DIGITAL
CURRENCIES
GOVERNANCE
GROUP

Response to Public Consultation on the European Data Protection Board's Guidelines 02/2025 On Processing of Personal Data Through Blockchain Technologies

About DCGG

Digital Currencies Governance Group ("DCGG") is a boutique trade association that represents digital assets issuers and service providers in the UK, EU, UAE, LATAM, and Africa. Our mission is to facilitate an open dialogue and encourage communication between policymakers and digital asset experts to support the design of a sound and proportionate regulatory framework.

Background

- On 14 April, the European Data Protection Board (the "**EDPB**") published guidelines on the processing of personal data using blockchain technology (the "**Guidelines**")[1].
- The Guidelines address several issues in a non-linear fashion, which could be grouped into three thematic blocks: *(i)* the data protection risks posed by blockchains; *(ii)* taking those risks into account, necessity assessments as a first line of defence against such risks; and *(iii)* technical and organisational measures that can mitigate data protection risks. Other issues, such as global node distribution and smart contracts, are also addressed.
- On **Data Protection Risks**, the Guidelines start by pointing out that public keys that can be used to identify individuals and the payload of a transaction constitute personal data.
    - The Guidelines outline some tension between data protection principles and blockchains, namely with the principles of purpose limitation, data minimisation and storage limitation.
    - The Guidelines emphasise that the decentralised governance model used by blockchains leads to a multiplicity of actors and roles in the processing of data, warning that this cannot be a reason not to comply with the GDPR. Therefore, the position of data controller and processor vary with the governance model of the blockchain, with the Guidelines showing preference for permissioned blockchains with clearer roles, while suggesting that in public permissionless blockchains, nodes themselves can be considered, in some cases, data controllers.

[1] One must be mindful that the General Data Protection Regulation ("**GDPR**"), although not predating blockchains chronologically, was drafted when blockchain and other DLT technologies had very limited use.

  - The Guidelines also emphasise that the permanence of personal data stored on a blockchain with no practical possibility of deletion as a significant risk.

- Given these risks, the Guidelines emphasise the need for **a necessity assessment** by data controllers, on whether they need blockchains to process data, and, if so, they should prefer for permissioned and/or private blockchains over public and permissionless models.
- Thereafter, the Guidelines suggest a **series of operational and technical measures to mitigate the data protection risks**, including, once again, choice permissioned blockchains over public and permissionless blockchains and, in any case, encryption algorithms, hashing of personal data and cryptographic commitments. The EDPB is cautious and frequently introduces the caveat that the use of any such mitigation measures might not be enough to make a given blockchain compliant.
- On **international transfers**, it is emphasised that blockchain usually involves international data transfer, especially in public blockchains, where nodes, which might be outside the EU, are neither chosen nor vetted, which may "raise compliance concerns".
- On **data retention periods**, the Guidelines emphasise there is no reason to assume that the lifetime of the blockchain is an appropriate data retention period, and data should be deleted when the end of the processing activity is reached.
  - In any case, personal data should be integrated within a blockchain in a way that allows for its deletion at the data subject's request.
- Last but not least, **there is the tension between the right to object to a solely automated decision of Article 22 GDPR and smart contracts** – the data controller should ensure that the safeguards in that provision are satisfied, including the possibility of human intervention, and allowing the data subject to contest the decision, even if the smart contract has already been performed and regardless of what is registered on the blockchain.

Assessment

The Guidelines' Approach to Public Permissionless Blockchains – a Policy Misstep

When laying out data protection governance risks, the Guidelines emphasise that the decentralised governance model used by blockchains leads to a multiplicity of actors and roles in the processing of data, warning that this cannot be a reason not to comply with the GDPR. Therefore, they argue, the position of data controller and processor vary with the governance model of the blockchain.

In particular on permissionless public blockchains, the Guidelines state that, in such cases, it is difficult to ascertain the role of the participants, with nodes carrying out various processing activities and, in some cases, nodes should be qualified as controllers.

