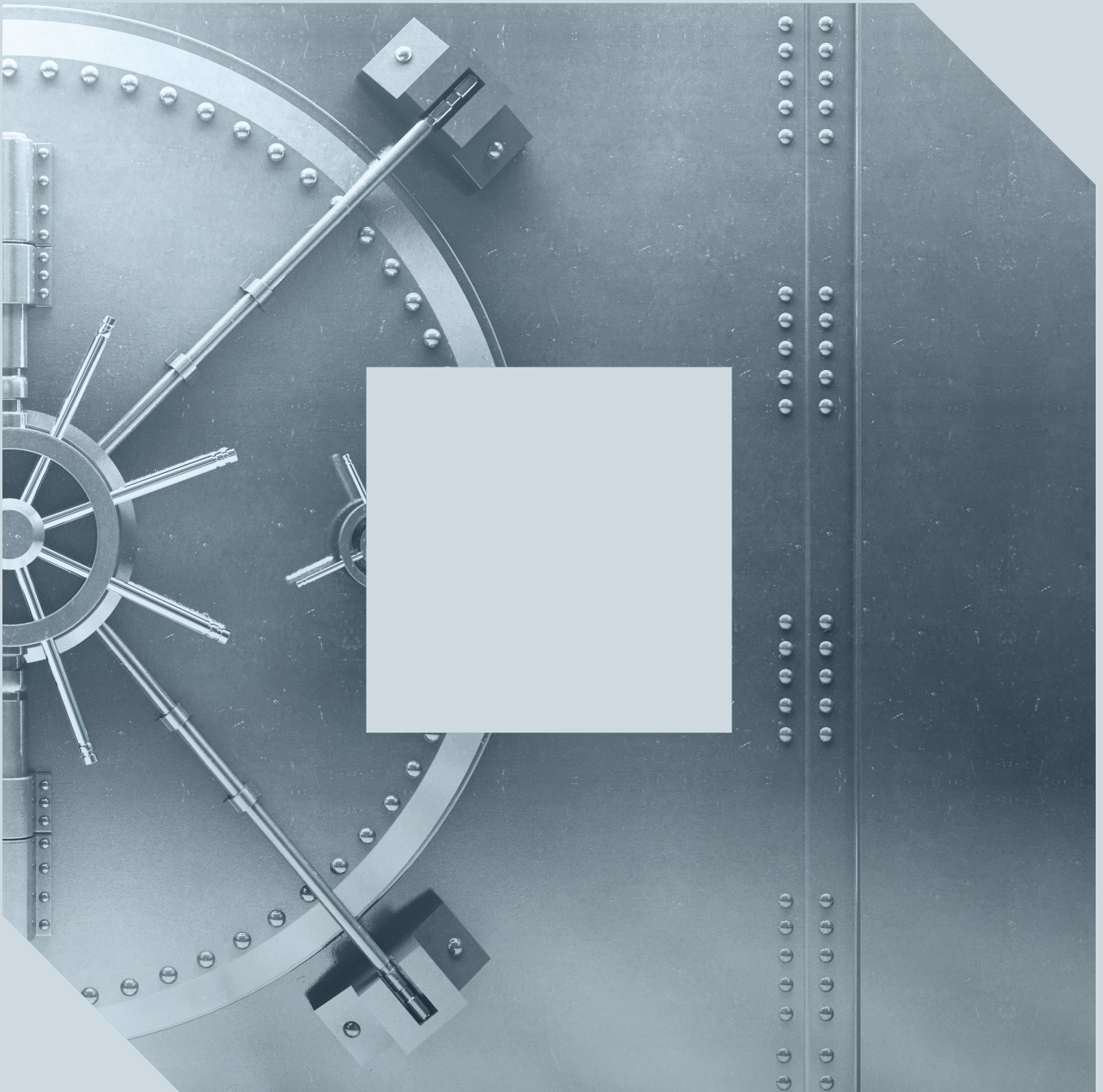


# General Data Protection Regulation [GDPR]

## Status Report on the implications for Blockchain and Privacy



# General Data Protection Regulation [GDPR]

Authored by Dr. Jörn Erbguth

	<b>Executive Summary</b>	<b>5</b>
<hr/>		
<b>1</b>	<b>Introduction</b>	<b>6</b>
1.1	The role of EDPB guidelines	7
1.2	Types of blockchains and blockchain actors	7
1.3	Structure and scope of this paper	8
<hr/>		
<b>2</b>	<b>Blockchain, an architecture that enables data sovereignty and privacy - by - design</b>	<b>9</b>
2.1	Blockchain as a means to privacy and data sovereignty of data subjects	9
2.1.1	Limits of user control in centralised Web 2.0 applications	9
2.1.2	Immutability as a means for accountability	10
2.2	Blockchains as infrastructure	11
2.3	Are GDPR and EDPB guidelines technology - neutral?	12
2.4	User autonomy and choice	13
2.5	Public blockchains compared to book publishing	14
2.6	The role of financial and crypto - asset regulation	15
2.7	Better coordination of regulation	16
<hr/>		
<b>3</b>	<b>Applying the GDPR to data stored on blockchains</b>	<b>17</b>
3.1	Applicability of the GDPR	17
3.2	Identifiers, hashes and commitments: when do they qualify as personal data?	17
3.2.1	Definition of personal data	18
3.2.2	Identifiers	20
3.2.3	Hashes of personal data	21
3.2.4	Use of hashes as identifiers	22
3.2.5	Hash values used as commitments	23
3.2.6	Do commitments constitute personal data?	24
3.2.7	Salt, pepper and keyed hashing	29
3.2.8	Limits of hashes and security considerations	30
3.2.9	Zero - knowledge proofs	30



3.3	Roles under the GDPR: Controllers and processors	31
3.3.1	Blockchain level	32
3.3.2	Smart contract and DAO level	33
3.3.3	Transaction level	34
3.3.4	Joint controllers	34
3.3.5	The household exemption or the data subject as a controller	35
3.3.6	Consequences of technical impossibility	36
3.3.7	Processors	38
3.4	Lawfulness of processing (Art. 6(1) GDPR)	39
3.4.1	Consent (Art. 6(1)(a) GDPR)	39
3.4.2	Contract (Art. 6(1)(b) GDPR)	41
3.4.3	Legal obligation (Art. 6(1)(c) GDPR) and public task, official authority (Art. 6(1)(e) GDPR)	43
3.4.3.1	<i>Qualified electronic ledgers under eIDAS</i>	43
3.4.3.2	<i>Crypto-asset transactions</i>	44
3.4.3.3	<i>Public service blockchains</i>	45
3.4.4	Legitimate interest (Art. 6(1)(f) GDPR)	46
3.5	Special categories of personal data (Art. 9 GDPR)	47
3.6	International transfers	48
3.7	Data retention	50
3.8	Security and governance	51
3.9	Data subject rights	53
3.9.1	Information to be provided and right to access (Arts. 12-15 GDPR)	53
3.9.2	Right to erasure (Art. 17 GDPR), withdrawal of consent (Art. 7(3) GDPR) and right to object (Art. 21 GDPR)	54
3.9.3	Right to rectification (Art. 16 GDPR)	55
3.9.4	Right to restriction of data processing (Art. 18 GDPR)	56
3.9.5	Right to data portability (Art. 20 GDPR)	57
3.10	Automated decision-making (Art. 22 GDPR)	58
3.11	Data protection impact assessments (Art. 35 GDPR)	60
3.12	Result	61

---

<b>4</b>	<b>Outlook</b>	<b>63</b>
----------	----------------	-----------

---

<b>5</b>	<b>Use cases</b>	<b>67</b>
5.1	Certifying diplomas through a smart contract on a public blockchain	67
5.1.1	Description of the use case	67
5.1.2	Data stored on a blockchain	67
5.1.3	Does this data qualify as personal data? If so, how is this justified?	67
5.1.4	How does the use case support fundamental rights of the data subjects?	68
5.2	Proof of reserves	68
5.2.1	Description of the use case	68



5.2.2	Data stored on a blockchain	68
5.2.3	Does this data qualify as personal data? If so, how is this justified?	68
5.2.4	How does the use case support fundamental rights of the data subjects?	69
5.3	TRISA travel rule data exchange for crypto-asset service providers	69
5.3.1	Description of the use case	69
5.3.2	Data stored on a blockchain	69
5.3.3	Does this data qualify as personal data? If so, how is this justified?	70
5.3.4	How does the use case support fundamental rights of the data subjects?	70
<hr/>		
<b>6</b>	<b>Proposed amendments to the GDPR</b>	<b>71</b>
6.1	Motivations for amendments	71
6.1.1	Trust services	71
6.1.2	Crypto-asset service providers	71
6.1.3	Verification artefacts	71
6.1.4	Explicitly integrate Lindqvist	72
6.2	Proposed amendments to Recitals for the GDPR	72
6.2.1	Recital 65: Right of Rectification and Erasure	72
6.2.2	Recital 47: Overriding Legitimate Interest	73
6.2.3	Recital 49: Network and Information Security and Trust Services as Overriding Legitimate Interest	74
6.2.4	Recital 45: Fulfilment of Legal Obligations	75
6.2.5	Recital 26: Not Applicable to Anonymous Data	76
6.2.6	Recital 101: General Principles for International Data Transfers	77



# Executive Summary

The European Data Protection Board's draft guidelines on the processing of personal data via blockchain technologies do not yet fully reflect the positive role that blockchains – combined with privacy-preserving technologies – can play by removing intermediaries and thereby empowering users and enabling better protection of privacy and fundamental rights. They may also not yet be fully aligned with the intent of EU legislation on electronic ledgers and qualified electronic ledgers (eIDAS as amended by Regulation (EU) 2024/1183), financial regulation (AMLR, TFR), and crypto-asset regulation (MiCA). Moreover, the draft appears to adopt a relatively technology-conservative interpretation of the GDPR that, in our view, is difficult to reconcile with the Regulation's text and the case-law of the Court of Justice of the European Union (CJEU).

When examined against the GDPR and the CJEU's case-law in detail, the draft appears to reflect an expansive conception of "personal data" that characterises crypto-shredding and perfectly hiding commitments as personal data. It seems the draft's discussion of role allocation under the GDPR could benefit from greater conceptual precision. More than a cursory treatment of possible legal bases would be desirable. The draft also does not currently discuss the CJEU's Lindqvist judgment on the publication of personal data on the internet and its relevance for public permissionless blockchains.

We fully recognise that the draft guidelines seek to strengthen the protection of data subjects, and the analysis in this paper is intended to help attain that objective by showing how decentralised and privacy-preserving architectures can further the GDPR's objectives while remaining aligned with its regulatory requirements.

This paper proceeds in five parts: first, a general discussion; second, a detailed analysis of the GDPR that, in turn, provides guidance on its application to blockchain technology; third, a discussion of selected use cases, fourth, an outlook to the evolution of privacy preserving blockchain architecture, and fifth, a proposal for amendments of Recitals of the GDPR to reflect other EU legislation and CJEU rulings that have been passed since the EDPB draft.



Early development and adoption of blockchain technology were driven by a cypherpunk ethos: empowering users and reducing the leverage of central intermediaries. This overlaps with interests in the data protection community. While the GDPR also endorses privacy-preserving technologies<sup>1</sup>, its governance model presupposes hierarchical, identifiable parties that determine purposes and means. This assumption fits traditional centralised IT architectures found in the age of mainframes and does not match decentralised systems and organisations.

When applying the GDPR to blockchain-based processing, the Regulation should not be read as mandating centralisation. A technology-neutral interpretation must account for the privacy gains achievable through decentralisation, the possible gains in digital sovereignty and fundamental rights while setting guardrails so that risks to data subjects remain comparable to those of centralised designs. Centralised and decentralised systems come with different risks. When zero-risk is unattainable, users should not be forced to accept a particular risk but should have the right to choose among different risk profiles.

Although the GDPR was conceived primarily with centralised systems in mind – and applying it to blockchains can at first seem like squaring the circle – the Regulation’s text does provide room to accommodate decentralised architectures – including blockchains. In 2018, the French CNIL sought to balance the privacy-enhancing potential of decentralised technology with the specific risks associated with such technology. The EDPB’s long-announced guidance (first signalled in 2019/2020<sup>2</sup>) could have further developed that balance. Instead, the current draft guidelines on the processing of personal data through blockchain technologies appear to adopt a relatively restrictive reading that, in our view, may not be fully grounded in a contextual reading of the GDPR’s text, recitals, and CJEU case-law.

