SUBJECT: Recommendations to the European Data Protection Board on Blockchain and the Processing of Personal Data

European Data Protection Board
Rue Wiertz 60, 1047 Bruxelles, Belgium
7 June 2025

Dear Members of the European Data Protection Board,

We write in response to the public consultation on the European Data Protection Board's (EDPB) Guidelines 02/2025 on processing of personal data through blockchain technologies. We commend the Board's proactive efforts to clarify how blockchain-based applications can comply with the General Gata protection Regulation's (GDPR) requirements. The draft Guidelines thoughtfully acknowledge the unique challenges posed by blockchain's features – for example, how immutability can conflict with the right to erasure and rectification, and how decentralization complicates compliance with principles like data minimization and storage limitation. The emphasis on Data Protection by Design and by Default and the recommendation to conduct a Data Protection Impact Assessment (DPIA) for any blockchain use of personal data are especially welcome. We fully agree that careful up-front assessment is needed before choosing blockchain over alternative, less risky technologies.

While the Guidelines provide a strong foundation, we have identified several gaps and areas where further guidance or clarification would greatly assist organizations. In this correspondence, we outline key issues in the current guidance and offer additional recommendations to enhance the safe and lawful processing of personal data on blockchain systems. Our goal is to support the EDPB in finalizing a robust framework that protects individual rights without unduly hindering beneficial blockchain innovation.

Key Gaps and Challenges in the Current Guidance

Decentralized Governance and Controller Accountability:

The Guidelines acknowledge that blockchain's decentralized nature involves numerous actors, but stress that this is "not a reason not to comply with the GDPR". A factual, case-by-case assessment of roles is advised, referring to existing EDPB guidance on controller/processor concepts. However, in practice there remains uncertainty over how to attribute the role of data controller in permissionless public networks where no single entity controls the ledger. The EDPB notes that nodes in a public blockchain may be considered controllers and encourages the formation of a legal entity (e.g. a consortium) when participants jointly determine purposes.

This approach works for private or consortium blockchains, but in truly open networks (like public cryptocurrencies) it is unclear how to implement such governance. The lack of a central authority or formal agreement among global participants makes it difficult to assign GDPR responsibility – potentially leaving every node operator at risk of being deemed a controller. Stakeholders have voiced concern that, without further clarity, running a blockchain node in the European Union (EU) could become legally risky. We urge the Board to provide more concrete examples or criteria for determining responsibility in common blockchain scenarios (for instance, distinguishing roles of application developers, miners/validators, and end-users). Clearer guidance on joint controllership arrangements in decentralized networks would help resolve ambiguity and ensure accountability without discouraging participation.

Immutability vs. Data Erasure and Rectification Rights:

It is widely recognized that blockchain's immutability – one of its core features – conflicts with GDPR rights that require data to be modified or deleted upon request. The Guidelines highlight this tension and rightly insist that the right to erasure ("right to be forgotten") and right to rectification must be respected "by design" in any blockchain system. In practice, however, the guidance leans on solutions that may be technically challenging or infeasible in decentralized ledgers.

Paragraph 63 of the draft suggests that if selective deletion of personal data on-chain is impossible, "this may require deleting the whole blockchain" to honor an erasure request. Such an extreme measure is practically unenforceable on a distributed network – as noted by commentators, "asking to delete the entire blockchain… is like asking to delete the internet to enforce privacy". The Guidelines themselves acknowledge the difficulty of achieving true deletion in blockchain and recommend considering alternative technologies if the application does not genuinely require the strong integrity of an immutable ledger.

In essence, the current guidance warns not to put personal data on an immutable chain unless one can somehow reverse or anonymize it later – but it stops short of describing a practical method for doing so on public chains. This gap leaves controllers unsure how to handle erasure and rectification requests in scenarios where data has been recorded across many nodes. Without additional guidance, organizations may face a compliance deadlock: forced to choose between violating GDPR by leaving personal data indelible, or violating the fundamental design of blockchain by attempting to alter history. More nuanced solutions are needed to reconcile these conflicts.

