BLOCKCHAIN FOR EUROPE

Blockchain for Europe
Rue Montoyer 47
1000 Brussels
Belgium

# BC4EU Response to EDPB Consultation on Guidelines 02/2025: Processing of Personal Data through Blockchains

## Executive Summary

Blockchain for Europe (BC4EU) welcomes the opportunity to contribute to the European Data Protection Board's (EDPB) consultation on its draft guidelines regarding the processing of personal data through blockchains. As the leading European trade association representing the blockchain industry, we strongly support the foundational objectives of the General Data Protection Regulation (GDPR), in particular the protection of fundamental rights and freedoms of individuals, the empowerment of data subjects, and the establishment of trust in digital ecosystems.

However, we have serious concerns about several key recommendations in the draft guidelines. The suggestion in paragraph 63 that the inability to delete personal data from a blockchain may require deletion of the entire blockchain is technically unfeasible, legally disproportionate, and incompatible with both EU constitutional principles and the structure of public blockchain networks. If upheld, this interpretation would effectively prohibit the deployment of such systems within the EU, leading to significant negative consequences for innovation, competitiveness, and consumer choice. As such, we find the Guidelines technology-prohibitive rather than technology-neutral.

We urge the EDPB to adopt a more nuanced, technologically proportionate, and legally balanced interpretation of the GDPR that respects both the technical realities of decentralised systems and the broader strategic objectives of the EU.

## Introduction

Blockchain for Europe reiterates its strong support for the GDPR's foundational objectives: ensuring individual data protection, promoting trust, and preventing abusive practices in data processing. We also fully support the EDPB's goal of clarifying how these objectives can be met in evolving digital environments, including decentralised blockchain systems.
However, we respectfully express our concerns that the current draft guidelines fall short of offering a viable framework for the adoption of blockchains, in particular public and permissionless blockchains. If interpreted literally, they would render many of these technologies legally untenable in the EU, with detrimental effects for innovation, privacy-enhancing design, economic competitiveness, and the EU's broader digital strategy.

Blockchain for Europe
Rue Montoyer 47
1000 Brussels
Belgium

To address these concerns, we suggest the EDPB consider the following recommendations:

1. **Policy and risk approaches for diverse DLT architectures:** Public blockchains (whether permissioned or permissionless) cannot be simply assimilated into pre-existing legal categories designed for centralized architectures. Recognizing the distinct advantages of each architecture, without mandating specific preference to one, is essential to fostering an effective and future-ready regulatory environment.

2. **Data controller and processor roles must reflect decentralisation:** Validators, node operators, and protocol-level actors should not be deemed controllers or processors absent discretionary influence over data processing. Responsibility should focus on actors whose business models depend on collecting, aggregating, and monetizing personal data—not on neutral blockchain infrastructure providers who do not actually have visibility of personal data and do not handle its content.

3. **Rethinking Applicability of the Erasure Requirement and Article 17 GDPR:** Where technical deletion is not feasible or desirable due to the immutable nature of blockchains, solutions such as key deletion, zero-knowledge rollups, or off-chain dereferencing should be recognized as valid under Article 17 of the GDPR. Industry stands ready to provide greater detail as to how these features work in practice and how they can support policy objectives.

4. **Clarification of What Constitutes "Personal Data" on Blockchains:** Not all technical identifiers on a blockchain, such as hashes or public keys, should be treated as personal data by default. Identifiability must be assessed based on contextual access, linkability and reasonable likelihood, consistent with Recital 26 and CJEU precedent (e.g. Breyer).

5. **Encourage the use of privacy enhancing technologies:** There are numerous industry solutions designed to enhance and protect privacy in decentralised systems, which the EDPB should consider further as part of its evolving understanding of these issues and also as an effective way to protect data subject rights through technology instead of just through regulation alone. These include, among others, zero-knowledge proofs, homomorphic encryption, and selective disclosure.

6. **Why the EDBP's Interpretation of Technological Neutrality Fails Blockchain Networks:** Tech neutrality cannot be interpreted to mean that fundamentally different architectures must be treated as if they are the same. The problem with applying the GDPR to blockchain systems is not a lack of technological neutrality - it is that the regulation's core assumptions are built for an entirely different model of the internet.

