Pınar Çağlayan Aksoy

Associate Professor of Civil Law at Bilkent University, *Avukat*, Member of Meta MENAT Privacy Expert Group

Hüseyin Can Aksoy

Associate Professor at Bilkent University Faculty of Law, *Avukat*, Member of Meta MENAT Privacy Expert Group

Luigi Cantisani

Ph.D. Candidate at the University of Warwick, and *Avvocato* at Futura Law Firm

Misaligned Frameworks: A Critical Examination of EDPB Guidelines 02/2025 on Blockchain and Personal Data Processing[1]

1. Introduction

1.1. The European Data Protection Board's (EDPB) Guidelines 02/2025 aim to provide clarity on processing personal data through blockchain technologies under the General Data Protection Regulation (GDPR). The issue of alignment with data protection laws has been discussed by many lawyers working on the blockchain realm. There have been many articles and reports addressing the tension between the GDPR and blockchain. Key areas of tension include, but are not limited to: challenges in enforcing data subjects' rights—such as the 'right to be forgotten'—given the immutability of public blockchains; difficulties in clearly defining roles and responsibilities within the public blockchain data processing ecosystem, especially in identifying data controllers and processors; and uncertainties about which laws apply due to the decentralized nature of blockchains. There has been a study carried out in 2023 (two years ago from the writing of this note) which relies on a systematic literature review of 114 research papers discussing and/or addressing such the tension between data protection laws and blockchain, which shows how big an impact this issue has.[2]

---

[1] Although the work is the result of joint collaboration, authorship is divided as follows: Pınar Çağlayan Aksoy and Hüseyin Can Aksoy co-authored sections 1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 5.1, 6.1, 7.1, 7.2, 8.1, 9.1, 10.1, 11.1, and 11.7. Luigi Cantisani authored sections 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 3.1, 3.2, 3.3, 3.4, 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 5.2, 9.2, 11.2, 11.3, 11.4, 11.5. Pınar Çağlayan Aksoy, Hüseyin Can Aksoy, and Luigi Cantisani co-authored section 11.6. The author wishes to thank Pietro Calorio, Lawyer and Founder at CDM Studio Legale, for reviewing the content and providing valuable comments. All views expressed in this document remain the sole responsibility of the author. The author wishes to thank Pietro Calorio, Lawyer and Founder at CDM Studio Legale, for reviewing the content and providing valuable comments. All views expressed in this document remain the sole responsibility of the author.

[2] See *Rahime Belen-Saglam, Enes Altuncu, Yang Lu, Shujun Li: A systematic literature review of the tension between the GDPR and public blockchain systems, Blockchain: Research and Applications, Volume 4, Issue 2, 2023, 100129, ISSN 2096-7209,* https://doi.org/10.1016/j.bcra.2023.100129 (https://www.sciencedirect.com/science/article/pii/S2096720923000040).

1.2. The EU itself has also been focusing on this intersection and tension since 2019.[3] Considering the underlying logic of the GDPR, the immutability of blockchain technology poses a direct challenge to the rights of data rectification and erasure (Articles 16 and 17 GDPR). Moreover, the decentralized structure of blockchain complicates compliance with core GDPR principles such as data minimization, storage limitation (Article 5), and data protection by design (Article 25). Cross-border data transfers also present significant challenges in this context.

1.3. While critically engaging with the EDPB's Guidelines on Data Protection and Blockchain, it is important to acknowledge that several national data protection authorities within the EU had already begun grappling with these issues well before the EDPB's intervention. For instance, France's CNIL was among the first to issue a comprehensive analysis of blockchain's compatibility with the GDPR. Similarly, the Spanish data protection authority (AEPD) published a detailed report in 2018 addressing the legal challenges posed by blockchain, especially in relation to data subject rights and the identification of data controllers. In Germany, both the Federal Commissioner for Data Protection and Freedom of Information (BfDI) and various regional authorities (such as the Bavarian DPA) have examined blockchain in the context of GDPR compliance, focusing particularly on data minimization and the legal qualification of hashed data. The Italian Data Protection Authority (Garante) has also discussed the implications of blockchain-based smart contracts and their interaction with privacy principles. Additionally, the Austrian Data Protection Authority (DSB) has provided guidance on blockchain's immutability and its potential conflict with erasure rights under Article 17 GDPR. These national-level efforts underscore the decentralized and diverse regulatory approaches taken by EU member states in tackling the tension between blockchain technology and European data protection law, often predating and informing the EDPB's eventual stance. Receiving specific advice on how the GDPR applies to blockchain technologies across the EU from the EDPB would prevent the fragmentation that arises from national initiatives (the different interpretation of core GDPR concepts by different supervisory authorities within the EU).

