Global Blockchain Business Council (GBBC): Response to the UK Information Commissioner's Office (ICO) Consultation on the Draft Guidance on Distributed Ledger Technologies and Data Protection under the UK GDPR

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The Global Blockchain Business Council (GBBC) welcomes the ICO's Draft Guidance on *How Data Protection Law Applies to Distributed-Ledger Technologies*.

The document represents a meaningful advancement in aligning data-protection law with technological realism, distinguishing itself from the EDPB's more doctrinal approach by adopting a pragmatic, risk-based methodology suited to the UK's innovation-friendly regulatory culture.

GBBC particularly supports the ICO's treatment of the household exemption and its emphasis on proportional application of the UK GDPR.

However, several substantive issues warrant further refinement before finalisation:

- The discussion of controller and processor roles should be expanded to address miners, validators, wallets, and oracles, drawing on comparative legal scholarship.
- The guidance should analyse more deeply the rectification and erasure dilemma, including both the utility and limitations of the *hashing-out* technique. While hashing enables compliance with deletion requests, it also risks re-centralising control in off-chain databases — a tension that the ICO should explicitly acknowledge.
- Cross-border data-transfer mechanics remain under-defined; a pragmatic interpretation is required to ensure that blockchain's inherent replication model does not render compliance impossible.
- The ICO's draft guidance rightly places emphasis on achieving data-protection compliance through system design — ensuring that privacy safeguards are embedded in technical architecture rather than retrofitted. GBBC strongly supports this principle but notes that such an approach also raises practical questions around operational evidence of "data beyond use" and how firms can demonstrate compliance without over-centralising data custody. It is also notable that, in decentralised environments, not all participants have equivalent technical or governance control over how compliance is achieved. This asymmetry underscores the importance of proportional, role-based expectations and of regulatory guidance that distinguishes between actors with direct control and those who operate under network rules or protocols.
- Finally, the ICO should consider complementing the guidance with illustrative decision trees and case studies to help organisations demonstrate compliance in practice. These should remain non-prescriptive and illustrative in nature, ensuring that the guidance continues to allow flexibility in how roles and risk assessments are applied — particularly for permissionless networks.

Taken together, these refinements would transform a strong conceptual framework into a fully operational one, reinforcing the UK's position as a jurisdiction that combines regulatory credibility with technological foresight.

Q10. Do you think the guidance presents additional: cost(s), benefit(s), both, neither, or are you unsure?

GBBC considers that the ICO's draft guidance introduces both benefits and costs, though the overall balance is strongly positive. The primary benefit is conceptual clarity: it situates blockchain within the existing UK data-protection framework without seeking to re-invent core principles. By translating complex technological realities into familiar legal concepts — data controllership, data minimisation, and data-protection-by-design — the ICO provides a baseline for consistent regulatory interpretation.

The compliance implications for organisations are likely to vary significantly depending on their role, the type of DLT used, and their existing interpretation of data-protection obligations. In practice, this may involve retraining compliance teams, refreshing Data Protection Impact Assessments (DPIAs), re-documenting data-flow governance to reflect the ICO's taxonomy of actors, or adjusting systems to externalise personal data off-chain.

GBBC recognises that many of these steps are not new obligations, but rather a clarification of existing requirements as applied to DLT. While the guidance inevitably remains conceptual in parts — reflecting both the evolving nature of technology and the need for case-by-case nuance — GBBC considers that it would nonetheless benefit from a few illustrative case studies showing how the principles could be applied in practice across different sectors, to help achieve more consistent interpretation.

GBBC recommends annexes focused on specific operational archetypes — such as regulated custodial networks, permissioned finance platforms anchoring data to public ledgers, and DAO-governed protocols — to translate principles into repeatable compliance models.

Q11. What, in your view, are the benefits of using our guidance on DLTs?

The guidance offers clear benefits by anchoring the application of the UK GDPR to a fast-moving technological field. Unlike the European Data Protection Board's (EDPB) Draft Guidelines 02/2025, which remain largely doctrinal, the ICO's approach is pragmatic and context-specific, addressing the realities of hybrid, permissioned, and public networks.