In certain cases of public and permissionless blockchains, the Guidelines say that nodes do not act "*on behalf of the controller*" and they do not take any instructions from any controller; on the contrary, they may, in some cases, meaningfully decide to modify purposes and/or essential means to pursue their own objectives (e.g. a decision on forking) in relation to mining and validation activities. As nodes can exercise, in such situations, a decisive influence on the processed transactions or mining, or in deciding on a fork, the EDBP strongly encourages "*the establishment of a consortium or any other type of legal entities among the nodes. This entity, when it exists, would then be the controller of this processing*".

First of all, as the Guidelines themselves acknowledge several times, permissionless blockchains operate without any administrative control or central authority. In case of proof-of-work blockchains, such as Bitcoin, they operate by consensus of the participating validator nodes – the more nodes a certain blockchain has, the lower the likelihood of a given node to be able to control the transactions in a given blockchain. In such cases, the network nodes of a permissionless blockchain cannot be considered data controllers as they do not decide about the purposes of data processing, performing merely technical activities[2].

There is one reason why the first and widely-used blockchains, such as Bitcoin, are public and permissionless by nature – the underlying idea of the blockchain and DLT technologies in general is to provide a public (but not State or company-controlled) ledger that determines which public address owns a certain unit and therefore which address has the legitimacy to transfer it, without the possibility of any central authority reverting a transaction once it is validated.

The Guidelines therefore disown permissionless blockchains in several instances because, in the EDPB's view, the lack of a central authority which can implement data protection rules, namely delete personal data, is a risk to data protection principles. The Guideline's suggestions and views favouring permissioned blockchains make sense in a company or enterprise environment (e.g., a given company wants to deploy a blockchain for supply-chain management or interaction with other businesses), but not for general use of permissionless blockchains, such as Bitcoin or Ethereum.

[2] Shrisha Sapkota, *The Right to be Forgotten and the Immutability of Blockchain Technology,* in Good Law Software Blog, available at https://goodlawsoftware.co.uk/law/the-right-to-be-forgotten-and-the-immutability-of-blockchain-technology/?elementor-preview=5472&ver=1643212792#_ednref34.

Even though the Guidelines themselves fall short of saying, clearly, if permissionless blockchains are, in general, compliant with the GDPR, they do leave room for ambiguity and hint at permissionless blockchains being considered uncompliant with the GDPR by default. We argue that the identification of such a consequence shows a clear misunderstanding of the functioning of public/permissionless blockchains in general - which technical characteristics were not taken into account during the drafting of GDPR, and should certainly not apply to them in the first place. It is not only a policy misstep but would be, in addition, unenforceable.

Why a misstep? To take this conclusion in a direction that would result in public permissionless blockchains being considered uncompliant by default would result in potentially cutting Europe from the global (and borderless) blockchain ecosystem and discouraging the use of public permissionless blockchains which are widely used across the world, such as Bitcoin, Ethereum, Cardano, Solana or TRON for a variety of purposes in various domains, each specific to their respective protocol.

As the EU is trying to position itself as a leading and innovation-friendly jurisdiction in the blockchain space, considering permissionless blockchains uncompliant by default risks creating an environment of mistrust and ambiguity which would push innovation outside of the EU. Furthermore, it creates a reputational risk for the EU itself in this sector, as the EU could be seen as attacking the original, untainted concept of the blockchain as a decentralised and distributed ledger system which cannot be controlled or changed by a single entity. These overreach and reputational concerns are particularly important in a context where the first mover advantage the EU had in the Web3 sector because of MiCA is fading away, as many jurisdictions are moving forward with less prescriptive and burdensome regulatory frameworks and requirements for cryptoassets and blockchain in general.