1.4. In a recent article that was published in 2025, the author draws attention to the urgency of finding a solution to the problem of GDPR compliance. The author writes: *"A central finding of this study is* ***the urgent need for legal clarity regarding the application of European data protection laws to blockchain technologies****. This uncertainty stems from two primary factors: first, blockchain's inherent technical structure and governance models often clash with established legal requirements; second, applying the GDPR to blockchain technologies exposes broader ambiguities in how the regulation is interpreted and applied. The GDPR, built on broad principles, aims to be flexible and adaptable in an era of rapid technological change. However, this flexibility*

[3] See Michèle Finck, *Blockchain and the General Data Protection Regulation Can distributed ledgers be squared with European data protection law?*, a study written (at the request of the Panel for the Future of Science and Technology (STOA) and managed by the Scientific Foresight Unit, within the Directorate-General for Parliamentary Research Services (EPRS) of the Secretariat of the European Parliament, available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf).

also makes it difficult to determine how specific provisions should be applied in particular contexts.[4]

1.5. Taking all this background into account, while the intent of the EDPB is commendable, the guidelines exhibit a disconnect from the operational realities of blockchain systems, potentially hindering innovation and practical compliance.

2. Overlooking the Immutable Nature of Blockchain

2.1. A fundamental characteristic of blockchain is its immutability; once data is recorded, it cannot be altered or deleted. The guidelines suggest that to comply with the right to erasure, one might need to delete the entire blockchain—a proposition that is both impractical and contrary to the technology's design principles. As noted by Marina Markezic of the European Crypto Initiative, this is akin to "*asking to delete the internet to enforce privacy.*"[5]

2.2. The comparison is entirely accurate. **The fundamental mistake lies in treating blockchains merely as distributed databases**. In reality, blockchains, and other forms of public and permissionless distributed ledgers, go beyond this: **they are distributed open networks, much like the internet itself**. However, they operate on top of the internet and are maintained by nodes, much like the internet is.

2.3. The concept of distributed networks emerged in the 1960s. In 1964, Paul Baran demonstrated that information could be split into packets, transmitted separately, and reassembled—an idea that laid the groundwork for ARPAnet, the first computer network launched by the U.S. Department of Defense. Connecting a few research universities, ARPAnet enabled remote file sharing through a system of nodes and communication protocols—the core model still underpinning today's networks.

2.4. In the 1970s and 1980s, both public and private actors began developing their own communication networks, often incompatible with one another due to proprietary protocols. To resolve this, the Internetting Project introduced the TCP/IP protocol suite (adopted in 1983), which enabled different networks to interoperate. This marked the birth of the internet: an open network of networks, defined by standard protocols and decentralized nodes.

2.5. While the internet evolved primarily through client-server architectures, early peer-to-peer (P2P) networks—such as USENET (1979) and later Napster (1999)—pushed the model further. In the early 2000s, BitTorrent adopted this approach with a distributed protocol for file sharing, while Tor introduced an anonymity-focused network built on layered encryption and voluntary relay nodes.

2.6. A major shift came in 2008 with the launch of Bitcoin, the first blockchain architecture network. Unlike previous open networks, a blockchain is a network that integrates a

---

[4] See Ammar Zafar, *Reconciling blockchain technology and data protection laws: regulatory challenges, technical solutions, and practical pathways, Journal of Cybersecurity, Volume 11, Issue 1, 2025, tyaf002,* https://doi.org/10.1093/cybsec/tyaf002.