Blockchain for Europe
Rue Montoyer 47
1000 Brussels
Belgium

7. **International Transfers of Personal Data:** The EDPB should clarify that public accessibility of data on global blockchains does not automatically constitute a "transfer" of personal data to a third country under Chapter V of the GDPR.

8. **Alignment with EU Digital Strategy and Fundamental Rights:** The EU cannot strive for competitiveness and to be a leader in digital innovation if its regulatory actions end up stifling innovation into digital technologies and pushing it outside of the EU.

BC4EU remains committed to constructive dialogue with the EDPB and stands ready to collaborate on further refining a GDPR framework that protects individuals while enabling innovation in decentralised technologies.

## 1. Policy and Risk Approaches for Diverse DLT Architectures

The EDPB guidelines express a preference for permissioned blockchain systems. This appears to stem from their apparent structural resemblance to traditional models of centralised control, which mistakenly makes them seem more readily compatible with the existing GDPR framework. However, in addition to being against the principle of technological neutrality, this approach also ends up overlooking the unique benefits of permissionless blockchains, including resilience, censorship resistance, and user autonomy, which they achieve without relying on central intermediaries or retrofitted compliance layers.

Public blockchains (whether permissioned or permissionless) cannot be simply assimilated into pre-existing legal categories designed for centralised architectures. Recognising the distinct advantages of each architecture, without mandating specific preference to one, is essential to fostering an effective and future-ready regulatory environment.

We urge the EDPB to work towards developing a balanced approach to compliance that reflects the degree of decentralisation and control in different blockchain systems by assessing the full technology stack. Compliance expectations should be proportionate to risks posed. Treating all blockchains identically, or failing to protect the unique benefits of each, imposes an unjustified burden on systems that, by design, cater to different consumers and market needs. We urge the EDPB to uphold the principle of technological neutrality and to evaluate compliance based on practical data protection outcomes, not structural conformity.

## 2. Data Controller and Processor Roles Must Reflect Decentralisation

We are concerned by the draft's suggestion that validators or node operators may be deemed data controllers. This assumption fails to account for the nature of the role that these actors play in public blockchains.

The GDPR defines 'controllers' as the "natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the

Blockchain for Europe
Rue Montoyer 47
1000 Brussels
Belgium

processing of personal data". The concept of 'data controller' assumes centralised authority or a certain hierarchy, which doesn't exist in public blockchains. The nodes (validators or miners) do not meet this legal definition. The nodes do not decide why personal data is included in the chain. Instead, they automatically execute a protocol chosen by end-users or dApp developers who initiate transactions and encode data.

The nodes do not decide on how the personal data is processed because consensus rules provide for pre-coded parameters, which cannot be amended unilaterally by a node without causing economic self-harm. Within these parameters, any malicious acts by validators are penalised and may cause self-harm (e.g. slashing). Validators do not initiate or select transactions based on their content. Instead, they execute deterministic protocol logic. They do not interpret or modify the content of transactions and have no discretion over the transactions they process, which is instead a key criterion for determining data controllers.
Similarly, smart contract developers often publish open-source code without any control over its subsequent use. While off-chain actors such as front-end providers or API services may interact with users and influence how data is presented or used, infrastructural participants should not be deemed controllers absent evidence of discretionary control.

The Article 29 Working Party's Opinion 1/2010 clearly distinguishes between those who initiate data processing and those who merely transmit data, such as telecommunications providers. Validators could be viewed as the blockchain equivalent to those providing telecommunication infrastructure services. We would like to ask the EDPB to recognise this similarity and to encourage the EU to create a telecom-style "transmission" exemption for validators, as this would clearly set them outside the scope of the GDPR due to the fact that they do not initiate the transactions themselves.

The CJEU's ruling in *Breyer v. Germany* (C-582/14) reinforces the idea that identifiability requires access to contextual information. Most blockchain actors lack such access, and they are agnostic to such information. Imposing controller liability on infrastructure providers would create systemic legal uncertainty, discourage participation in decentralised networks, and undermine the resilience and openness of blockchain systems.

In public permissionless blockchains specifically, the set of nodes (whether validators or miners) is fluid (with entry and exit not being controlled or restricted), which is a defining feature of such networks. Consequently, a recommendation that these freely entering and exiting nodes consolidate into a fixed consortium contradicts the inherently decentralised nature of these networks.