Data Minimization and On-Chain Personal Data:

SUBJECT: Recommendations to the European Data Protection Board on Blockchain and the Processing of Personal Data

The draft Guidelines correctly underscore that storing personal data directly on-chain should be avoided whenever it conflicts with data protection principles. In fact, the EDPB advises against recording personal data even in protected forms like encryption or hashing on the blockchain, stating that it is "not advisable to register personal data in cleartext, encrypted or hashed data on a blockchain" and that such data instead should be stored off-chain. We agree with this privacy first approach. However, some ambiguity remains around what constitutes personal data in a blockchain context, and how far organizations must go in stripping data from blocks. Even when no obvious identifiers are written to the ledger, metadata and pseudonymous identifiers (user addresses, transaction references, etc.) can qualify as personal data if they relate to an identifiable individual.

Completely avoiding any personal data on-chain may not always be practical; for example, certain decentralized applications might inherently involve user public keys or transactional details that link to individuals. The Guidelines do mention techniques to limit identifiability, including strong encryption, hashing, and cryptographic commitments. These measures can reduce risk, but as noted, they generally do not render the data fully anonymous – encrypted or hashed data on chain is still considered personal data under the GDPR if someone (with the key or through brute-force means) can re-identify it.

They also suggest that any personal data stored on-chain must be configured such that it can be "effectively rendered anonymous" when needed, which presupposes that off-chain data (like decryption keys or original datasets) can be erased to break any link. The gap here is a lack of clarity on what level of anonymization is sufficient and how to assess that in practice. For instance, if personal data is hashed with a secret salt key and that key is destroyed, is the remaining on-chain hash considered anonymous? The current Guidance hints at this solution, but could be more explicit.

Organizations would benefit from a clearer standard on when data is considered irreversibly anonymized in a blockchain setting – e.g. guidance on using keyed-hash pseudonymization or encryption plus key destruction to comply with erasure. Additionally, controllers may need more concrete advice on minimizing metadata: for example, using one-time addresses or aggregating transactions to prevent linkability. In summary, while "store off-chain or anonymize" is a sound principle, more detail is needed to implement data minimization effectively without undermining the utility of the blockchain.

<u>Legal Basis and Consent Challenges:</u>

Determining an appropriate legal basis (Art. 6 GDPR) for blockchain data processing is another area where the Guidelines could offer more direction. The draft notes that the

legal basis must be identified for each processing purpose and context, and it mentions consent (Art. 6(1)(a)) and legitimate interests (Art. 6(1)(f)) as potential options in a blockchain scenario. It also warns of the pitfalls of consent: consent must be freely given and withdrawable without detriment, which is incompatible with an immutable ledger unless technical means exist to honor withdrawal.

We agree with the EDPB's caution that consent should not be used if the data cannot be deleted or altered later – otherwise, data subjects would be giving consent that, in practice, they can never revoke. This effectively narrows the viable bases for many blockchain use-cases. The Guidelines do not explicitly discuss other bases like contract necessity, legal obligation, or public interest in detail, though these could apply in certain blockchain applications (for example, a smart contract for a service might rely on "performance of a contract" under Art. 6(1)(b), or a public register on blockchain might claim a legal obligation basis). A potential gap is guidance on how those bases intersect with blockchain's constraints. For instance, using legitimate interests as a basis requires a balancing test and honoring the right to object – but if a data subject objects to processing on a public blockchain, how can a controller truly cease processing their data, given existing records remain on-chain?

The EDPB indicates that rights to object and erasure must be built in by design, implying that if such rights cannot be facilitated, the legitimate interest basis may not be appropriate either. We believe the final guidance should explicitly underscore that not all legal bases are feasible for blockchain processing of personal data, and it should encourage bases that align with the technology's features. For example, if a blockchain is used in the fulfillment of a contract with the data subject (Art. 6(1)(b)), the design should ensure the data recorded is only what is necessary and that data subjects are fully informed of the permanence of that record.

If legal obligation or public task (Art. 6(1)(c) or (e)) is relied upon (as might be the case for blockchain in government services), the Guidelines should stress the need for the law mandating blockchain to also mandate appropriate safeguards (indeed, Recommendation 6 touches on the need for legal provisions regarding acceptable levels of public exposure when blockchain use is compelled by law). In short, additional clarity on choosing and implementing the legal basis would be helpful – especially cautioning against using consent or legitimate interests unless the system is engineered to allow effective exercise of rights like withdrawal or objection.

