Feedback to Public Consultation 02/2025 of EDBP

Regarding: Guidelines 02/2025 on processing of personal data through blockchain technologies

Date: June, 6th 2025

21X AG

Title of the Proposal	Guidelines 02/2025 on processing of personal data through blockchain technologies – Version 1.1 (Adopted on 08 April 2025)
Submitting Entity	**21X AG** Große Gallustraße 16-18 60312 Frankfurt am Main Germany BaFin license number: 40034974
Recipient	**European Data Protection Board** Rue Wiertz 60 1047 Brussels Belgium
Contact Person	**Thomas Zraunig**
Position	Data Protection Officer
Email	t.zraunig@21x.eu
Confidentiality	This feedback may be published in full.
Executive Summary	21X AG welcomes the EDPB's efforts to ensure data protection in blockchain environments but cautions that the current draft Guidelines risk discouraging innovation by restricting the use of public blockchains. This position is at odds with existing EU frameworks such as the DLT Pilot Regime and MiCAR, which permit regulated use of permissionless networks.

Contents

1. Introduction 3
2. Classification of Blockchain Wallet Addresses as Personal Data 3
3. Broadening the Interpretation of Anonymization for Blockchain Data 4
4. Alignment with EU Strategic Goals for Digital Finance and Innovation 6
5. Recognizing the Benefits of Public Blockchains & Supporting Off-Chain Data Models 8
6. Recommendations for Specific Changes to the Draft Guidelines 9
7. Conclusion 11
8. Signatures 11

1. Introduction

We appreciate the European Data Protection Board's effort in drafting Guidelines 02/2025 on processing of personal data through blockchain technologies and the opportunity to provide feedback. As a new market infrastructure operating under the EU's DLT Pilot Regime, we are committed to innovative yet compliant use of public blockchain technology. In this submission, we express concerns and recommendations regarding the draft Guidelines, focusing on the treatment of blockchain wallet addresses, the definition of anonymization in this context, and alignment with broader EU objectives. We also offer constructive suggestions to clarify the language of the Guidelines to support responsible innovation.

2. Classification of Blockchain Wallet Addresses as Personal Data

The draft Guidelines suggest that blockchain identifiers (wallet addresses/public keys) may be considered personal data under GDPR in many cases. For example, the Guidelines note that an alphanumeric public key "which looks random" can qualify as personal data if it can be used to identify a natural person by reasonably likely means (e.g. through a data breach revealing the link to an identity)[1]. It is further emphasized that even pseudonymized on-chain data (such as hashed or encrypted identifiers) may still be deemed personal data under GDPR. We are concerned that this interpretation is overly broad, especially in contexts where no other on-chain data can be attributed to an individual.

Classifying wallet addresses *per se* as personal data in all circumstances could have negative consequences for blockchain-based innovation:

- **Data Minimization Disincentive:** Paradoxically, controllers who deliberately limit the personal data they collect (e.g. using only wallet addresses on-chain and no names or IDs) would still be burdened with full GDPR obligations. This undermines the spirit of data minimization, as even minimal pseudonymous identifiers would trigger compliance requirements equivalent to those for clear personal data.
- **Operational Feasibility:** Treating every public blockchain address as personal data could make routine operations extremely cumbersome. For instance, node operators or infrastructure providers on public chains might be considered data controllers for every transaction they relay (since they "process" wallet addresses). This interpretation would introduce significant legal uncertainty and liability for participants who have no relationship with the data subjects, potentially deterring participation in public blockchain networks.

[1] EDBP Guidelines 02/2025 on processing of personal data through blockchain technologies, V1.1

- **Innovation and Competition:** A blanket classification could stifle innovation by raising compliance costs for startups and SMEs leveraging blockchain. Requiring heavy GDPR processes (DPIAs, consent or other legal bases, data subject rights mechanisms, etc.) for systems that never actually know the real identity behind on-chain addresses might be seen as disproportionate. Smaller firms in the EU's burgeoning blockchain ecosystem could be disadvantaged, and some may choose to relocate or avoid EU projects, ultimately hindering the EU's competitiveness in this strategic field.

We urge the EDPB to refine the guidance on when a blockchain address should be considered personal data. In particular, the final Guidelines should acknowledge context: where on-chain data (e.g. public addresses) are not, by themselves, sufficient to identify a data subject without recourse to separate, securely governed systems, they should not automatically be treated as personal data for all actors in the network. This approach is in line with Recital 26 of the GDPR[2], which emphasizes identifiability must be assessed in light of the means "reasonably likely to be used", considering time, cost, and technological state.