While there is an observable trend toward the professionalisation of validator operations (particularly on more mature networks like Ethereum), this does not reflect the full picture. Despite the emergence of large, structured staking firms, a substantial proportion of validators are still individuals or small informal teams. These operators typically run nodes out of technical interest or financial incentive. They often operate from home set-ups and are dispersed globally without a common governance structure or legal framework.

Blockchain for Europe
Rue Montoyer 47
1000 Brussels
Belgium

On Ethereum alone, there are 1,000,000 active validators, and participation is open to anyone meeting the protocol's basic staking requirements. These validators can freely join or exit the network at any time, without needing to register or disclose their identity. Expecting this diverse, anonymous, and highly dynamic group to comply with the full scope of the GDPR – including obligations such as maintaining detailed privacy policies, entering into SCCs, or responding to data subject access requests – is not only unrealistic, but fundamentally unenforceable.

We believe that these expansive interpretations of data protection law could thus introduce systemic risks that undermine the viability of public blockchain networks. Furthermore, altering these fundamental pillars of blockchain technology would jeopardise the very security that the technology is designed to provide.

Therefore, we recommend that accountability is focused on actors whose activities and operations derive from the collection, aggregation, and monetisation of personal data – specifically, actors who exploit or seek benefit in the personal nature of that data as part of their activities. For example, platforms that collect user data to build profiles, sell targeted advertisements, or resell data to third parties are directly profiting from the processing of personal information.

In contrast, infrastructure participants in open blockchain networks – such as node operators, validators, developers – as well as wallets and interfaces that enable user connectivity to such networks – are agnostic to the personal nature of the data to the extent that they are not seeking to monetise personal data as a business model. Neutral infrastructure providers do not pose the same personal data related risks to users who wish to engage with blockchains.

In summary, once data is 'on-chain', there's really no data controller – control is lost by design. Only off-chain actors processing data before it's committed could be considered controllers from a GDPR perspective. And even in that case, web apps and front ends that only display on-chain data aren't controllers of off-chain data unless they actually process or collect personal data themselves.

This functional approach focuses on imposing appropriate legal obligations and responsibilities on actors which have the means to comply without altering the functionality and characteristics of the network and aligns with GDPR's aim to ensure accountability where influence and control are truly exercised.

Even if certain on-chain data such as wallet addresses are deemed personal under specific contexts, this should not result in a default assumption that all participants – such as validators – bear GDPR responsibility. The classification of data must be distinguished from the allocation of accountability.

Blockchain for Europe
Rue Montoyer 47
1000 Brussels
Belgium

## 3. Rethinking Applicability of the Erasure Requirement and Article 17 GDPR

Paragraph 63 of the draft guidelines seems to suggest that if personal data cannot be deleted individually from a blockchain, it may be necessary to delete the entire chain in some extreme cases. This interpretation is not only technically impossible in public blockchain systems, but legally disproportionate and counterproductive.

Blockchain data is replicated across thousands of globally distributed nodes. No single party can affect its deletion, and attempting to do so would destroy the utility of the system for all users – not only in regards to data stored but also in regards to the values created and the applications built on top of the infrastructure.

A useful analogy is the internet itself: the notion of "once on the internet, always on the internet" reflects the fact that centralised controllers may delete content they host, but cannot prevent other participants across the network from copying and redistributing it indefinitely. Although the underlying technologies differ, the practical effect is similar in public blockchain networks. Data, once recorded on a blockchain, is replicated across thousands of globally distributed nodes, making deletion technically infeasible. This persistence is not a feature unique to blockchains, but a broader characteristic of decentralised systems where control is diffuse and enforcement boundaries are blurred.

Requiring the deletion of a blockchain to satisfy the erasure request of a data subject would breach the principle of proportionality under EU law, harm all other impacted data subjects who have not made an erasure request, and violate the legitimate interests of data controllers. It would discourage adoption of GDPR-compliant blockchain solutions in the EU and push EU startups to relocate outside of the EEA or avoid innovating on blockchain technology.