SUBJECT: Recommendations to the European Data Protection Board on Blockchain and the Processing of Personal Data

International Data Transfers in Global Networks:

By design, public blockchains operate globally, with nodes distributed across many countries. This raises the question of GDPR's Chapter V (international transfer) compliance whenever personal data on the ledger is accessible to or stored by nodes outside the European Economic Area. The Guidelines note this concern and recommend that organizations consider measures such as Standard Contractual Clauses (SCCs) for node operators or other transfer mechanisms to ensure compliance if data flows to third countries. However, this advice may be difficult to operationalize. In a permissionless blockchain, a European data controller has no contractual relationship with the multitude of independent node operators around the world who might process the data. It is not realistic for, say, an EU-based participant to have SCCs in place with every overseas miner or node that maintains a copy of the ledger.

The draft's overarching advice to "avoid public blockchains unless truly necessary" is one way to mitigate this risk – implying that if one sticks to private or permissioned networks with known participants, transfers can be controlled via agreement. Even so, additional guidance could be valuable on how to approach transborder data flow in blockchain. For example, if an EU controller does use a public blockchain, should they presume a transfer has occurred the moment data is written (since any foreign node might receive it), and thus should they limit usage to blockchains that have a significant number of nodes in jurisdictions with adequate protection? This is a complex issue that the Guidelines only begin to address.

We encourage the EDPB to elaborate on this in the final text. Possible considerations include the use of community codes of conduct among blockchain participants to commit to GDPR-level protection, technical measures to localize certain data, or even future legal arrangements for distributed processing. As it stands, the guidance might leave controllers wary that using global blockchain infrastructure is per se non-compliant. Greater clarity or creative solutions here would be welcome, so that data controllers know how to meet transfer requirements or at least assess the risks if they engage with a global network.

Emerging Privacy-Enhancing Technologies and Compliance Tools:

The draft Guidelines mention advanced techniques like encryption, hashing, and "zero-knowledge" methods (presumably zero-knowledge proofs) as means to protect personal data on blockchain. This recognition is important, because modern privacy-enhancing technologies (PETs) can allow useful computations or verifications on-chain

without revealing personal information. However, the guidance does not extensively discuss newer developments such as zero-knowledge proof-based (ZKP) systems, fully homomorphic encryption (FHE), secure multiparty computation (MPC), or other cryptographic protocols that are increasingly relevant in blockchain projects.

A gap exists in illustrating how these technologies might be used to reconcile blockchain operations with data protection requirements. For example, zero-knowledge proofs could enable a blockchain to verify that a condition is met (e.g. that a user is over 18) without ever exposing the user's age or identity on-chain. Such approaches directly support the principle of data minimization by "keeping personal data off the chain" while still using the ledger for verification. The EDPB's final guidance could expand on or encourage the exploration of these PETs in the blockchain context. This not only helps compliance, but also pushes the blockchain industry towards more privacy-preserving architectures, which the Board itself suggests are the future: the Guidelines explicitly "push the technology toward privacy-preserving architectures, and away from entirely see-through blockchains".

We agree strongly with this direction. Indeed, as an observation, many blockchains today were not built with privacy in mind, and tools that were once viewed as supporting anonymity have now become essential for compliance. The guidance could do more to reinforce this positive trend by highlighting successful implementations or promising research that embeds privacy-by-design into distributed ledgers. In particular, clarifying that using such PETs (when properly implemented) is encouraged and can be compatible with GDPR would give developers and organizations confidence to adopt them.

<u>Consistency with Other Regulatory Domains:</u>

One final challenge we wish to highlight is the potential conflict between privacy-preserving measures and other regulatory demands, which is touched on only briefly in the current guidance. As the EDPB encourages stronger data protection controls in blockchain (such as robust encryption and anonymity), it must be acknowledged that other regulators (for instance, in the financial crime or law enforcement domains) sometimes push in the opposite direction, seeking more traceability and less anonymity. A notable example is the tension with anti-money-laundering (AML) regulations: technologies like coin mixers or privacy-enhancing cryptocurrency wallets have attracted regulatory scrutiny and even enforcement actions, despite their privacy benefits.

The Guidelines do recognize that governance and trust mechanisms are important (Recommendation 5 calls for mechanisms assuring trust, such as certification of nodes or

software), but they do not directly address how to balance privacy against legitimate needs for transparency in certain use-cases. We believe this is a gap that might be beyond the remit of data protection guidance alone, yet it is crucial for the EDPB to consider in its final recommendations.