[5] See, Fatemeh Fannizadeh, *EU privacy laws to delete see-through blockchains, in Forbes, Digital Asset*s, 2025, May 1, 2025, available at https://www.forbes.com/sites/digital-assets/2025/05/01/eu-privacy-laws-to-delete-see-through-blockchains/.

payment system and a native currency, while relying on no central institution to update or validate the ledger. Instead, the ledger is maintained in a decentralised manner by the network's nodes through a consensus mechanism. When it is said that a blockchain ledger is 'immutable,' this should not be taken in a literal or absolute sense. Rather, it means that any modification which contradicts the recorded movement of assets cannot occur unless it is approved by a majority—typically 51%—of the network's participants. For example, Ethereum's ledger was altered following the exploit of smart contract underpinning 'The DAO' in 2016. The community, through a coordinated hard fork, chose to revert the effects of the attack, effectively rewriting part of the ledger's history. This illustrates that immutability in blockchain systems is best understood as conditional and subject to social consensus, not as an unbreakable technical property.

2.7. Today, there are numerous blockchain networks, such as Ethereum, Polkadot, and Solana, etc. —each with its own communication protocol, consensus mechanisms, and applications compatible with them. While these networks are independent, interoperability is possible through so-called bridges, which facilitate the transfer of assets or data across chains.

2.8. The above suggests that, as it would be unreasonable to demand the erasure of the internet to enforce privacy rights, it is equally misguided to call for the erasure of a public, permissionless blockchain maintained by tens of thousands of nodes across the globe. Instead, attention should shift to those who build services, platforms, or applications on top of blockchain networks and who actively process personal data that are possibly stored in a chain. These are the actors responsible for the potential introduction of personal information into blockchain environments. Blockchains themselves were never meant to store personal data. It is actually the opposite: blockchains' foundations were intended by the cypherpunk movement to disintermediate central entities, banks, and institutions, and allow individuals to transact on a peer-to-peer basis through privacy-preserving technology. As a matter of fact, even when transactional data is publicly visible—such as wallet addresses on a public ledger—this information alone does not identify an individual unless matched with additional data. The most compelling example of this is Satoshi Nakamoto: whether a person or a group, despite the full transparency of the Bitcoin blockchain, his/her/their true identity remains unknown.

3. Reassessing WP29 Opinion 05/2014 in Light of Recent CJEU Case Law

3.1. The WP29 Opinion 05/2014[6] considered hash functions—widely used by design in blockchains as a privacy-preserving mechanism—as a technique of pseudonymisation rather than anonymisation. A closer reading of Opinion 05/2014 shows that all examples used to support its classification of hashing as pseudonymisation presuppose the presence of an actor who has access not only to the hashed value but also to an external dataset containing at least one data point that allows re-identification. In such

[6] Article 29 Data Protection Working Party, *Opinion 05/2014 on Anonymisation Techniques, Adopted on 10 April 2014,* 0829/14/EN WP216 Available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

scenarios, the actor can iterate through potential inputs to the hash function and compare them against the external dataset to identify a match. This is not the case in most public blockchain networks. On the blockchains (which, we reiterate, are networks, not the platforms or services built on top of such networks), there is typically no actor with additional identifying information about users, and no external datasets involved. This explains why, to this day, no one has been able to identify Satoshi Nakamoto.

3.2. This **'substance over form' approach to identifiability**, where the broader informational environment must be considered, has been further clarified by the Court of Justice of the European Union (CJEU) in recent years. In *Breyer v Germany*,[7] the Court interpreted the definition of personal data under Directive 95/46/EC in a case concerning dynamic IP addresses. It found that although such addresses do not allow identification by the online service provider alone, they could qualify as personal data if combined with additional information held by a third party (in that case, the internet service provider). The Court emphasised that **re-identification must be reasonably feasible, considering time, cost, and manpower, from the perspective of the data controller in question**. In *Breyer*, the online service provider lacked access to that additional information, and therefore, the IP address, in its hands, was not personal data.

