Adan's response

EDPB Guidelines on the processing of personal data through blockchain technologies

Adan welcomes the European Data Protection Board's (EDPB) initiative to provide guidance on the application of the General Data Protection Regulation (GDPR) to blockchain technologies. These Guidelines contribute to an essential dialogue between innovation and regulation, and Adan supports the objective of ensuring that blockchain-based systems can operate in a way that is respectful of fundamental rights and compliant with European legal standards.

However, while the Guidelines are a valuable first step, certain recommendations raise legal and practical concerns that risk undermining the capacity of the European Union to support the development of a sovereign and innovation-oriented digital infrastructure. In particular, the interpretation of key GDPR provisions - such as data controllership, the qualification of personal data, or the right to erasure - sometimes departs from the principles of legal certainty, technological neutrality, and proportionality enshrined in EU law.

Rather than seeking to render blockchain technologies incompatible with GDPR, the objective should be to clarify the conditions under which their design and operation can be aligned with the Regulation. This includes recognising that legal obligations and public interest objectives (notably, traceability; compliance; and fraud prevention) may justify the persistence of certain data in a secure, decentralised, and transparent way.

To this end, Adan proposes considering specific carve-outs for validators and technical or infrastructure players, such as node operators or miners, whose roles are confined to technical functions like transaction validation and ledger maintenance, without determining the purposes or means of data processing. Such exemptions would recognize the limited control these actors have over personal data, reduce undue regulatory burdens, and foster participation in decentralized networks, thereby supporting innovation while remaining consistent with the GDPR's risk-based approach. Such an approach would remain fully consistent with the GDPR's risk-based, contextual, and balanced logic.

Adan's contribution aims to highlight these challenges, provide constructive legal interpretation of the relevant provisions, and propose clarifications that could help the Guidelines better reflect the reality of decentralised infrastructures, and the role they can play in supporting responsible innovation within the European digital economy.

*

Table of contents

1. Identifying Data controllers and Processors

1.1. Complexity of defining the Data controllers under Article 4 (7)

A critical aspect of regulatory compliance involves identifying the data controller, responsible for ensuring compliance with obligations under the GDPR. According to Article 4(7), the data controller is the natural or legal person, public authority, agency, or other body that, alone or jointly with others, determines the purposes and means of processing personal data.

To establish who qualifies as a data controller, it is thus essential to determine who decides the purposes (why) and means (how) of the data processing activities. However, blockchain's unique characteristics highlight the complexities attached to clearly distinguishing between data controllers and processors. The various actors within a blockchain ecosystem- such as nodes, miners, or users themselves or governance structures- could qualify as data controllers depending on their role in determining the means and purposes of data processing.

These multiple players might take different functions, each potentially influencing certain aspects of the network's operations. This diffuse architecture blurs the line between who decides the 'purposes' of processing, making it challenging to attribute the role of data controller to any or a single natural or legal person.

1.2. Node operators and control criteria

In Section 3.3, the EDPB discusses whether nodes could be considered as Data controllers. Whether responsibility should be assigned to the operators of nodes is a significant topic that warrants further exploration.

The extent to which node operators meet the criteria for data controllership needs to be evaluated case-by-case, as often they are not inherently acting as data controllers under GDPR. While nodes store and transmit transaction data, they typically do so as a necessary function of maintaining the distributed ledger's integrity and security, rather than with the intent of analyzing, profiling, or otherwise actively using this data in a typical controller-like manner.

Indeed, their primary role is to validate, transmit, and store transaction data, ensuring transactions are recorded according to predefined protocols, often without influence over the purpose or scope of the data being processed for the specific transfer. In other words, their activities are typically limited to technical validation and propagation of transactions, rather than determining the purposes of processing the underlying personal data contained within those transactions. In those cases, the nodes' role is not strategic or data purpose-driven.

Given that, according to the GDPR, the criterion for determining who is the data controller requires the satisfaction of both criteria (deciding the purpose and the means), in many cases, node operators might qualify as data processors rather than data controllers.

Therefore, the level of control and the purpose of data processing necessitate a case-by-case analysis to determine data controllership.

