Pellecchia E, 'GDPR and Blockchain Technologies: a complex relationship' (2025) 2 EJPLT.
DOI: https://doi.org/10.57230/EJPLT252EP

EJPLT
ISSN 2704-8012



GDPR and Blockchain technologies: a complex relationship

GDPR e tecnologie blockchain: una relazione complessa

ENZA PELLECCHIA
Full Professor of Private Law
University of Pisa

Abstract

The contribution starts from the consideration of the apparent radical incompatibility between blockchain technologies and personal data protection regulations and proposes a case-by-case assessment of the different technologies to focus on the actual critical issues. The solutions proposed by the EDPB guidelines and the reactions to them are illustrated.

Il contributo muove dalla considerazione della apparente radicale incompatibilità tra tecnologie blockchain e disciplina della protezione dei dati personali e propone una valutazione caso per caso delle differenti tecnologie per mettere a fuoco le effettive criticità. Vengono illustrate le soluzioni proposte dalle linee guida EDPB e le reazioni ad esse.

© The author(s) 2025, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: blockchain; data protection; GDPR

Summary: 1. Apparent incompatibilities and case-by-case assessments. – 2. Blockchain technologies and personal data processing. – 3. Tensions between Blockchain and GDPR. – 4. The guidelines of the European Data Protection Board (EDPB). – 5. - Reactions to the guidelines of the European Data Protection Board (EDPB). – 6. The potential of blockchain technologies for the protection of personal data.

1. Apparent incompatibilities and case-by-case assessments.

Blockchain exploits the characteristics of a computer network of nodes and allows for the management and updating, in a unique and secure manner, of a register containing data and information (e.g. transactions) in an open, shared and distributed way without the need for a central control and verification entity, preserving the historical memory of transactions in an immutable way. The register is structured as a chain of blocks (accompanied by hashes linked together by referencing the hash of the previous block in the next one) containing the transactions, and consent is distributed across all nodes in the network.

All nodes can participate in the process of validating transactions to be included in the ledger, and each participant has a copy of each transaction, thus ensuring security and resilience against potential attacks. Each block is cryptographically linked to the previous one after being evaluated and subjected to a consensus decision. As new blocks are added, older blocks become more difficult to modify. New blocks are replicated in all copies of the ledger within the network, and any conflicts are automatically resolved using established rules.

At first glance, the General Data Protection Regulation and blockchain technologies appear to be two irreconcilable worlds: this irreconcilability could be summarised in the formula centralisation vs. distribution.[1]

The centralisation that inspires the GDPR is well represented by the principle of accountability, which expresses a concept of risk that is not limited to the stage of violation, but also extends to the previous stage: imposing on the data controller a risk management approach that involves the adoption of precautionary technical and organisational measures to protect data from external tampering or unauthorised disclosure. The principle of accountability is accompanied – as is well known – by the principles of privacy by design (from the design stage) and privacy by default (by default setting).

Distribution – as the most advanced frontier even compared to decentralisation – is instead the soul of blockchains. In centralised networks, network participants need a central authority to communicate with each other.

[1] M Pilkington, 'Blockchain Technology: Principles and Application', in F Xavier Olleros, M Zhegu (eds.), *Research Handbook on Digital Transformation* (Elgar 2016); ML Perugini, *Distributed Ledger Technologies e sistemi di blochchain. Digital currency, Smart contrats e altre applicazion*i (Giuffrè 2018).

Decentralised networks have multiple authorities that act as centralised "hubs" for a subgroup of participants, and participants can communicate with others through their hub. Distributed networks, which are more flexible than centralised and decentralised networks, allow each participant to communicate with others without the need for a centralised point: each full node in the network maintains a copy of the entire blockchain to ensure the validity of transactions.

Immutability, accessibility, sharing and transparency are strengths of blockchain that clash with the very philosophy that inspires personal data protection legislation. There have even been fears that this technology, by its very nature, may not be able to comply with European data protection rules, which in turn could stifle its development to the detriment of the European digital single market project.[2]

The potential friction between the way the law is structured and the way technologies operate is an interesting and much-debated topic. It has been observed that individuals' behaviour can be regulated by legal provisions, but also by the "architecture" of the physical or virtual environment in which they operate.[3] When the law conflicts with the hardware and software architecture that structures the environment in which a technology operates, several situations can arise. The technology can survive and be used, and violate the law. Or the law can prevail over the architecture, and the technology cannot be adopted or its benefits exploited. Or decisions are made on a case-by-case basis on costs and benefits, with confusing and unpredictable outcomes. Each of these outcomes is imperfect and leaves many with the belief that important social interests have been neglected or ignored. It is with this conflict in mind, that between architecture and law, that the question of the relationship between GDPR and blockchain must be understood.[4]

On closer inspection, a different perception of a complex relationship emerges, one that does not lend itself to clear-cut conclusions, especially given that blockchains are a "class" of technologies: there is no single version, as the term refers to many different forms of distributed databases that vary greatly in their technical and governance arrangements and in their structure.