3.3. More recently in *SRB v EDPS*,[8] a case involving the sharing of alphanumeric codes referring to individuals with third parties, the General Court aimed at clarifying the legal test. It rejected a purely theoretical approach to re-identification, ruling instead that what matters is the realistic **likelihood of re-identification in practice**. If the recipient lacks access to any additional information enabling identification, and has no legal or practical means of obtaining such data, the shared data should be considered anonymous.

3.4. Taken together, recent developments in EU case law offer useful guidance for reinterpreting WP29 Opinion 05/2014. In light of this, it is submitted that when data is processed exclusively on a public blockchain—such as Bitcoin or Ethereum—and no additional user information is available, such data should not be classified as personal under the GDPR. This applies as long as no additional data processing activity is carried out that could reasonably lead to data subjects' identification. The term 'exclusively on a public blockchain' refers to processing that begins and ends within the digital environment of a public and permissionless blockchain, without involving external systems or datasets. This distinction is essential. If, for example, the provider of a blockchain-based platform or service collects user data beyond the wallet address—such as an email, name, or other identifying information—the provider (if identifiable) could establish a link between the wallet and a real individual. In that scenario, the wallet address would likely lose its (substantially) anonymous character and fall within the GDPR's scope.

---

[7] C-582/14, EU:C:2016:779, paragraphs 45-78, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62014CC0582.

[8] Case T-557/20, ECLI:EU:T:2023:219, paragraphs 76-106, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62020TJ0557.

3.5. As Mikołaj Barczentewicz, Associate Professor in Law at the University of Surrey, correctly remind us, "*There are many nuances to this, including a debate whether data is personal to you only if you (and not just someone else) are reasonably likely to link the data to an individual*" (See Mikołaj Barczentewicz, *Does the EU GDPR make public blockchains illegal?*, May 19, 2025, available at https://goodcrypto.net/does-the-eu-gdpr-make-public-blockchains-illegal/). In sum, one should assess on a case-by-case basis whether a data subject is not or no longer identifiable in practice, thereby meeting the threshold of anonymity under Recital 26 of the GDPR—even if, from a purely technical standpoint, the technique adopted qualifies as pseudonymisation.

4. Blockchains as the Internet of Value

4.1. It is important to consider not only that blockchains are open networks structurally analogous to the internet and operating on top of it, but also that they represent an entirely new kind of network. First described by the industry and now increasingly recognised in academic literature, blockchains have been termed the 'Internet of Value', a kind of network that natively embeds, without the need for additional technological layers or intermediaries, functions enabling the transfer of assets.[9] In contrast to the internet, which transmits data only unless other layers are built on top of it, blockchains are natively capable of representing and transferring value.

4.2. This has had a profound impact on the development of alternative financial markets outside the traditional system—markets which are now also regulated within the EU. These include crypto-asset markets covered Regulation (EU) 2023/114 on Markets in Crypto-Assets ('MiCA'), as well as tokenised financial instruments falling under the Directive 2014/65/EU on Markets in Financial Instruments ('MiFID II') and the Regulation (EU) 2022/858 on a Pilot Regime for Market Infrastructures based on Distributed Ledger Technology ('DLT Pilot Regime').

4.3. Even hypothetically mandating the technical erasure of a blockchain network would entail erasing the native crypto-assets that underpin the economic logic of these networks (e.g. BTC for Bitcoin, ETH for Ethereum, SOL for Solana), as well as disrupting the operation of token issuers and platforms/services that facilitate circulating and trading crypto-assets.