This paper seeks to restore that balance. The intention is not to question the importance of robust data protection enforcement, but rather to contribute to an informed dialogue on how existing principles can be applied in ways that reflect both technological realities and fundamental rights.

<sup>1</sup> While the term privacy-enhancing technology is more common, the term privacy-preserving technology seems to be more on the point and is used throughout this paper.

<sup>2</sup> EDPB Work Programme 2019–2020, 12 February 2019, [https://www.edpb.europa.eu/sites/default/files/files/file1/edpb-2019-02-12plen-2.1edpb\\_work\\_program\\_en.pdf](https://www.edpb.europa.eu/sites/default/files/files/file1/edpb-2019-02-12plen-2.1edpb_work_program_en.pdf)



Thus, this paper offers a detailed analysis of the GDPR's provisions as applied to blockchain and illustrates use cases in which decentralised designs support fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data - the objective of the GDPR as defined in Art. 1(2) GDPR. Those benefits could be reduced if courts were to endorse the draft's approach without substantial refinement.

## 1.1

### **The role of EDPB guidelines**

The EDPB brings together representatives of the supervisory authorities of the member states of the EU/EEA and the European Commission. Its task is to ensure consistent application of the GDPR across Member State authorities (Art. 70(1) GDPR). EDPB guidelines are not binding on courts and do not change the law. They are instruments intended to guide supervisory practice. They are influential, but the binding sources remain the GDPR, its recitals, and the case-law of the CJEU.

## 1.2

### **Types of blockchains and blockchain actors**

The blockchain ecosystem has developed into a broad variety of types of chains and is further advancing and diversifying. To limit the scope, this paper only distinguishes between permissionless public and permissioned (public or private) blockchains with a focus on permissionless public blockchains since these exhibit the largest differences to centralised computer systems.

This paper addresses roles such as miners, validators, sequencers and block producers, as well as entities that can govern a chain, people signing and transmitting a transaction, developers, deployers and operators of smart contracts (if there are any), and service providers that act for others on a chain. For reasons of simplicity, this paper, like the EDPB draft guidelines, does not differentiate between different consensus mechanisms and different blockchain models and refers to all actors involved in mining, validating, sequencing or block production as "miners/validators". Differentiating between different architectures and actors involved in the production of blocks could be done in a more nuanced case-by-case analysis in the future.



## 1.3

### **Structure and scope of this paper**

This paper consists of five parts. Part One examines blockchains, privacy and data sovereignty in general. Part Two offers an in-depth analysis of applying the GDPR to blockchains – particularly permissionless public blockchains. Part Three provides an outlook to the next generation of privacy-preserving blockchains.

Part Four then offers some exemplary use cases where the use of decentralised blockchain technology provides a significant privacy benefit.

Finally, Part Five proposes amendments to recitals to prevent interpretations of the GDPR that impose disproportionate burdens on decentralised technologies delivering privacy benefits.



## 2

# Blockchain, an architecture that enables data sovereignty and privacy-by-design

Within the data protection community, public permissionless blockchains are often portrayed as lacking compliance-critical features – clear controllership and accountability, mutability enabling rectification and erasure, and a central contact point for data subject rights. This paper takes the view that the GDPR is technology-neutral and does not prescribe specific roles or architectures. This chapter shows how blockchain-based systems are often motivated by resilience, censorship resistance, data sovereignty, and by the protection for privacy and fundamental rights that is at least equivalent to – or better than – centralised alternatives. Therefore, they should not be rejected on the basis of a restrictive, non-technology-neutral reading of the GDPR.

### 2.1

#### Blockchain as a means to privacy and data sovereignty of data subjects

Many blockchain projects are motivated by a lack of trust in centralised service providers. While GDPR establishes legal oversight of data controllers, this legal oversight is often regarded as ineffective. Blockchain design partly removes the need to trust centralised parties and replaces it with privacy-preserving technology and decentralisation. Validators or miners within blockchain networks come to consensus through mechanisms such as Proof-of-Work or Proof-of-Stake, which reduce reliance on central authorities. This fosters trust in decentralised systems, which are inherently more transparent and secure than traditional centralised systems that rely on trust in a single entity. Sometimes a bit of privacy is traded for transparency, verifiability, and sovereignty. Since all of these aspects are among the goals of the GDPR, users should be free to set priorities.

#### 2.1.1

##### Limits of user control in centralised Web 2.0 applications

While GDPR-compliant Web 2.0 systems promise user control over who can access their data, the reality is often different. While data protection authorities have imposed significant fines, material concerns persist including limited transparency and user control, continued extensive commercial use of personal data, and uneven enforcement suggesting the GDPR's objectives for large platforms are not yet fully achieved.



Web 2.0 companies, while legally obligated to provide users with information on how their data is used, often do so in a manner that is opaque and difficult to understand. As highlighted by Zeadally and Winkler<sup>3</sup> (2016), Facebook has faced repeated criticism and legal action for failing to adequately disclose how it shares user data with third parties – it often buries key information about data sharing practices deep in its terms and conditions, making it hard for users to make informed decisions about their data. Centralised repositories also concentrate risk: a single misconfiguration or insider can expose data at massive scale (e.g., the 533M Facebook dataset<sup>4</sup>). By contrast, decentralised peer-to-peer architectures, including blockchains, can reduce single points of failure when they combine self-custody, client-side encryption and least-privilege governance.

## 2.1.2

### **Immutability as a means for accountability**

Blockchain provides a transparent, immutable record of every transaction or action performed, which is – depending on the type of blockchain – visible to all network participants. This provides data integrity, which is a basis for accountability and the right to information. At the same time, privacy-preserving technologies can protect the privacy of actors and thereby also limit accountability. This renders it necessary but also possible to find a good balance between accountability and privacy. In a traditional Web 2.0 space, users have limited visibility into whether their data has truly been erased or if it still exists on e.g. Google's servers. Google controls the database, and users cannot independently verify whether their request has been fully implemented.

The GDPR balances accountability and other rights with the right to be forgotten; so can blockchain systems. While on-chain verification artefacts and metadata provide a basis for accountability, privacy-preserving technology restricts the use of the data for the targeted purpose and minimises the amount of data processed. Storing data off-chain allows data to be deleted.

The GDPR defines *accountability* not only as transparency of records but also as the responsibility of the controller to demonstrate compliance with GDPR (Art. 5(2) GDPR). This also applies to decentralised systems.

<sup>3</sup> Stefanie Winkler and Sherali Zeadally, "Privacy Policy Analysis of Popular Web Platforms," IEEE Technology and Society Magazine, Volume: 35, Issue: 2, June 2016, <https://doi.org/10.1109/MTS.2016.2554419>

<sup>4</sup> Aaron Holmes, Data breach affects more than 500M Facebook users worldwide, 3 April 2021, Business Insider, <https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4>



Every controller is accountable for their part of the processing but not for the entire chain of processing if that chain is controlled by the data subject themselves or other actors. The lack of control of intermediaries needs to be regarded as a gain in the data subject's data sovereignty and not as a lack of accountability of the controller.

## 2.2

### Blockchains as infrastructure

Telecom providers have content-agnostic obligations defined in the ePrivacy Directive. The ePrivacy Directive and its implementations are *lex specialis*<sup>5</sup> to the GDPR. A similar solution would fit blockchain infrastructure providers. eIDAS<sup>6</sup> now recognises *electronic ledgers* in Chapter III, Section 11. eIDAS distinguishes between electronic ledgers in general and qualified electronic ledgers meeting specific requirements. While the term *electronic ledgers* should encompass most blockchains, *qualified electronic ledgers* are limited to permissioned systems operated by qualified trust service providers. eIDAS does not create a GDPR exemption but imposes obligations concerning the ordering and integrity of records, which can justify continued storage of personal data on a blockchain. As discussed in 3.4.3.1, the draft implementation act of eIDAS clarifies that the integrity of a qualified electronic ledger requires immutability. For other electronic ledgers, integrity is a prerequisite for recognition. This can justify immutability under the GDPR on the basis of legitimate interest as discussed in 3.4.4. The EDPB draft guidelines do not yet contain a reference to the eIDAS Regulation that regulates *electronic ledgers* and *qualified electronic ledgers* in Arts. 45k-45l, while they do cite the Data Act for a definition of "smart contracts" – a term the GDPR does not itself use. Nodes of public, permissionless blockchains are usually not considered controllers, which means that they have no GDPR obligations as discussed in 3.3.1. Infrastructure requires legal certainty for those who operate it; a *lex specialis* regime would provide that certainty. If the eIDAS implementing act is adopted as drafted, legal certainty will at least improve. Ultimately, recognising eIDAS as *lex specialis* – coupled with a GDPR exception for blockchain nodes analogous to Article 95 and Recital 173, which applies particularly to telecom providers – would not only enhance clarity but also help ensure that data protection authorities properly account for the specialised regulatory framework for electronic ledgers.

5 "lex specialis" is a legal principle that the more specific law takes precedence over the more general law.

6 eIDAS as amended by Regulation (EU) 2024/1183, sometimes called "eIDAS II".



## 2.3

### Are GDPR and EDPB guidelines technology-neutral?

The GDPR claims to be technologically neutral in Recital 15. However, in practice core GDPR concepts seem to presuppose centralised governance. Applying them to decentralised systems with distributed roles and no single controller is difficult. However, a technology-neutral interpretation is possible and can be illustrated by two examples:

- a) The EDPB writes that the roles of controller and processor stem from factual elements or circumstances and are not negotiable<sup>7</sup>. This supports an allocation that fits decentralised systems – i.e., roles follow actual control, not assumptions that attribute control to actors who do not have it<sup>8</sup>. The blockchain community has been very active developing models for decentralised governance for blockchains and DAOs that go far beyond the limited models offered by the GDPR consisting of controllers with a hierarchy of processors and special duties for joint controllers. The EDPB could have pointed to positive models of decentralised governance. However, in “Recommendation 8. Governance” it only asks to document software changes and set out technical and organisational measures (TOMs). Rather than showing how positive decentralised governance models could be recognised *de lege ferenda*<sup>9</sup> in the future, the EDPB strongly recommends establishing a legal entity to bear the responsibility as a controller.

<sup>7</sup> EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, 7 July 2021, para 12, [https://www.edpb.europa.eu/system/files/2023-10/EDPB\\_guidelines\\_202007\\_controllerprocessor\\_final\\_en.pdf](https://www.edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf)

<sup>8</sup> See the discussion in 3.3.

<sup>9</sup> “*de lege ferenda*” means from a law-reform perspective.



- b) Blockchain can complement or substitute centralised public-key infrastructures (PKI) for digital IDs, qualified electronic signatures, seals and certificates as regulated in eIDAS. This technology, although important for a digital society, has seen uneven adoption rates in EU countries. In Switzerland, a non-EU country with a similar regulation, referendums have shown that the population is lacking the required trust in this centralised approach. Live revocation checks can leak usage data. At the same time, the EDPB draft tends to qualify blockchain-based artefacts like perfectly hiding commitments as personal data, as long as they are able to prove the integrity of a document<sup>10</sup>, whereas PKI artefacts with a similar function and identifiability are not regarded as personal data. A technology-neutral interpretation, however, will treat both verification artefacts similarly as discussed in 3.2.6 and 5.1.3.

Although the GDPR provides a regulatory framework that best fits centralised systems, it does not demand centralised systems. A technologically neutral interpretation of the GDPR might sometimes be difficult, but it is required according to Recital 15 GDPR. The GDPR does not provide a basis to privilege centralised technology.

## 2.4

### User autonomy and choice

The GDPR aims to reduce risks to data subjects. While decentralised systems may reduce risks associated with centralised actors, may provide greater control and may employ privacy-preserving technologies, they also introduce some new risks due to different governance models.

Although these new risks are usually lower and can be minimised, it should be left to the user to choose the type of risks they want to accept. No model is completely risk-free. If there is no centralised controller who might steal funds or abuse personal data, there is also no centralised controller to reset passwords, recover keys, or reverse transactions. There is an obligation to inform users about the consequences of their choices, but the GDPR is not an excuse for paternalism which is why it does not offer a legal basis to force users into accepting the risks of centralised systems.

