revealing the actual data itself. This can be useful in scenarios where confidentiality is important, such as in intellectual property or digital identity verification.

132. **Proof of stake**
A consensus mechanism used to secure blockchain networks. In proof of stake, nodes are chosen to create new blocks based on the amount of cryptocurrency or other assets they hold (i.e., their "stake"). This is in contrast to proof of work, which relies on computational power.

133. **Proof of work**
A consensus mechanism used to secure blockchain networks. In proof of work, nodes compete to solve complex mathematical problems, with the first to solve the problem getting to add a new block to the blockchain and receive a reward. This requires significant computational power and energy consumption.