Monero Policy Working Group (MPWG)
MoneroPolicy.org
**Date:** 08/06/2025

Response to Guidelines 02/2025 on processing of personal data through blockchain technologies, published by the European Data Protection Board

**Submitted by:** Monero Policy Working Group

**Contact:** policy@getmonero.org

## Introduction

1. The Monero Policy Working Group (MPWG) is a loosely formed quorum of individuals that contribute to the Monero open-source project.[1] Monero is a permissionless, privacy-preserving cryptocurrency network. The goal of MPWG is to work with regulators, policy makers, and the wider financial services sector to ensure a broad understanding of Monero, and other privacy-preserving cryptocurrencies, is communicated. We have specific interest in interacting with entities so they may understand Monero's component technologies, especially in the context of evolving regulatory and compliance requirements.

2. We would like to take the opportunity to acknowledge the publication of the European Data Protection Board's (EDPB) Guidelines 02/2025 on processing of personal data through blockchain technologies.[2] **Blockchain and Distributed Ledger Technologies (DLTs) are a nascent technology, allowing immutable records to be published publicly since 2008.** These processing guidelines can now support responsible development and deployment of the technology with respect to the protection of personal data, a fundamental right.

3. Firstly, we would like to communicate our support for the majority of the guidelines. We feel they are considered and informative. **We understand the complexity of aligning the principles of data protection with the characteristics of DLT.** In this respect, the guidelines provide some clarity for the wider European ecosystem. Irrespective of our support, we would like to draw attention to some key aspects, focused on the interplay with adjacent European regulations, the application of privacy enhancing technology (PET), and the guidelines' potential impact on the use and deployment of public and permissionless DLT systems.

[1] see The Monero Project, https://github.com/monero-project and https://getmonero.org

[2] https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-022025-processing-personal-data_en

## European regulations and deployment of privacy-enhancing technology

4. Our main concern stems from the EDPB's unwillingness to acknowledge the difficult regulatory interplay impacting the current DLT ecosystem, specifically the obligations stemming from recently enacted Anti-money Laundering Regulation (AMLR)[3] and Market in Crypto-Assets Regulation (MiCAR).[4] **Obligations in these adjacent frameworks, currently prohibit or limit entities from offering DLT services related to privacy-enhancing technology (PET), zero-knowledge cryptography, privacy-enhanced protocols, and/or 'zero-knowledge blockchains'.** This restricts individuals' ability to interact with these privacy-preserving DLT systems. The obligations also inhibit how data-protection-by-design-and-default methods can be applied to the development and deployment of DLT systems and, ultimately, create a 'chilling effect' on the application of privacy-preserving technology to the DLT ecosystem.

5. Further to the above, it has been recently acknowledged, in a report[5] published by the Bank of International Settlements (BIS), that privacy and data protection in digital payments should move to the centre of the public policy debate. In the report, the BIS categorise privacy as being 'hard' or 'soft', with the degree of centralisation playing an important role in the differentiation. **We feel the EDPB should clearly acknowledge that 'hard' privacy is critical for permissionless systems, as there is no easily identifiable controlling authority that is responsible or liable for ensuring data protection risks are mitigated.**

6. **AMLR, Article 79(1), prohibits obliged entities from offering services to customers related to "anonymity-enhancing coins"**, and defines these as such: "*'anonymity-enhancing coins' means crypto-assets that have built-in features designed to make crypto-asset transfer information anonymous, either systematically or optionally*;" (AMLR, Art 2(25)). **This effectively limits the technologically focused data protection measures available to DLT users as AMLR obliged entities are prohibited from offering 'anonymity-enhanced' DLT products and services.**

7. **MICAR, Article 76(3), prohibits obliged entities from offering services related to tokens that include "an in-built anonymisation function":** *"3. The operating rules of the trading platform for crypto-assets shall prevent the admission to trading of crypto-assets that have an inbuilt anonymisation function unless the holders of those crypto-assets and their transaction history can be identified by the crypto-asset service providers operating a trading platform for crypto-assets."* (MiCAR, Art 76(3)). **We view the included condition of 'transaction histories' is not consistent with fundamental data protection principles such as 'purpose limitation' and 'data minimisation', and may be questionable in terms of proportionality and/or necessity.** Currently, when