4.4. Furthermore, widely used stablecoins are increasingly integrated into global financial markets. In 2024, the issuers of USDT and USDC— respectively Tether and Circle—collectively purchased close to $40 billion in US Treasury bills to back the reserves underlying their stablecoins.[10] This amount exceeded China's holdings over the

---

[9] See Hasse, F., von Perfall, A., Hillebrand, T., Smole, E., Lay, L., & Charlet, M., 2016, *Blockchain-an opportunity for energy producers and consumers?*, Pricewaterhousecoopers: Technical report; Ripple, 2017, *The internet of value: What it means and how it benefits everyone*; Vadgama, N., Xu, J., & Tasca, P., 2022, *Enabling the Internet of Value How Blockchain Connects Global Businesses: How Blockchain Connects Global Businesses*, 10.1007/978-3-030-78184-2.

[10] See Ahmed, R., and Iñaki A., *Stablecoins and Safe Asset Prices*, BIS Working Papers No. 1270, Basel: Bank for International Settlements, Monetary and Economic Department, May 2025, p. 2, available at https://www.bis.org/publ/work1270.htm).

same period, placing these issuers among the largest private holders of US sovereign debt. Such figures underscore the systemic relevance stablecoins are acquiring, not only as digital payment instruments but as major conduits of demand for safe and liquid assets.

4.5. In sum, if privacy laws were to be applied in a way that requires the erasure of blockchains, this could result in the dismantling of an entire generation of startups and fintech firms operating under the latest financial regulatory frameworks. Economic actors affected would include:

(a) Issuers of asset-referenced tokens (ARTs) and e-money tokens (ETMs), the two categories of stablecoins regulated under MiCA;
(b) Issuers of crypto-assets other than ARTs and ETMs, including utility tokens;
(c) Crypto-asset service providers (CASPs), which are making substantial investments in infrastructure, human resources, and legal compliance to be authorised under the MiCA framework;
(d) 'DLT market infrastructures' under the DLT Pilot Regime, which are slowly emerging as financial players authorized to provide multilateral trading facilities and settling systems for tokens qualifying as financial instruments under MiFID II.

4.6. Financial instruments derived from crypto-assets—such as exchange-traded funds (ETFs), futures and options contracts—are also becoming increasingly common, and would be impacted by measures targeting the underpinning blockchain networks.

4.7. In addition, it is important to consider similar legislative initiatives emerging globally, aimed at regulating crypto-asset markets and tokenised securities—such as the UK's Digital Securities Sandbox and the GENIUS Act currently under development in the United States.

4.8. Removing even a single public permissionless blockchain could severely undermine the stability of this parallel global financial ecosystem, triggering cascading effects that may extend well beyond the token space and into the traditional financial system—with consequences that remain difficult to fully foresee. Even with advance notice, the risk of a crisis of confidence—prompting a mass withdrawal or conversion of crypto-assets—could result in severe and potentially systemic disruption.

4.9. **Proportionality is therefore crucial**: the protection of the privacy of individuals should not come at the cost of global financial stability, nor should it end up harming the very individuals it seeks to protect.

5. Inadequate Consideration of Decentralized Architectures

5.1. The guidelines emphasize clear delineation of roles, such as data controllers and processors. However, in decentralized, permissionless blockchains, participants often operate anonymously and without centralized control, making such classifications challenging (not to mention that, if no data processing is involved, talking about roles is sterile). The suggestion to form legal entities or consortia to assume these roles may not align with the decentralized ethos of blockchain networks.

5.2. The suggestion to form legal entities or consortia also seem unfeasible on a widely distributed network. Based on estimations by Bitcoin Core developer Luke Dash Jr, about 83,000 Bitcoin Core nodes were active in January 2021, during the so-called 'bull market' phase, while recording a steep decline in 2022 to roughly 50,000.[11] Getting to know the exact number is impossible because, through the so-called crawler, it is possible to calculate only the number of the 'reachable nodes', meaning nodes accepting inbound traffic. Many nodes, by contrast, are considered 'unreachable,' meaning they do not accept incoming connections, even though they remain active participants in the network. This happens when the node runs behind a router or security layer that blocks unsolicited inbound traffic (e.g. NAT, firewall). It can still connect to other nodes but cannot be connected to directly. In addition, some nodes are configured to operate exclusively through the Tor network. These nodes are fully functional—they propagate transactions and blocks—but remain hidden from IP-based network scanners and public node maps. This underscores why the proposal to form legal entities or consortia is not only impractical, but also unenforceable. In many cases, it is simply unknown who operates the nodes, where they are located. The majority of nodes may in fact be deliberately configured to prevent inbound connections or to operate exclusively over privacy-preserving networks such as Tor. This also highlights that, even if one were to argue in favour of enforcing data erasure obligations on blockchain infrastructure, the practical feasibility of such enforcement appears negligible. When a substantial proportion of the network is effectively shielded from identification and geolocation, any meaningful implementation becomes unrealistic. Worse still, public efforts to mandate such measures could further incentivise operators to adopt stronger anonymity practices, leading to even lower network transparency and reducing—not increasing—the effectiveness of regulatory oversight.