Especially in public and permissionless blockchain systems, determining controllership becomes intricate and requires a contextual, case-by-case analysis. The core difficulty lies in the fact that, in decentralized networks, no single actor exercises decisive influence over the purposes and means in a manner consistent with the GDPR's definition of control. Instead, decision-making may be distributed or governed collectively, which complicates the attribution of controller responsibilities and accountability. In these contexts, nodes may simply process and store transactions as dictated by the protocol, without setting the actual purposes or the nature of the data involved.

In paragraph 40, the EDPB problematically states: *"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."*

This statement disregards that in blockchain networks, forking and other decisions are usually community or consensus-driven decisions. Participating entities coordinate or agree on whether to implement a protocol upgrade, change rules, or support an alternative chain. A single node does not usually have the authority to unilaterally create or support a fork without broader consensus, especially in decentralized networks like Ethereum.

Overall, the act of validating transactions according to protocol rules shall not be translated into an exercise of purpose or means determination. Nodes process data because they are required to by the protocol, not because they have decided on the processing rationale. The actual purposes and the data processing intents are typically set by a separate governance body, such as the blockchain's developers, operators, or users, rather than the nodes themselves.

For example, the French GDPR supervisor, CNIL states that **Miners *"are only validating transactions submitted by participants"* and** *"are* ***not involved in the object of these transactions; therefore, they do not define the purposes and the means of the processing****."*

The Guidelines propose that nodes operating on public, permissionless blockchains could be considered controllers or joint controllers under the GRPD. However, Adan respectfully submits that this interpretation does not accurately reflect the technical function of nodes.

Nodes passively validate transactions according to predefined consensus protocols and do not exercise discretion or determine the purposes or means of data processing. Functionally, they are more akin to network routers than data controllers.

Classifying nodes as controllers risks deterring participation in decentralised systems and could inadvertently undermine the privacy benefits that decentralisation itself provides. Adan encourages the EDPB to adopt a more nuanced, case-by-case approach that differentiates between passive infrastructure participants and entities with meaningful decision-making authority over personal data processing.

Therefore, the Guidelines should make clear that operating a node, in itself, does not equate to controllership. The assignment of GDPR roles should be based on an entity's actual influence and involvement in determining the purposes and means of processing. This can be determined by performing a comprehensive Data Protection Impact Assessment.

1.3. Community governance and decentralised decision-making

While the Guidelines rightly point out that certain actors, such as the node operators described in section 1.2, may sometimes exercise influence over network operations (e.g., through participation in forks or protocol changes), they do not sufficiently acknowledge the alternative governance mechanisms that structure decision-making in decentralised ecosystems. The absence of a centralised legal entity does not equate to a governance void: on the contrary, blockchain networks often operate under collective, transparent, and auditable governance frameworks involving core developers, DAOs, and broader community stakeholders.

This distributed governance model reflects a legitimate and increasingly recognised form of organisational coordination, where decisions (including those impacting data processing purposes or protocol changes) are made through structured, community-led processes. These may include on-chain voting, consensus mechanisms, or multistakeholder forums. **As such, Adan considers that attributing GDPR responsibilities solely through the lens of traditional hierarchical control overlooks these novel models and may distort the reality of control and accountability in decentralised systems.**

Consequently, the Association recommends that the Guidelines explicitly recognise community-led governance as a relevant factor when assessing controllership and accountability under Article 4 (7) GDPR, ensuring that legal interpretation evolves in step with technological and organisational innovation.

1.4. End users as potential controllers

An unresolved issue not clarified by the guidelines is whether data users who are also natural persons can also exercise control over the processing activities. That decision-making power could also reside with the end-users, who might specify what data is uploaded and for what reasons.

In the context of blockchain network activities, individuals are the ones who determine the purpose and the way data is collected in line with the protocol rules. Validators and nodes do not exercise any discretion; more precisely, they do not exercise meaningful discretion over the purposes or essential means of processing but follow deterministic, protocol-defined rules, and their actions are purely technical and procedural. As a consequence, validators do not choose how data is structured, stored, or processed; they cannot opt out of protocol-mandated operations without ceasing to be validators, and their role is to mechanically apply a consensus algorithm, not to architect or modify data processing logic.

When a data user decides on the types of personal data to process, the processing objectives, how data is structured, and who has access, they could be deemed to be exercising control over the processing activities and thus be deemed a data controller.