The French National Commission on Informatics and Liberty (CNIL) noted in 2018 that blockchain compliance "necessarily calls for a response at the European level" and indicated it would work with other national regulators (like financial market authorities) to develop a coordinated approach. We encourage the EDPB to continue in this cooperative spirit. Ensuring that privacy guidance for blockchain does not inadvertently clash with financial compliance requirements (and vice versa) will require dialogue between data protection authorities and other regulatory bodies. This is not so much a shortcoming of the Guidelines as it is a broader governance challenge: how to reconcile privacy with other public interests in the context of immutable, decentralized ledgers. We flag it here so that any additional recommendations or future frameworks can take a holistic view of blockchain regulation across domains.

Considering the above gaps and challenges, we respectfully offer the following additional recommendations for the EDPB to consider. These suggestions aim to enhance the guidance and provide more practical support to organizations that seek to leverage blockchain technology in a privacy-compliant manner.

Additional Recommendations to Enhance Blockchain Data Processing Compliance

Provide Clearer Guidance on Distributed Roles and Liability:

To resolve uncertainty around accountability, the EDPB should include more concrete guidance or examples mapping GDPR roles to typical blockchain actors. This could involve illustrative use-cases (e.g. a public cryptocurrency, a consortium chain for supply chain tracking, a private blockchain for record-keeping) and an analysis of who is the controller, joint controller, or processor in each. Establishing a clear accountability framework will help organizations assign responsibilities in advance. For instance, if multiple entities jointly launch a blockchain platform, the guidance could suggest establishing a formal consortium agreement defining each member's GDPR duties.

In permissionless networks, the EDPB might recommend that major participants (such as core developers or organizations running significant nodes) consider forming an association or legal entity to act as a point of contact for data subjects and supervisory authorities. Even if not every node can be part of such an entity, having an identifiable governing body could prevent a situation where "everyone and no-one" is responsible. We

also suggest the Board leverage its "Guidelines 07/2020 on the concepts of controller/processor" to clarify joint controllership in decentralized environments, so that all participants understand their shared obligations. By removing doubt about roles, these measures encourage proactive compliance rather than a wait-and-see approach. This recommendation aligns with policy experts' calls for more certainty and transparency in how data protection law applies to blockchain.

Emphasize "Privacy by Design" Technical Solutions for Immutability Issues:

The final guidance should strongly endorse specific technical measures that enable functional compliance with erasure and rectification requests without literally deleting blockchain data (since direct deletion is often impossible). One such measure is the use of encryption with managed keys: personal data can be encrypted before being recorded on-chain, and if a data subject invokes the right to erasure, the encryption key for that data is securely destroyed. This renders the on-chain data unreadable (effectively anonymized), achieving the goal of erasure in practice. The French CNIL has noted that while such solutions are not identical to classical deletion, they "enable stakeholders to come closer to the GDPR's compliance requirements" by blocking access to data (through techniques like keyed hashing, commitments, or encryption).

We recommend the EDPB explicitly validate this approach as an acceptable means of compliance, provided that the keys are managed with strict controls. Likewise, where rectification is needed, the guidance could suggest adding a new corrected entry and then cryptographically revoking the trust in the inaccurate data (for example, by tagging the old record as superseded or by consensus agreement to ignore it in queries). Another design strategy is the use of off-chain storage with on-chain references: rather than store personal data on the ledger, store it in a secure off-chain database and put only a reference (e.g., a hash or pointer) on-chain. If an erasure is required, the off-chain data can be deleted and the on-chain reference becomes meaningless.

The Board already advises avoiding on-chain storage of cleartext, hashed, or encrypted personal data; we suggest expanding on how to implement off-chain storage in combination with blockchain so that integrity of the system is maintained. Finally, the EDPB could mention emerging approaches like the use of selective redaction forks in private blockchains: for example, the Spanish Data Protection Agency (DPA), Agencia Espanola de Proteccion de Datos (AEPD), recently demonstrated a proof-of-concept for "securely erasing data on a blockchain" via controlled modifications (hard forks) on a private Ethereum network. While such solutions (essentially editing the chain's history by

consensus) are not viable for public chains, they show that with governance frameworks in place, even immutability can be bent to fulfill legal requirements.

The EDPB guidance can draw inspiration from these innovations, encouraging organizations to build erasability features into permissioned ledger designs. By emphasizing and approving these privacy-by-design techniques, the Board will give practitioners a toolbox for tackling the thorny issue of data permanence.