<sup>10</sup> EDPB, Guidelines 02/2025 on processing of personal data through blockchain technologies, Version 1.1, adopted on 8 April 2025 for public consultation, para 53, [https://www.edpb.europa.eu/system/files/2025-04/edpb\\_guidelines\\_202502\\_blockchain\\_en.pdf](https://www.edpb.europa.eu/system/files/2025-04/edpb_guidelines_202502_blockchain_en.pdf)





Ideally, data protection authorities would positively encourage use cases of applying privacy-preserving technology with blockchain technology. These use cases could be whitelisted so that a data protection impact analysis (DPIA) would not be required (Art. 35 (5) GDPR).

The EDPB is called to give greater weight to the proportionality principle. Proposing the forced deletion of an entire blockchain because of a single block containing personal data without proper legitimisation would – if mandated – potentially infringe on the fundamental rights of many other data subjects.

## 2.5

### **Public blockchains compared to book publishing**

Public blockchains can be seen as a digital equivalent of book publishing. Through printing and the distribution of copies to libraries worldwide, the content of a book becomes almost immutable. While the author and the publisher are responsible for the publication of the content and can be liable for libellous or defamatory content, the publication can only be halted at the publisher or during distribution. Once the book is distributed, it can no longer be recalled. There is effectively no right to be forgotten for the data subjects concerned. However, data subjects can demand compensation if their rights have been violated by the publication of a book.

Book printing including the practical immutability of published content has enabled the advancement of society and is not regarded as a threat to the private life of citizens or other fundamental rights – rather the opposite. The respect for distributed books and libraries even in case of illegal content is due to proportionality. Even though a distributed book may infringe the right of an individual, the damage of removing distributed books or even entire libraries would be so huge that courts refrain from demanding it.



A similar proportionality check should be done for blockchains: Deleting an entire blockchain because of a single infringing block seems to be disproportionate<sup>11</sup>. Additionally, blockchains are usually not used to preserve content, but content is typically stored off-chain. They are often used to preserve metadata and proofs regarding off-chain data. One prominent example is NFTs. With the right balance, blockchain-based architectures can enable the right to be forgotten for the content while preserving proofs and metadata for accuracy, which is also a data protection principle in Art. 5(1)(d) GDPR. Even if the on-chain data, like a published book, infringes the rights of a data subject and even if central control would allow deletion of the entire blockchain, it is difficult to see how such a measure would generally be proportionate in the sense discussed by the EDPB<sup>12</sup>.

## 2.6

### The role of financial and crypto-asset regulation

Financial regulation aims at reducing anonymity and pseudonymity in asset transactions. The Markets in Crypto-Assets Regulation (MiCA), the Anti-Money Laundering Regulation (AMLR), Transfer of Funds Regulation (TFR), and other EU-level regulations, the Recommendations by the Financial Action Task Force (FATF) – notably Recommendation 16 (“travel rule”) and national laws impose strict requirements on the identification of transacting parties. Crypto-asset transactions on public blockchains can increasingly be related to the transacting parties. Crypto-asset service providers (CASPs)<sup>13</sup> are required to perform focused transaction monitoring. FATF considers transaction monitoring as an appropriate measure of risk mitigation and as part of AML/CFT obligations<sup>14</sup>. If this pseudonymous public transaction data is considered personal data that is not directly mandated by financial regulation, it should still be justified, because it is effectively required to be able to trade crypto-assets on EU exchanges and is used by crypto-asset service providers to detect scam and fraud.

11 But see para 63 of EDPB, Guidelines 02/2025 on processing of personal data through blockchain technologies, Version 1.1, adopted on 8 April 2025 for public consultation, [https://www.edpb.europa.eu/system/files/2025-04/edpb\\_guidelines\\_202502\\_blockchain\\_en.pdf](https://www.edpb.europa.eu/system/files/2025-04/edpb_guidelines_202502_blockchain_en.pdf)

12 EDPB, Guidelines 02/2025 on processing of personal data through blockchain technologies, Version 1.1, adopted on 8 April 2025 for public consultation, para 53, [https://www.edpb.europa.eu/system/files/2025-04/edpb\\_guidelines\\_202502\\_blockchain\\_en.pdf](https://www.edpb.europa.eu/system/files/2025-04/edpb_guidelines_202502_blockchain_en.pdf)

13 The FATF uses the term VASP (Virtual Asset Service Provider) whereas the EU legislation calls them CASP (Crypto-asset Service Provider). For readability purposes, the term CASP is used consistently in this paper.

14 Financial Action Task Force (FATF), Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, 2021, paras 167 and 295, <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.inline.pdf>



## Better coordination of regulation

This paper shows that the guidelines of the EDPB have the potential to support the goals of the GDPR in the blockchain context. Currently, they give limited explicit consideration to the objectives and obligations set forth in eIDAS, AMLR, TFR and MiCA. New legislation often includes a clause like *“This Regulation is without prejudice to Regulation (EU) 2016/679 of the European Parliament and of the Council”* that can be found in Art. 2(4) eIDAS II. This should not be interpreted as a signal to ignore those regulations when applying the GDPR. Digital innovation faces a complex set of regulatory regimes in the EU which, if not well coordinated, may create uncertainty and could inadvertently incentivise innovation to develop outside the EU. Different regulators should coordinate to avoid pushing innovators into opposing directions at the same time. The EDPB has announced Guidelines on transfers of personal data in the context of transfers of crypto assets. This is an opportunity to provide coordinated guidance with EBA, ESMA and AMLA that aims for a consistent and fundamental rights-oriented level of privacy and helps prevent situations in which CASPs feel pulled towards simultaneously offering both stronger and weaker privacy features.



## 3

# Applying the GDPR to data stored on blockchains

Blockchains are rarely used to directly store payload data, including payload data relating to natural persons, but they are used to store identifiers, hash values, commitments, zero-knowledge proofs and transaction metadata. This chapter discusses whether the GDPR applies and if it does, who is obliged by the GDPR, possible justifications for the processing of personal data and obligations connected to that processing. This chapter applies the definitions of the GDPR and the jurisprudence of the CJEU and arrives at considerably different results than the EDPB, for example regarding the scope of personal data, which is limited to information reasonably linkable to a natural person.

### 3.1

#### Applicability of the GDPR

The applicability of the GDPR has two main conditions: First, it has to fall into the material scope of the GDPR (Art. 2). This means it only applies to personal data<sup>15</sup> and it must not fall into the household exemption (Art. 2(2)(c) GDPR, see 3.3.5) or other exemptions. Second, it has to fall into the territorial scope of the GDPR (Art. 3). It is within the territorial scope of the GDPR if a controller or processor is established within the EEA (Art. 3(1) GDPR), or if goods or services are offered to data subjects in the EEA or behaviour of data subjects in the EEA is monitored (Art. 3(2) GDPR).

### 3.2

#### Identifiers, hashes and commitments: when do they qualify as personal data?

Most blockchain use cases write blockchain addresses and hashes on a blockchain. The EDPB draft states in paragraph 52 that hashes of personal data as well as identifiers will be considered personal data. Does this broad assumption hold in the light of the text of the GDPR and the jurisprudence of the European Court of Justice (CJEU)?

<sup>15</sup> The German Bundesbeauftragte für den Datenschutz und Informationsfreiheit (BfDI) held the rare view that GDPR also applies to anonymous data that was generated by anonymising personal data in 2021, but later retracted that decision. See « Fruit of the poisonous tree « -Doktrin im Datenschutz, ZD 2022, 249, <https://erbguth.ch/ZD05-2022-Editorial.pdf>, BfDI, 13-317/018#0127, 17 February 2021, <https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/AccessForAll/2021/2021-Studie-Kindeswohl-Umgangsrecht.pdf>, BfDI, 13-317/018#0127, 27 July 2023, <https://media.frag-den-staat.de/files/foi/891333/anderungsbescheid-27-07-2023.pdf>



### 3.2.1

#### Definition of personal data

Art. 4(1) GDPR defines personal data as any information relating to an identified or identifiable natural person ('data subject'). Recital 26 adds that anonymous information is not personal data. *To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.*

In Breyer<sup>16</sup>, the CJEU held that log files containing IP addresses can be personal data because the internet service provider (ISP) stores data to identify the IP addresses with natural persons and the website operator had legal means to access that data. In EDPS v SRB<sup>17</sup> the CJEU insisted on an actor-specific, case-by-case approach in determining personal data and considers other persons only insofar as they have access to the data and are reasonably likely to identify the data subject.

The Court confirmed that identifiability must be assessed per actor using the "means reasonably likely" test; merely theoretical or unlikely re-identification is insufficient. Pseudonymised data must not be regarded as constituting, in all cases and for every person, personal data for the purposes of the application of the GDPR, in so far as pseudonymisation may, depending on the circumstances of the case, effectively prevent persons other than the controller from identifying the data subject in such a way that, for them, the data subject is not or is no longer identifiable.

In EDPS v SRB, SRB provided a pseudonymised data set to Deloitte on a virtual server. In the assessment of identifiability for Deloitte, the CJEU did not take into account that SRB had access to that virtual server and was able to re-identify the pseudonymised data with the data subjects since it had the complete data set including the names of the data subjects.

<sup>16</sup> Patrick Breyer v Bundesrepublik Deutschland, Court of Justice of the European Union (CJEU), Judgment of 19 October 2016, Case C-582/14, ECLI:EU:C:2016:779, para 49, <https://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=EN>

<sup>17</sup> EDPS v Single Resolution Board (SRB), Court of Justice of the European Union (CJEU), Judgment of 4 September 2025, Case C-413/23 P, ECLI:EU:C:2025:645, para 86, <https://curia.europa.eu/juris/document/document.jsf?docid=303863&doclang=EN>



The CJEU did not provide a detailed reasoning for this. However, given the risk-based nature of the GDPR and the definition of the personal data that requires “information” and not mere data, this would perfectly fit into the system of the GDPR. Additional pseudonymous data becomes personal data only if it contributes information about a natural person beyond what is contained in the dataset used to relate the data to that person.

Conversely, if the identifier that links otherwise non-identifiable data to a natural person already includes all relevant information, and the linked dataset merely mirrors what is inherent in that identifier, then no new information relating to the data subject is introduced. The linked dataset therefore neither adds information relating to a natural person nor creates any additional risk to the data subject. It should therefore not be considered personal data.



### Identifiers

Identifiers are mentioned as a means to relate information to a natural person. Some identifiers can also consist of combinations of several factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Other identifiers do not contain any information about a person but might link some information to a natural person and thereby provide information about that natural person, the data subject. Sometimes, this detail is lost, and those identifiers themselves are already seen as personal data. However, the definition of personal data requires linking information – an identifier linking to nothing does not do so. In the case of IP addresses, for example, the list of all IPv4 addresses, a list of  $2^{32}=4294967296$  numbers that could easily be stored on any computer, would not constitute a file with personal data about most internet users.

In the case of Breyer, the CJEU had to decide whether internet log files, including the IP addresses where the requests came from, constitute personal data. The CJEU even stated that it is common ground, that a dynamic IP address does not – as such – constitute personal data, but that the specific situation, the storage of log files of an institution operating a website had to be considered<sup>18</sup>. The log files provide information on what pages have been viewed using an IP address and the German law provided legal means to demand the ISP to identify the customer that had been assigned the dynamic IP address at a given time. If identifying the customer were either *prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power*, it would not have constituted personal data, the court held in paragraph 46. Wallet addresses and public keys can be identifiers that relate to natural persons if held by or for natural persons. However, the identifiability might be restricted to the data subjects themselves if the wallet address has not been shared with anybody. Then, the wallet address (and in some cases only the visible hash of a wallet address) rather has the character of a commitment (see 3.2.5). If wallet addresses are not reused, the potential for identifiability across transactions decreases substantially. In line with the recent CJEU decision<sup>19</sup>, the transaction data may only be considered personal data, by those who can effectively identify the transactions with the holder. In case the identity has been registered by a crypto-asset service provider ready to be queried by authorities and other entities when conditions are met, and transaction data beyond the mere blockchain address is available, the situation could be similar to the Breyer case on IP addresses, which the CJEU decided in 2016.