We would recommend the EDPB to ponder whether it is actually public permissionless blockchains that offer less data protection risks *vis-à-vis* permissioned blockchains. As the GDPR is built upon the assumption that traditional databases have a data controller who can access personal data and make it available or unavailable, one of the reasons blockchains were created was to ensure, through decentralisation, that there is no single point of failure, no “honey pots” for data. While a hacking of a data controller in a permissioned blockchain compromises the information contained therein, the hacking of a single node in a permissionless blockchain does not. Data protection risks also emerge from the existence of unitary data controllers, something that does not exist in a permissionless blockchain – their decentralised and distributed nature actually make them more resilient to data attacks, protecting the data stored therein.

In summary, not only is the disfavour of public permissionless blockchain a risky approach policy-wise but it would also be unenforceable. The Guidelines should therefore take a more nuanced and collaborative approach and consider suggesting a carve-out from the GDPR for public permissionless blockchains, whereby they suggest national authorities refrain from enforcing or enforce more lightly the GDPR framework to public permissionless blockchains in light of the arguments above.

That brings us to the next point, the technical impracticability of the deletion – partial or total – in public permissionless blockchains.

The Impracticability of Partial or Total Deletion of Public Permissionless Blockchains

When the Guidelines remind readers of data protection principles, they emphasise that the principle of storage limitation is at peril, as data deletion at an individual level in a blockchain is challenging. This leads to the conclusion that "*when deletion has not been taken into account by design, this may require deleting the whole blockchain*". On data retention periods, the Guidelines emphasise that blockchain is tamper-proof but that there is no reason to assume that the lifetime of the blockchain is an appropriate data retention period, and data should be deleted when the end of the processing activity is reached. The Guidelines also acknowledge, however, in several instances, that it is impracticable or impossible for a data subject to ask for the deletion of specific "personal data" on a blockchain, in particular, public permissionless blockchains.

And indeed they are right. As the very name blockchain implies, data on a blockchain is grouped into blocks that chain to the existing ledger through a hash, such a hash being created from the data that was in the previous block, and so on. The blocks are then linked to one another chronologically.

Therefore, changes in one block imply changes to the precedent sequence of blocks. This makes the ledger difficult (if not impossible) to tamper with and usually immutable – that is precisely one of the main points of blockchains originally – to be general purpose, immutable and trusted public registries that were not controlled by a public or private entity or intermediary.

Data in permissionless blockchains could be altered or deleted via *forking*, a process in which a new version of a blockchain is created in which the information that was individually deleted is no longer there.

This deletion or destruction of specific data on a blockchain would be, as the Guidelines themselves acknowledge, difficult, as the participants of a given blockchain would have to agree on process to jointly execute a lawful request for deletion and control of at least 51% of the nodes would be required[3].

[3] AMMAR ZAFAR, "Reconciling blockchain technology and data protection laws: regulatory challenges, technical solutions and practical pathways", *Journal of Cybersecurity* (2025), 8; GIANLUIGI MARIA RIVA, "What Happens in Blockchain Stays in Blockchain. A Legal Solution to Conflicts Between Digital

Even in such a case of modification or deletion of blocks, the old block remains to prove the chronology of transactions – someone will most likely keep a copy of the original blockchain[4 & 5].

Additionally, to remove old transactions, the majority of the nodes would have to backwards verify the legitimacy of every affected transaction and unbuild the entire blockchain, which is difficult and uneconomic and would reach a computational limit, due to the exponential increase in computational capacity needed to reverse modify the whole chain[6].

Furthermore, because permissionless blockchains have no effective controller to whom any deletion request or administrative order could be sent to, there is no one to execute a deletion request. One might think about the Bitcoin blockchain – to whom would a data protection NCA address an order? To whom would a data subject request a deletion? To 51% of the nodes of the whole network? That would be impossible.

Faced with the technical difficulties in deleting specific data on a given blockchain, the Guidelines ponder the hypothetical need for a full deletion of the whole blockchain. Not only would that possibility be an ill-advised policy move for the reasons indicated above, but it would also be technically impossible for the reasons outlined for the deletion of individual data – in such blockchains, there is no kill switch, no single person who can delete the whole ledger.