Strengthen Data Minimization and Anonymization Standards:

We recommend that the Board elaborate on what constitutes sufficient anonymization in a blockchain context. Since the Guidelines already warn that even encrypted or hashed data on-chain remains personal data if it can be linked, it would help to specify when data is deemed anonymous. For example, the guidance might clarify that personal data should be processed on-chain only in a pseudonymized form that cannot be attributed to an individual without additional information, and that this additional information must be rigorously safeguarded off-chain (or disposed of when not needed) to prevent re-identification.

The Board could cite techniques such as salting hashes with secret keys, using one-way commitments, or aggregation of data, and indicate that once the link (key or reference) is destroyed, the remaining on-chain data would no longer be considered personal data. Providing a clear test or examples for “effectively rendered anonymous” data would remove ambiguity. We also propose encouraging the practice of pseudonym rotation – generating new addresses or identifiers for users for different transactions or contexts, to limit the build-up of an identifiable profile on the public ledger. Many privacy-minded blockchain projects already do this (for instance, some wallets generate a new address for each transaction to reduce linkability). By recommending such practices, the EDPB would promote compliance with the GDPR’s data minimization and purpose limitation principles.

In essence, organizations should collect, use, and expose the absolute minimum personal data necessary for the blockchain’s function. The guidance can include a recommendation that any data which is not required to be on-chain (for the distributed consensus or verification purposes) should reside off-chain under the controller’s direct control. Only derived data or irreversible tokens (like a hash that cannot be decoded without a key) should be on the blockchain, if possible. These clarifications would reinforce the message that transparency of the ledger must not come at the expense of privacy – a balance that can be achieved by thoughtful anonymization and minimization strategies.

SUBJECT: Recommendations to the European Data Protection Board on Blockchain and the Processing of Personal Data

Clarify the Use of Appropriate Legal Bases and Consent Mechanisms:

We advise the Board to expand guidance on selecting a legal basis for blockchain processing, to help controllers steer away from problematic choices. In particular, the final document should clearly discourage reliance on data subject consent unless the system is designed to allow effective withdrawal (which, as noted, is rarely the case in an immutable ledger). Instead, where personal data is processed on a blockchain, other bases might be more suitable. For example, if a blockchain is used in the context of a contractual service with the individual (such as decentralized identity management or a blockchain-based payment service), contractual necessity could be the basis – but the controller then must ensure the data recorded is indeed necessary and that the individual is aware of and agrees to the immutable nature of the record.

If legitimate interest is chosen, the guidance should stress that controllers must conduct a particularly stringent balancing test given the data subject's lack of control post-publication, and that measures to enable the right to object (such as those anonymity techniques noted above) should be in place. Moreover, the Board may want to mention that if special category data (Art. 9 GDPR) is ever involved – which ideally should be avoided on blockchain altogether – then an explicit Art. 9(2) condition (such as explicit consent or substantial public interest under law) must be satisfied, adding another layer of complication. We also suggest including a reminder that where children's data might be processed on blockchain (e.g., in an educational credentialing system), extra care must be taken with consent and rights, as minors have enhanced protections under GDPR.

Overall, by giving more nuanced advice on legal bases, the EDPB will help controllers choose a path that aligns with both GDPR and the realities of the technology. For instance, the guidance can highlight that if a blockchain cannot accommodate data deletion, then basing processing on consent or on an interest that permits objections is essentially inviting non-compliance. In those cases, controllers should either redesign the system or use a legal basis (like legal obligation or contract) where the GDPR rights are more restricted – and even then, they must still honor principles of fairness and data minimization. In summary, additional text on legal bases would ensure organizations do not inadvertently choose an approach (like naive use of consent) that would put them at odds with data protection rights.

Address International Transfer Solutions for Blockchain Data:

We urge the EDPB to integrate more guidance on handling the international dimension of blockchain networks. The Board should clarify that writing personal data to a

globally accessible blockchain constitutes a disclosure to potentially worldwide recipients, and thus controllers must consider GDPR's transfer regime. In the final guidelines, it would be helpful to recommend practical steps, such as restricting node locations when deploying private or consortium blockchains (e.g., confining node hosting to the EEA or countries with adequate protection, where feasible). For public blockchains, one possible recommendation is to encrypt personal data with keys held in the EEA, so that even if ledger data is stored on foreign nodes, those nodes do not possess personal data in intelligible form – in effect, only an EU entity holds the means to decrypt and "use" the personal information, thereby localizing the real data processing.