The most important classification criteria are now fairly well known and relate to a few key distinctions: that between "permissionless" and "permissioned" blockchains, and that between public and private blockchains.

In the first subset – "permissionless" and "permissioned" blockchains – the main differences concern the identifiability of subjects, the method of node selection and the size of the network, the shared consensus mechanism, and the transparency of block content. In permissionless blockchains, access is not subject to restrictions, the network has no theoretical limits to its development, with consequences in terms of immutability given the extreme difficulty of obtaining the necessary consensus for any change; furthermore,

[2] F Faini, 'Blockchain e diritto: la «catena del valore» tra documenti informatici, smart contracts e data protection' (2020) Resp. Civ. Prev. 305.
[3] L Lessig, *Code: And Other Laws Of Cyberspace* (Basic books 1999).
[4] U Tatar, Y Gokce, B Nussbaum, 'Law versus technology: Blockchain, GDPR, and tough tradeoffs' (2020) Computer law & security review 38.

each user can view the entire blockchain, bringing transparency to the highest possible level.

In permissioned blockchains, on the other hand, centralisation is greater because access is controlled through a pre-identification mechanism, with repercussions on the level of immutability (in abstract terms, it is easier to achieve the majority needed to make changes) and transparency (the complete view of the blockchain could be inhibited at certain nodes).

In the second subset – public and private blockchains – the emphasis is on IT infrastructure management. Public blockchains do not have a "top", as they are the result of the progressive addition of participants to the network. Private blockchains, on the other hand, can be traced back to an organiser who normally uses the characteristics of the blockchain to strengthen the security of traditional databases. Normally, public blockchains are also permissionless, but pre-identification upon entry could make them permissioned.[5]

These preliminary distinctions have implications for data protection, with the result that an assessment of the compatibility of distributed ledgers with the GDPR should preferably be based on a detailed case-by-case analysis that takes into account the specific technical design and governance structure: not all blockchains are compatible or incompatible with data protection regulations, as each use of the technology must be examined on the basis of its own characteristics.[6]

This article aims to highlight some critical issues but also some potential benefits of the relationship between blockchain and the GDPR, bearing in mind that not all blockchains are compatible or incompatible with data protection regulations, as each use of the technology must be examined on its own specific characteristics.

The European Data Protection Board also appears to be moving in this direction with its 2025 guidelines, which have not resolved all issues but – despite some criticism – provide guidance on harmonising personal data protection and blockchain technologies.

Not all issues are addressed in this paper, which is not intended to answer every possible question but rather to highlight the benefits of a case-by-case approach.

2. Blockchain technologies and personal data processing.

Article 4(2) of the GDPR provides a very broad definition of "processing",[7] according to which the addition of personal data to a distributed ledger, its continued storage and any further processing may be considered personal data processing.

---

[5] AM Gambino, C Bomprezzi, 'Blockchain e protezione dei dati personali' (2019) Dir. inf. 627.

[6] For this approach to the issue, see the study by European Parliamentary Research Service (EPRS), 'Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?' (2019) 4.

[7] Processing is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

However, it is above all the broad concept of personal data – and its even broader interpretation – that brings blockchain operations within the scope of the GDPR (obviously when they involve personal data).

Article 4(1) defines "personal data" as any information relating to an identified or identifiable natural person ("data subject"); a natural person is considered identifiable if they can be identified, directly or indirectly, with particular reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity.

The Regulation adopts a binary perspective between personal data and non-personal data and only subjects the former to its scope. According to recital 26 of the GDPR, the Regulation does not apply to anonymous data.

In contrast to this binary legal perspective, reality operates on a spectrum between clearly personal data, clearly anonymous data (an uncontroversial example would be climate data from outer space that does not reveal information about those who collected it) and "a lot in between".[8]

The broad definition of personal data is generating much debate and has led some to observe that data protection law has become the "law of everything",[9] as in the near future all data could be personal data and therefore subject to GDPR requirements.[10] This is because technology is rapidly moving towards the perfect identifiability of information; datafication and advances in data analysis mean that everything contains information; and in increasingly "smart" environments, any information is likely to relate to a person by purpose or effect. [11] Anonymisation is increasingly difficult to achieve with the advancement of modern information technology and the indiscriminate availability of information.