For blockchain systems designed with strict off-chain handling of personal information, where likability is carefully compartmentalized and not accessible to third parties, public addresses on the ledger may not constitute personal data in the hands of many participants.

This nuanced approach would prevent over-classification of purely pseudonymous references as personal data in cases where identification is practically infeasible. It would also send a clear signal that data controllers who truly limit their knowledge of data subjects are not unfairly penalized. We believe this change will encourage privacy-friendly technical architectures without compromising data protection, and we provide further reasoning on anonymization in the next section.

3. Broadening the Interpretation of Anonymization for Blockchain Data

We respectfully submit that the EDPB should adopt a more nuanced interpretation of anonymization in the blockchain context. Even where off-chain systems exist that could link a wallet address to a data subject, if those systems are functionally and operationally isolated, and the on-chain data cannot be used independently or without disproportionate effort to identify the individual, the on-chain information should be regarded as effectively anonymized or strongly pseudonymized.

This reflects the GDPR's focus on practical identifiability rather than theoretical possibility. The use of robust compartmentalization—whereby identifying data is securely stored in a

[2] EUR-Lex: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27.04.2016, Recital 26

separate domain under limited access controls—significantly reduces the identifiability of on-chain data. We recommend the Guidelines clarify that *"pseudonymized data stored on-chain should not be considered personal data in all contexts, particularly where re-identification requires access to segregated off-chain datasets under independent controls."*

We ask the EDPB to consider treating robustly pseudonymized blockchain data as "anonymous" (and thus not personal data) when certain conditions are met. Those conditions could include:

- The controller has no reasonable means to re-identify the person from the on-chain data without consulting separate, securely-held information.
- No third party is likely to identify the person from the on-chain data alone, taking into account current technology and available datasets. (In other words, the data is effectively anonymous to any outside observer)
- Proportionate effort: Identification would require disproportionate effort, computing power, or cross-referencing that goes beyond what any typical participant or even determined adversary could reasonably do. This follows the GDPR's test that if identification requires "a disproportionate amount of time, effort or resources", the data can be seen as anonymous.

By embracing this interpretation, the Guidelines would encourage blockchain practitioners to implement strong data protection by design. Controllers would know that if they truly anonymize or strongly pseudonymize personal data (e.g. via one-way cryptographic hashes, zero-knowledge proofs, or other advanced techniques) such that individuals are not identifiable, they can step outside certain GDPR constraints legitimately. This creates a positive incentive to minimize identifiability of on-chain data. We note that the draft Guidelines already recommend techniques like hashing, encryption, and cryptographic commitments to limit identifiability. However, the current text also warns that encrypted or hashed data remains personal under GDPR.

We respectfully suggest to EDPB to modify the language to clarify that *pseudonymized blockchain data should be assessed on a spectrum of identifiability*. For instance, a statement could be added: *"Where state-of-the-art technical measures (encryption, hashing, cryptographic commitments, etc.) are applied such that the on-chain data cannot be linked to an identity by any party without disproportionate effort, controllers may consider the data as meeting the standard of anonymization in Recital 26 GDPR. In these cases, the information would no longer be regarded as personal data."* This clarification would be consistent with GDPR's text and would alleviate undue burdens when high

anonymization standards are in fact achieved. It balances privacy protection (by encouraging maximum de-identification) with innovation.

4. Alignment with EU Strategic Goals for Digital Finance and Innovation

The draft Guidelines, in their current form, risk being perceived as discouraging the use of public (permissionless) blockchain networks. For example, organizations are advised to assess the type of blockchain and use a public blockchain "only if necessary" – effectively advising that public blockchains should be avoided unless essential. While we understand this guidance is motivated by caution (since public chains make data visible to many and raise certain risks), we wish to highlight a potential misalignment with major EU strategic initiatives that explicitly promote responsible use of innovative technologies, including public blockchains.

The DLT Pilot Regime (Regulation (EU) 2022/858) is a flagship EU initiative under the Capital Markets Union that allows financial market infrastructures to experiment with distributed ledger technology. Notably, the DLT Pilot Regime permits the use of permissionless (public) blockchains for trading and settling financial instruments in a controlled environment. Several participants in this pilot (including our market infrastructure) are exploring or using public blockchain networks to issue and trade tokenized securities. The European Securities and Markets Authority (ESMA) and national regulators overseeing the pilot have approved the use of permissionless blockchain under regulatory safeguards, illustrating the EU's openness to public blockchain innovation in finance. If the EDPB Guidelines implicitly cast public blockchains as a last-resort or undesirable option, this creates a tension with the DLT Pilot framework, which is built on the premise that public blockchains can be harnessed in a compliant way.