This approach could be coupled with legal measures: for example, if an EU company utilizes a public blockchain, they might include contractual clauses or user agreements stating that any participating node processing the data must abide by GDPR standards (admittedly non-trivial to enforce, but it sets expectations). Another suggestion is leveraging the GDPR's provisions for approved codes of conduct or certification (Art. 40-42) as transfer tools: the Board could invite industry consortia to develop a blockchain code of conduct that, among other things, binds participants globally to EU data protection principles. If such a code were approved, adhering nodes or services could be deemed to provide appropriate safeguards. Similarly, the creation of a GDPR-compliant blockchain certification could allow EU data controllers to choose platforms or service providers that meet recognized standards for data protection, including how they handle cross-border data distribution.

We believe the EDPB is able to encourage these innovative solutions. By acknowledging the transfer problem and suggesting mechanisms (technical and organizational) to cope with it, the Board will give more confidence to those who wish to use blockchain in a globally interconnected manner without breaching EU transfer rules. This could be as simple as a paragraph noting that "if personal data will be replicated globally, controllers should either ensure an Art. 46 transfer instrument is in place or, preferably, design the system such that data is encrypted and only processed (decrypted) within a jurisdiction offering adequate protection.". Such guidance aligns with the underlying goal: protecting individuals' data when it leaves the EU, even in the novel context of decentralized networks.

<u>Promote the Use of Privacy-Enhancing Technologies (PETs):</u>

Building on the Guidelines' references to encryption and hashing, the EDPB should explicitly promote emerging privacy technologies as part of the compliance toolkit. For example, zero-knowledge proofs (ZKPs) allow verification of facts (like credentials or

transaction validity) without revealing underlying personal data. Integrating ZKPs can significantly reduce the need to put any personal information on-chain, supporting data minimization and confidentiality. We recommend the guidance encourage developers to explore ZKP-based protocols, selective disclosure techniques (often used in decentralized identity frameworks), and anonymous credential systems. The Board could cite existing frameworks (such as using Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARK) in Ethereum-based applications, or the Hyperledger Indy approach for identity) as illustrations of privacy by design.

Additionally, techniques for unlinkability – like mixing services or ring signatures – could be mentioned as ways to prevent personal data trails on a blockchain from becoming too transparent. Of course, these techniques must be deployed lawfully and with caution (to avoid abuse), but from a pure privacy perspective, they can be very effective. The EDPB's endorsement of privacy-preserving techniques would signal to the industry that investing in these technologies is not only positive for users but expected for compliance. Notably, the recent commentary on the Guidelines has observed that the EDPB is essentially calling for privacy features to be "baked in" to blockchain as a design mandate.

This marks an opportunity: if regulators acknowledge and encourage privacy tech, it legitimizes those tools. We therefore suggest that the final document lists a few PETs and state that their use is encouraged where appropriate, as they can help achieve GDPR objectives (like minimization, security, and data subject control) in distributed environments. This could also tie into certification – e.g., a blockchain solution that demonstrably uses strong PETs might qualify for a privacy seal in the future.

<u>Encourage Ongoing DPIAs and Governance Oversight:</u>

The Guidelines highlight the importance of conducting a DPIA before implementing blockchain processing. We propose adding that DPIAs for blockchain projects should be treated as living documents. Blockchains and the applications built on them are not static; they evolve (through software updates, new node operators joining, changes in consensus mechanisms, etc.). The EDPB could recommend periodic reviews and updates to the DPIA and privacy risk assessments as the system grows and changes. For example, if a permissioned blockchain later connects with another network or if new data types begin to be stored on-chain, the initial DPIA should be revisited. Moreover, governance procedures should be in place to manage changes in the network with privacy in mind – the Guidelines' Recommendation 8 and 14 hint at having governance rules and documenting protocol evolution.

We support this and suggest making it an explicit recommendation that any consortium or entity running a blockchain maintain a privacy governance policy. This policy would outline how software upgrades are evaluated for privacy impact, how compliance will be monitored continuously, and who is responsible for ensuring that the network's operation remains within legal bounds. Including this point reinforces accountability over time, not just at launch. It would prevent situations where a blockchain might start in a compliant manner but drift into non-compliance as features change or new participants enter. Essentially, this is an extension of the "by design and by default" principle – not only should blockchain systems be designed for privacy from the outset, but they must also be continually managed and audited to sustain compliance throughout their lifecycle.