Furthermore, deleting a whole blockchain because of the data erasure request of a user would also jeopardise the goal of ensuring transparency and traceability for AML purposes. Regulated entities have an obligation under the AML framework to collect and maintain personal information for the purposes of fighting money laundering and terrorist financing. Deleting a whole blockchain means also making it harder to trace transactions and combat ML/TF risks. Finally, blockchain analytics providers would not be able to provide the same level of information and visibility over transactions if the data was deleted or was not public.

We thus urge the EDPB to recognise that Article 17 of the GDPR does not require literal deletion in all cases, particularly where it is technically unfeasible. The principle of proportionality under EU law demands that rights be interpreted in a balanced way, taking into account competing fundamental rights and the public interest. The rights of other users, the integrity of the blockchain, and innovation must also be considered.

Blockchain for Europe
Rue Montoyer 47
1000 Brussels
Belgium

We support the view expressed by the French Commission Nationale de l'Informatique et des Libertés (CNIL) in its 2018 report on the compatibility of blockchains with GDPR that it is acceptable to use technical measures to render data practically inaccessible where deletion is impossible. This position was also supported by the Austrian data protection authority, which held that deletion under Article 17 does not have to be physical deletion and that removing the effective identifiability of the data and thus rendering it anonymous is sufficient.

Functional equivalents to deletion include:

- Encryption key destruction (crypto-shredding), rendering data permanently unreadable;
- Off-chain storage with revocation or dereferencing mechanisms;
- Zero-knowledge rollups, which enable proof-based data verification without revealing content;
- Smart contract-based "tombstoning", to mark data as deprecated or non-discoverable.

While these solutions do not, strictly speaking, result in an erasure of the data, insofar as the data would still exist in the blockchain, the CNIL acknowledges that these solutions are consistent with Recital 26 and Article 17(1)(c), as they effectively allow data subjects to get closer to an effective exercise of their right of erasure when deletion is not technically feasible.

These approaches should thus be explicitly recognised by the EDPB as sufficient to fulfil the right of erasure under Article 17(1)(c), in line with Recital 26 and the principle of privacy by design.

## 4. Clarification of What Constitutes "Personal Data" on Blockchains

While we can understand the arguments for which blockchain wallet addresses and transactional data could be considered as personal data, we still urge the EDPB to provide clearer criteria for determining when data recorded on blockchains qualifies as personal data. Current interpretations risk extending the concept of personal data to nearly all blockchain data only because this might be linkable "in theory", which is both unnecessary and impractical.

We recommend the following clarifications:

- **Public keys, wallet addresses, and hashes should not be treated as personal data by default.** Identifiability depends on whether contextual data is available to link them to an individual, and in this case, the collector of personal data that makes the link between the technical data and the person should be the addressee of the regulation.
- **We acknowledge that, in certain contexts, blockchain addresses may qualify as personal data** depending on the role of the actor, the availability of off-chain or other

Blockchain for Europe
Rue Montoyer 47
1000 Brussels
Belgium

on-chain information, and the intent behind data processing. However, such classification should not be used to expand liability to all participants indiscriminately but should be addressed at the off-chain collector of personal data.

- **Where pseudonymisation measures such as key rotation, mixers, or zero-knowledge layers are in use**, data should be considered anonymised unless real-world identification is reasonably possible and likely – meaning that there is a concrete risk that someone could actually identify a person from this data, given the available technology and access to the information.
- **Hashes of off-chain personal data should not be treated as personal data** unless the hashing party or another actor has access to the original data – in which case the holder of the original data should be the subject regulated by the rules.
- **Blockchain data should not be considered personal data** simply because a third party may hold legal obligations (e.g. under AMLR) to store identifiable off-chain data. Identification that depends solely on a separate legal obligation does not render the on-chain data itself inherently personal.

The EDPB should emphasise that **identifiability must be assessed based on the actor's capacity, access to auxiliary information, and the likelihood of re-identification** – not hypothetical or theoretical scenarios.

## 5. Encouraging the Use of Privacy-Enhancing Technologies

We share the EDPB's view (paragraph 77) that a data protection by design and by default approach is vital in the context of blockchain. In particular, we strongly agree that privacy-enhancing technologies (PETs) are essential tools for ensuring sufficient levels of data protection for data subjects in decentralised systems. Blockchain developers are increasingly leveraging PETs to reconcile decentralisation with compliance, embedding privacy safeguards at all levels of blockchain architecture.