<sup>18</sup> Patrick Breyer v Bundesrepublik Deutschland, Court of Justice of the European Union (CJEU), Judgment of 19 October 2016, Case C-582/14, ECLI:EU:C:2016:779, para 49, <https://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=EN>

<sup>19</sup> EDPS v Single Resolution Board (SRB), Court of Justice of the European Union (CJEU), Judgment of 4 September 2025, Case C-413/23 P, ECLI:EU:C:2025:645, para 86, <https://curia.europa.eu/juris/document/document.jsf?docid=303863&doclang=EN>



### 3.2.3

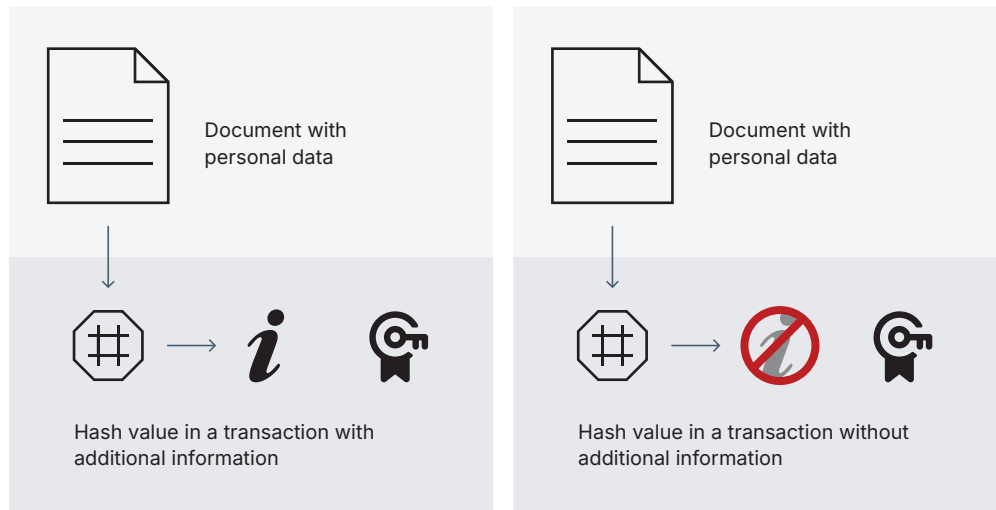
#### Hashes of personal data

A cryptographic hash function is a one-way function that maps possibly large amounts of data to a relatively short bit sequence (e.g. 256 bits). It is practically impossible to find an input value for a given output value. While theoretically many inputs lead to the same output, it is practically impossible to find a second input value that generates the same output. Cryptographic hash functions can therefore be used to hide data from everyone that does not already know it and to make it verifiable to all that know it. As such, hashes are a perfect tool to provide privacy while still allowing verification for those who hold the data. It is impossible to infer the hashed data if done correctly. A hash value allows to set a unidirectional link from the hashed document to the hash value without modifying the original document. In general, this does not create a link from the hash value to the original document. Still data protection authorities claim that hashes of personal data generally constitute personal data.

According to the definition of personal data, for something to be considered personal data, it has to be identifiable with a natural person, *and* it must convey information. A hash only reflects the result of a one-way computation and conveys no additional information. It does not link to the document hashed but the mathematical calculus allows to link the document to the hash, not the other way round. The hash value does not convey the information in the document, but the information in the document is needed to calculate it. Holding the document that was hashed allows linking to the hash value. However that process does not disclose but presupposes the content of the document. Arguing that the hash value through this process discloses the information in the document ignores the fact that the process only uses the information to compute the hash value. It is only visible to the person that already has it – like in an empty mirror. An empty mirror does not constitute personal data. In terms of the GDPR definition of personal data, the hash can be identified with a natural person only if this information is already present in the document needed to link the document to the hash. Therefore, it does not convey any information relating to that person.

The opinion of the data protection authorities, read literally, would mean that the root of a Merkle tree where a leaf contained personal data, would also be considered personal data. It would mean that in a block-chain where a block created years ago contained personal data, every new block contains a hash of hashes of the old block and therefore were also considered to be personal data. Such an interpretation would appear overly broad and may be particularly difficult to reconcile with CJEU case-law. So, why do data protection authorities arrive at the statement that hashes of personal data are personal data?





*Figure 1: Example: When a transaction contains a hash value of personal data and additional information, it relates the additional information to the data hashed. If it does not contain additional information, it can only be used to verify the data that was used to compute the hash.*

### 3.2.4

#### **Use of hashes as identifiers**

A specific use case for cryptographic hashes is to use them as identifiers in pseudonymised data. For example, in a table of records the name and the date of birth are replaced by a hash of this information. The data remains usable, and the identity of the data subjects is not directly visible. However, even random identifiers will not render data anonymous if partial knowledge of the data about a person would allow singling out one record and then identify further information regarding this person. Hash values used as identifiers would even allow calculating the hash value with the basic personal data like name and the date of birth and then select all records relating to that person.<sup>20</sup> In these kind of use cases, hash values calculated from personal data can indeed constitute personal data. As seen in Figure 1, the hash value does not link to the document containing personal data, but it allows the document with personal data to be linked to additional information contained in the transaction. The document serves as a key to link the additional information to the document via the hash value. Since the document with personal data relates to a natural person, the additional information on the blockchain is indirectly related to the natural person. If that information has not been part of the document already, this turns the transaction data that includes the hash value into personal data. However, this is not the dominant use case of hash values in the domain of blockchain applications.

<sup>20</sup> WP29, Opinion 05/2014 on Anonymisation Techniques, 10 April 2014, p. 22, [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf)



### 3.2.5

#### Hash values used as commitments

A commitment is defined by the French data protection authority CNIL as *a cryptographic mechanism that allows one to “freeze” data in such a way that it is both possible – with additional information – to prove what has been frozen and impossible to find or recognise such data by using this sole “commit”*<sup>21</sup>. Hash values can be used for commitments if they are perfectly hiding.

Hash values are not perfectly hiding if the hashed information can be obtained independently of the verification process either by guessing or because it is available somewhere. With the data that was hashed at hand, the hash value can be calculated and verified. To avoid guessing the data that is hashed, it must have enough entropy. With sufficient entropy, guessing would take centuries or more and is therefore practically impossible. With commonly used hash functions like SHA256, high-performance mining hardware needs to be taken into account. The EDPB therefore recommends using hash functions that require more memory where mining hardware is not available like argon2<sup>22</sup>. Using them, less entropy is needed.

However, even with SHA256, it is easy to provide enough entropy. The total hash rate of Bitcoin seems like a useful upper limit of currently available hashing power. The complete hash rate of Bitcoin can be roughly estimated as 1 billion TH/s<sup>23</sup> or  $10^{21}$  hashes per second or  $3.2 \cdot 10^{28}$  hashes per year. Including a random 128-bit UUID as “salt” with an entropy of about  $3.4 \cdot 10^{38}$  provides enough entropy. This is in line with 2019 NIST requirements of 112 bits for HMAC keys<sup>24</sup> and the recommendation of 128-bit salt for Argon2 password hashing<sup>25</sup>. It is well above the 32-bit NIST minimum<sup>26</sup> for salt.

Scanned documents usually have much more entropy and do not require the addition of salt.

21 CNIL, Solutions for a responsible use of the blockchain in the context of personal data, 2018, [https://www.cnil.fr/sites/default/files/atoms/files/blockchain\\_en.pdf](https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf)

22 EDPB, Guidelines 01/2025 on Pseudonymisation, 16 January 2025, para 89, footnote 26, [https://www.edpb.europa.eu/system/files/2025-01/edpb\\_guidelines\\_202501\\_pseudonymisation\\_en.pdf](https://www.edpb.europa.eu/system/files/2025-01/edpb_guidelines_202501_pseudonymisation_en.pdf)

23 Blockchain.com, Total Hash Rate, <https://www.blockchain.com/de/explorer/charts/hash-rate>

24 NIST, Special Publication 800-131A, Revision 2, Transitioning the Use of Cryptographic Algorithms and Key Lengths, March 2019, <https://doi.org/10.6028/NIST.SP.800-131Ar2>

25 Argon2 Memory-Hard Function for Password Hashing and Proof-of-Work Applications, RFC 9106, December 2023, <https://datatracker.ietf.org/doc/rfc9106/>

26 NIST, Special Publication 800-63B, Digital Identity Guidelines, June 2017, last updated March 2020, <https://doi.org/10.6028/NIST.SP.800-63b>





Even with enough entropy, the hash is not perfectly hiding if the document is known outside of the verification context. Therefore, data protection authorities like the EDPB or the CNIL recommend using a “keyed hash”. This secret key is also called “pepper”. This key, however, is redundant, if the document does not exist outside the verification context, when it is made verifiable by the original author and the hash does not act as an endorsement. Then the document itself acts as the key. More details on this below in 3.2.7.

### 3.2.6

#### **Do commitments constitute personal data?**

Although the EDPB recognises the privacy-preserving value of commitments, it states in para 52 of its draft guidelines<sup>27</sup> that a salted or keyed hash written on-chain is personal data; only after deletion of the key/salt the hash should not be linkable to the original data. This means, even a commitment consisting of a keyed hash is considered personal data as long as it has not been disabled by securely deleting the key.

<sup>27</sup> EDPB, Guidelines 02/2025 on processing of personal data through blockchain technologies, Version 1.1, adopted on 8 April 2025 for public consultation, para 52, [https://www.edpb.europa.eu/system/files/2025-04/edpb\\_guidelines\\_202502\\_blockchain\\_en.pdf](https://www.edpb.europa.eu/system/files/2025-04/edpb_guidelines_202502_blockchain_en.pdf)



In our view, this approach does not yet fully take into account the following considerations:

- a) The hash value does not link to the document but the document is linked to the hash. The properties of cryptographic hash functions enable to establish a link from the document to the hash value without touching the document. That enables verification of a document that the verifier already has, but it is not linking information about a natural person to the hash value.
- b) The hash value does not reveal or enable reconstruction of the original document. The hash value is useless if the document is not known. Guessing is not possible if the document contains enough entropy.
- c) Pseudonymised data where the controller has no way to obtain information that allows them to identify the data subject are not considered personal data. Here, the hash value does not even allow anyone to derive anything about the data hashed let alone identifying natural persons. Only the document itself allows that. Being written on a blockchain enables one to derive the approximate date and possibly the address responsible for recording the hash value on that blockchain. With the document at hand this can serve as a time stamp. Without the document, it cannot even be determined whether such a document exists.

Regarding (a) The hashed document can be used to find the hash value, but the hash value is not used as an identifier to link additional information to the hashed document, as described in 3.2.4. It only allows verifying the authenticity or integrity of the hashed document. A commitment or hash that, by itself, only enables verification (which means it is perfectly hiding) and is not connected to information about a person (which means it cannot be used as an index or lookup key) is not personal data. Verifying a document that contains personal data is, of course, processing personal data – but that processing concerns the document, the verification artefact only serves as a tool to do so.

Hashes used as commitments serve a similar purpose as centralised public-key infrastructure (PKI). Qualified electronic certificates enable the verification of qualified electronic signatures (natural persons) or qualified electronic seals (legal persons) on documents.

An electronically sealed document may contain personal data, yet the qualified electronic certificate itself is not regarded as personal data; likewise, when looking at the definition of personal data, a perfectly hiding commitment is no more “about” the data subject than the qualified certificate is. Both artefacts allow the original document to be verified, but neither adds information beyond the document itself as shown in Figure 2.



The fact that a certificate is typically generated beforehand as part of a neutral infrastructure and a commitment is generated after the verified document exists does not change this legal characterisation.

