Global Blockchain Business Council (GBBC): Response to EDPB Draft "Guidelines 02/2025 on Processing of Personal Data through Blockchain Technologies"

About us:

Global Blockchain Business Council (GBBC) is the trusted non-profit association for the blockchain, digital assets, and emerging technology community. Founded in 2017 in Davos, Switzerland, GBBC comprises more than 500 institutional members and 284 Ambassadors across 124 jurisdictions and disciplines.

GBBC furthers adoption of blockchain and emerging technologies by engaging regulators, business leaders, and global changemakers to harness these transformative tools for more secure and functional societies.

GBBC industry verticals: Financial Services, Global Commerce/Supply Chain, and Commodities, underpinned by AI, digital identity, governance, hardware, infrastructure, policy, regulation, and security.

GBBC initiatives: BITA Standards Council (BITA), Food for Crisis, Global Standards Mapping Initiative (GSMI), International Journal of Blockchain Law (IJBL), InterWork Alliance (IWA), and U.S. Blockchain Coalition (USBC).

Executive summary

The Global Blockchain Business Council (GBBC) welcomes the European Data Protection Board's engagement with distributed-ledger technology and its recognition that applying the GDPR to blockchain poses unique technical challenges. We share the Board's commitment to safeguarding fundamental rights, but believe this objective is best achieved through a *technology-neutral, risk-based* reading of EU data-protection law. Several positions in the draft, notably the discouragement of permissionless blockchains, the near-universal designation of participants as data controllers, and the dismissal of viable privacy-enhancing tools — risk undermining innovation, legal certainty, and the EU's own Digital Finance and Data strategies. We therefore urge the EDPB to recalibrate the guidelines in five key areas, detailed below.

1. Immutability and data-subject rights

The draft states that "technical impossibility cannot be invoked to justify non-compliance." In practice, blockchain actors can already deliver an *equivalent protective outcome* through measures such as:

- **Cryptographic erasure (key destruction or "crypto-shredding").** If the sole decryption key for encrypted payloads anchored on-chain is securely destroyed, the remaining data become permanently unintelligible while the ledger's integrity is preserved.

- **Salted or keyed hashes plus off-chain storage.** Deleting the salt or key severs any link between the on-chain hash and the off-chain data set, satisfying the functional aims of Articles 17 and 18.

- **Perfectly hiding commitments** (i.e., cryptographic commitments that reveal nothing about the underlying value once the witness is deleted) and selective use of burn addresses to help break token traceability in combination with other unlinkability techniques.

Recommendation. Where a controller can demonstrate—through a data-protection impact assessment (DPIA)—that such techniques make re-identification "not reasonably likely", the right to erasure and storage-limitation principle should be deemed fulfilled. A purely categorical rejection would ignore solutions that regulators in several Member States have already accepted for other immutable media (e.g., WORM backups).

2. Allocation of controller and processor roles

The current guidelines suggest that nodes participating in public permissionless blockchains may fall under the definition of controllers or joint controllers under the GDPR. We

respectfully disagree with this interpretation, as it does not accurately reflect the technical role of these nodes. They operate automatically, following predetermined protocols to validate transactions, without exercising discretion or making decisions about the purposes or means of processing. In this regard, their function is more akin to that of Internet routers than data controllers. Classifying them as controllers risks disincentivizing participation and weakening the decentralization that inherently supports privacy and resilience.

We encourage the EDPB to take a more nuanced, case-by-case approach that clearly differentiates between passive infrastructure and entities with meaningful influence over data processing. The guidelines should state that operating a node, in and of itself, does not constitute controllership under the GDPR.

Recommendation. Adopt a *functional role* framework:

- **Governance and protocol developers**—entities that set purposes or alter core logic—are likely controllers.
  Application-layer operators (e.g., dApp front-ends, RPC providers) may be processors or controllers depending on whether they set purposes beyond mere relay.
- **Infrastructure validators and relay nodes** that cannot influence purposes or means should be treated as neutral intermediaries, comparable to internet service providers.

National practice may vary; the guidelines should therefore encourage DPAs to apply this functional analysis consistently rather than impose strict-liability obligations on passive actors.

3. Public-key identifiability

The draft treats any public key as personal data if it *could* be linked to a natural person using means "reasonably likely" to be employed. GBBC agrees with the principle but cautions that "reasonably likely" must account for cost, lawfulness and technical difficulty. In well-designed pseudonymous systems, re-identification may require disproportionate effort or illicit data sources.