On the other hand, pseudonymisation – understood as the processing of personal data in such a way that the personal data cannot be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person – does not remove pseudonymised data from the scope of the GDPR: according to the authoritative guidance of the Article 29 Working Party, pseudonymisation is not a method of anonymisation. It simply reduces the linkability of a set of data to the original identity of a data subject and is therefore a useful security measure, but pseudonymised data are still personal data, processed with a high degree of security in the perspective of Article 25 GDPR.[12]

In light of the taxonomy outlined by the GDPR with regard to data, interpreters' attention – in the specific context of blockchains – has focused primarily on so-called public keys, which serve as user identifiers, and on data

[8] N Purtova, 'The law of everything. Broad concept of personal data and future of EU data protection law' (2018) 1 Law, Innovation and Technology 40.
[9] L Edwards, *Law, Policy and the Internet* (Hart Publishing 2018) 84, according to whom 'what constitutes personal data is one of the central causes of doubt in the current data protection regime'.
[10] N Purtova (n 8) 40.
[11] E Pellecchia, 'Dati personali, anonimizzati, pseudonimizzati, de-identificati: combinazioni possibili di livelli molteplici di identificabilità nel GDPR' (2020) Le nuove leggi civ. comm. 360.
[12] Art. 29 Working Party, Opinion 5/2014 on anonymisation techniques, adopted on 10 April 2014.

relating to transactions carried out via blockchain (so-called transactional data).[13]

In the context of blockchain, public keys serve as the identifiers mentioned in recital 30 of the GDPR. Blockchains are based on a two-step verification process with asymmetric encryption. Each user has a public key (a string of letters and numbers representing the user) and a private key (also a string of letters and numbers, which is best thought of as a password that should never be shared with others). Both keys have a mathematical relationship whereby the private key can decrypt data that has been encrypted using the public key.

Public keys therefore conceal the identity of the individual, unless they are linked to additional identifiers. A public key is therefore data that "can no longer be attributed to a specific data subject" unless it is combined with "additional information" such as a name, address or other identifying information, in line with the definition of pseudonymous data in Article 4(5) of the GDPR.[14] Identification, linkability and even inference can allow public keys to be linked to an identified or identifiable natural person, both on public and permissionless blockchains and on private and authorised blockchains alike.[15] Measures should therefore be taken to make it unlikely that the public key can be linked to an identified or identifiable natural person: the use of single-use public keys appears to be a good practice in this regard, but this is more easily achievable on private and authorised blockchains than on public and permissionless ones.[16]

Transactional data, on the other hand, refers to other categories of data that can be used on blockchains but are not public keys: this is data about the transaction itself, which could be a name, address or date of birth contained in the payload of a given transaction.

Transactional data constitutes personal data when it refers directly or indirectly to an identified or identifiable natural person.

Both public keys and transactional data can be used in plain text, encrypted form or hashed form when placed on the blockchain. When personal data is used in plain text, it undoubtedly remains personal data and is clearly subject to the GDPR. There is debate as to whether encryption or hashing are methods capable of transforming personal data into anonymous data. A cryptographic hash is a mathematical function that is fed with an input value that is transformed into a fixed-length output value. The same input always produces the same output; it is not possible to deduce the input of the hash from the output of the hash.

Hash functions are often used to remove personal identifiers (such as a name or customer number) and replace them with a pseudonym that is difficult to reverse. Whether hashed data always remains personal data for the purposes of the GDPR is a matter of debate. However, hashing will often generate pseudonymous, not anonymous, data: hash functions can reduce the linkability

[13] M Fink, 'Blockchains an Data Protection in the European Union' (2018) European Data Protection Law Review 24.
[14] M Berberich, M Steiner, 'Blockchain Technology and the GDPR - How to Reconcile Privacy and Distributed Ledgers' (2016) Eur. Data Prot. L. Rev. 422.
[15] A M Gambino, C Bomprezzi (n 5) 633.
[16] J Barcelo, 'User Privacy in the Public Bitcoin Blockchain' (2007) 6 Journal of Latex Class Files 3.

of a data set to the original identity of a data subject; as such, they are a useful security measure but not a method of anonymization.[17]

3. Tensions between Blockchain and GDPR.

As mentioned at the beginning, according to some interpretations, certain characteristics of blockchains would make them incompatible with the GDPR: among these, the impossibility of identifying a data controller, the impossibility of applying the rights of the data subject, the incompatibility with the right to erasure, and the conflict with the principle of data minimization.[18]

A more careful analysis reaches less drastic conclusions about the compatibility between the GDPR and blockchain, starting with the variety of blockchain technologies referred to in the previous pages. Permissioned/private blockchains have a significant degree of compatibility with the GDPR, while greater tensions undoubtedly exist with regard to permissionless/public blockchains.

The conflicts between the GDPR and blockchain technology are not all unsolvable: according to some, they can be managed by leveraging commonalities, developing new approaches and interpretations to shift the balance between the GDPR and blockchain technology, and adapting blockchain technology to the requirements of data protection law. In other words, the discrepancies should not manifest themselves as a zero-sum game in which technology survives at the expense of breaking the law or the law unilaterally dictates its terms on technology to the point of overriding it.[19]

For example, blockchain technology and the GDPR share the goal of strengthening data privacy and security. But they differ on how to achieve this goal. Transparency, increased individual control over data, data minimisation and encryption are fundamentals of blockchain technology that are broadly in line with some fundamental rules of the GDPR. The immutable and decentralised nature of the technology ensures the integrity and accuracy of data stored on the blockchain, greatly reducing the risk of it being illegally altered and distorted, since – unlike centralised archives – information is stored across a variety of systems. And the integrity and accuracy of personal data are among the fundamental aspects that, according to Article 25, must be taken into account when designing and developing a technology.