[3] Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (Text with EEA relevance), available at: https://eur-lex.europa.eu/eli/reg/2024/1624/oj

[4] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (Text with EEA relevance), available at: https://eur-lex.europa.eu/eli/reg/2023/1114/oj

[5] Auer, R., Böhme, R., Clark, J., & Demirag, D. (2025). Privacy-enhancing technologies for digital payments: mapping the landscape.BIS Working Papers, No. 1242. Available at: https://www.bis.org/publ/work1242.pdf

interacting with Euros at many existing banks (either cash or digitally), deposits are not subject to the same level of investigation. The receiving bank will know the transactions in the user's account, but are not expected to know the complete transaction history associated with any deposit made. We accept that due diligence should be applied as to the 'source of funds', but that should not require the knowledge of an entire transaction history.

8. We understand the necessity of ensuring proper due diligence on financial service customers, but **we question whether the language used in these frameworks is consistent with existing data protection legislation, and associated data protection and information security standards, guidelines, and recommendations.**

9. We urge the EDPB to clarify how developers and deployers should navigate the current compliance juxtaposition, as we feel it has led to crypto-asset service providers and financial service providers feeling they are unable to provide services related to privacy-preserving DLT systems (or "zero-knowledge blockchains"), which negatively impacts the overarching privacy and data protection landscape in Europe and, potentially, has ramifications for how DLT systems will be integrated into the European information technology ecosystem.

10. To further clarify the above point, we would like to draw attention to guidance from adjacent entities, such as the European Cybersecurity Agency (ENISA), the Spanish Data Protection Board (AEPD), the European Parliamentary Research Service (EPRS), and standards organisations such as the International Standards Organization (ISO).

11. **The EDPB should unequivocally acknowledge that technological methods for protecting personal data in DLT systems should be classified as 'pseudonymisation techniques'. This perspective is supported by the European Cybersecurity Agency (ENISA).**[6] Techniques such as Asymmetric Encryption, Ring Signatures, Group Pseudonyms (Group Membership schemes), Merkle Trees, Cryptographic Accumulators, Zero-Knowledge Proofs, etc are all used in varying degrees within DLT systems – especially privacy-preserving DLT systems (or "zero-knowledge blockchains"). They are classified as "advanced pseudonymisation techniques" by ENISA.

12. Further to the above, **it should be clearly stated that such functions, in the interest of data protection, should be deployed as "inbuilt-functions".** For the majority of these technologies to work effectively, from a data protection and privacy perspective, they are required to be deployed at the protocol layer.[7] This is critical, given the immutable and public nature of many DLT systems. **To avoid all ambiguity, it should also be clearly stated that when these functions are deployed at the protocol layer, they are "zero-knowledge blockchains".** From our perspective it is not technically feasible to deploy a "zero-knowledge blockchain" without also deploying an "inbuilt anonymisation function" into the protocol.

[6] ENISA, https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases, p.14-22

[7] For a comprehensive overview of the wide range of privacy-enhancing technologies being deployed at the protocl layer, please see: Nardelli, M., De Sclavis, F., & Iezzi, M. (2025). A Hitchhiker's Guide to Privacy-Preserving Cryptocurrencies: A Survey on Anonymity, Confidentiality, and Auditability. arXiv preprint arXiv:2505.21008.

13. Information on technologies is also provided within international reports such as "ISO/TR 23244:2020 Blockchain and distributed ledger technologies — Privacy and personally identifiable information protection considerations"[8], international specifications, in development, such as "ISO/WD 24946.2 Requirements and guidance for improving, preserving, and assessing the privacy capability of DLT systems"[9], and European standards, in development, such as "CEN/CLC JTC 19/WG 3 - Personal identifiable information (PII) in Blockchain and DLT". **Acknowledgement should detail specific technologies available for reducing personal data and privacy related risks when developing, deploying, and using DLT systems.**