Its treatment of the *household exemption* is especially commendable: by distinguishing genuinely private or domestic blockchain use from commercial or professional activity, the ICO provides a sensible boundary that prevents over-application of the UK GDPR. This reflects a risk-based, proportionate stance appropriate for a technology whose use cases range from consumer wallets to institutional finance.

More broadly, the guidance promotes internal coherence between technical architecture and legal design, offering a shared reference point for regulators, developers, and custodians. It creates a lingua franca for the market — essential for maturing compliance discourse.

Q12. What, in your view, are the costs of using our guidance on DLTs?

Implementation costs are primarily governance-related rather than infrastructural. Large financial-market infrastructures and custodians already operate under stringent accountability regimes, but smaller developers and open-source contributors may find the compliance expectations demanding. The guidance presumes organisational capacity to conduct DPIAs, manage joint-controllership arrangements, and maintain auditable records — capacities that many decentralised projects lack.

The ICO could mitigate this asymmetry by embedding proportionality more explicitly: for example, clarifying when a participant acting under a protocol's technical rules but without discretion is unlikely to be a controller. Without such nuance, there is a risk that over-formalised compliance disincentivises open innovation while failing to improve actual data-protection outcomes.

Q13. Please provide an estimate of the costs and benefits and briefly how you calculated them.

For most GBBC members, the expected costs lie primarily in internal resource allocation rather than capital investment.

It is difficult to quantify with precision how much additional time or cost may arise from technical development work, such as adapting legacy code to externalise personal data off-chain. The resources required for such activities will vary widely depending on each organisation's existing data-governance framework, IT architecture, and available technical capacity.

Similarly, some firms may need to review or put in place governance mechanisms and contractual arrangements between certain blockchain participants, where such relationships are feasible. These factors could raise the overall resource requirement, though their impact will differ across business models.

While GBBC notes that these compliance activities may be significant, it also recognises that, from the ICO's perspective, they largely reflect existing obligations now applied more explicitly to DLT, rather than entirely new regulatory burdens. Over time, greater clarity and consistency *may help to yield* offsetting benefits in the form of reduced external advisory costs and more predictable supervisory dialogue — provided that subsequent guidance remains stable for a multi-year horizon.

Q14. Do you agree that the draft impact assessment adequately outlines the likely main impacts of this guidance?

GBBC agrees in principle but notes that the impact assessment under-represents three critical realities.

First, it does not sufficiently capture the operational significance of hybrid architectures — Layer-2 networks, roll-ups, or bridge systems — where personal data may flow between public and permissioned environments.

Second, it treats controller/processor allocation as static, whereas in practice these roles are dynamic, varying by layer and governance model.

Third, the assessment glosses over international-transfer mechanics. Replication across globally distributed nodes is intrinsic to DLT and challenges traditional "transfer" definitions under the UK GDPR. The ICO rightly flags this issue but stops short of offering workable interpretive criteria.

Addressing these three areas would ensure the final impact assessment mirrors the operational complexity faced by UK-based blockchain participants.

Q15. To what extent do you agree that the first part of the guidance ("What are DLTs and blockchains?") clearly explains the key features of these technologies?

GBBC agrees that Part 1 is clear, well-structured, and accessible to non-technical readers. It succeeds in demystifying core blockchain concepts — immutability, decentralisation, and consensus — without unnecessary jargon. However, it still treats these as static properties rather than design variables that can be configured to support data-protection compliance.

A brief typology illustrating how decentralisation and transparency vary across architectures would make the guidance more operational. This would allow data-protection officers to assess where their systems sit on the *centralised-to-decentralised spectrum* and tailor safeguards accordingly.

However, the guidance would benefit from clarifying that immutability does not equate to permanent data availability — blocks can be pruned or made economically inaccessible. This distinction is essential for interpreting storage-limitation principles.

Q16. Do you agree that using the more familiar term "blockchain" interchangeably with DLT helps make the guidance easier to follow?