While this doesn't preclude that there could be other data controllers, in case where for example a natural person might be deemed data controller, it remains uncertain who would be responsible of the implementation of Recommendation 3 according to which data controllers must inform data subjects on the rationale of the processing, the existence of their rights and the modalities to exercise them.

While Adan argues that a case-by-case analysis is always needed, the guidelines do not shed light on this regard, while other National Authorities have certainly tackled this subject.

Following the laid down criteria in Article 4 (7) of the GDPR, the French CNIL has observed that participants, who have the right to write on the chain and who decide to send data for validation by the miners, can be considered as data controllers. In parallel, Article 2 states that GDPR does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity.

According to CNIL, natural persons who enter personal data on the blockchain which do not relate to a professional or commercial activity shall not be deemed data controllers and fall under the *"purely personal or household activity"* exclusion set out in Article 2 of the GDPR.

CNIL highlighted that: *"For example, a natural person who buys or sells Bitcoin, on his or her own behalf, is not a data controller. However, the said person can be considered a data controller if these transactions are carried out as part of a professional or commercial activity, on behalf of other natural persons*."

In the context of crypto-assets this is a key criterion as for instance, a user initiating a Bitcoin transaction may be seen as the controller of the data involved in that transaction.

Beyond crypto-assets transfers, we might find other analogous examples where data users can upload, manage, or interact with data on a blockchain platform (that do not relate to a professional or commercial activity).

Overall, correctly identifying the controller responsible for each personal data processing activity is essential. It clarifies to whom data subjects can turn for exercising their rights under the Regulation. However, in the context of blockchains, this becomes particularly complex.

The **multiple participants and actors operating within the network may take on different roles, each influencing certain aspects of the blockchain's operation. But importantly, these roles should not necessarily imply that each participant influences the core purpose of the data processing itself**.

Thus, **an expansive view on determining when there is an object of the data process and who is setting the objective risks labelling all blockchain participants as controllers, which creates significant ambiguity about who actually bears ultimate responsibility.**

This ambiguity further complicates the implementation of recommendations like controllers' obligation to inform data subjects (Recommendation 3). Determining who should provide such information becomes unclear when responsibility is diffused across numerous actors.

Moreover, under GDPR, joint controllers are required to establish clear contractual arrangements to define roles and responsibilities. In decentralized, diffuse governance models typical of blockchain ecosystems, creating such contractual relationships becomes not only impractical but often unfeasible. The very nature of decentralization presents challenges in fulfilling GDPR obligations, such as responding to data subject requests for access, erasure, or portability.

Blockchain technologies and decentralized digital ecosystems fundamentally alter traditional data management and governance paradigms. The decentralized and distributed nature makes it difficult to pinpoint a single, identifiable controller. This decentralization makes it difficult to identify a single data controller responsible for compliance with GDPR, since multiple participants may influence processing decisions collectively or independently, especially in permissionless environments.

Therefore, the current GDPR Guidelines often struggle to provide clear applicability to these novel decentralized structures, leading to ambiguity in attributing responsibilities for fulfilling data subject rights.

2. Qualification of "Personal data"

The definition of Personal data under Article 4 (1) of the GDPR is intentionally broad. It encompasses any information relating to an identified or identifiable natural person (whether directly or indirectly) and includes identifiers such as names, identification numbers, location data, or "*factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person*".

In blockchain networks, certain data types, including but limited, public keys, hashed information, and transaction metadata, **are not inherently personal, but can become**

personal data when they relate to an identifiable person, either alone or in combination with other data. This position is reflected in EDPB guidance and confirmed by national supervisory authorities such as the CNIL.

The key criterion (*see* Recital 26, GRPD) is whether a person is identifiable "*by means reasonably likely to be used*", taking into account all objective factors (costs, time and technology available). In practice, this means that even pseudonymous identifiers like blockchain addresses or hashed values, may fall within the scope of personal data if they can be linked to a natural person through contextual information.

For example, a public address used repeatedly in transactions, or shared on a forum, can be associated with a user profile, then rendering the data "relating to" that individual. Also, a hash of personal data might retain identifiability if the underlying data is known or guessable.