6. Limited Practical Solutions for Data Subject Rights

6.1. While the guidelines recommend off-chain storage and advanced cryptographic techniques to uphold data subject rights, they fall short in addressing scenarios where on-chain data is essential. The reliance on off-chain solutions may not always be feasible, especially in applications where transparency and decentralization are paramount.

7. Potential Stifling of Innovation

7.1. By advocating for permissioned blockchains over public ones and discouraging on-chain storage of personal data, the guidelines may inadvertently stifle innovation. Public blockchains play a crucial role in various sectors, primarily fintech, and overly restrictive guidelines could deter their adoption in the EU, pushing innovation to more permissive jurisdictions.

7.2. According to the guideline, "*As a general rule, storing personal data on a blockchain should be avoided, if this conflicts with data protection principles.*" However, this

[11] So reported by Guneet Kaur, *What is a Bitcoin node? A beginner's guide on blockchain nodes*, in *Cointelegraph*, August 19, 2023, available at https://cointelegraph.com/learn/articles/what-is-a-bitcoin-node-a-beginners-guide-on-blockchain-nodes.

general rule lacks sufficient nuance and fails to acknowledge that in many legitimate blockchain use cases—such as decentralized identity systems, notarization services, and public transparency registries—on-chain storage is not only functionally necessary but also legally defensible under a contextual, risk-based interpretation of the GDPR. Such a blanket discouragement may have a chilling effect on EU-based innovation, despite the GDPR's own emphasis on proportionality, necessity, data protection by design, and, importantly, on free movement of personal data.

8. Need for a More Nuanced Approach

8.1. The guidelines adopt a one-size-fits-all approach, not accounting for the diversity of blockchains and their applications. A more nuanced framework that considers the specific context, purpose, and design of blockchain systems would be more effective in balancing data protection with technological advancement.

9. International Data Transfers

9.1. The guidelines note that blockchain often entails international data transfers and suggest using mechanisms like standard contractual clauses before accepting a node. However, this overlooks the structural reality of public blockchains, where nodes are potentially unidentifiable, dynamic, and not subject to centralized control. Requiring formal agreements in such contexts is impractical and would effectively exclude major public blockchains from lawful use in the EU. Instead of imposing infeasible obligations, the Guidelines should have proposed realistic, risk-based solutions tailored to decentralized architectures.

9.2. To reinforce the previous argument, a parallel can be drawn from the financial regulatory domain, where the European Securities and Markets Authority (ESMA) has clarified that the use of permissionless distributed ledger technology (DLT) does not constitute an outsourcing arrangement under Article 73 of MiCA. This is because no contractual relationship—such as a service-level agreement—exists between the crypto-asset service provider (CASP) and the decentralized blockchain infrastructure. In such cases, the network functions as a neutral, open-access infrastructure, more akin to a 'common good' than a third-party provider. By contrast, permissioned DLT systems operated by identifiable commercial entities may fall within the scope of outsourcing obligations, precisely because they involve a formal service relationship. This distinction is highly relevant in the data protection context as well. Treating nodes on public blockchains as data processors requiring prior contractual safeguards—such as standard contractual clauses—not only misconstrues the nature of these systems but also imposes obligations that simply cannot be met in practice.[12]

10. The Implementation Problem

10.1. If the blockchain structure is not in accordance with the guidelines, then what will happen? How will these guidelines be implemented? Will that mean that for example BTC or ETH no longer be used? All the problems highlighted in the document have

[12] ESMA, Consultation Paper: Technical Standards specifying certain requirements of Markets in Crypto-Assets Regulation (MiCA) – Second Consultation Paper, 5 October 2023, ESMA75-453128700-438, p. 19.

already been discussed for some time now, but the guidelines fail to bring a practical solution that can be implemented.