Regarding (b), both artefacts do not allow anyone to derive anything about the content of the document and relate to the document only passively. The document cannot be generated from either the certificate or the commitment; given the document, however, each serves as a verification artefact. Treating the certificate as “neutral” but the commitment as “document-bound” therefore misconceives the definition of personal data in Article 4(1) GDPR: in both cases the artefact is merely a verifier and does not, as such, convey information about a natural person absent any additional contextual information.<sup>28</sup>

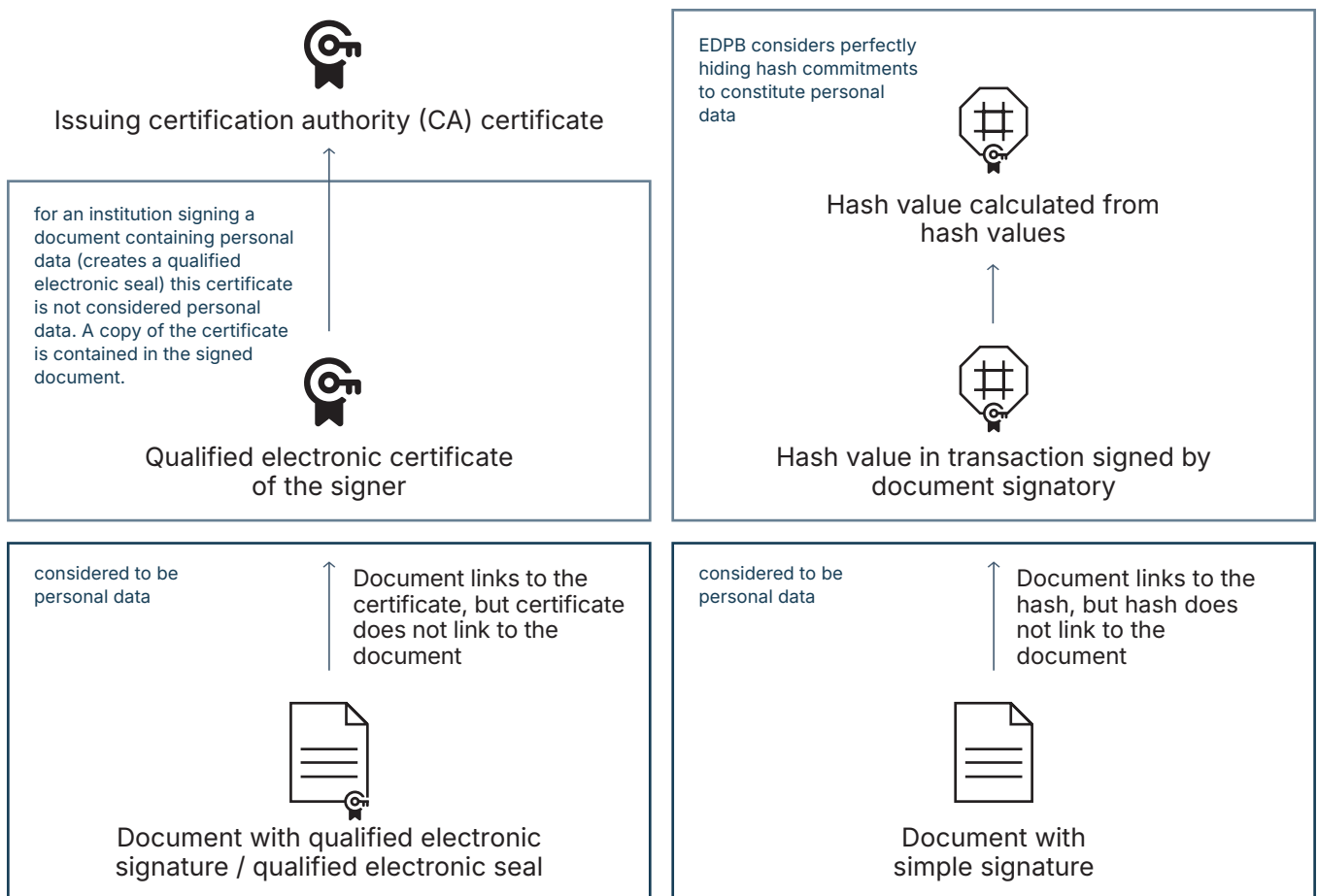


Figure 2: Comparison of verification through public key infrastructure (PKI) and blockchain-based hashes

<sup>28</sup> If the certificate or hash themselves link to the signer and the signer is not an institution but a natural person, both might be considered personal data for that reason. This aspect is being excluded here because the discussion focusses on the question whether these verification artefacts are considered personal data because they are used to verify a document containing personal data.

Regarding (c) the European Court of Justice recently argued for a practical approach regarding pseudonymised personal data.<sup>29</sup> If the pseudonymisation is sufficiently robust, the identification of the data subject is not reasonably likely and therefore the data is not considered personal data. Although the identification was probably possible for the entity that held the non-pseudonymised data, this did not turn the pseudonymised data into personal data for another controller that did not have the means to reidentify the pseudonymous data.

Applying this to hashes of personal data stored on a blockchain, they do not constitute personal data for actors who do not have the document that has been hashed. When further comparing certificates with hashes, there is also no general cardinality distinction that would matter for the legal test. A single certificate can validate none, one or many signatures depending on the usage pattern; a commitment can likewise cover none, one or many documents (for example by committing to a Merkle root). Even if there were a difference in cardinality, this would not affect whether the artefact itself constitutes personal data.

Qualified electronic timestamps are a trust service also regulated by eIDAS Regulation<sup>30</sup>, just like signatures and seals. They rely on qualified trust service providers' (QTSP) certificates and status information. They also share the same PKI architecture and the same verification-privacy characteristics. A commitment recorded on a blockchain can have the meaning of a signature, seal or can be used purely as a proof-of-existence/timestamp. In these use cases they are verifying a document and not providing information about a natural person.

Regarding data protection risks, PKI-based verification often entails consulting revocation/status information (e.g., the Online Certificate Status Protocol (OCSP) or Certificate Revocation Lists (CRLs)), which can reveal which certificate is being checked to the status service; a commitment with revocation information stored on a blockchain has no similar trust-status channel. These verification channels can be abused to monitor the usage of a certificate. Although techniques exist to reduce this privacy risk, they are not generally used with PKI. Decentralised technology cannot be comprehensively monitored. Providing verification information on-chain, therefore, reduces the privacy impact for the data subjects as long as revocation information should be publicly visible to all verifiers.

**29** EDPS v Single Resolution Board (SRB), Court of Justice of the European Union (CJEU), Judgment of 4 September 2025, Case C-413/23 P, ECLI:EU:C:2025:645, paras 84-88, <https://curia.europa.eu/juris/document/document.jsf?docid=303863&doclang=EN>

**30** Under eIDAS Arts. 41–42, a qualified timestamp binds date/time provided by a certified trust service to the data and is electronically sealed using a qualified electronic certificate.



In a technology-neutral reading of the GDPR, verifying a document that contains personal data is processing personal data (regardless of whether the verifier uses a simple hash, a Merkle root, or a certificate). The verification artefact itself (hash/commitment/certificate), however, will generally not constitute personal data where it is perfectly hiding the verified content<sup>31</sup>.

In the same reading, the deletion of a key or salt of a hash used by the commitment and thereby the removal of the possibility to verify the content, does not appear necessary to avoid rendering the verification artefact personal data, and risks creating unnecessary obstacles for decentralised solutions that provide privacy benefits.

**31** Here it is only discussed whether the verification artefact needs to be considered personal data because the verified document contains personal data. Other reasons for the verification artefact being considered personal data, e.g. because the certificates enables a natural person and not an organisation to sign, are excluded from this discussion.



### 3.2.7

#### Salt, pepper and keyed hashing

The use of salt or pepper in hashes has been partly motivated by the desire to be able to destroy the functionality of the verification artefact. As shown above that there is no GDPR-requirement to destroy the verification artefact, due to the artefact not being personal data, such a key does not have to be added unless required otherwise. Other reasons can be insufficient entropy of the data to be certified, or the document is known in an unverified state and the verification serves as an endorsement by someone other than the author.

When the hash serves as an endorsement by a third party, this provides additional information. In this case, this additional information might need to be shielded from the original document. A way to shield this information is a keyed hash where the hash is provided only to those for whom the endorsement is meant to be visible. The same functionality could be achieved by creating a new document combining the original document and the endorsement and then hashing this new document.



### 3.2.8

#### Limits of hashes and security considerations

Hashes come with certain rather technical risks: The risks of not having enough entropy or hashing a known document already have been addressed. Precomputed hash tables for known information can also increase the risk of effectively reversing the hash function.

Some hash functions like MD5<sup>32</sup> are known to be broken. Other hash functions might be able to be broken by quantum computers in the future. Therefore, new, quantum-resistant hash algorithms are proposed<sup>33</sup>. Although broken hash functions impact the verification functionality of a hash function, they still do not allow anyone to derive the hashed data from the hash value and do not create an additional privacy risk when hash values are used for verification purposes.

### 3.2.9

#### Zero-knowledge proofs

A commitment binds to a hidden value (hiding + binding) but by itself proves no property about that value. A zero-knowledge proof (ZKP) allows a prover to convince a verifier that a statement about a (possibly hidden) value is true without revealing that value. ZKPs can be interactive or non-interactive; plain non-interactive ZKPs are transferable, while designated verifiers or interactive proofs can restrict who can verify. To prove properties of committed data without revealing it, a commit-and-prove scheme can be used.

While zero-knowledge proofs can provide unmatched privacy protection, they also create artefacts that are only passively related to natural persons when an assertion about a natural person is proven. The artefact does not allow to identify a natural person but there is a link from the proven information to the artefact. So, the same argumentation is applicable: The verification artefacts as such are not considered personal data since – by design – they do not provide additional information when proving some assertion.

**32** Gorka Ramirez, MD5, the broken algorithm, 28 July 2015, <https://www.avira.com/en/blog/md5-the-broken-algorithm>

**33** Manju Singh, Sunil K. Singh, Sudhakar Kumar, Mehak Preet, et al., Quantum-Resilient Cryptographic Primitives: An Innovative Modular Hash Learning Algorithm to Enhanced Security in the Quantum Era, 14 March 2024, <https://doi.org/10.21203/rs.3.rs-4052058/v1>



### 3.3

## Roles under the GDPR: Controllers and processors

Where personal data is processed, the roles of controllers and processors must be established. Are there controllers and processors in a decentralised system like a blockchain? The GDPR defines the controller in Art. 4(7) GDPR as the entity “which, alone or jointly with others, determines the purposes and means of the processing of personal data”. The GDPR does not specify how many controllers there must be. It is also not possible to assume the role of controller; rather, it depends on the factual situation. As the French CNIL did in 2018, the EDPB takes a differentiated view here. This functional definition, however, is hard to apply to decentralised systems. Decentralised and distributed systems where several actors engage on the basis of open protocols rather than a closed ecosystem exhibit a fragmented set of control. Blockchains are specifically engineered to minimise control by a single actor. Depending on the system and situation, three levels of control can be identified as shown in Figure 3: the transaction level, the level of a smart contract (if smart contracts are available and used) and the blockchain infrastructure level. Since blockchain technology inherently disperses and limits control, and Article 4(7) GDPR defines a controller by reference to actual determination of purposes and means rather than by mandatory designation, some blockchain contexts may have no entity that qualifies as a controller.

Controller on which level?

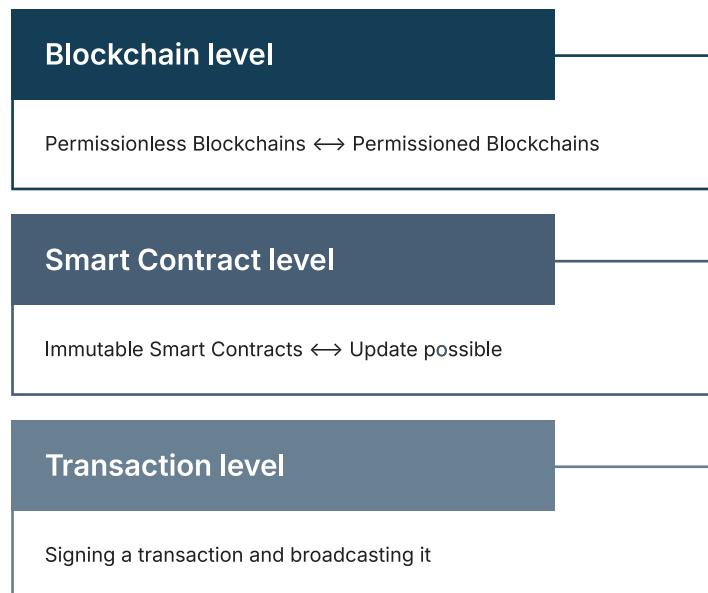


Figure 3: Levels of control in the context of blockchains



### Blockchain level

The blockchain level comprises the execution, consensus and data layers. Depending on the architecture, these layers are either performed by the same actors or split between different actors. While the architecture of many blockchains includes several layers and various structural components (such as sidechains or rollups), these specific architectural elements and corresponding roles are not differentiated for the purposes of this paper.