Ledgers and Privacy Rights", *Frontiers in Blockchain* Volume 3 (2020), available at https://www.frontiersin.org/journals/blockchain/articles/10.3389/fbloc.2020.00036/full; Shrisha Sapkota, *The Right to be Forgotten and the Immutability of Blockchain Technology,* in Good Law Software Blog, available at https://goodlawsoftware.co.uk/law/the-right-to-be-forgotten-and-the-immutability-of-blockchain-technology/?elementor-preview=5472&ver=1643212792#_ednref34.

[4] Gianluigi Maria Riva, "What Happens in Blockchain Stays in Blockchain. A Legal Solution to Conflicts Between Digital Ledgers and Privacy Rights", *Frontiers in Blockchain* Volume 3 (2020), available at https://www.frontiersin.org/journals/blockchain/articles/10.3389/fbloc.2020.00036/full

[5] A good example would be the 2016 Ethereum DAO fork, which followed the hacking of USD 60 million in Ether – such "hacking" had been an exploitation of the DAO's code and therefore fully legitimate under the rules of the Ethereum blockchain, though it was widely known it was an attack. The Ethereum community held a controversial vote to decide on whether a hard fork that would revert the "hack" through the modification of previous blocks would be implemented or not. Although a majority of the community decided to revert the "hack", the original blockchain still continued as Ethereum Classic. This shows how difficult it is to erase past blocks. For more details, see https://www.coindesk.com/consensus-magazine/2023/05/09/coindesk-turns-10-how-the-dao-hack-changed-ethereum-and-crypto.

[6] Gianluigi Maria Riva, "What Happens in Blockchain Stays in Blockchain. A Legal Solution to Conflicts Between Digital Ledgers and Privacy Rights", *Frontiers in Blockchain* Volume 3 (2020), available at https://www.frontiersin.org/journals/blockchain/articles/10.3389/fbloc.2020.00036/full; Shrisha Sapkota, *The Right to be Forgotten and the Immutability of Blockchain Technology,* in Good Law Software Blog, available at https://goodlawsoftware.co.uk/law/the-right-to-be-forgotten-and-the-immutability-of-blockchain-technology/?elementor-preview=5472&ver=1643212792#_ednref34; Ammar Zafar, "Reconciling blockchain technology and data protection laws: regulatory challenges, technical solutions and practical pathways", *Journal of Cybersecurity* (2025), 8.

The EDPB does therefore need to consider a more balanced approach to public permissionless blockchains, especially existing ones. Many of them, such as Bitcoin and Ethereum, are an integral part of the global Web3 ecosystem and support many other applications and tokens. A more pragmatic approach that recognises the impossibility of tampering with permissionless blockchains is highly recommended, together with a possible exemption of blockchains in a future targeted review of GDPR.

The Impracticability of Human Intervention to Contest or Override Smart Contracts

The Guidelines state that, when the execution of a smart contract is an automated decision (which is generally the case) and, when such automated decisions fall into the scope of Article 22 of the GDPR (which enshrines the right of the data subject not to be subject to a decision based solely on automated processing) the data controller *“should ensure that the safeguards in that provision are satisfied, including the possibility of human intervention, and allowing the data subject to contest the decision, even if the smart contract has already been performed and regardless of what is registered on the blockchain.”*

The requirement for the possibility of human override in the context of smart contracts, as outlined in Article 22 of the GDPR, presents both technical and conceptual challenges and this requirement is not only technically impracticable and even impossible, but also conceptually very problematic.

The technical challenges of blockchain deletion and its immutability are also present in smart contracts, which function on top of a blockchain - therefore, many of the technical issues are addressed.