Adan does not dispute that public keys and hashes can, in certain cases, qualify as personal data. However, this qualification depends on the actual context and identifiability risk, not on the technical format alone. **The same data may or may not be personal depending on how it is generated, combined, and used in practice.**

While we hold the understanding that a wallet address is not personal data under the GDPR when it cannot lead to identifying the data subject, it is important to consider how we would analyze the issue if a wallet address were considered personal data as well. An integral part of the analysis is understanding that when a user uses the blockchain for a transaction, they inherently and voluntarily opt into sharing their data on a public ledger. The user consented to their data existing on the blockchain when they performed the transaction, and now, to maintain the blockchain's operations and integrity, the controlling party would have a legitimate interest in retaining that data in the public ledger.

Then, Adan urges EDPB to avoid a formalistic or "static view" of "identifiability". A more nuanced and contextual based interpretation is necessary to reflect the technical realities of blockchain systems.

Indeed, the threshold for identifiability, and thus the determination of whether data is "personal", is context-dependent and can vary widely based on available datasets, analytics tools and the actors capabilities.

The Guidelines could explicitly encourage a risk-based, contextual analysis of whether data is "*personal*" in a given scenario. For example, a public key may be considered personal data in a retail DeFi application with persistent identifiers, but not in a purely technical infrastructure layer where keys are rotated frequently and no external profiling occurs.

The potential for linking on-chain data to off-chain identities is a critical vector of risk. Even when only hash or pseudonymised data is stored on-chain, re-identification may still be possible through external data correlation or behavioural pattern analysis. **Then, the**

Association recommends that the Guidelines provide concrete examples of what constitutes sufficient pseudonymisation in blockchain settings, and differentiate it from anonymisation, which is rarely achievable on-chain.

The Guidelines should also recognise the distinction between "*functional identifiers*" and traditional personal identifiers, and thus suggest more appropriate design measures to minimise identifiability risk (e.g., address rotation, ZKP, mixers….).

Adan believes the Guidelines would benefit from a more in-depth treatment of the question: what constitutes personal data in blockchain contexts? Blockchain systems, especially public permissionless ones, often rely on cryptographic identifiers (*e.g.,* wallet addresses, transaction hashes, or smart contract interactions) that may not directly identify individuals but could be linked to them through auxiliary data. To further clarify this, Adan recommends that the EDPB provide additional guidance on assessing identifiability in blockchain contexts, including a spectrum of examples ranging from clear cases of personal data to borderline pseudonymous or hashed data. This will help developers, privacy professionals, and regulators alike apply GDPR requirements more consistently and proportionately.

If the definition of "personal data" is applied too broadly and without proportionality, even non-intrusive or privacy-preserving, blockchain uses may be captured un necessarily under GDPR obligations. This risks creating regulatory chilling effects, stifling innovation and discouraging the adoption of beneficial decentralisation practices. A balanced interpretation, grounded in technical realities and actual re-identification risk, would support more pragmatic compliance.

3. Obligation of erasure and deletion of the whole blockchain

3.1. Architectural fragmentation and accountability

One of the core difficulties of implementing these Guidelines is the difficulty in pinpointing who should be held accountable for safeguarding data subjects' rights, particularly when it comes to responsibilities like the right to erasure.

The network models assumed by the Guidelines seem outdated, presenting scenarios where a single, unified blockchain network handles the entire data processing operations. In practice, blockchain ecosystems are decentralized and increasingly modular, involving multiple networks and actors performing different functions such as execution, consensus, or data storage.

Decentralization shouldn't thus be viewed only through the lens of decision-making authority (who sets the data processing goals), but also from the perspective of functional division, where different entities carry out separate, yet interconnected, aspects of data management.

This diversity means that **roles are spread across various entities,** some being individual persons, others being entities, each taking care of diverse aspects of the data process lifecycle. The notion of a controller or responsible entity doesn't necessarily fit the operational reality of many blockchain networks, especially those built on modular architectures, where responsibilities are distributed, and no one entity has complete oversight of the entire data management process.

This fragmentation intensifies challenges around compliance with data subject rights, particularly the right of erasure, because it's not always clear which actor has the authority or capability to (solo) fulfill such requests. As previously outlined, this challenge is accentuated by a broad interpretation of what constitutes a data process objective and who is responsible for setting this objective, resulting in ambiguous accountability that does not align well with the roles typically envisioned under GDPR. This fragmentation challenges "traditional" notions of responsibility, making compliance with data privacy rights in decentralized, modular blockchain environments a significantly more intricate affair than in conventional, centralized systems.