Furthermore, blockchain technology gives users a great deal of power and allows them to exercise individual control over the personal data they store in the blockchain database. This means that they can decide whether to share their personal data and can do so to the extent required by the respective

[17] M Fink (n 13) 22.

[18] For an initial in-depth analysis of the relationship between privacy and blockchain, V Devi, V Sabareshwaran, R Saravana Kumar, M Sivasankar, 'Privacy-Preserving Healthcare Architecture Using Blockchain', (2020) 9 IJCSMC, 116-120; S Sakho et al., 'Privacy Protection Issues in Blockchain Technology', (2019) 17 IJCSIS, 124-131; R De Le Cruz, 'Privacy Laws in the Blockchain Environment', (2019) Annals of Emerging Technologies in Computing, vol. 3, 34-44; G Alpa, 'Tecnologie e diritto privato', (2017) Rivista italiana per le scienze giuridiche; P De Filippi, 'The Interplay Between Decentralization and Privacy: The Case of Blockchain Technologies', (2016) Journal of Peer Production, 1.

[19] U Tatar- Y Gokce-B Nussbaum, (n.4), 6.

transaction on the blockchain. In other words, they can limit the data shared to the minimum necessary to achieve the specific purpose.

The main critical issue concerns immutability, since once data is entered into the blockchain, it cannot be revoked or "forgotten": not because of centrally organised and enforced rules (which can be changed), but because of "architectural" rules based on the digitally constructed environment (at the hardware and software design stage). Any attempt to intervene on the stored data – even as a result of exercising the "right to be forgotten" – would alter the consistency of the entire blockchain, damaging its reliability.

It should nevertheless be noted that some of the critical issues identified in blockchain technology in relation to the GDPR are not attributable exclusively to the way in which its architecture is designed, but also to some extent to critical issues inherent in the GDPR itself: for example, the lack of a clear definition of erasure. In this regard, it has been argued that the European Court of Justice and national supervisory authorities could choose to interpret the GDPR in a way that accommodates the immutable nature of blockchain: deletion and immutability, it has been said, are irreconcilable only to the extent that deletion means something that is not possible in the context of blockchain architecture; there would instead be room for a definition of erasure that includes the minimisation of information that allows the identity of individuals to be traced.[20]

Some Scholars note that almost all blockchain incompatibilities can be resolved with a practical approach by the competent public authorities, recognising the peculiarities of the technology in question and giving priority to the commonalities between the EU regulation and blockchain. To this end, bringing the relevant stakeholders from public bodies and industry together around the same table is of the utmost importance in order to build a constructive dialogue aimed at achieving practical and balanced approaches.

Like many regulatory challenges, this stems from the fact that data regulation is a difficult issue. The GDPR is an important step forward in attempting to resolve this difficult issue, but as in most regulatory environments, a push-and-pull between regulators and the regulated, including emerging definitions (and redefinitions), has the potential to make a series of very difficult questions more tractable.[21]

4. The guidelines of the European Data Protection Board (EDPB).

During its April 2025 plenary, the European Data Protection Board (EDPB) has adopted guidelines on processing of personal data through blockchain technologies.[22]

As the use of blockchain technologies is expanding, the Board considers it important to help organisations using these technologies to comply with the GDPR.

[20] M Fink (n 13) 30 ff.; U Tatar, Y Gokce, B Nussbaum (n 4) 7.
[21] U Tatar, Y Gokce, B Nussbaum (n 4) 7.
[22] <https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-022025-processing-personal-data_en>.

One of the most complex and debated issues regarding the application of the GDPR to blockchain technologies concerns the allocation of responsibilities amongst the various parties participating in the network. Decentralisation, a distinctive feature of many DLT architectures, cannot and must not be interpreted as an exemption from the obligations set out in the Regulation: on the contrary, the GDPR is based on the principle of accountability, requiring a clear identification of which of the parties involved determines the purposes and means of personal data processing.

The Guidelines refer to the previous EDPB guidelines on the concepts of controller, joint controller and processor (WP29, Version 2.0, 2021), reiterating that the distributed nature of a technology does not exempt from the obligation to identify legal roles and responsibilities. The technical complexity of a blockchain cannot result in a de facto removal of responsibility.

In the context of a blockchain, the entity that determines the purposes and essential means of processing (e.g. the type of data stored on the chain, the methods of access, the rules for participation in the network) must be classified as the data controller.

However, in many blockchain applications, these choices are the result of a joint decision between multiple parties (e.g. consortia, groups of validators), meaning that joint controllership under Article 26 of the GDPR is frequently established. Such joint controllership entails the need to define, in a transparent manner through agreements between the parties, their respective responsibilities and methods of cooperation, as well as to adequately inform data subjects of the main elements of such an agreement.