Beyond the pilot, the EU's broader Capital Markets Union (CMU) and the recently launched Savings and Investment Union (SIU) strategy emphasize *modernizing Europe's financial markets through technology*. For instance, the European Investment Bank (EIB) – a key EU institution – has explicitly called for "facilitating the growth of digital bond issuance using public blockchains across Europe" to improve access to capital for smaller companies.[3] This is part of the EU's vision to leverage blockchain to democratize finance and boost market efficiency. Public blockchains offer unique benefits in this regard: they remove centralized gatekeepers, potentially lower transaction costs, and enable wider participation across member states. Indeed, an EU-commissioned report in 2024 observed that permissionless blockchains can be more neutral and foster competition, avoiding the siloing effect of closed, private networks. These policy directions underscore that the EU sees *value in public blockchain networks*, provided they are used responsibly.

[3] European Investment Bank – Capital markets union

Furthermore, the forthcoming Markets in Crypto-Assets Regulation (MiCA) (Regulation (EU) 2023/1114) reflects a balanced approach of supporting innovation in the digital asset space while safeguarding users. MiCA's stated objective is *"to support innovation and fair competition, while ensuring a high level of protection"* for investors and market integrity.[4] This demonstrates that encouraging new technologies (like blockchain) and ensuring strong protections are not mutually exclusive goals in EU law – they must be pursued in tandem. In the context of public blockchains, this means we should strive to enable their use under conditions that protect personal data, rather than impose an outright bias against their use.

We respectfully recommend that the EDPB align its final Guidelines with these strategic EU objectives by *tempering any blanket discouragement of public blockchain use*. The focus should be on how to use public blockchains in a data-protective manner, rather than implying they are inherently problematic.

- The Guidelines could acknowledge the legitimate use-cases for public blockchains in finance and other sectors. A statement might be added such as: *"the use of a public blockchain may be justified and beneficial if the controllers ensure appropriate safeguards in such cases"* This assures industry that compliant use of public networks is feasible, in line with EU innovation policy.
- Where the draft currently says public blockchains should be avoided unless necessary, we suggest rephrasing to a more neutral tone. For instance: *"Assess the necessity of a public (permissionless) blockchain for your use-case. If a public blockchain is chosen, implement commensurate measures (encryption, access controls at application layer, etc.) to protect personal data from unwarranted exposure."* This still urges caution and data protection, but stops short of making public chains sound taboo.
- The final Guidelines might explicitly refer to EU initiatives (perhaps in a preamble or footnote) to show awareness that this guidance is not made in a vacuum. Recognizing, for example, that *"the EU is simultaneously fostering distributed ledger technology in finance (see e.g. DLT Pilot Regime and CMU initiatives) and these Guidelines seek to support such innovation in a privacy-compliant way*," would reassure stakeholders that data protection regulators are working hand-in-hand with innovation regulators.

Aligning with the EU's strategic goals serves a dual purpose: it reinforces the credibility and relevance of the Guidelines, and it ensures that privacy guidance does not unintentionally

[4] EUR-Lex: Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023, Recitals 1, 2, 5, 6 & 16

become an obstacle to policy objectives democratically endorsed by the EU. We believe it is possible to protect fundamental rights (privacy) while also promoting technological progress – indeed, that is the essence of Europe's approach to digital innovation. We urge the EDPB to make this balance clear in the final text.

We support the Guidelines' existing advice to process personal data off-chain and record only pseudonymous or minimized identifiers on-chain. This approach allows for full control over personal data in regulated environments, while ensuring that the on-chain component does not expose any identity information to third parties.

We encourage the EDPB to explicitly recognize this model as an effective implementation of Data Protection by Design and by Default (Art.25 GDPR). Where personal data is processed off-chain in controlled environments and only pseudonymous references appear on-chain, the risk of identifiability from the blockchain data itself is significantly reduced. This approach should be considered a recommended practice for GDPR compliance in blockchain systems.

5. Recognizing the Benefits of Public Blockchains & Supporting Off-Chain Data Models

We encourage the EDPB to include in the Guidelines an acknowledgment of the positive role public blockchain technology can play in financial markets (and beyond), when used with appropriate data protection measures. As noted, public blockchains can provide transparency, security, and interoperability benefits. For financial market infrastructures, a public blockchain can serve as a single source of truth for transactions and ownership, reducing reconciliation errors and potentially enabling faster settlement of trades. The transparency of a public ledger can enhance market integrity (e.g., regulators with access can audit transactions in real-time), and the global accessibility can lower barriers to entry for new market participants across the EU. These benefits align with the goals of the Capital Markets Union to *"allow money to flow more freely across the EU"* and improve financing opportunities for businesses and investors.[5]

However, these benefits can only be realized if data protection is built into the system design – which brings us to the importance of off-chain processing models.