On a permissioned blockchain, the blockchain is governed by a single entity or a governance consortium. Such an entity could, in theory, grant rights only to those that are willing to accept a patch that changes the functionality of the blockchain or modifies a specific block. This theoretical possibility could be regarded as the possibility to determine purpose and means. However, in practice, any governance decision is subject to the acceptance of the participants. They could resist and fork the chain. Therefore, even with permissioned blockchains, the power of the governing entity is limited, and it must be determined whether the governing entity can determine purposes and means of the blockchain, and thus be considered a controller under the GDPR.

On a permissionless blockchain, nobody, typically, has control over the blockchain as such. This means that nobody – neither as a single actor nor jointly with others – determines purposes and means of processing<sup>34</sup>. The CNIL (2018) held that miners are not controllers, because they *are only validating transactions submitted by participants and are not involved in the object of these transactions: therefore, they do not define the purposes and the means of the processing*<sup>35</sup>. The EDPB confirms this in para 42: In some blockchain systems, mining nodes have only a limited decision-making power [...]. *In such circumstances, nodes would not determine the purposes and means of the processing itself, and therefore might not be considered as controllers.* In paras 43 and 44, the EDPB lists exceptions where control could exist, for example, by colluding nodes. In this context, the discussion in paras 42-44 may blur the distinction between permissionless and consortium/permissioned blockchains. Paragraph 42 is framed in the context of permissioned blockchains, whereas the advice to have a central legal entity is presented in paragraph 44 in relation to public permissionless blockchains. This appears in tension with the definition of public permissionless blockchains, where no single entity coordinates the processing. As a result, the draft only indirectly states that nodes of permissionless blockchains would typically not be considered controllers save for exceptional circumstances.

<sup>34</sup> Jörn Erbguth, Wer ist Verantwortlicher einer Bitcoin Transaktion?, ZD 2017,560 and Jörn Erbguth in Louisa Specht-Riemenschneider, Datenrecht in der Digitalisierung, 2020, § 6.2, para 84.

<sup>35</sup> CNIL, Solutions for a responsible use of the blockchain in the context of personal data, 2018, p. 2, [https://www.cnil.fr/sites/default/files/atoms/files/blockchain\\_en.pdf](https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf)



### 3.3.2

#### Smart contract and DAO level

Many blockchains support smart contracts. Smart contracts are small code fragments that can program transactions and that can be triggered by external calls. Smart contracts can manage crypto-assets and store a limited amount of data. Smart contracts can be used for a large variety of purposes. They can be used to control crypto-assets, for governance purposes – particularly of a DAO, to collect votes, for rental contracts, to certify documents or any kind of files. Their usage can be limited to the deployer, open to a specific group, or accessible to anybody.

A smart contract is deployed to a blockchain via a signed transaction. It is typically written by a developer and published by a deployer (these may be the same or different persons). Some contracts include admin functions (e.g., upgrade, pause/kill, parameter changes) that are controlled by a private key, a multisig arrangement or the governance scheme of a DAO. Users interact with the contract by sending transactions to its address. Access can be permissionless or restricted via access-control mechanisms. Contracts may define privileged roles such as oracles, which supply data authenticated by designated keys. Depending on the blockchain and tooling, the contract's bytecode is public by default; the source code may be made available for verification so that users can review the contract's functionality.

The rationale from the blockchain-level controller analysis can also be applied to smart contracts or DAOs. Only if the contract was deployed with the ability to update, pause/stop, or otherwise control its use, the entity holding those powers may retain the power to determine purpose and means of the processing of the smart contract. If no such powers exist, there is no controller after the deployment. Oracles may just provide neutral data like weather data or may provide arbitration decisions by human arbitrators. Oracles usually do not determine purposes and means of the processing except for edge cases where their input is effectively determining the purposes and means of the processing of the smart contract. The purposes and means of individual transactions of a smart contract may be determined by the callers who sign and send them, but this does not, by itself, amount to becoming a controller of the processing of the contract as such. Where there is a controller on the chain-level, this controller may be able to block interactions of a smart contract running on such systems – though such powers may be limited in practice.

The blockchain community has developed well-advanced decentralised governance models. The GDPR cannot be applied to most of the models because members determine purposes and means neither individually nor jointly. Having no controller might feel unsatisfactory, however, assigning the role of controller *contra legem*<sup>36</sup> to participants that have no control in determining purposes and means would be worse.

<sup>36</sup> "contra legem" means an interpretation contrary to the wording of the law.



Providing a statutory framework for new governance models could be proposed de lege ferenda. This would allow for DAOs to have legal power to act and legal responsibility at the same time.

### 3.3.3

#### Transaction level

Transactions are controlled through the private key. Signing the transaction and sending it to a node is controlling the transaction. The transaction level control usually ends when the transaction is sent.

Transactions can also be submitted on behalf of a natural person or legal entity, e.g. when a crypto-asset service provider signs and sends them for a client.

### 3.3.4

#### Joint controllers

Under the GDPR multiple entities can be considered controllers. Several controllers may be considered joint controllers, if they jointly determine purposes and means of processing of personal data (Art. 26(1) GDPR). The EDPB holds: *Not all processing involving several entities give rise to joint controllership. The overarching criterion for joint controllership to exist is the joint participation of two or more entities in the determination of the purposes and means of a processing. More specifically, joint participation needs to include the determination of purposes on the one hand and the determination of means on the other hand*<sup>37</sup>. If these elements are jointly determined, meaning together and not independently by each controller, the controllers might be joint controllers of the processing at issue.<sup>38</sup> Joint controllers do not have to have equal control.

Members of consortium blockchains might be regarded as joint controllers unless there is a legal entity like an association that exercises the decision-making power. The EDPB points out that this entity or consortium will be the controller of the blockchain<sup>39</sup> which means that it bears the legal responsibility. However, the EDPB suggests this for public permissionless blockchains which runs contrary to the concept of a permissionless blockchain. A central entity that is not determining the purposes and means would not be considered a controller and a central entity that does determine both aspects runs counter to the very concept of permissionless blockchains.

<sup>37</sup> Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH (Facebook Fanpage), Court of Justice of the European Union (CJEU), Judgment of 5 June 2018, Case C-210/16, ECLI:EU:C:2018:388, para 43, <https://curia.europa.eu/juris/document/document.jsf?docid=202543&doclang=EN>

<sup>38</sup> EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, 7 July 2021, [https://www.edpb.europa.eu/system/files/2023-10/EDPB\\_guidelines\\_202007\\_controllerprocessor\\_final\\_en.pdf](https://www.edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf)

<sup>39</sup> EDPB, Guidelines 02/2025 on processing of personal data through blockchain technologies Version 1.1, adopted on 8 April 2025 for public consultation, para 44, [https://www.edpb.europa.eu/system/files/2025-04/edpb\\_guidelines\\_202502\\_blockchain\\_en.pdf](https://www.edpb.europa.eu/system/files/2025-04/edpb_guidelines_202502_blockchain_en.pdf)



Miners/validators in permissionless blockchains adhere to a set of rules for building the next block. By design, they do not have the power to alter these rules. If they deviate from the rules, their blocks will be rejected by other miners/validators, and they will lose their block reward. Even if the block building rules include a regime to block certain transactions, this will not render miners/validators joint controllers. Only when miners/validators collude to jointly decide on altering the rules, there might be a point of joint control.

### 3.3.5

#### **The household exemption or the data subject as a controller**

Article 2(2)(c) GDPR excludes from its scope the processing of personal data by a natural person in the course of personal or household activity. In 2018, the CNIL noted that this exemption may apply to some blockchain use cases by natural persons acting on their own behalf and outside a professional or commercial context (e.g., buying/selling Bitcoin for oneself).<sup>40</sup> Applying the household exemption avoids qualifying such natural persons as controllers, since imposing controller obligations would require the disclosure of their identity and would therefore turn the GDPR from an instrument of privacy protection into a source of privacy intrusion.

The CJEU has interpreted the household exemption narrowly where personal data are made accessible to an indefinite audience on the internet<sup>41</sup> or the public sphere is affected<sup>42</sup>. Recital 18 GDPR, however, does include social networking and online activity in the household exemption. Bäcker<sup>43</sup> as well as Schmidt<sup>44</sup> therefore argue for the application of the household exemption to social media posts when the access is limited.

Normatively, the household exemption safeguards Article 7 CFREU and should be restricted only where a household activity causes a meaningful privacy impact on others, consistent with Article 52(1) CFREU (essence, necessity, proportionality). Publication seems too broad; what matters is effective identifiability and impact.

**40** CNIL, Solutions for a responsible use of the blockchain in the context of personal data, 2018, p. 2, [https://www.cnil.fr/sites/default/files/atoms/files/blockchain\\_en.pdf](https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf)

**41** Criminal proceedings against Bodil Lindqvist, Court of Justice of the European Union (CJEU), Judgment of 6 November 2003, Case C-101/01, ECLI:EU:C:2003:596, para 47, <https://curia.europa.eu/juris/document/document.jsf?docid=48382&doclang=EN>

**42** František Ryneš v Úřad pro ochranu osobních údajů, Court of Justice of the European Union (CJEU), Judgment of 11 December 2014, Case C-212/13, ECLI:EU:C:2014:2428, para 33, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62013CJ0212>

**43** Bäcker in BeckOK Datenschutzrecht, Wolff/Brink/v. Ungern-Sternberg 52nd edition, August 2023, Art. 2 GDPR, paragraph 19-21

**44** Wolff/Brink/v. Ungern-Sternberg as well as Schmidt in Taeger/Gabel, DSGVO - BDSG - TTDSG, 4<sup>th</sup> edition, 2022, Art. 2, paragraph 25-26



Therefore, this paper proposes an impact-based reading. This is supported by the GDPR's own architecture: Recital 26 requires assessing identifiability by the means reasonably likely to be used, and the recent decision of the CJEU in *EDPS v SRB* confirmed that whether data are "personal" can depend on the recipient's position and realistic means (i.e., a contextual, actor-relative test).<sup>45</sup>

Accordingly, for public, permissionless ledgers, the mere fact of on-chain publication should not automatically exclude the household exemption. Where the published artefacts are effectively unintelligible to the general public and not reasonably linkable to natural persons without specialised datasets or powers, the household actor's processing may remain within Article 2(2)(c) if the processing concerns personal data at all. When a person covered by the household exemption uses a processor to deploy the transaction to a blockchain, this processor, providing the means for the processing under the household exemption may be subject to the GDPR (Recital 18, sentence 3 GDPR) where the processing concerns personal data and the GDPR applies in general. Where actors use the on-chain transaction data, e.g., for analytics capabilities, it must be independently assessed, whether their processing falls within the scope of the GDPR.

As discussed, declining to apply the exemption to personal P2P transactions would often re-characterise individuals as controllers and impose disclosure duties that may themselves burden privacy without commensurate benefit. Consistent with GDPR's purpose and structure, peer-to-peer blockchain transactions by natural persons acting outside a professional or commercial context should, in a fundamental-rights-conform interpretation, therefore fall within the scope of Article 2(2)(c).