This challenge is further illustrated in the Guidelines approach to accountability mechanisms, particularly regarding the maintenance of a register of processing activities under Article 30 GDPR.

Section 3.4. p.112 of the Guidelines states that *"A record of processing activities (RoPA) must be maintained pursuant to Article 30 GDPR. It is not sufficient to claim that, because the blockchain is decentralised, no one is in charge of keeping such a record."*

However, this statement does not reflect the operational and governance realities of decentralised blockchain ecosystems, where no single entity may have the ability, or even the legitimacy, to maintain such a register on behalf of the entire network, as described above.

While the principle of accountability remains fully applicable, its implementation may differ in decentralised settings. For example, many projects may rely on smart contracts that self-declare certain data processing parameters, or public interfaces maintained by the community to describe data structures, access rules, or retention logic. These decentralised and often open-source compliance tools provide meaningful levels of transparency, traceability, and user information.

Adan therefore recommends that the Guidelines acknowledge the possibility of distributed or decentralised accountability frameworks, provided they allow for effective documentation, regulatory oversight, and user protection.
Smart contracts can automate decisions that may have legal or significant effects on individuals, potentially invoking Article 22 of the GDPR. EDPB should offer guidance on ensuring transparency, contestability, and human oversight in smart contract deployments that process personal data.

Recognising such mechanisms would remain fully consistent with the outcome-oriented logic of the GDPR and better reflect the diversity of compliance models emerging in decentralised environments.

3.2. Data minimisation and off-chain storage

Adan supports the EDPB's guidance advocating for data minimisation and the avoidance of storing personal data directly on the blockchain. This principle is particularly vital given the immutability of blockchain ledgers, which can render any inclusion of personal data effectively permanent and inaccessible to modification or deletion.

Many service providers utilise off-chain storage solutions to house any data that could be linked to identifiable individuals, storing only hashed pointers or identifiers on-chain to maintain the necessary functionality without compromising privacy.

However, further elaboration in the Guidelines would be helpful in these key areas:

- **Standardisation of off-chain architectures**: while many blockchain service providers adopt off-chain storage to remain GDPR-compliant, the lack of harmonised standards leads to inconsistent implementations and potential security risks.
- **Linkability and reversibility risks**: even when only hashed or pseudonymised data is stored on-chain, there remains a risk of re-identification, especially when such data can be linked with off-chain datasets or metadata.

Adan advocates for a more concrete guidance or alignment with existing frameworks (*e.g.,* ISO/IEC 27001, NIST) would be valuable to ensure that off-chain environments meet an appropriate threshold for data protection and security.

The Guidelines could benefit from a more in-depth analysis of the residual risks posed by linkability and recommendations for appropriate safeguards, such as cryptographic commitments or zero-knowledge proofs (ZKPs).

3.3. International data transfers

Adan welcomes the EDPB's inclusion of international data transfer considerations in the context of blockchain networks, where nodes may be geographically dispersed and the flow of data often transcends jurisdictional boundaries.

However, the practical application of *Chapter V* of the GDPR to decentralised blockchain environments remains ambiguous and presents substantial compliance challenges. In traditional architectures, data exporters can identify recipients, assess the legal environment of the third country, and implement appropriate safeguards such as Standard Contractual Clauses (SCCs) or Binding Corporates Rules (BCRs). In contrast, blockchain participants, particularly in public, permissionless networks, cannot easily identify where nodes are located, nor who controls them, making it nearly impossible to determine if a transfer has occurred, let alone establish a lawful mechanism for it.

Therefore, here's are the key challenges and areas needing clarification:

- **Definition of "Transfer" in decentralised systems:**
  - The Guidelines would benefit from a more precise definition of what constitutes a "Transfer" in blockchain settings. For instance, is it a transfer when a transaction is validated by a node located in a third country, even if the transaction was initiated within the EEA? More clarity on when and how blockchain activity triggers the transfer regime would support consistent application of GDPR obligations.
- **Applicability of transfer mechanisms (e.g., SCCs, BCRs):**
  - Current mechanisms for international data transfers were designed with centralised data exchanges in mind. Their application in open networks, where data may be propagated to unknown entities in unknown jurisdictions is highly impractical. The Guidelines should acknowledge this gap and provide interim solutions or endorse alternative approaches (e.g., contractual obligations at the application layer, technical access restrictions, or architectural segregation between EEA and non-EEA nodes).
- **Risk-based approach to global validation:**
  - In many blockchain use cases, the on-chain data is either pseudonymised or rendered non-personal via robust design strategies (*e.g.,* storing only hashes or encrypted values). In such contexts, the risks traditionally associated with international transfers are significantly reduced. We encourage the EDPB to adopt a proportional, risk-based perspective when considering enforcement of transfer rules for blockchain systems.
- **Support for privacy-enhancing network designs**:
  - Emerging blockchain designs, such as permissioned networks with geographic node controls or consortium chains with enforced jurisdictional restrictions, offer practical avenues for transfer compliance. The Guidelines could highlight these as examples of best practice, encouraging privacy-aware architecture design.

Therefore, Adan recommends that the EDPB provide greater clarity on how international transfer rules apply to decentralised networks, and explore the development of transfer-compliance frameworks specifically tailored for blockchain systems. Additionally, the EDPB should consider recognising the value of technical and organisational measures that reduce re-identification and cross-border exposure as part of a proportionate risk-based assessment.

3.4. Data Protection Impact Assessments (DPIAs)

Adan strongly supports the EDPB's emphasis on conducting Data Protection Impact Assessments (DPIAs) for blockchain-based processing activities. Given the innovative and often complex nature of blockchain systems, DPIAs serve as an essential tool to identify, assess, and mitigate data protection risks early in the design process, aligning with the principles of privacy by design and by default (Article 25 GDPR). However, we believe the Guidelines would benefit from additional specificity regarding how DPIAs should be tailored to blockchain contexts, particularly where the conventional assumptions of controllership, centralisation, and data lifecycle management do not hold.

To enhance practical compliance, the EDPB should provide guidance on addressing blockchain-specific risks that are often absent from existing DPIA templates or risk libraries. For instance, the irreversibility of data recording, the lack of central governance, and the potential for linkability or re-identification of pseudonymous data present unique challenges. These risks are particularly pronounced in scenarios such as the use of smart contracts for automated decision-making, the storage of metadata on-chain, or the replication of data across nodes in multiple jurisdictions. Offering typical risk ratings and mitigation options for these scenarios would support organizations in designing privacy-compliant systems. Similarly, in permissionless or consortium-led blockchain networks, where no single entity fully controls data processing, DPIAs must account for shared governance models. The Guidelines should clarify how to document residual risks transparently when mitigation measures cannot be fully implemented by a single actor and encourage collaboration across entities, such as through joint DPIAs or cooperative governance frameworks.

Furthermore, the EDPB could streamline the DPIA process by recommending screening criteria tailored to distributed ledger technology systems to determine whether a DPIA is necessary. Questions such as whether personal data is written to the blockchain directly or indirectly, whether smart contracts trigger automated actions with legal or significant effects, or whether nodes operate in third countries without adequate decisions would help organizations assess the need for a DPIA early in the design phase. Additionally, effective DPIAs for blockchain projects require cross-functional collaboration. Privacy professionals must work closely with system architects, smart contract developers, and network designers to ensure risks are accurately understood and mitigated. The Guidelines should advocate for embedding DPIA processes into agile and DevOps cycles, particularly in the fast-evolving Web3 environment, to foster privacy-aware development practices.

Adan urges the EDPB to develop or endorse DPIA guidance and templates specifically tailored for blockchain applications. These should address the unique technical and governance challenges of decentralized systems, promote standardized risk identification, and provide practical advice on documenting mitigation strategies even in the absence of full control over the processing ecosystem.

3.5. Immutability vs. data subject rights

Adan appreciates the EDPB's recognition of the tension between blockchain's inherent immutability and the exercise of data subject rights under the GDPR, particularly the rights to rectification (Article 16) and erasure (Article 17). While the Guidelines rightly advocate for off-chain storage of personal data as a practical mitigation measure, further clarity is needed on how to address residual risks and exceptions, especially when personal data may be written on-chain inadvertently or through user actions beyond the service provider's control.