Yes - this enhances readability for non-specialist audiences. Yet the ICO should include an early terminological clarification acknowledging that not all DLTs are blockchains and that data-governance implications differ for directed acyclic graphs, Layer-2 roll-ups, or permissioned ledgers. A short definitional note would preserve accessibility without sacrificing technical accuracy.

Q17. To what extent do you agree that this guidance clearly explains the roles of participants, validators, and other actors?

GBBC agrees that the ICO identifies the issue correctly but finds the treatment too cursory. The section "Who is the controller in a blockchain?" does not provide the granularity required for consistent application. The ICO concludes, broadly, that transaction originators are likely controllers and validators are likely processors — yet this overlooks complex intermediate actors such as miners, wallets, oracles, sequencers, and bridge operators.

Drawing on comparative analysis from *Artzt & Richter, International Handbook of Blockchain Law (2nd ed., 2024)*, these actors cannot be grouped under simple binary categories. Oracles, in particular, exercise discretion in selecting and transmitting off-chain data; they arguably determine both purpose and means, making them controllers in certain contexts.

GBBC therefore recommends a functional rather than categorical approach: controllership should be assessed by the degree of decision-making power over data inputs and outputs, not by technical role labels. Without this, the guidance risks creating formal certainty without practical clarity.

Q18. Does this guidance clearly explain what on-chain information can include?

The ICO accurately identifies key categories — transactions, smart contracts, and metadata — but could expand its analysis of how these interact. For instance, **metadata** such as block headers, event logs, and Merkle roots can indirectly reveal user patterns even where primary data are pseudonymised.

GBBC supports the ICO's recognition that pseudonymised data remain personal data when linkable through reasonable means, yet believes the guidance should further discuss **re-identification risks from analytics**. The ICO's own Anonymisation guidance could be cross-referenced here to illustrate how probabilistic identification thresholds apply in decentralised contexts.

Cross-referencing the ICO's 2023 *Anonymisation and PETs Guidance* would help firms apply consistent thresholds for 'reasonable means of identification'

Q19. To what extent do you agree this guidance clearly explains the features and differences between permissioned and permissionless blockchains?

GBBC agrees, though the binary framing of permissioned versus permissionless is increasingly outdated. Many deployments now operate as public-permissioned hybrids — networks with open readability but controlled write access (e.g., LACChain, EBSI). These hybrids complicate assumptions about governance and data controllership: while access is restricted, data visibility remains global. The ICO could strengthen the section by acknowledging this continuum of decentralisation rather than treating the two categories as discrete.

Recognising this continuum is crucial because accountability and lawful-basis analysis differ across it: in hybrids, access control may render some actors processors, while public transparency still triggers controller obligations for transaction originators

Q20. To what extent do you agree that this guidance explains when on-chain information could meet the definition of personal information?

GBBC supports the ICO's contextual interpretation of identifiability, which aligns with Recital 30 UK GDPR. However, it would be useful to articulate a structured analytical test — distinguishing data that are inherently identifying from data that become identifying only when combined with off-chain information such as KYC records or IP logs.

This nuance matters because the same dataset may be personal for a regulated custodian (who holds KYC records) but anonymous for a protocol-level participant with no such linkage. The guidance should caution against assuming a uniform perspective on identifiability across all network participants.

Q21. To what extent do you agree that the sections on smart contracts, automated decision-making (ADM), and contract exemption are clear?

GBBC welcomes the ICO's balanced treatment but finds the section too high-level to be applied consistently. The guidance recognises that smart contracts can involve solely automated decisions under Article 22 UK GDPR but stops short of offering practical interpretive examples.

In particular, the role of data oracles — which introduce external information into automated decisions — is underexplored. Where an oracle determines the dataset or timing that triggers a contractual outcome (for example, liquidation of collateral in a DeFi protocol), that discretion may itself constitute "meaningful human involvement," breaking the Article 22 threshold.

GBBC recommends including concrete case studies illustrating how Article 22 applies in blockchain contexts and clarifying the evidentiary standard for "necessary for the performance of a contract."

Q22. To what extent do you agree this guidance provides practical and actionable suggestions to ensure compliance (off-chain storage, putting data beyond use, pruning/purging)?