### 3.3.6

#### **Consequences of technical impossibility**

The EDPB draft Guidelines state that technical impossibility cannot be invoked to justify non-compliance (para 50). When technical impossibility means that the software used does not offer a certain feature, this is understandable. However, when "technical impossibility" means that the original controller has ceased to determine the purposes and means of processing, the original controller is no longer the controller and therefore no longer obliged. The GDPR obliges in Arts. 12-22 only the controller and not former controllers. The CJEU limits the duties of the controller to *the processing of personal data in respect of which it actually determines the purposes and means*.<sup>46</sup>

<sup>45</sup> *EDPS v Single Resolution Board (SRB)*, Court of Justice of the European Union (CJEU), Judgment of 4 September 2025, Case C-413/23 P, ECLI:EU:C:2025:645, para 86, <https://curia.europa.eu/juris/document/document.jsf?docid=303863&doclang=EN>

<sup>46</sup> *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e.V.*, Court of Justice of the European Union (CJEU), Judgment of 29 July 2019, Case C-40/17, ECLI:EU:C:2019:629, para 100, <https://curia.europa.eu/juris/document/document.jsf?docid=216555&doclang=EN>



A former controller only has to *justify non-compliance* in regard to its obligations. An entity that is no longer a controller, therefore does not have to justify current non-compliance with obligations that no longer apply to it. Therefore, the EDPB is formally correct that technical impossibility does not justify non-compliance, but technical impossibility has an effect on the role of entities involved and their obligations. A counter argument could be that ending the determination of purposes and means should not allow controllers to evade their accountability. However, while obligations end, liability towards data subjects as well as responsibility towards data protection authorities remain and cannot be evaded.

The statement of the EDPB therefore must not be interpreted as establishing obligations on non-controllers that do not exist under the GDPR.

Responsibility and liability are caused by and limited to the role of controller. The controller has the obligation to comply with the GDPR which includes implementing privacy by design and choosing appropriate means of processing. Any liability, however, is limited to the processing the entity was able to determine the purposes and means<sup>47</sup> applying an ex-ante view. The test is, whether the processing at the time an entity was considered a controller violated the GDPR. This is different from the responsibility and liability a current controller would have.

**47** EDPS v Single Resolution Board (SRB), Court of Justice of the European Union (CJEU), Judgment of 4 September 2025, Case C-413/23 P, ECLI:EU:C:2025:645, para 86, <https://curia.europa.eu/juris/document/document.jsf?docid=303863&doclang=EN>



### 3.3.7

#### Processors

When data processing is carried out on behalf of a controller, the data processing entity is considered a processor. The processor may have factual/technical control over all or some means of the processing, but it does not determine purposes or essential means that are ultimately decided by the controller. A typical example is a data centre operating a set of servers for a client under the control of a client.

When nodes in private blockchains operate on behalf of a central entity or when running a blockchain node is provided as a service, the nodes might be considered processors. As mentioned above (3.3.1), paras 40-44 in the EDPB draft guidelines show a degree of inconsistency. While the first two sentences in para 44<sup>48</sup> describe scenarios typically found in permissionless blockchains where nodes have limited control, the third sentence refers to processors without a clear linkage to the aforementioned scenarios. A node that does not sufficiently determine the purposes and means of data processing can be a processor only if there exists another entity that has the missing control and on whose behalf the node processes the data. Absent a controller that can fill that control gap, the party that does not qualify as controller necessarily cannot qualify as processor either.

**48** Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e.V., Court of Justice of the European Union (CJEU), Judgment of 29 July 2019, Case C-40/17, ECLI:EU:C:2019:629, para 100, <https://curia.europa.eu/juris/document/document.jsf?docid=216555&doclang=EN>



## 3.4

### Lawfulness of processing (Art. 6(1) GDPR)

In case all of the following conditions are true: data written on-chain constitutes personal data, the processing is subject to the GDPR and not covered by the household exemption and there is a controller, then the GDPR applies and requires one of the six justifications in Art. 6(1) GDPR for the lawfulness of processing:

#### 3.4.1

##### Consent (Art. 6(1)(a) GDPR)

Consent is a valid legal basis only if it is freely given, specific, informed, and unambiguous (Arts. 4(11), 7 GDPR). The controller bears the burden of proof (Art. 7(1) GDPR); withdrawal must be as easy as giving consent and is possible at any time (Art. 7(3) GDPR); tying consent to unnecessary conditions is restricted (Art. 7(4) GDPR; cf. *Planet49*<sup>49</sup>, *Orange România*<sup>50</sup>). Consent does not waive design and security duties under Arts. 25 and 32 GDPR.

In a public, permissionless blockchain setting, once a signed transaction is broadcast, the originator no longer determines the purposes and means of subsequent decentralised replication. Upon withdrawal, the (former) controller must stop all processing within its control if there is still any (no re-broadcasting or further dissemination; no own indexing or display), erase off-chain linkages, and, where applicable, render the on-chain artefact not reasonably linkable to a natural person (e.g., destruction of keys/mapping tables).

Controllers that legally made personal data public, are not responsible for any further processing of the data by others. The right to be forgotten does not oblige controllers to force other controllers to delete the data but Art. 17(2) GDPR requires them only to take reasonable steps to inform other controllers processing those data of the erasure request. This obligation to inform other controllers only applies to current controllers. Current controllers, here, refer to a local, not necessarily public copy of the data. If the entity that has sent a transaction to a chain no longer stores a copy of the transaction, it may no longer be a controller and therefore not be subject to this obligation.

<sup>49</sup> Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH, Court of Justice of the European Union (CJEU), Judgment of 1 October 2019, Case C-673/17, ECLI:EU:C:2019:801, paras 61-63, <https://curia.europa.eu/juris/document/document.jsf?docid=218462&doclang=EN>

<sup>50</sup> Orange România SA v ANSPDCP, Court of Justice of the European Union (CJEU), Judgment of 11 November 2020, Case C-61/19, ECLI:EU:C:2020:901, paras 50-52, <https://curia.europa.eu/juris/document/document.jsf?docid=233544&doclang=EN>



If the on-chain data cannot be de-linked or anonymised such that withdrawal becomes ineffective in practice, the EDPB argues that *consent should not be used for a processing which requires transactions with individuals if the blockchain architecture does not provide a way to delete the personal data regarding the parties in a transaction*<sup>51</sup>. In that case, the controller's fault would not be the failure to erase the on-chain data (which it does not control), but in the ex ante<sup>52</sup> choice of an architecture that foreseeably prevents effective rights (Arts. 25/32 GDPR).

Comparable situations where deletion cannot be guaranteed include publication (e.g., printed books) and third country transfers. Explicit consent for a third country transfer under Art. 49(1)(a) GDPR is possible. The third country transfer might also lead to a loss of control and an inability of data subjects to exercise their rights. Still, consent is possible if the data subject provides explicit consent. This could be seen as providing data subjects with the right to digital self-determination rather than paternalizing them. Art. 49(1)(a) GDPR mitigates ex ante liability of the transferring controller for the fact that deletion may no longer be possible after a transfer. It can be argued that data subjects should be granted a similar freedom in the case of using blockchain technology.

Data protection authorities claim that consent cannot legitimise lesser security<sup>53</sup>; if the use of blockchain technology were considered a decision to lower security, an analogy to Art. 49(1) GDPR might fail, therefore. However, the choice to use a blockchain does not lower security but is a choice to use a different technology. Under the EDPB Guidelines 07/2020, the choice of technology forms part of the essential means and is not merely a technical and organisational measure (TOM). On that view, an analogy remains arguable.

Result: It can be argued that by analogy to Art. 49(1) GDPR allows explicit consent to the use of blockchain technology. Such consent does not waive the right to withdraw consent, but it can remove the original controller's liability for the fact that withdrawal may not be effective to remove a transaction from a public blockchain. Since this argumentation is based on an analogy, caution is suggested when relying on consent for writing personal data on a blockchain.

51 EDPB, Guidelines 02/2025 on processing of personal data through blockchain technologies, Version 1.1, adopted on 8 April 2025 for public consultation, para 116, [https://www.edpb.europa.eu/system/files/2025-04/edpb\\_guidelines\\_202502\\_blockchain\\_en.pdf](https://www.edpb.europa.eu/system/files/2025-04/edpb_guidelines_202502_blockchain_en.pdf)

52 «ex ante» means «before the event», this means taking the perspective of the time before some data to a specific blockchain was written.

53 Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, 8 January 2018, p. 2, <https://www.dr-datenschutz.de/wp-content/uploads/2018/02/schreiben-der-aufsichtsbehoerde.pdf>



### 3.4.2

#### Contract (Art. 6(1)(b) GDPR)

The processing of personal data might be required for the performance of a contract to which the data subject is a party, or at the data subject's request prior to entering into a contract.

Any declaration of consent could be transformed into part of a contract. However, in the context of a social media network the CJEU restricted Art. 6(1)(b) GDPR to situations where the data processing is not merely a contractual clause, but held that *it must be objectively indispensable for a purpose that is integral to the contractual obligation intended for the data subject. The controller must therefore be able to demonstrate how the main subject matter of the contract cannot be achieved if the processing in question does not occur. The fact that such processing may be referred to in the contract or may be merely useful for the performance of the contract is, in itself, irrelevant in that regard. The decisive factor for the purposes of applying the justification set out in point (b) of the first subparagraph of Article 6(1) of the GDPR is rather that the processing of personal data by the controller must be essential for the proper performance of the contract concluded between the controller and the data subject and, therefore, that there are no workable, less intrusive alternatives. In that regard, as the Advocate General observed in point 54 of his Opinion, where the contract consists of several separate services or elements of a service that can be performed independently of one another, the applicability of point (b) of the first subparagraph of Article 6(1) of the GDPR should be assessed in the context of each of those services separately.*<sup>54</sup>

The approach to second-guess whether a contract is optimised to minimise data processing activities has been criticised as limiting contractual freedom and the free market, which are themselves guaranteed by the EU Treaties and the EU fundamental rights (Art. 26(2) TFEU and Art. 16 CFREU),<sup>55</sup>

When services can be performed independently, they are not essential to each other. Payment with personal data is explicitly possible pursuant to EU Directive 2019/770 Art. 3(1), Recital 24. However, in the above case of the contract for the use of a social network and behavioural advertising, the CJEU concluded that a clause regarding behavioural advertising that is tied to the social media usage contract, does not offer a justification under Art. 6(1)(b) GDPR.

<sup>54</sup> Meta Platforms Inc and Others v Bundeskartellamt, Court of Justice of the European Union (CJEU), Judgment of 4 July 2023, Case C-252/21, ECLI:EU:C:2023:537, paras 97-102, <https://curia.europa.eu/juris/document/document.jsf?docid=275125&doclang=EN>

<sup>55</sup> For example, Martin Nettesheim, Data Protection in Contractual Relationships (Art. 6 (1) (b) GDPR), 24 April 2023, p. 52, [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4427134](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4427134)



When a data subject directly buys or sells a crypto-asset, it is notable that the transaction on-chain is indispensable for the performance of the contract about the sale of the crypto-asset and that there are no less intrusive alternatives.

The EDPB offers an example where a contract can impose a payment method (e.g. credit card) and does not question whether the payment by credit card is an unnecessarily intrusive method of payment, but only whether the imposed payment method is executed in the least intrusive way.<sup>56</sup> This likely extends to payment with cryptocurrencies.

To determine whether contracts can serve to legitimise writing personal data such as transaction data on a blockchain, it must be determined whether this is indispensable for the performance of the main contract or if this could be indispensable, for example, for an optional additional contractual service.

When the contract has been terminated, the processing might no longer be necessary for the purposes of the contract. Other justifications, such as legal obligations to keep records, may justify continuing to process data about the contract.<sup>57</sup> The obligation to end the processing does not mean that after the termination of the contract, blockchain transactions need to be deleted, which would imply reversing them. This is not required for two reasons: a) there is no obligation in the GDPR to reverse the performance of a contract at the termination of a contract; b) if the performance of a contract required sending a transaction to a blockchain, the control over data processing concerning this transaction by the contracting partner has already ended after the transaction has been sent. Control regarding the processing of off-chain data might continue after sending the transaction. This processing might need to be ended after the contract is terminated. This could also lead to the anonymisation of on-chain data.