14. The implementation of privacy-enhanced technologies into DLT systems has caused compliance risks for obliged entities under AMLR and MiCAR, as 'non-compliance risk' has ensured they prohibit offerings related to systems that have these features 'in-built'. This is due to their classification as "anonymity-enhancing coins" or systems that have "inbuilt anonymity-enhancing functions". **Without clear guidance on these specific technologies (and their application to personal data protection in the DLT ecosystem), implementations of such technologies may be marginalised, vilified, or 'effectively' prohibited (as we are currently seeing in the DLT ecosystem).**

15. **Important privacy-related technologies will be 'effectively prohibited' should clear guidance on their correct application for personal data protection not be provided by the EDPB.** Such technologies might include:

    a. the Taproot signature scheme on Bitcoin[10] (which aggregates signatures to improve privacy and increase anonymity of related transactional information).

    b. network-level routing schemes such as Onion Routing (used on the Bitcoin Lightning Network), and Dandelion+.

    c. group membership-based technologies such as 'MimbleWimble'[11], and/or FCMP++[12].

    This would have substantial implications for overarching data protection and privacy in the DLT ecosystem, impacting a number of domains in which DLT might be deployed such as digital identity, digital product passports, local-energy trading networks, financial products, gaming, and the metaverse.

16. **All the above-mentioned PETs are specific methods designed and deployed to provide users with methods for protecting personal data. However, under current regulations, they are problematic under AMLR and MiCAR.** Entities are unwilling to consider the AMLR and MiCAR compliance risk for privacy-preserving assets. The EDPB should urge DLT systems to include more advanced features, especially as they relate to the

[8] https://www.iso.org/standard/75061.html
[9] https://www.iso.org/standard/88614.html
[10] https://www.kraken.com/learn/what-is-taproot
[11] https://www.elliptic.co/blog/explaining-mimblewimble-the-privacy-upgrade-to-litecoin
[12] https://www.getmonero.org/2024/04/27/fcmps.html

current state of the art, to ensure data protection risks such as 're-identification', 'membership inference', and 'data linkability' are minimised. As the AEPD (along with the EDPB)[13] have noted, hashing as a pseudonymisation technique is not entirely effective, so more advanced technologies are required, especially given the characteristics of DLT systems.

17. **We urge the EPDB to draw attention to this matter, and provide clarity that "inbuilt anonymisation functions" should not be directly targeted for regulation. They should be welcomed – as they provide the necessary (and required) tools to ensure personal data is not published directly on-chain in a public and immutable manner.** They are also integral components of "zero-knowledge blockchains". This should be clearly clarified, so as to not create confusion in the legal interpretation and implementation process.

18. The position outlined above is supported by the European Parliament's own research service[14], who acknowledge the complexity of achieving anonymisation in immutable data sets, especially those that might include direct and indirect identifiers.

19. The position is also supported by the AEPD, who clearly state that many DLT systems have not been built according to data-protection-by-design-and-default methods.[15] Further to this, the EDPB's own guidance on data-protection-by-design-and-default reinforces controllers' obligation to implement appropriate measures to ensure data protection obligations are met.[16] **The EDPB should urge developers and deployers to deploy more advanced data protection features, especially when the DLT systems in question publish direct identifiers, such as public keys (also known as wallet addresses).**

20. If a DLT developer or deployer wishes to ensure personal data (eg., a public key) is not published directly on a public blockchain, it stands to reason they will be required to deploy a privacy-enhancing technology directly within the protocol (ie., an inbuilt privacy-enhancing technology). This means the DLT system:

    a. invokes a non-trivial 'non-compliance risk' for obliged entities under AMLR and MiCAR and creates 'non-compliance risks' regarding data minimisation, necessity and proportionality, due to 'transaction history' obligations, under MiCAR.

    b. ensures the privacy-preserving DLT system is not offered to the public through regulated entities, forcing Europeans to navigate unregulated decentralized exchanges, where the identification of data controllers and processors is sometimes problematic.