Recommendation. State clearly that persistent pseudonyms are **not automatically personal data**. Their status must be determined case by case—ideally within the DPIA—using the objective factors in Recital 26 GDPR.

4. Permissionless versus permissioned blockchains

The current draft of the EDPB's guidelines appears to implicitly favor permissioned blockchain systems, potentially overlooking the societal and technical value of public permissionless architectures. While permissioned blockchains may offer clearer governance structures, permissionless networks enable transparency, censorship resistance, and open participation—features that underpin critical applications such as decentralized finance and

tokenization. Overlooking these systems risks discouraging innovation and the development of privacy-preserving solutions that do not rely on centralized control.

To ensure fairness and legal certainty, we urge the EDPB to adopt a technology-neutral approach. GDPR compliance should be assessed based on the nature and context of data processing activities, not the underlying infrastructure.

Permissionless architectures can also contribute to EU policy goals around transparency, citizen empowerment, and trust in digital services, where public verifiability is essential.

Recommendation. Replace the "permissioned-first" rule with a proportionality test: if the processing purpose *intrinsically requires* public verifiability or open participation, a permissionless architecture is proportionate provided suitable privacy-enhancing technologies and governance measures are in place.

5. International data transfers (Chapter V GDPR)

Global replication means on-chain data will routinely traverse jurisdictions. Requiring standard contractual clauses between thousands of pseudonymous nodes is not feasible, yet treating the entire chain as an international transfer subject to localisation would render many networks inoperable.

Recommendation. Endorse a *layered, location-agnostic* safeguard package:

1. Strong pseudonymisation of on-chain data (e.g., hashed anchors, zero-knowledge proofs);

2. Storage of any identifying off-chain data within the EEA under strict access controls;

3. Contractual and organisational commitments by governance bodies and primary user-facing entities;

4. Transfer-impact assessments updated as threat environments evolve.

Where only robustly pseudonymised data remain on-chain, the residual risk approximates that of anonymised data, materially lowering localisation concerns.

6. Practical compliance playbook

GBBC proposes adding a non-binding annex that controllers can reference, including:

- A decision tree for selecting public versus permissioned architectures;
- A DPIA checklist covering data flows, privacy-enhancing technologies (PETs), data-minimisation metrics and key-rotation processes for exercising rights; Examples of good-practice controls such as zero-knowledge proofs for selective

disclosure, threshold signatures, stealth addresses and on-chain consent-revocation registries.

This concrete guidance would translate the guidelines' high-level principles into implementable steps.

7. Policy coherence

- **MiCA, PSD3 and DORA** already impose custody segregation, transaction monitoring and security obligations that dovetail with cryptographic erasure and layered safeguards.
- **The Data Act and upcoming Open Finance framework** promote cross-border interoperability—best served by proportionate treatment of permissionless ledgers.
- **eIDAS 2 Self-Sovereign Identity pilots** rely on public anchors; mandating permissioned-only solutions would fragment the trust layer.
  Innovation Principle (Commission Communication COM(2016) 733) requires that regulatory measures support innovation where possible; guidance that discounts viable PETs or strong public-chain use-cases would conflict with this principle.

8. Recommendations to the EDPB

GBBC respectfully recommends that the EDPB:

1. **Formally recognise cryptographic erasure and unlinkability** as GDPR-compliant when re-identification is demonstrably not reasonably likely.
2. **Adopt a functional controller test** that exempts passive validators lacking effective influence.
3. **Apply a proportionality standard** allowing permissionless blockchains where their unique properties are essential to the processing purpose.
4. **Provide layered Chapter V solutions** combining pseudonymisation, off-chain EEA storage and targeted contractual safeguards in lieu of blanket localisation.
5. **Convene a technical workshop** with industry and academic experts before finalising the guidelines to validate practical feasibility.
6. **Clarify that node operation alone** does not imply controllership under the GDPR, and distinguish between passive technical roles and entities with actual influence over data processing
7. **Ensure technological neutrality** by avoiding architectural bias, allowing both permissioned and permissionless blockchains to meet compliance through appropriate, risk-based safeguards.
8. **Recognize off-chain storage and cryptographic anchoring** as effective safeguards for GDPR compliance in decentralized systems, enabling data minimization without compromising transparency or immutability.

We remain at the Board's disposal and stand ready to contribute empirical evidence and technical expertise.