We would also add that PETs have the ability to achieve the protection of a data subject's rights through **technological means** rather than regulation, thereby minimising legal obligations while maximising privacy.

We commend the EDPB for its recognition of technologies such as:

- zero-knowledge proofs (ZKPs),
- selective disclosure,
- anonymisation techniques that de-link past and future transactions,
- and references to privacy-preserving design choices such as "zero-knowledge" architectures.

These references, including those in paragraphs 24, 27, 64, and 108, reflect a welcome understanding of the technical means through which privacy can be enhanced in public

Blockchain for Europe
Rue Montoyer 47
1000 Brussels
Belgium

decentralised networks, and how PETs can help support compliance with core GDPR principles like data minimisation, purpose limitation, and privacy by design.

However, while the guidelines do mention approaches like encryption (para. 51) and the use of salted or keyed hashes (para. 52), they are also quick to discount their value. The EDPB emphasises that encrypted data remains within the scope of personal data, and suggests that future advances in computing may compromise encryption's protective power. Similarly, the guidelines note that salted or keyed hashes might still be considered personal data, particularly where re-identification remains theoretically possible.

These reservations are understandable but risk being overly cautious and leading to impractical or extreme results. For example, **considering a hash of personal data always as personal data would mean treating every new block of a blockchain as containing personal data once a single piece of personal data has been stored on one of the previous blocks.**

We urge the EDPB to go further in examining whether advanced encryption and hashing mechanisms – particularly when properly implemented and safeguarded – can achieve **effective anonymisation under Recital 26 and Article 4(1).** GDPR requires that anonymised data no longer relate to an identified or identifiable person by means reasonably likely to be used.

The omission of a more robust analysis in this area leaves unresolved the important role that PETs could play in removing data from the scope of GDPR altogether, whereby privacy and the protection of data subjects can be achieved through technological measures rather than only regulatory oversight.

More detailed and constructive guidance would be valuable to developers seeking to deploy blockchain systems that offer privacy-by-design and avoid the on-chain processing of personal data entirely – thereby not only enabling compliance with GDPR but also **removing the exposure of personal data on-chain**, further safeguarding the data subject's rights.

We recommend the EDPB **explicitly endorse a range of PETs** and develop technical annexes or supplementary guidance that address:

- The sufficiency of anonymisation in blockchain contexts;
- Thresholds for effective anonymisation in line with Recital 26 and Article 4(1);
- The acceptability of not only PETs but PET-based architectures as compliant-by-design solutions.

Among the PETs that should be specifically recognised, supported, and endorsed are:

- **Zero-knowledge proofs (ZKPs):** Allow for the verification of facts (e.g. age, credential ownership) without revealing underlying data. Examples include zk-SNARKs and zk-STARKs.

Blockchain for Europe
Rue Montoyer 47
1000 Brussels
Belgium

- **Selective disclosure credentials:** Built on verifiable credentials and decentralised identifiers (DIDs), enabling users to share only what is necessary.
- **Homomorphic encryption:** Enables computation on encrypted data without the need for decryption.
- **Mixnets and privacy pools:** Enhance anonymity by obfuscating transaction links.
- **View keys and privacy layers:** Permit regulators or law enforcement to audit specific transactions under tightly controlled circumstances while protecting user privacy in normal operations.
- **Hashes** that are not used as identifiers to access additional information but are only used to verify content.
- **Modular privacy-preserving decentralised technology solutions:** Where privacy-preserving technologies are embedded at all levels of the technology stack to ensure a comprehensive protection of personal data.

The EDPB's endorsement of these technologies would send a clear message that data protection compliance is achievable without requiring centralisation and would demonstrate how innovative technologies can be used to address specific privacy and data protection challenges identified by the EDPB.

This would significantly strengthen the position of developers seeking to align blockchain systems with EU law and help ensure that data subjects' rights and privacy are robustly protected in decentralised environments.

At the same time, we **caution against broader EU regulatory trends** that conflate the use of privacy-enhancing features with illicit activity. For instance, the European Banking Authority's guidelines identify the use of mixers or privacy-enhanced technologies as potential risk factors under AML/CFT rules, prompting enhanced due diligence obligations.