GBBC supports the ICO's pragmatic orientation but considers the section too narrow in scope. It focuses primarily on "off-chain storage" as a compliance technique, describing "hashing-out" — deleting off-chain data while leaving a null pointer on-chain — as the main mitigation for erasure and rectification rights.

While hashing-out is operationally important, the ICO overlooks its structural consequences: off-chain storage re-introduces centralisation by placing personal data under the control of a single identifiable entity. This can erode the decentralisation and trustless governance that

make DLT attractive in the first place. The guidance should explicitly acknowledge this trade-off and explore safeguards such as multi-party custody, encrypted enclaves, or privacy-preserving computation to distribute control.

Equally, "putting data beyond use" and pruning techniques would benefit from deeper treatment — including conditions for verifying that data cannot be feasibly re-linked.

For instance, where an exchange maintains an off-chain user database to support erasure rights, it should be clear whether that off-chain copy constitutes the authoritative record — effectively shifting controllership from a decentralised ledger to a central administrator.

Q23. To what extent do you agree that our description of blockchain and the rights to rectification and erasure clearly explains the technical challenges to compliance?

GBBC agrees that the ICO correctly identifies the tension between immutability and data-subject rights.. The guidance discusses hashing-out and off-chain pointers but does not address alternative models such as append-only correction, key destruction, or zero-knowledge attestations. GBBC believes these deserve fuller exploration as they align more closely with blockchain's distributed ethos.

Moreover, the ICO could examine the juridical implications of partial erasure: when a controller removes off-chain data but leaves an immutable pointer, is the remaining on-chain reference itself still personal data? This question is critical for defining when an erasure request is considered fulfilled.

GBBC therefore urges the ICO to articulate clearer criteria for "effective erasure" in decentralised systems — perhaps through a case-based annex.

Q24. To what extent do you agree this guidance clearly outlines the choices organisations have when considering Data Protection by Design and by Default (DPbD)?

GBBC largely agrees but suggests greater emphasis on the sequencing of design choices. The ICO outlines DPbD principles but not the logical process by which a controller should apply them. A concise "decision tree" would translate the abstract obligation into a practical workflow: first, assess necessity of blockchain; second, decide whether personal data can remain off-chain; third, select appropriate privacy-enhancing technologies (zero-knowledge proofs, differential privacy, homomorphic encryption).

This would make the guidance genuinely actionable and align it with the ICO's own PETs framework. In its absence, firms may comply formally but not meaningfully demonstrate data-protection-by-design.

Q25. Is there anything else this guidance should cover, or any way it can be improved further?

The ICO's Draft Guidance on DLT and the UK GDPR is commendably comprehensive and compares favourably with the EDPB's draft Guidelines 02/2025, which remain more theoretical. Nevertheless, several gaps remain.

First, the controller analysis requires deeper engagement with hybrid and decentralised ecosystems; it should specify treatment of miners, wallets, and oracles.

Second, the guidance should examine the trade-offs of off-chain storage and the potential re-centralisation this introduces, so that privacy compliance does not come at the expense of decentralisation.

Third, cross-border data-transfer rules remain conceptually unresolved. Since data replication across global nodes is intrinsic to public blockchains, a strict territorial interpretation could render compliance impossible. The ICO should explore pragmatic interpretations — for instance, treating replicated encrypted data as non-transfer where decryption keys remain within the UK's jurisdiction.Absent such clarification, firms may avoid public-ledger deployments altogether, pushing innovation offshore and undermining the UK's competitiveness.

Finally, GBBC supports the creation of a living annex of use-case studies and operational templates, co-developed with industry, to ensure the guidance remains adaptable as both law and technology evolve.

Section 4 – General Comments on the Guidance

Q27. Are you currently planning to use blockchain?

GBBC's membership base spans the full spectrum of blockchain adoption across the UK and international markets.

Members include regulated financial-market infrastructures, custodians, service providers, protocol developers, and legal advisors, operating on private permissioned, public permissioned, and public permissionless systems.