The first challenge concerns irreversibility - once a smart contract is deployed on a blockchain, it is immutable and cannot be altered. This means that any decision made by the smart contract is final and cannot be changed, even if a human override is desired; also, as blockchains, namely public and permissionless blockchains, are decentralised and rely on consensus mechanisms to validate and execute transactions. In such cases no single entity has control over the entire network, making the implementation of a human override mechanism unfeasible and, even if possible, such an option would disrupt the consensus mechanisms that underpin blockchains.

More specifically, smart contracts are characterised by autonomy and automation - they are designed to execute automatically when predefined conditions are met - as this autonomy is a core feature of smart contracts, introducing human intervention would undermine their purpose and functionality, and put users at risk due to the possibility to tamper with such contracts. This goes hand in hand with the speed and efficiency objectives of smart contracts - part of the reason for their automation and self-executing nature is precisely to foster speedy execution without the need for human intervention, something that would be hindered by the introduction of a human override.

Besides the technical challenges, there are important conceptual challenges in implementing a human override option in smart contracts. Smart contracts are meant to be self-executing so that they can operate in a trustless environment, allowing parties who do not trust each other to interact without the need for intermediaries - the strict but transparent “code is law” ethos underlying smart contracts provides them with their appeal - all parties know what the code provides and agree to enter into such contract in order to mitigate human fallibility in executing “normal” contracts. Human intervention would severely undermine this trust and the very rationale to resort to smart contracts.

Finally, implementing a human override mechanism in a decentralized and immutable system would be complex and costly. It would require significant changes to the underlying technology and could introduce new vulnerabilities and risks. Also (but this applies for blockchain in general) there is a jurisdictional issue when determining applicable law and the person required to implement the human override - in a global environment by nature.

The requirement for human override in the context of smart contracts presents significant technical and conceptual challenges. The immutability, autonomy, and decentralisation of blockchain technology make it technically infeasible to implement such a requirement. Conceptually, it undermines the self-executing and transparency principles underpinning smart contracts as well as their efficiency. Balancing regulatory compliance with technological innovation remains a key challenge in the evolving landscape of data protection and blockchain, which naturally calls for an exemption of public/permissionless blockchains in a future targeted review of GDPR.

Looking Beyond the Proposed Technical and Organisational Measures

The Guidelines indicate that, despite the pseudonymous and cryptographic nature of the blockchain, if the user is a natural person, public keys can still be used to identify individuals by “*means reasonably likely to be used (…) in case of a data breach, then those identifiers qualify as personal data*”, such data being usually visible to all participants in order to fulfil and validate transactions. When developing the processing of personal data on blockchains, the Guidelines remind that, pursuant to Article 25(2) GDPR, controllers must implement technical and organisational measures to ensure personal data is not made accessible without the data subject's intervention.

The Guidelines then propose a number of technical and organisational measures that can be implemented when designing blockchains, namely "state-of-the-art encryption algorithms and keys" (though the EDPB recalls that encrypted personal data is still personal data and that encryption alone does not remove the need for GDPR compliance, and that decryption techniques evolve), hashing of personal data (though the Guidelines say the hash will also be considered personal data and the GDPR will still apply to that processing activity); and cryptographic commitments (i.e., cryptographic protocols that enable one to commit to a chosen value while keeping it hidden to others, with the ability to reveal the committed value later – in this case, the Guidelines argue that they can be used to store the personal data off-chain and the commitment on-chain), showing preference for the latter.

While hashing and cryptographic commitments are adequate tools to render personal data on a blockchain less accessible or inaccessible, there are already additional mechanisms that can be implemented and used to enhance users' privacy, such as tumblers and mixers or privacy coins.

Tumblers and mixers[7] – a cryptoasset tumbler or mixer is a service that mixes several streams of traceable cryptoasset units together, breaking the connection between a given wallet from where the units originated, rendering access to the user's public key difficult.

Tumblers and mixers offer anonymity and enhance user privacy because they break the link between the user's transaction and their wallet and make financial transactions untraceable on the public ledger.