## <u>Permissionless and public DLT systems</u>

[13] https://www.edps.europa.eu/sites/default/files/publication/19-10-30_aepd-edps_paper_hash_final_en.pdf
[14] https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf
[15] https://www.aepd.es/guias/Tech-note-blockchain.pdf
[16] https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en

21. **It should be acknowledged by the EDPB that use of public and permissionless systems have wider data protection ramifications for entities** than other types of systems or deployments (private and permissioned, public and permissioned, etc). We urge the EDPB to clearly state this at the forefront of the document.

22. Permissioned chains are most certainly deployed, and maintained, by an entity, or group of entities easily identifiable as the data controller, and/or data processors. Attributing responsibility and accountability is straightforward. **There is no logical reason for data protection principles or rights not to be exercised when dealing with these deployment types, including the rights that have been identified as 'creating non-compliance risks', such as the 'right to deletion', 'right to rectification', or 'right to portability'.**

23. It is not clear why the EDPB does not provide clear guidance that any permissioned chain's deployer should ensure that all data protection rights are respected if personal data is appended to the chain. As **the guidelines clearly state types of data that are classified as personal data (e.g., a public key), then the guidelines should also clearly state that specific PETs should be deployed, including those that may be defined (in other regulations) as 'in-built anonymisation functions'.** This might be included in the Guidance, Para.77 – in which the EDPB urges entities to consider the appropriate PETs to safeguard data subjects.

24. Additionally, it is not entirely clear why the EDPB doe not urge entities that wish to offer services related to public and permissionless systems, to use systems that have applied PETs in an "in-built" manner. **Not formally recommending existing privacy-preserving DLT systems is an oversight that will ultimately harm the European consumer**, as they engage with DLT systems in a broader manner as the ecosystem evolves. Limiting access to these systems will merely increase risks related to public access to personal (and sometimes sensitive) data that is appended on chain, raising risks such as behavioural profiling, financial profiling, targeted advertising, etc – as previously outlines by the BIS in their recent report on privacy in digital payments.[17]

25. We view paragraphs 43 and 44 as problematic for permissionless systems. **Expecting nodes to group together and assume data protection liability is wholly unrealistic, and unworkable, mainly due to the concept, and ideology of 'decentralisation', and the non-territorial character of the DLT networks. Coordinating such activity would be unfeasible in decentralised architectures, and would undermine the permissionless nature of these systems.** It is much more realistic to urge the deployment of privacy-enhancing technologies to mitigate data protection and privacy risks.

26. Moreover, we would like to bring to the EDPB's attention the European Declaration on Digital Rights and Principles for the Digital Decade (2023/C 23/01) which provides, in Article 16, that everyone should have access to digital technologies, products and services that are

[17] Auer, R., Böhme, R., Clark, J., & Demirag, D. (2025). Privacy-enhancing technologies for digital payments: mapping the landscape.BIS Working Papers, No. 1242. Available at: https://www.bis.org/publ/work1242.pdf

**by design safe, secure, and privacy-protective**, resulting in a **high level of confidentiality, integrity, availability and authenticity of the information processed**. The EDPB should make clear that privacy-preserving DLT systems are safe and compliant with EU legislation. This clarification is essential for safeguarding the personal autonomy of EU citizens and fostering technological neutrality in the digital age.

27. Finally, it is worth mentioning that a restrictive approach towards privacy-preserving DLT systems

    a. harms European citizens' privacy by effectively forcing them to transact on transparent and public DLT systems.

    b. ensures Europe will not cultivate privacy-enhancing DLT technologies through invention and implementation, restricting its technological leadership in the data protection realm.

    c. does little to stop criminals from accessing or using privacy-preserving DLY systms.

    d. effectively limits the investigative abilities of law enforcement agencies as they cannot monitor on- and off-ramps in the DLY ecosystem.

28. To conclude, we thank you for taking the time to read our response, and are grateful for the transparent manner in which you published the proposed Guidelines. **As stated, we welcome an inclusive, open, and transparent discussion – preferably in public forums – through which this discussion may take place.** Technological innovation often precedes regulation but that is not to say that regulation, based on common understanding and guiding principles, cannot be conducive to continued technological evolution and innovation, creating harmonious relationships between entities that represent public, private, or open-source initiatives.

29. We are happy for our response to be published publicly, and welcome any questions that you may have. These may be directed at the email provided in the front matter of this response.