Foster Cross-Regulatory Dialogue and Coherence:

As noted earlier, blockchain sits at the intersection of multiple regulatory domains – data protection, financial regulation, cybersecurity, to name a few. We recommend that the EDPB, perhaps in the explanatory memorandum or accompanying materials, acknowledge the need for a harmonized approach and indicate its willingness to cooperate with other authorities. This could involve sharing the final Guidelines with financial regulators, anti-fraud agencies, and others, and jointly developing FAQs or guidance for cases where regulations intersect. A concrete suggestion is to form a joint task force or working group with relevant bodies (for example, including representatives from the European Banking Authority (EBA), European Securities and Markets Authority (ESMA), or law enforcement cyber units) to discuss how privacy-by-design can coexist with legitimate monitoring needs.

The CNIL's action plan to liaise with financial regulators for blockchain oversight is a good model. By embedding this recommendation, the EDPB would reassure stakeholders that adopting privacy measures (like encryption or anonymity) on blockchains will not be viewed negatively by other regulators if done responsibly. Over time, this collaborative stance could lead to integrated standards – where a blockchain platform can be designed to satisfy data protection requirements, and provide auditability or traceability features for financial compliance, without one undermining the other. Our suggestion is simply that the EDPB explicitly encourage such multi-stakeholder engagement. This will pave the way for balanced solutions, such as privacy-preserving analytics or permissioned access for regulators under strict conditions.

Ultimately, the goal is to avoid a scenario in which adhering to EDPB privacy guidance inadvertently causes conflict with other legal obligations. A unified framework

that satisfies different regulatory aims will enable blockchain innovation to flourish under the rule of law.

Consider Long-Term Legal Developments:

Finally, we ask the EDPB to remain forward-looking in this area. The Guidelines are a major step in clarifying existing law, but there is recognition even among regulators and experts that some issues may require new legal interpretations or reforms in the future. It has been suggested that upcoming evaluations of the GDPR or other digital legislation might explicitly address technologies like blockchain. We encourage the Board to use the insights gained from this public consultation to inform any such future policy debates. For example, if certain GDPR provisions prove almost impossible to reconcile with decentralized architecture without hampering functionality, the EDPB could communicate these findings to EU lawmakers as part of the GDPR review process.

This is beyond the scope of changes to the Guidelines themselves, but it is an important consideration. In this vein, the Board might include a concluding note in the guidance recognizing that blockchain technology continues to evolve, and that the EDPB remains committed to refining its guidance or supporting adaptations in the legal framework if needed to achieve the correct balance of innovation and fundamental rights protection. By doing so, the Board signals flexibility and openness to futureproofing data protection in the face of technological change. That assurance will be greatly appreciated by industry and global civil society alike.

Conclusion

We appreciate the opportunity to provide feedback on the EDPB's draft guidance. Blockchain technology holds great promise for innovation, but it also tests the robustness of our data protection regime. The EDPB's Guidelines 02/2025 are a vital instrument in navigating this complex intersection and ensuring that fundamental privacy rights are upheld even as databases become decentralized and tamper-proof. Our comments above are offered in a constructive spirit, aiming to fill certain gaps and suggest additional measures that can strengthen the final Guidelines.

We believe that more detailed clarification of roles, pragmatic solutions for data subject rights (such as emphasizing encryption/key destruction as a means of compliance), and encouragement of privacy-enhancing technologies will greatly assist organizations in designing compliant blockchain systems. Likewise, fostering standardized best practices (through codes of conduct, certifications, or other frameworks) and

coordinating across regulatory domains can mitigate conflicts and provide a clearer path forward for blockchain deployments in Europe (and eventually for all of humanity).

We trust that the EDPB will find these suggestions useful as it refines the Guidelines. The draft already sends a clear message that privacy must be a cornerstone of any blockchain application handling personal data, and we fully support that stance. By addressing the remaining ambiguities and embracing the recommendations above, the EDPB can ensure its guidance is not only theoretically sound but also practical and future ready. We remain at your disposal for any further information or clarification. Thank you for your leadership in this area and for considering our input. Protecting individuals' data rights in emerging technologies is a challenging endeavor, and the Board's work is indispensable to achieving that goal in the Age of AI.

Respectfully,

Matthew H. Kilbane
Athena's Zephyr Consulting LLC.
CEO