Where, on the other hand, a participant acts on behalf of the controller and in accordance with binding instructions, the role of data processor (Article 28 of the GDPR) applies, with a consequent obligation to draw up a contract in accordance with legal requirements.

The definition of governance plays a central role in correctly identifying the roles of the various actors.

In permissioned or private blockchains, the existence of a coordinating authority (e.g. a consortium or a promoting organisation) facilitates the distribution of responsibilities and the conclusion of agreements between participants. In this context, it is often possible to: specify precisely who determines the purposes and means of processing; determine which nodes have access to personal data and under what conditions; regulate the procedures for exercising data subjects' rights and managing requests. Conversely, in public (permissionless) blockchains, the absence of formal governance and a central organisation makes it more difficult to identify who has effective control over data processing. In such cases, the EDPB suggests considering the possibility of setting up consortia or ad hoc legal entities that can perform a coordinating and representative role, not least to ensure an effective channel for data subjects to exercise their rights.

In its guidelines, the EDPB explains how blockchains work, assessing the different possible architectures and their implications for the processing of personal data.

The guidelines highlight the importance of implementing technical and organisational measures at the earliest stages of the design of the processing.

The EDPB also clarifies that the roles and responsibilities of the different actors in a blockchain-related processing of personal data should be assessed during the design of the processing.

In addition, organisations should carry out a Data Protection Impact Assessment (DPIA) before processing personal data through blockchain technologies, where the processing is likely to result in a high risk to the rights and freedoms of individuals.

According to the Board, organisations should also ensure the highest protection of individuals' personal data during the processing so that they are not made accessible to an indefinite number of persons by default.

The guidelines provide examples of different techniques for data minimisation, as well as for handling and storing personal data. As a general rule, storing personal data in a blockchain should be avoided if this conflicts with data protection principles.

Finally, the Board highlights the importance of the rights of individuals especially regarding transparency, rectification and erasure of personal data.

One of the key points of the EDPB Guidelines 02/2025 is the recommendation that the adoption of blockchain technologies should be the result of an informed assessment, based on an analysis of necessity, proportionality and adequacy in relation to the purposes of the processing.

The principle of data protection by design and by default (Article 25 of the GDPR) requires that, from the design stage of the technological solution, all measures – both technical and organisational – be taken to minimise the exposure of personal data, limiting its dissemination and ensuring compliance with the principles of minimisation and purpose limitation.

The correct selection of the blockchain architecture is one of the most important decisions for compliance purposes. The guidelines emphasise the need to carefully assess the type of blockchain to be used based on:

- the characteristics of the intended processing;
- the nature and sensitivity of the data involved;
- the rights and freedoms of the data subjects potentially affected.

In addition to choosing the type of blockchain, the Guidelines encourage the adoption of Privacy-Enhancing Technologies (PETs) that limit the dissemination of personal information without compromising the functionality of the system. Among the most relevant solutions are:

- Zero-Knowledge Proofs (ZKPs): cryptographic techniques that allow the veracity of information to be demonstrated without revealing its content. These can be used, for example, to demonstrate a subject's suitability to carry out a transaction without exposing their identity or other sensitive information.
- Salted Hashing or secret keys, commitment schemes and advanced pseudonymisation techniques: methods that allow only digital fingerprints (hashes) or references to data to be stored in the blockchain, keeping the actual identification data off-chain and reducing the risk of exposure.
- Decentralised Identifiers (DID) and Verifiable Credentials: emerging approaches in the field of digital identity, which can help reconcile verification requirements with compliance with the principles of minimisation and control by the data subject.

The EDPB recommends accurately documenting the reasons that led to the selection of a particular architecture or technical solution, within the broader accountability required by the GDPR (Art. 5, para. 2 and Art. 24). In particular, it is suggested to specify: the reasons why blockchain is considered the most appropriate technology for the specific use case; the alternatives evaluated and the reasons why they were rejected; the risk mitigation measures envisaged.

This documentation will be essential both in the event of checks by the authorities and to ensure transparency towards data subjects.

In light of the guidance provided by the EDPB in the new Guidelines, organisations that use or intend to implement blockchain solutions are faced with the need to significantly update their personal data protection documentation. Far from being a mere formal requirement, this review is a strategic imperative to ensure compliance with the GDPR and mitigate the risks associated with the use of emerging technologies: corporate privacy documentation is, in fact, the backbone of the accountability required by the Regulation, serving as the tool through which the data controller can demonstrate that it has taken appropriate technical and organisational measures to ensure, and be able to prove, that the processing is carried out in accordance with the law (Article 5(2) of the GDPR).

5. Reactions to the guidelines of the European Data Protection Board (EDPB).

Reactions to the guidelines have been cautious and concerned.[23] There has been no real hostility, but some critical issues that still need to be resolved have been reported, noting that the guidelines risk undermining Europe's digital sovereignty by mischaracterising blockchain as a traditional IT service model rather than a foundational public infrastructure, especially in the case of permissionless blockchains. The EDPB's approach, while grounded in valid concerns, risks deterring innovation in Europe if not recalibrated. A more informed, differentiated, and decentralisation-aware regulatory stance will empower Europe to lead in responsible digital infrastructure.