In public and permissionless blockchain environments, where any participant can write to the ledger, preventing the inclusion of personal data altogether is technically challenging. For example, metadata embedded in transactions, such as wallet addresses, IP-related data, or user-generated content, may contain or infer personal data. Similarly, smart contracts may encode user-specific terms or identifiers that become permanently etched into the chain. **These realities present an operational dilemma: once personal data is on-chain, it cannot be modified or deleted without undermining the fundamental structure and trust model of the blockchain**. However, suggestions such as "deleting the entire blockchain" are unhelpful to the industry and fail to address practical compliance needs.

To support stakeholders in these challenges, the EDPB should clarify how "effective erasure" can be interpreted in contexts where deletion is technically infeasible. For instance, rendering data inaccessible through methods like key deletion or cryptographic obfuscation could, in certain scenarios, fulfil the intent of Article 17. A more definitive position on such approaches would guide controllers in developing compliant blockchain architectures. Additionally, emerging privacy-preserving technologies, such as chameleon hashes, zk-SNARKs, and commit-reveal schemes, offer promising ways to reconcile immutability with GDPR requirements. While not yet mainstream, the EDPB's recognition of their potential could incentivise innovation and accelerate their adoption in blockchain ecosystems.

The Guidelines should provide a more nuanced treatment of whether all on-chain information, such as pseudonymous addresses, transaction hashes, or smart contract identifiers, should be treated as personal data per se, or whether context and re-identifiability thresholds should apply. Distinguishing between personal data and metadata based on their identifiability risk would enable stakeholders to assess compliance obligations proportionately and avoid overly broad interpretations that could stifle innovation.

Adan urges the EDPB to provide additional interpretive guidance on how data subject rights, particularly erasure and rectification, can be respected in immutable environments, including through alternative technical means. Additionally, the Association recommends that the Guidelines promote a risk-based, proportionality-driven approach that recognises the technical limitations of decentralised systems while encouraging innovative privacy safeguards.

3.6. Deletion of the whole blockchain and legal proportionality

3.6.1. Conditional nature of the right to erasure

According to the guidelines, once those purposes have been achieved, data should either be rendered anonymous or deleted. Paragraph 63 states that when deletion has not been taken into account by design, this may require deleting the whole blockchain.

Such a conclusion appears to rest on a partial reading of Article 17 of the GDPR, which enshrines the "*right to erasure*". Pursuant to Article 17 (1), the data subject has the right to obtain the erasure of personal data concerning them "*without undue delay*", but only where one of a limited set of legal grounds is satisfied. These include that the data are no longer necessary in relation to the purposes for which they were collected **(a)**, that the data subject withdraws consent **(b)**, or that the data have been unlawfully processed **(d)**. **Therefore, the right to erasure is not absolute but conditional.**

Article 17 (3) explicitly provides for circumstances where this right does not apply. In particular, Article 17 (3) (b) states that the right to erasure shall not apply where the processing is necessary for compliance with a legal obligation or for the performance of a task carried out in the public interest. These exceptions are especially relevant in the context of blockchains, which may serve purposes linked to public interest or legal compliance (not limited to regulated use cases). The continued storage of data on a blockchain may thus be not only legitimate but also required by law, including in diverse contexts such as legal certainty, traceability, or the prevention of misuse.

Then, interpreting Article 17 as mandating the wholesale deletion of a whole blockchain - especially where no erasure mechanism has been foreseen by design - disregards the legal architecture of the GDPR. The Regulation strikes a balance between data subjects' rights and other legal or public interest obligations. Requiring erasure "*whenever deletion has not been considered by design*" would amount to imposing a duty that is neither grounded in the letter of the GDPR nor consistent with its proportionality rationale.

3.6.2. Permissible restrictions to the right of erasure

Adan considers that this rigid interpretation also overlooks Article 23 of the GDPR, which allows Union or Member State (MS) law to restrict data subjects rights - and including Article 17 - where such restrictions are necessary and proportionate to safeguard objectives such as the prevention of criminal offences or the protection of important economic or financial interests. These limitations are essential when assessing how data protection rights apply within decentralised, transparent, and immutable infrastructures such as blockchains.

In that sense, the Association highlights that transparency is one of the key features and value propositions of blockchain technology, often seen as a way to build trust and accountability for the activities carried out on the network. While we agree that user data should always be protected, taking such an all-or-nothing approach to deletion can create additional complexities for users and businesses that go beyond data protection discussions.