This framing overlooks the fact that in traditional finance, **transaction histories are not made publicly accessible**. Public blockchains, by contrast, expose transaction data by default – which is a massive benefit to understanding and mitigating AML risk (provided suitable tools are used) – but also means that **there is greater necessity for adding privacy protections**.

Similarly, EU co-legislators have introduced prohibitions for CASPs to provide privacy-enhancing technologies and assets to users, such as with Article 79 in the AMLR and Article 76.3 in MiCA, on the basis of the perceived risks for money laundering and obfuscation of transactions.

We strongly urge the EDPB to champion a **risk-based, context-sensitive approach** to PETs. Their use should not be automatically considered suspicious but assessed based on the context, purpose, and technical design.

A supportive regulatory stance would empower developers and organisations to integrate PETs that strengthen user protections and fulfil GDPR's core objectives.

Blockchain for Europe
Rue Montoyer 47
1000 Brussels
Belgium

**Clear and positive guidance for the use of PETs** would provide legal certainty, foster innovation, and uphold the GDPR's vision of privacy by design – particularly in decentralised systems that lack a central data controller but offer unparalleled opportunities for user empowerment and autonomy.

Furthermore, recognising the potential for PETs to achieve data protection through technical means – and in some cases, remove data from GDPR's scope entirely – would also encourage **privacy-preserving innovation** and reduce unnecessary regulatory burdens.

## 6. Why the EDPB's Interpretation of Technological Neutrality Fails Blockchain Networks

Tech neutrality cannot be interpreted to mean that fundamentally different architectures must be treated as if they are the same. The problem with applying the GDPR to blockchain systems is not a lack of technological neutrality – it is that the regulation's core assumptions are built for an entirely different model of the internet.

The GDPR was designed for a centralised, client-server model where clear data controllers define the purposes and means of processing, and users interact through intermediaries who control the flow of data. Blockchains, by contrast, are distributed networks where data is replicated across many nodes by design, and no single actor determines the purposes or means of processing in the traditional sense.

Simultaneously, blockchains are fundamentally designed to prioritise the anonymisation of data, inherently relying on robust encryption techniques and decentralised consensus mechanisms. These features collectively ensure the integrity, security, and resilience of the network. By distributing data across multiple nodes and using cryptographic methods, blockchains effectively minimise the risk of unauthorised access and manipulation, safeguarding user privacy while maintaining the trustworthiness of the system.

Forcing the same data protection rules that were developed for centralised networks onto these decentralised architectures creates perverse incentives. It favours one type of architecture over another, which is against the principle of technological neutrality and reduces market choice. This has negative effects on innovation and competition and ultimately harms user autonomy and transparency – values that blockchain technology is designed to promote.

Rendering public and permissionless blockchains legally untenable in the EU would undermine Europe's digital competitiveness, as developers and projects would relocate to other more innovation-savvy jurisdictions, and equally, diminish its ability to shape global technology standards.

Blockchain for Europe
Rue Montoyer 47
1000 Brussels
Belgium

Rather than forcing blockchain systems into a framework they were never designed for, regulators should focus on **outcomes-based, risk-oriented enforcement**. Accountability should be targeted at actors who derive commercial value from the exploitation of personal data – not at technical infrastructure providers whose roles do not create material risks to data subjects.

## 7. International Transfers of Personal Data

The draft guidelines only briefly touch on the implications of international data transfers in public blockchain environments. However, this is a topic that warrants more detailed consideration.

Public blockchains are inherently global and decentralised, meaning that data – once published – can be accessed by nodes and users worldwide, including from jurisdictions outside the European Economic Area (EEA).

We urge the EDPB to clarify that **public accessibility of data on blockchains does not automatically constitute a "transfer" of personal data to a third country** under Chapter V of the GDPR. As recognised by the Court of Justice of the European Union (CJEU) in the *Lindqvist* case (C-101/01), making data accessible online does not in itself amount to a regulated transfer to third countries. This interpretation remains highly relevant to blockchain systems, where data is not actively sent to third-country recipients but simply published in a way that makes it available globally.

Applying Chapter V to data that is publicly posted on a blockchain – without any targeted transfer – would render most blockchain activity legally untenable within the EU, as it would require adequacy decisions or transfer mechanisms for each possible jurisdiction in which a node may be located. This would place an impossible burden on developers and users of public networks and contradict the principle of technological neutrality.