The main concerns relate to the following issues: mischaracterisation of blockchain as controllable infrastructure; oversimplified application of gdpr roles; overly broad interpretation of personal data; infeasible erasure and rectification expectations; inadequate distinction between blockchain types.

In summary: criticisms are focused on the fact that the EDPB Guide lines treat blockchain as a technology akin to cloud computing, implying centralised control and deployment decisions. This conflation ignores the nature of permissionless blockchains (e.g., Bitcoin, Ethereum), which are already operational, autonomous infrastructures. The assumption that entities interacting with blockchains are automatically "controllers" overlooks the distinction between node operation and data determination. On permissionless networks, nodes typically do not determine processing

[23] <https://europeanblockchainassociation.org/2025/06/09/a-turning-point-for-blockchain-regulation-in-europe/>.

purposes or means; instead, they adhere to software protocols and act similarly to Internet routers or telecommunications relays. The guidelines regard metadata (e.g., public keys, hashes) as personal data, even in the absence of feasible re-identification. This presumption creates legal uncertainty for developers and users and could criminalise the use of privacy-preserving technologies that operate pseudonymously by design and in consequence, effectively driving decentralised innovation out of Europe. Imposing expectations like the right to erase on immutable infrastructures ignores both technical constraints and the public utility logic of blockchain. The focus should be on minimising personal data on-chain (data scarcity) and enabling privacy-preserving architectures, rather than forcing technical features that contradict the nature of permissionless blockchain. Finally, the guidelines fail to sufficiently distinguish between permissionless/public and permissioned/private blockchains.[24]

The guidelines adopted have generated wide and articulated reactions among institutional actors, market participants, civil society organisations and legal scholars. While there is broad recognition of the central role played by the EDPB in promoting consistency in the interpretation and application of the GDPR, the reception of its guidance reveals persistent tensions between legal certainty, technological development and regulatory flexibility.

From an institutional perspective, EU bodies and national data protection authorities generally regard the EDPB's guidelines as an essential instrument for ensuring the uniform application of data protection law across Member States. The guidelines are widely perceived as contributing to legal harmonisation and to the reduction of enforcement fragmentation, particularly in cross-border processing scenarios. This positive assessment is especially evident in areas where the EDPB has sought to clarify the interaction between the GDPR and other EU regulatory frameworks, such as competition law or digital market regulation. At the same time, institutional actors explicitly acknowledge the non-binding nature of the guidelines and the fact that their ultimate authority remains contingent upon judicial interpretation, most notably by the Court of Justice of the European Union.

The reaction of industry stakeholders is more ambivalent. On the one hand, business associations and sector-specific organisations frequently welcome the EDPB's efforts to provide interpretative guidance in areas characterised by legal uncertainty, such as international data transfers, the identification of controllers and processors, or the allocation of responsibility in complex processing chains. In this respect, the guidelines are valued for their potential to enhance predictability and compliance planning, particularly for operators engaged in transnational activities or operating in highly regulated sectors.

On the other hand, industry responses often express strong criticism where the EDPB's interpretations are perceived as excessively restrictive or insufficiently attuned to technological realities. This criticism is particularly pronounced in relation to guidelines addressing emerging technologies and data-management techniques, such as pseudonymisation, anonymisation, blockchain technologies and advanced tracking methods. In these contexts,

[24] <https://eudecentralisation.org/blockchain-and-gdpr/>.

stakeholders argue that the EDPB tends to adopt a precautionary approach that risks extending GDPR obligations beyond the text of the Regulation itself, thereby increasing compliance burdens and potentially discouraging innovation. Concerns are also raised regarding the timing of certain guidelines, especially where parallel judicial proceedings before the CJEU may significantly affect the underlying legal concepts.

Civil society organisations and consumer groups generally adopt a more favourable stance towards the EDPB's guidance, viewing it as a necessary counterweight to market-driven pressures and as a means of safeguarding the fundamental rights enshrined in the EU legal order. These actors often support the Board's strict interpretations, particularly where they reinforce data subject rights and accountability obligations. Nonetheless, even within this group, some concerns emerge regarding the accessibility and practical comprehensibility of the guidelines, especially for smaller organisations and individual data subjects.

Academic commentary tends to situate the reactions to the EDPB guidelines within a broader systemic analysis of EU data protection law. Scholars frequently emphasise the quasi-normative function of the guidelines, noting that, despite their formal non-binding status, they exert significant influence on supervisory practice and judicial reasoning. At the same time, academic debate highlights the structural tensions exposed by the guidelines, particularly the friction between legal principles rooted in centralised accountability models and technological architectures based on decentralisation, immutability or data replication. In this sense, divergent reactions to the EDPB's guidance are often interpreted not as a rejection of data protection objectives, but as a manifestation of deeper unresolved issues within the GDPR framework itself.