Off-Chain Personal Data Storage as Best Practice: We strongly support the draft Guidelines' emphasis on not storing personal data on-chain and using off-chain techniques to minimize on-chain personal data. In our operational model, all personal information is stored in traditional systems under our control (off-chain), and only hashed references or wallet addresses appear on the blockchain. This approach embodies Data Protection by

[5] European Investment Bank – Capital markets union

Design and by Default (GDPR Art.25) – it ensures that the blockchain ledger, which is immutable and widely replicated, contains no directly identifying information about individuals. If a data subject exercises their GDPR rights (rectification, erasure, etc.), we can comply by updating or erasing the off-chain records without needing to alter the blockchain. The on-chain data, being pseudonymous, poses minimal risk: for example, if a user wishes to be "forgotten," we can delete their off-chain personal details and simply cease associating their identity with a given wallet address. That address on the public chain then becomes just a random string with no link to an identifiable person from any viewer's perspective.

The draft Guidelines already hint at supporting such models, for instance by recommending off-chain storage with on-chain references to address scalability and confidentiality. They also list privacy-enhancing technical measures like cryptographic commitments and keyed-hash functions that effectively keep data off-chain or unreadable on-chain. We applaud these recommendations. To reinforce them, the final Guidelines should explicitly endorse off-chain data minimization as a preferred approach.

By acknowledging this, the EDPB will send a message that it recognizes and supports innovative privacy-friendly solutions. This is critical because many stakeholders in the blockchain community still fear that GDPR compliance and blockchain are fundamentally at odds. Highlighting off-chain data storage as a solution demonstrates that *compliance can be achieved through smart architecture choices*. It will encourage more projects to adopt this architecture, thus improving overall compliance in the ecosystem.

In summary, we recommend the final Guidelines explicitly recognize that public blockchains, when implemented with off-chain personal data handling and strong pseudonymization, can be compatible with EU data protection law. This acknowledgement in an EDPB document would carry significant weight and would encourage the responsible adoption of blockchain technology in Europe – achieving both innovation and privacy protection.

6. Recommendations for Specific Changes to the Draft Guidelines

To ensure the above points are incorporated, we propose the EDPB consider the following specific changes or clarifications in the final Guidelines:

- Clarify the status of blockchain addresses: Refine the language (in Section 3.1 or where applicable) to state that *public keys/wallet addresses should be treated as personal data only if they relate to an identifiable individual.* Add that if identification of the individual behind an address is not realistically possible for the controller or any likely third party (per Recital 26), then the address alone may be considered anonymous and outside the GDPR's scope. This change will prevent over-

generalization that all addresses are personal data, focusing instead on whether an address is linkable to a person in context.

- Broaden guidance on anonymization: In the sections discussing pseudonymization and encryption, acknowledge that irreversible techniques can achieve anonymization. For example, when discussing hashing or commitments, add: *"If the original personal data is deleted or kept entirely separate such that re-identification is not feasible, the on-chain data may be deemed anonymous."* This aligns with Recital 26 and gives credit to truly robust anonymization efforts. It will encourage controllers to go the extra mile in privacy-by-design, knowing that doing so could alleviate certain GDPR obligations.
- Soften the stance on public blockchain usage: Revise the recommendation that *"public blockchains should be avoided unless essential"*. We suggest rephrasing this along the lines of: *"Carefully consider the necessity of using a public (permissionless) blockchain. Where a public blockchain offers significant benefits for the purpose at hand, it may be used provided that additional safeguards are implemented to protect personal data."* This change keeps the caution (rightly encouraging justification and safeguards) but removes the negative presumption against public networks. It also implicitly recognizes scenarios (like cross-border financial infrastructures) where public blockchains have legitimate advantages.
- Highlight EU policy alignment: In the introduction or a contextual footnote, mention that these Guidelines are meant to facilitate GDPR compliance in blockchain without hindering innovation. Potentially reference that the guidance is *"complementary to EU initiatives promoting blockchain and DLT in finance and other sectors (e.g., the European Commission's Digital Finance Strategy, the DLT Pilot Regime under Regulation EU 2022/858, and the objectives of MiCA to support innovation), by ensuring that such technologies are deployed in a privacy-preserving manner."* Even a brief mention would go a long way to reassure stakeholders that EDPB's guidance is integrated with the broader EU vision. It reinforces that data protection is a cornerstone of sustainable innovation, not an obstacle to it.
- Endorse off-chain data minimization explicitly: Strengthen the language recommending off-chain storage of personal data. We propose adding a sentence in the data minimization techniques section, such as: *"The EDPB considers the approach of storing personal data off-chain and keeping only pseudonymous pointers or hashed values on-chain to be a good practice in achieving GDPR compliance on blockchain. This model should be explicitly considered by any organization planning to process personal data using blockchain."* This clear endorsement will validate and encourage privacy-centric designs. It also aligns with