We agree that users' data shall be protected at any moment, however, such a harsh approach could also inject other complexities, potentially damaging the businesses and the users themselves in other aspects beyond data protection reasons. Blockchains allow for transparency, and transparency allows for accountability. And that transparency and accountability might be needed in other contexts, including from a regulatory perspective.

3.6.3. Relevance for regulatory oversight and AML compliance

Although deleting the blockchain might seem appealing from a privacy or data minimization standpoint, it clashes fundamentally with the legal and regulatory framework established to prevent illicit activities, ensuring that authorities can perform their oversight functions effectively.

From a supervision perspective, authorities often require access to transaction histories and user data to monitor and investigate suspicious activities related to AML concerns. If the entire blockchain were to be deleted, it would eliminate the records that regulators rely on for compliance checks and investigations.

The data on the blockchain also enables sophisticated blockchain analytics tools to trace the flow of illicit funds, identify potential illicit activities and suspicious patterns, contributing to unmasking criminal networks. Therefore, this would severely hinder enforcement efforts, weaken transparency, and potentially diminish the capacity to comply with legal obligations.

The transparency of the blockchain is one of its biggest advantages in combatting financial crime and it acts as a disincentive for bad actors due to the ability of law enforcement to trace illicit transactions.

Importantly, **under EU law, obliged entities are mandated to implement AML due diligence measures, which include continuous monitoring of transactions, pattern analysis, and timely reporting of suspicious activities to authorities. Deletion of data on the blockchain would essentially obstruct their ability to fulfill these obligations, rendering oversight ineffective and disproportionate to the risks involved. Moreover, such deletion could create significant blind spots, enabling malicious actors to exploit the absence of records to obfuscate their actions, thereby undermining the very purpose of AML regulations and potentially facilitating criminal activitie**s.

4. Lack of technological neutrality

Paragraph 49 of the Guidelines suggests that public blockchains should only be employed if public access to the ledger is necessary for at least one of the purposes of the processing. This formulation raises significant concerns as it departs from the principle of technological neutrality, which is a foundational element of EU law and policy — including in the field of data protection. The GDPR does not prescribe or favour any specific technology, nor does it limit the means by which data processing activities can be carried out, provided that the principles and obligations of the Regulation are respected. In this regard, introducing an implicit hierarchy between technological architectures (i.e., favouring permissioned or private ledgers over public, decentralised ones) risks undermining both the innovation potential of blockchain technologies and the legal coherence of the Guidelines themselves.

Moreover, this stance overlooks the fact that public blockchains can fulfil functions of legal, societal, or economic importance that extend beyond data protection — including transparency, accountability, fraud prevention, and support for decentralised governance. Limiting their use on the sole basis that public access is not strictly required for personal data processing purposes narrows the regulatory lens and may result in unintended consequences for the European digital economy.

The role of data protection authorities should not be to determine the appropriateness of a given technological stack, but rather to assess whether a given implementation complies with the GDPR's principles, including data minimisation, purpose limitation, and security. Such an approach preserves innovation, encourages responsible design, and ensures that the rules are applied consistently across sectors and architectures. Public Layer 1 blockchains in particular should be understood as general-purpose infrastructure, analogous to the internet itself. They support a broad range of applications, from identity management to supply chain traceability, and constitute a key component of the emerging decentralised digital ecosystem. Restricting their use through narrow interpretation risks pushing innovation and infrastructure development outside of the EU, to jurisdictions with more permissive or adaptive regulatory frameworks.

In light of this, Adan urges the EDPB to reaffirm its commitment to technological neutrality and adopt a principle-based, risk-oriented approach that enables diverse architectural models to co-exist, provided that appropriate safeguards are implemented.

❖ Who is Adan

Adan brings together over 200 professionals - new players and established companies - who develop innovation and use cases for the decentralised web in all areas of the economy on a daily basis. By removing obstacles to their growth and competitiveness, Adan works to promote the emergence and influence of French and European leaders for our digital sovereignty. Adan promotes an appropriate, proportionate and dynamic framework for innovation, as well as a better understanding of new blockchain and Web3 technologies and their opportunities.

❖ Contacts at Adan

- Stanislas Barthelemi, President: stanislas.barthelemi@adan.eu
- Adriana Torres Vergara, EU Policy Officer: adriana.torresvergara@adan.eu
- Alizée Van Den Schrieck, Legal Officer: alizee.vandenschrieck@adan.eu

*