Overall, the reactions to the EDPB guidelines can be characterised as a combination of cautious endorsement and targeted criticism. While the legitimacy of the EDPB's coordinating role is rarely questioned, significant debate persists as to the appropriate scope and intensity of its interpretative intervention. This debate is especially salient in technologically complex domains, where the risk of regulatory over-reach must be balanced against the need to ensure effective and uniform protection of personal data within the European Union.

The reactions to the guidelines of the European Data Protection Board (EDPB) must be understood against the broader theoretical architecture of the GDPR, which combines a fundamental-rights-based approach with a risk-oriented and accountability-driven regulatory model. The EDPB's interpretative activity occupies a pivotal position within this architecture, functioning as a mechanism for ensuring consistency while simultaneously shaping the practical meaning of open-textured legal concepts.

From the perspective of EU institutional actors and national supervisory authorities, the guidelines are generally perceived as an essential instrument for realising the principle of consistency enshrined in Article 63 GDPR. In this sense, the EDPB's guidance is regarded as a functional extension of the GDPR's system of cooperative governance, aimed at preventing divergent national interpretations that could undermine both legal certainty and the uniform

protection of fundamental rights. This institutional reception reflects a conception of the GDPR as a composite regulatory framework, in which soft-law instruments play a structural role in ensuring the effectiveness of the Regulation.

At the same time, the institutional discourse surrounding the guidelines consistently emphasises their non-binding nature, thereby acknowledging the limits imposed by the principle of legality and by the CJEU's monopoly over authoritative interpretation of EU law. This tension illustrates a core theoretical feature of the GDPR: the reliance on flexible regulatory techniques that must nevertheless remain compatible with the requirements of democratic legitimacy and judicial oversight.

Industry reactions reveal a more ambivalent engagement with the EDPB's guidelines, which closely tracks the internal tensions of the GDPR itself. On the one hand, market actors tend to welcome guidance that clarifies the allocation of responsibilities, the conditions for lawful processing, or the application of GDPR provisions in complex processing ecosystems. From a theoretical standpoint, this support reflects the GDPR's accountability model, which presupposes that controllers and processors are able to assess risks and implement appropriate technical and organisational measures. Insofar as the guidelines reduce interpretative uncertainty, they facilitate the operationalisation of accountability and support compliance-oriented decision-making.

On the other hand, industry criticism becomes pronounced where the EDPB's guidance is perceived as transforming a risk-based framework into a quasi-categorical system of prohibitions. This criticism is particularly evident in relation to guidelines addressing emerging technologies or advanced data-management techniques, such as pseudonymisation, anonymisation or distributed ledger technologies. Here, stakeholders argue that the EDPB's precautionary approach risks undermining the GDPR's commitment to technological neutrality, by implicitly privileging certain technical architectures over others. From a theoretical perspective, such reactions highlight the difficulty of reconciling the GDPR's open-ended standards with the Board's tendency to stabilise interpretation through detailed guidance.

Civil society organisations and consumer representatives generally interpret the EDPB's guidelines through the lens of fundamental rights protection, which constitutes the normative core of the GDPR. These actors tend to support strict and rights-protective interpretations, particularly where the guidelines reinforce data subject rights or constrain expansive data-driven business practices. In theoretical terms, this reception reflects an understanding of the GDPR as a constitutional instrument of the EU legal order, designed to rebalance structural asymmetries between individuals and powerful data controllers. Nevertheless, even within this perspective, concerns occasionally arise regarding the accessibility and practical intelligibility of the guidelines, suggesting a tension between rights-maximisation and regulatory comprehensibility.

Academic commentary situates the reactions to the EDPB guidelines within a broader reflection on the normative function of soft law in EU data protection. Scholars frequently observe that, despite their formal non-binding

status, the guidelines exert a de facto normative influence on supervisory practice and judicial reasoning, thereby contributing to the progressive concretisation of GDPR principles. From this viewpoint, divergent reactions to the guidelines are not merely expressions of stakeholder interest, but symptoms of deeper structural tensions within the GDPR – most notably between decentralised technological architectures and a legal framework built around identifiable responsibility, controllability and ex post enforcement.

Overall, the reactions to the EDPB's guidelines reflect the inherent ambivalence of the GDPR itself: a Regulation that aspires to be technologically neutral yet rights-protective, flexible yet consistent, risk-based yet anchored in fundamental rights. The debate surrounding the scope and intensity of the EDPB's interpretative activity thus appears less as a contestation of the Board's legitimacy, and more as an ongoing negotiation over how GDPR theory should be translated into regulatory practice in an evolving technological environment.