the draft's advice that *"storing personal data on a blockchain should be avoided"* if it conflicts with data protection principles.

- Improve guidance on data subject rights in off-chain models: We suggest the Guidelines note that, in off-chain models, GDPR rights can be respected without needing to alter the blockchain ledger. For instance, if a data subject asks for erasure, the controller can erase the personal data in their off-chain system and disassociate that person from any on-chain address. The Guidelines could reassure that such a strategy is acceptable, provided that after disassociation, the on-chain data can no longer be linked to the individual (thus effectively anonymized). This would address the common concern about the "Right to be Forgotten" on immutable ledgers by showing a practical compliance solution. It complements existing guidance that *off-chain storage is "preferred" for handling deletion requests*.

Lastly, we encourage the EDPB to maintain an open dialogue with industry and continue to refine these Guidelines based on real-world feedback. The public consultation is a valuable step. As the blockchain sector evolves, so will best practices for privacy – the EDPB's ongoing engagement and openness to updates will be crucial. We stand ready to contribute further insights from the perspective of a regulated blockchain-based exchange licensed under the DLT Pilot regime.

7. Conclusion

In closing, we reiterate our support for the EDPB's initiative to clarify GDPR's application to blockchain. By incorporating the above recommendations, the Board can ensure its final Guidelines protect individuals' personal data without inadvertently hampering innovation in Europe. Striking this balance will empower exchanges like ours – and many other companies large and small – to harness public blockchain technology in a way that aligns with Europe's values and legal standards. We thank you for considering our feedback, and we remain at your disposal for any clarification or further discussion on these points.

8. Signatures

Thomas Zraunig

Thomas Zraunig (5. Juni 2025 21:16 GMT+2)

Data Protection Officer

(Thomas Zraunig)

Max Heinzle, CEO

Max Heinzle, CEO (6. Juni 2025 14:36 GMT+2)

Chief Executive Officer

(Max Joseph Heinzle)

202506_21X_Feedback_EDBP_Guidelines

Abschließender Prüfbericht 2025-06-06

Erstellt:	2025-06-05
Von:	Thomas Zraunig (t.zraunig@21x.eu)
Status:	Signiert
Transaktions-ID:	CBJCHBCAABAAhyv65kxaofW1HWhJwn4zTUiq1l9sxT6S

Verlauf für „202506_21X_Feedback_EDBP_Guidelines“

Thomas Zraunig, DPO (t.zraunig@21x.eu) hat das Dokument erstellt.
2025-06-05 - 19:14:56 GMT

Dokument wurde per E-Mail zur Signatur an Max Heinzle, CEO (m.heinzle@21x.eu) gesendet.
2025-06-05 - 19:15:03 GMT

Dokument wurde per E-Mail zur Signatur an Thomas Zraunig, DPO (t.zraunig@21x.eu) gesendet.
2025-06-05 - 19:15:03 GMT

Die signierende Person Thomas Zraunig, DPO (t.zraunig@21x.eu) hat bei der Signatur den Namen Thomas Zraunig eingegeben
2025-06-05 - 19:16:30 GMT

Thomas Zraunig (t.zraunig@21x.eu) hat das Dokument mit einer E-Signatur versehen.
Signaturlink wird erstellt von Thomas Zraunig (t.zraunig@21x.eu)
Signaturdatum: 2025-06-05 – 19:16:32 GMT – Zeitquelle: Server

Max Heinzle, CEO (m.heinzle@21x.eu) hat die E-Mail angezeigt.
2025-06-06 - 12:35:38 GMT

Max Heinzle, CEO (m.heinzle@21x.eu) hat das Dokument mit einer E-Signatur versehen.
Signaturdatum: 2025-06-06 – 12:36:50 GMT – Zeitquelle: Server

Vereinbarung abgeschlossen.
2025-06-06 - 12:36:50 GMT