A significant proportion of our members deploy or support hybrid configurations — permissioned systems that anchor proofs or commitments to public networks — as well as Layer-2 roll-ups and cross-chain bridges.

This diversity reinforces the need for technology-neutral regulatory guidance: most real-world deployments do not fit neatly within the binary "public/permissioned" taxonomy used in the draft.

GBBC therefore urges the ICO to ensure that its final guidance speaks equally to enterprise-grade permissioned networks and to open-protocol environments, providing examples that capture both.

Q28. Having read this draft guidance, how helpful did you find it to understanding blockchain and data-protection obligations?

GBBC and its members find the guidance highly helpful and conceptually mature. It marks a substantial improvement on earlier European treatments, including the EDPB's Draft Guidelines 02/2025, by directly engaging with the practicalities of UK data-protection law as applied to decentralised systems.

Where the EDPB document remains doctrinal, the ICO's draft adopts a more pragmatic orientation — recognising that data controllers and processors must balance privacy principles with technological feasibility.

This pragmatism makes the guidance useful not only for lawyers and DPOs, but also for engineers, compliance officers, and policy teams seeking to translate legal principles into design standards.

To reach its full potential, however, the document would benefit from additional operational aids: sample DPIA templates, role-allocation matrices, and schematic illustrations of permissioned and hybrid networks. These tools would make the guidance truly *implementable* rather than purely interpretive.

Q29. Does this guidance use language and examples that are clear and easy to understand?

We agree that the language is commendably clear. The ICO has succeeded in writing for a multi-disciplinary audience without oversimplifying the law.

Nonetheless, clarity could be enhanced through a short technical glossary explaining key terms such as *hashing-out*, *off-chain storage*, *hybrid network*, and *privacy-enhancing technologies (PETs)*.

A concise definitional annex would prevent semantic drift as the guidance is re-used by different stakeholders — from protocol developers to institutional compliance teams.

Equally, the inclusion of visual summaries — such as flowcharts depicting data flows and governance roles — would improve comprehension and make the guidance a practical reference document rather than a purely textual analysis.

Q30. Having read this guidance, how confident do you feel that you understand how data-protection law applies to information on blockchain?

The guidance successfully clarifies that immutability does not exempt actors from compliance, but rather requires compliance to be achieved through architectural design — via *off-chain storage*, *pseudonymisation*, and *key-management strategies*.

Confidence would rise further if the ICO addressed three persistent policy knots that surfaced during industry discussion:

1. **Controller mapping in decentralised governance** — clarifying how DAOs, validators, and oracles fit within the controller/processor framework.
2. **Cross-border data replication** — determining when global node distribution constitutes a restricted transfer under UK law.
3. **Operational evidence of "data beyond use"** — setting out how firms can demonstrate compliance without over-centralising data custody. It is notable that requiring compliance through architecture can result in some players in the blockchain ecosystem having limited influence in achieving compliance.

We believe that addressing these uncertainties would move the UK framework from interpretive adequacy to true regulatory operationalisation. In other words, the ICO has succeeded in clarifying the 'what' of compliance but must now address the 'how' through operational tooling.

Q31. Do you have any further comments or suggestions that would improve this guidance?

GBBC commends the ICO for taking a measured and forward-looking approach that recognises the legitimacy of distributed technologies within the UK data-protection regime.

However, given the pace of innovation, static guidance will date quickly. GBBC therefore recommends that the ICO establish a "living annex" — a continuously updated digital companion to the guidance, maintained in collaboration with industry and academic experts.

Such an annex could contain:

- Worked examples across core use-cases (financial settlement, tokenisation, decentralised identity, NFT platforms);
- A cross-reference table aligning ICO positions with emerging EU and global interpretations, ensuring consistency while preserving the UK's pragmatic edge.

GBBC and its members would be pleased to contribute anonymised materials and expertise to such a resource.

Finally, we encourage the ICO to engage internationally with peer authorities and standard-setting bodies to promote interoperability between data-protection frameworks. The UK has an opportunity to lead by example: demonstrating that robust privacy protection and decentralised innovation can coexist through proportionate, evidence-based regulation.