With a view to collaboration rather than confrontation, a number of strategic options have been put forward: recognise the purpose and architecture of blockchain applications, particularly those aligned with permissionless public utility models (e.g. Bitcoin, Ethereum); regulation must be rooted in the governance intention behind the technology, not merely its technical components; shift from a provider-centric model of liability to a user-centric one; limit the classification of metadata (e.g., hashes, public keys) as personal data to contexts where re-identification is reasonably likely; recognise that blockchain operates more like a public utility than a private service; adapt governance models to reflect decentralised coordination, where participants operate based on mutual protocol rather than contractual arrangements.

6. The potential of blockchain technologies for personal data protection.

It has been argued that blockchain technologies could be a suitable tool for achieving some of the objectives of the GDPR. Indeed, blockchain technologies are a data governance tool that could support alternative forms of data management and distribution and offer advantages over other current solutions. Blockchains can be designed to enable data sharing without the need for a central intermediary, offer transparency on who has accessed the data, and blockchain-based smart contracts can automate data sharing, reducing transaction costs.[25]

These features can be invoked to support compatibility with some of the objectives of the GDPR, such as providing individuals with greater control over personal data that directly or indirectly concerns them.[26] The European

[25] M Berberich, M Steiner, op. cit., 425; see also C Wirth, CM Kolain, 'Privacy by BlockChain Design: A Blockhain-enabled GDPR-compliant Approach for Handling Personal Data', Reports of the European Society for Socially Embedded Technologies, 2018.

[26] AM Gambino, C Bomprezzi (n 5) 629, observe that blockchain could also curb indiscriminate data collection by large platforms such as Facebook or Amazon: encryption would guarantee selective access to data, in line with the principle of minimisation, as is the case with some blockchains mentioned by the authors, such as ShoCard and BCDiploma, which offer the advantage of maximum transparency on what data is processed and who has access to it, in line with the strengthening of data subjects' rights established by the GDPR.

Parliament, in its Resolution of 3 October 2018 on "Distributed ledger technologies and blockchain: building trust through disintermediation", explicitly considered blockchain to be a tool that strengthens citizens' autonomy by giving them the opportunity to control their own data and decide what to share in the ledger, as well as the ability to choose who can see that data.

A two-pronged approach can be developed to foster a virtuous relationship: designing blockchains that incorporate data protection techniques with a view to privacy by design and by default; and designing "dedicated" blockchains, i.e. those specifically designed to protect personal data.

Ultimately, blockchain technology can be redesigned and adapted to meet the requirements of the GDPR, albeit with some inherent compromises.[27] To this end, the blockchain industry and innovators should have a good understanding of the principles and objectives of the GDPR so that they can add new features and configurations to adapt the technology to the requirements of the GDPR, with a view to privacy by design.[28] To align blockchain technology with the needs of the right to be forgotten, blockchain innovators should propose a solution that allows personal data to be removed from blockchain ledgers. However, this solution should not be detrimental to the integrity of the chain. In other words, personal data should be removed from blockchain ledgers without breaking the consistency of the blockchain. This means that blockchain technology aligned with the right to be forgotten would require keeping the hash functions that link blocks intact, while allowing personal data to be removed from them. Chameleon hashes are being tested in this direction to create modifiable blockchains. It is not unusual for law and regulation to lead to changes in "architecture", and often important technological innovations arise from these changes to satisfy regulatory environments.[29] Another attempt to ensure GDPR compliance is to store personal data in off-chain archives. According to this solution, personal data must be detached from any other transaction data and placed in a separate off-chain repository. The authenticity of that personal data can be verified using corresponding hash functions stored in the blockchain network.

Protocols can be generated in such a way as to allow personal data stored in off-chain memory to be deleted without necessarily breaking the consistency of the chain. Deleting personal data stored off-chain will render the hash value useless. However, this solution reverses the advantages of storing data in a blockchain database in an immutable, tamper-proof, secure and transparent manner. With this solution, in order to comply with the GDPR, one may have to expose the blockchain to the vulnerabilities of off-chain storage, as well as potentially reinstate the need for trusted third parties, undermining one of the pillars on which distributed ledger technology is based.[30]

It is important that computer scientists, engineers and technologists take the public interest issues represented in the GDPR seriously, and that they are

[27] AM Gambino, C Bomprezzi (n 5) 631.
[28] L Moerel, 'Blockchain & Data Protection…and Why They Are Not on a Collision Course' (2019) European Review of Private Law 842.
[29] P De Filippi (n 18).
[30] U Tatar, Y Gokce, B Nussbaum (n 4) 7.

able to talk – both to regulators and to the public – about the advantages and disadvantages that each has in the context of blockchain. Emphasising the common values and objectives between the GDPR and blockchain will help to reduce the areas of controversy and conflict. Reinterpreting particular concepts in the GDPR will also offer flexibility and regulatory space.

Redesigning elements of the blockchain to create GDPR-compliant blockchains could be part of the answer, although it is likely to sacrifice some of the advantages that make blockchain such an attractive solution to many problems.[31]

[31] For this approach, see U Tatar, Y Gokce, B Nussbaum (n 4) 8.