Instead, the focus should be on **ensuring that personal data is appropriately protected before it is posted to the blockchain**, and on encouraging the use of technical safeguards that minimise identifiability. In many cases, data recorded on-chain is anonymised or pseudonymised to the point where no identifiability exists without off-chain context. Provided this off-chain data remains within EU-controlled systems or subject to appropriate safeguards, the accessibility of the on-chain record should not trigger Chapter V obligations.

We encourage the EDPB to issue a clear statement that:

- **Publicly available data on blockchains should not automatically be regarded as international transfers**;

Blockchain for Europe
Rue Montoyer 47
1000 Brussels
Belgium

- **The relevant test should focus on whether a data controller or processor actively discloses personal data to a third-country recipient**;
- **The use of PETs and off-chain safeguards can mitigate international transfer risks and should be factored into any risk assessment**.

Clear guidance on this point will help ensure consistency with CJEU case law and avoid inadvertently criminalising the foundational design of public blockchains.

## 8. Alignment with EU Digital Strategy and Fundamental Rights

The European Union has positioned itself as a leader in digital innovation, competitiveness, and fundamental rights. These goals are reflected in the **Digital Decade targets**, the **European Blockchain Services Infrastructure (EBSI)**, the **EU Blockchain Strategy**, the **Digital Finance Package**, and strategic reports such as those by **Draghi** and **Letta**.

Rigid interpretations of the GDPR that exclude public blockchains from the regulatory perimeter are incompatible with these goals. They risk **violating the principles of proportionality and subsidiarity**, and **conflict with the Charter of Fundamental Rights** – especially:

- **Article 7** (Respect for private and family life),
- **Article 8** (Protection of personal data),
- **Article 16** (Freedom to conduct a business).

Blockchain systems – especially when designed with PETs and open governance – support privacy, autonomy, and user empowerment. They **remove reliance on intermediaries** and enable individuals to control their data.

We call on the EDPB to **align its final guidance with the EU's broader digital and constitutional vision**. This includes:

- Engaging in inter-institutional coordination with **ESMA**, the **EBA**, and the **ECB**;
- Ensuring that regulatory interpretations do not conflict across frameworks;
- Supporting a coherent implementation of **MiCA**, **DORA**, the **AML Package**, and the **GDPR**;
- Recognising that **regulatory friction** between these instruments risks harming the very innovation the EU aims to promote.

Blockchain for Europe
Rue Montoyer 47
1000 Brussels
Belgium

## 9. Conclusion and Recommendations

Blockchain for Europe reiterates its strong support for the GDPR's foundational objectives: ensuring individual data protection, promoting trust, and preventing abusive practices in data processing. We also fully support the EDPB's goal of clarifying how these objectives can be met in evolving digital environments, including decentralised blockchain systems.

However, we respectfully submit that the current draft guidelines fall short of offering a viable framework for public decentralised blockchains. If interpreted literally, they would render many of these systems legally untenable in the EU, with detrimental effects for innovation, privacy-enhancing design, economic competitiveness, and the EU's broader digital strategy – and therefore, its citizens.

**In conclusion, our response argues that:**

- **Privacy-enhancing solutions** can help ensure sufficient levels of data protection for data subjects in decentralised systems. PETs also have the ability to achieve the protection of a data subject's rights through **technological means** rather than regulation, thereby minimising legal obligations while maximising privacy.
- The concept of **data controllers needs to be redefined** in light of the technical characteristics of public blockchains and the difficulty of applying it to on-chain data.
- The EU should continue to promote **technology neutrality**, meaning that no particular technology should be favoured over another. However, tech neutrality **cannot be interpreted to mean** that fundamentally different architectures must be treated as if they are the same.
- There needs to be **more strategic alignment** with the EU's overarching digital agenda. The EU **cannot strive for competitiveness and to be a leader in digital innovation** if its regulatory actions end up stifling innovation into digital technologies and pushing it outside of the EU.

**BC4EU remains committed to constructive dialogue with the EDPB** and stands ready to collaborate on further refining a GDPR framework that protects individuals while enabling innovation in decentralised technologies.

**Blockchain for Europe**
secretariat@blockchain4europe.eu
tommaso@blockchain4europe.eu