Even though tumblers and mixers have no clear legislative framework in the EU, the concerns raised by the EDPB on the protection of personal data on the blockchain should foster an open-minded discussion about the legitimacy of the use of tumblers and mixers who can be subject to a balanced regime which ensures they are a usable tool to enhance privacy on blockchains while at the same time avoid making them a vessel for money laundering, financing of terrorism or criminal activities.

[7] Tumblers and mixers work as follows – instead of User A sending cryptoassets directly to User B (which would be easily identifiable), User A sends their cryptoassets to a mixer's address, registered for each user individually; the cryptoassets are then mixed (and usually divided into smaller fractions before mixing) with transactions of other users or distributed among wallets belonging to the mixer; and, once the process is completed, cryptoassets are transferred to the predetermined address of User B. Depending on whether they are owned or controlled by a specific entity or not, tumblers and mixers can be centralised or decentralised or custodial or non-custodial, the latter relying on smart contracts.

Privacy coins – privacy coins (or anonymity enhanced coins) are cryptoassets designed to enhance user privacy and anonymity, obscuring transaction details through cryptographic techniques and making traceability difficult.

These privacy coins use a variety of methods to enhance user anonymity, such as: (i) ring signatures to hide the true sender by mixing their transaction with other transactions (like a tumbler or mixer); (ii) stealth addresses, generating one time addresses for every transaction and preventing public wallet addresses from appearing on the public ledger; (iii) zero-knowledge proofs, which uses cryptography to enable one party to prove to another that a transaction is valid without revealing the details of the transaction.[8]

Though privacy coins have proven potential to mitigate the data protection risks outlined in the Guidelines, the EU is moving towards an effective ban of privacy coins. Article 79 of the new 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 systems for the purposes of money laundering or terrorist financing (also known as AML Regulation), which shall apply from 10 July 2027 on, prohibits anonymous accounts (including for crypto) very strictly and decisively, stating that *"…credit institutions, financial institutions and crypto-asset service providers shall be prohibited from keeping anonymous bank and payment accounts, anonymous passbooks, anonymous safe-deposit boxes or anonymous crypto-asset accounts as well as any account otherwise allowing for the anonymisation of the customer account holder or the anonymisation or increased obfuscation of transactions, including through anonymity-enhancing coins*". However, Article 79 only applies to CASPs such as exchanges, and does not ban users from using privacy coins and is not applicable to manufacturers of cold or hot wallets, as they have no control over the content of such wallets.

This shows a fundamental contradiction and lack of consistency in the EU's existing crypto policy – on the one hand, data protection principles are said to collide with the transparent and public nature of the blockchain; on the other hand, attempts at making transactions more private and anonymous raise AML/CFT concerns. We see two diametrically opposed approaches and objectives.

The EDPB should take this into account and show openness, in principle, to the use of more popular privacy-enhancing technology such as tumblers and mixers as well as privacy coins, highlighting their potential to mitigate data protection risks while, of course, alerting to the potential AML/CFT concerns they raise.

[8] Use cases of these technologies include ZKLogin, which allows users to sign into Apps built on the Sui blockchain, using invisible wallets, where interacting with the chain is fully abstracted from the user or offer an easier way for users to access their on-chain assets (https://sui.io/zklogin); and Concordium, a privacy-focused layer 1 blockchain with ID frameworks which allows businesses to interact while complying with GDPR. (https://www.concordium.com/article/gdpr-and-eprivacy-directive)

The EDPB should also distinguish in practice between public permissionless blockchains, and their decentralised, non-custodial nature, from private permissioned blockchains which may be unilaterally governed by a person or entity. Given the vast difference between public and private blockchain code and how these unique technologies operate, we urge the EDPB to consider solutions that will not impose a one-size-fits-all approach, but rather serve to sustain the EU's role as a leader in blockchain innovation.

The input to this response has been curated through member discussions and industry engagement. We remain available at your disposal for further questions or clarifications at info@dcgg.eu