11. Conclusion

11.1. In sum, while the EDPB's initiative to issue guidance on blockchain and data protection is commendable, the current guidelines fall short of fully capturing the technical and legal intricacies of blockchain systems. To ensure that the GDPR does not inadvertently hinder blockchain innovation, there is a pressing need for more adaptive and forward-looking policy frameworks—ones that acknowledge both the risks and the transformative potential of data-driven technologies.[13] A collaborative, interdisciplinary approach—bringing together technologists, legal scholars, and industry actors—is essential to designing regulatory models that protect individuals without stifling technological advancement.

11.2. Furthermore, any proposal that would, even in theory, require the deletion of an entire public, permissionless blockchain must be approached with extreme caution. Such an action could result in significant and unpredictable systemic disruption, undermining not only financial stability but also the integrity of regulatory frameworks—such as MiCA and the DLT Pilot Regime—that have been carefully designed to integrate blockchain technology within the rule of law and financial regulations. More broadly, the deliberate erasure of a blockchain would set a dangerous precedent for democracy and for the freedom to access open networks, one that would be comparable, in principle, to an attempt to erasure the internet itself.

11.3. More broadly, taking steps to shut down a global, open network would set a dangerous precedent in terms of digital rights and access to neutral infrastructure, with implications comparable in principle to restricting access to the internet itself.

11.4. Ultimately, the aim should not be to retrofit traditional data protection models onto decentralised technologies, but to develop regulatory tools that uphold the core principles of the GDPR—such as data minimisation, purpose limitation, and accountability, and proportionality—while fostering innovation, legal clarity, and economic resilience in the digital age.

11.5. As Mikołaj Barczentewicz aptly notes—citing Professor Michèle Finck and others—"*EU law allows for much more pragmatic and proportionate approaches, which would not amount to the kind of uncertainty, or even a de facto prohibition of a technology, we're now facing.*"[14]

11.6. Building on the arguments presented thus far, we suggest that the Guidelines be revisited in line with the following principles:

---

[13] See Houser KA, Bagby JW, *The Data Trust Solution to Data Sharing Problems*, *Vand. J. Ent. & Technol. L.* 2023; 25:113.

[14] See Mikołaj Barczentewicz, *ibidem*, which in turn refers to Finck, *M., Blockchains and Data Protection in the European Union European Data Protection Law Review, Volume 4, Issue 1* (2018), pp. 17 - 35, DOI: https://doi.org/10.21552/edpl/2018/1/6; and Centre for Information Policy Leadership, *Digital Assets and Privacy*, January 2023, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_discussion_paper_on_digital_assets_and_privacy__19_jan_2023_.pdf).

(a) Permissionless public blockchains, as such, should not be subject to erasure;

(b) In evaluating hashed data, the key question should be whether the data has been rendered anonymous in such a way that the data subject is not, or is no longer, identifiable. This assessment should be conducted on a case-by-case basis, following a substance-over-form approach;

(c) Principles of proportionality, technical feasibility, and the state of the art should guide the interpretation of erasure obligations. In this regard, rendering personal data inaccessible may be sufficient to achieve an outcome functionally equivalent to erasure;

(d) The application of the GDPR should not come at the expense of other important EU policy objectives, including the promotion of the digital economy and the preservation of financial system stability.

11.7. Ultimately, the goal should be to craft rules for blockchain ecosystems that uphold fundamental data protection principles while enabling innovative solutions that drive the data economy forward.