**56** EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8 October 2019, para 26-39, [https://www.edpb.europa.eu/sites/default/files/files/file1/edpb\\_guidelines-art\\_6-1-b-adopted\\_after\\_public\\_consultation\\_en.pdf](https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf)

**57** EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8 October 2019, para 40-44, [https://www.edpb.europa.eu/sites/default/files/files/file1/edpb\\_guidelines-art\\_6-1-b-adopted\\_after\\_public\\_consultation\\_en.pdf](https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf)



### 3.4.3

#### **Legal obligation (Art. 6(1)(c) GDPR) and public task, official authority (Art. 6(1)(e) GDPR)**

Processing of personal data can also be justified by a legal obligation. Obligations may arise from EU law or member state law (Art. 6(3)(1)). While there may be many possible legal obligations, this paper only discusses the Regulation of Electronic Identification, Authentication and trust Services (eIDAS) as well as financial regulations including crypto-asset regulations. Legal obligations have to be distinguished from legal prerequisites. If some processing of data is not mandated by law but only required to obtain a legal remedy or recognition, the data processing may be considered to be in the legitimate interest of the controller. This is discussed below in 3.4.4. If a deliberate choice of the controller, however, leads to a legal obligation from EU or member state law to perform some processing of personal data, this should be covered. The Irish Data Protection Commission advises, that *there does not have to be a legal obligation specifically requiring the exact processing activity which the controller is going to undertake; however, controllers should ensure that the overall purpose of the processing of the personal data is to comply with a legal obligation which has a sufficiently clear basis in either common law or legislation*<sup>58</sup>.

#### 3.4.3.1

##### **Qualified electronic ledgers under eIDAS**

On 11 April 2024 the EU adopted the revision of the eIDAS Regulation that includes electronic ledgers. Chapter III, Section 11 of eIDAS distinguishes between electronic ledgers in general and qualified electronic ledgers. Qualified electronic ledgers must be created and managed by one or more qualified trust service providers, provide the origin of the data records and ensure the unique sequential chronological ordering of data records in the ledger (Art. 45I(1) eIDAS). While electronic ledgers should include most blockchains, qualified electronic ledgers only include some permissioned blockchains operated by qualified trust service providers. eIDAS does not grant an exemption to the GDPR but it includes obligations for the ordering and integrity of records that might serve as a justification for the continued storage of personal data on a blockchain.

For qualified electronic ledgers, Art. 45I(1)(d) eIDAS requires that *any change to the data is immediately detectable*. Detectable changes could, in theory, be implemented by removing the old data and tagging the new data as changed, or by appending the ledger with the new value while leaving the old value recognisable, as it is done in Ethereum Smart Contracts and many other blockchain systems.

<sup>58</sup> Irish Data Protection Commission, Guidance Note: Legal Bases for Processing Personal Data, December 2019, p. 14, <https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20on%20Legal%20Bases.pdf>



The draft implementing act clarifies that a qualified electronic ledger needs to be immutable in Recital 2<sup>59</sup>. The Annex of the draft implementing act defines immutability in 1(b) as *the property of an electronic ledger wherein data records cannot be modified or removed once added to that electronic ledger*<sup>60</sup>. This definition implies that a qualified electronic trust provider has an indisputable obligation to preserve existing blocks and therefore also a justification under the GDPR to keep storing blocks even if they contain personal data. Without this implementing act, eIDAS could still be interpreted this way, but with lesser legal certainty.

For electronic ledgers that do not qualify as qualified electronic ledgers under eIDAS, the implementing act does not apply, but eIDAS still requires the integrity and the accuracy of the chronological ordering of the records to be ensured as a prerequisite for the recognition as electronic ledgers. However, eIDAS does not impose obligations on blockchain actors in this case. Complying with the prerequisites of recognition as electronic ledgers, however, could be considered a legitimate interest and is discussed below under 3.4.4. Having a justification for the continued storage of the blocks of a qualified electronic ledger, also blocks the right to be forgotten and the right to object<sup>61</sup>. It does, however, not remove other obligations of the GDPR that might apply, e.g. restriction of processing (Art. 18 GDPR). It also only applies to the qualified trust service providers managing a qualified electronic ledger.

### Crypto-asset transactions

#### 3.4.3.2

For crypto-asset transactions, processing on-chain transaction data could be justified by a legal obligation. Art. 76(3) MiCA restricts the admission of crypto-assets with an inbuilt anonymisation function to crypto-asset trading in the EU. However, it does not impose a direct legal obligation but might serve as a legitimate interest as discussed below.

Although the FATF guidance lists transaction monitoring as appropriate risk mitigation and part of AML/CFT obligations of CASPs<sup>62</sup>, it is the ensuing EU and Member State legislation that obliges CASPs in the EU and can serve as a justification under Art. 6(1)(c) GDPR.

**59** Draft Commission Implementing Regulation (EU) ... laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards reference standards and specifications for qualified electronic ledgers, Ref. Ares(2025)7285493, 05 Sep 2025, unadopted draft, [https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=PL\\_COM:Ares\(2025\)7285493](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=PL_COM:Ares(2025)7285493)

**60** Annex to the Draft Commission Implementing Regulation (EU) ... laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards reference standards and specifications for qualified electronic ledgers, Ref. Ares(2025)7285493, 05 Sep 2025, unadopted draft, [https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=PL\\_COM:Ares\(2025\)7285493](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=PL_COM:Ares(2025)7285493)

**61** Irish Data Protection Commission, Guidance Note: Legal Bases for Processing Personal Data, December 2019, p. 3, <https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20on%20Legal%20Bases.pdf>



Art. 25(c) AMLR requires CASPs to obtain the necessary information on the source of funds. Art. 26(1) AMLR obliges CASPs to ongoing monitoring including transactions undertaken by the customer and information about origin and destination of funds. Arts. 14(5) and (6) TFR require CASPs to verify the control of a blockchain address and the source of funds. The European Banking Authority (EBA) details these requirements that CASPs *should ensure that they have suitable and effective monitoring tools in place, including transaction monitoring tools and advanced analytics tools*<sup>63</sup>.

So far these obligations only compel CASPs to process existing on-chain data, but do not require them to write transaction data on-chain, the writing and storage of this data on-chain is not directly obligated and therefore no justification under Art. 6(1)(c) GDPR. However, it might still be in the legitimate interest of the CASPs, crypto-asset holders and other blockchain participants to write this on-chain data because otherwise they might not be able to offer their services in a compliant manner. This will be discussed below in 3.4.4.

Art. 76(3) MiCA prohibits the admission of crypto-assets with an inbuilt anonymisation function to crypto-asset trading *unless the holders of those crypto-assets and their transaction history can be identified by the crypto-asset service providers operating a trading platform for crypto-assets*. Anonymisation functions are known from privacy coins such as Zcash or Monero. Pruning old spent transactions has already been discussed in the Bitcoin paper to save storage space and then in DIN SPEC 4997:2020<sup>64</sup> as a privacy/anonymisation feature. As with monitoring obligations, the obligation to access transaction history is not a direct legal obligation to store transaction data on a public blockchain but it may be a legitimate interest to do so.

### 3.4.3.3

#### Public service blockchains

When blockchains are to be used for official purposes like land registries, as tested for example in Sweden<sup>65</sup>, mandating the use of such registries by law could then constitute a reason under Art. 6(1)(c) GDPR to also justify on-chain processing. If the processing is carried out in the public interest or in the exercise of official authority vested in the controller, the processing could also be justified under Art. 6(1)(e) GDPR.

<sup>62</sup> The FATF uses the term VASP (Virtual Asset Service Provider) whereas the EU legislation calls them CASP (Crypto-asset Service Provider). For readability purposes, the term CASP is used consistently in this paper.

<sup>63</sup> European Banking Authority, Guidelines EBA/GL/2021/02 amended by EBA/GL/2024/01, 16 January 2024, para 21.11, <https://www.eba.europa.eu/sites/default/files/2024-01/a3e89f4f-fbf3-4bd6-9e07-35f3243555b3/Final%20Amending%20%20Guidelines%20on%20MLTF%20Risk%20Factors.pdf>

<sup>64</sup> DIN SPEC 4997, Privacy by Blockchain Design, <https://www.dinmedia.de/de/technische-regel/din-spec-4997/321277504>



### 3.4.4

#### Legitimate interest (Art. 6(1)(f) GDPR)

A legitimate interest can justify the processing of personal data if the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject. Recital 47 GDPR further specifies that the reasonable expectations of data subjects based on their relationship with the controller need to be taken into consideration.

Examples range from direct marketing, video surveillance, the pursuit of legal claims to fraud prevention, which is explicitly mentioned in Recital 47 GDPR. The processing needs to be necessary<sup>66</sup> for the justified purpose. Legitimate interest cannot be claimed by public authorities in the performance of their tasks. According to the European Court of Justice, Art. 6(1)(f) GDPR requires three cumulative conditions. First, *the pursuit of a legitimate interest by the data controller or by a third party*; second, *the need to process personal data for the purposes of the legitimate interests pursued*; and, third, *that the interests or fundamental freedoms and rights of the person concerned by the data protection do not take precedence over the legitimate interest of the controller or of a third party*<sup>67</sup>.

As discussed in 3.4.3.2, accessing the transaction history of crypto-assets is a prerequisite for trading coins at an exchange. CASPs have the obligation to analyse transaction data. This would not be possible, if this data were to be purged from a blockchain. Crypto-asset holders would be very limited to trade their coins and CASPs would no longer be able to offer their services. Therefore, keeping this information available is in the interest of crypto-asset holders and CASPs. A simple, unverifiable copy would not suffice. Integrity, completeness and verifiability of the transaction history is ensured by storing it on-chain. Applying the test of the European Court of Justice, the trading of crypto-assets is a legitimate interest of the crypto-asset holder, the on-chain data is required to allow CASPs to trade the crypto-assets and the obligation to perform this analysis is a strong indication that there is no stronger legitimate interests by the data subjects with whom this transaction data may be identified, to delete this data.

<sup>65</sup> Proskurovska, Anetta & Dörry, Sabine. (2022). The blockchain challenge for Sweden's housing and mortgage markets. *Environment and Planning A: Economy and Space*. 54. <https://doi.org/10.1177/0308518X221116896>

<sup>66</sup> The text of Art. 6(1)(f) GDPR uses «necessary» while the EDPB writes «strictly necessary» in EDPB, Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, 8 October 2024, para 13, [https://www.edpb.europa.eu/system/files/2024-10/edpb\\_guidelines\\_202401\\_legitimateinterest\\_en.pdf](https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf)

<sup>67</sup> Koninklijke Nederlandse Lawn Tennisbond v Autoriteit Persoonsgegevens (KNLTB), Court of Justice of the European Union (CJEU), Judgment of 4 October 2024, Case C-621/22, ECLI:EU:C:2024:857, para 37, <https://curia.europa.eu/juris/document/document.jsf?text=&docid=290688&doclang=EN>



As discussed in 3.4.3.1, electronic ledgers need to ensure the integrity of their records to be recognised by eIDAS as such. For qualified electronic ledgers, integrity is an obligation imposed on the qualified trust service providers that operate them. For other electronic ledgers, integrity is a prerequisite for their recognition. For qualified electronic ledgers the draft implementing act details that “integrity” means “immutability”. There is no reason to assume that the “integrity” requirement in Art. 4(52) eIDAS should be interpreted differently than in Art. 45(1)(d). Suppose it were to be interpreted differently, qualified electronic ledgers were required to be immutable while other electronic ledgers would be required to not be immutable but to delete data that users have sent to the ledger and is considered personal data. A transition of an electronic ledger to a qualified electronic ledger would be impossible. The immutability requirement therefore is a prerequisite for an electronic ledger and can accordingly be in the legitimate interest of the blockchain participants. Applying the above test of the European Court of Justice, electronic ledgers are given legal recognition with eIDAS. This is an indicator that the processing is legitimate. The immutability is required to be recognised by eIDAS (as discussed in 3.4.3.1) and there is usually no stronger legitimate interest of the data subject.

However, according to Art. 21 GDPR, the data subject can object to data processing that is justified by a legitimate reason. Except for direct marketing, the objection must be based on grounds relating to the particular situation of the data subject which requires an atypical situation of a legal, economic, ethical, social, societal, and/or familial nature<sup>68</sup>. The controller can still demonstrate compelling legitimate grounds for the processing that override the interests, rights and freedoms of the data subject or the establishment, exercise or defence of legal claims. This requires a case-by-case analysis. However, given the strong requirements in eIDAS and financial regulations, compelling legitimate grounds should be able to be demonstrated in most cases.

## 3.5

### Special categories of personal data (Art. 9 GDPR)

Special categories of personal data are subject to special protection. They include *data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation* (Art. 9(1) GDPR). Processing requires a lawful basis under Art. 6(1) GDPR and, in addition, must satisfy one of the conditions in Art. 9(2) GDPR.

<sup>68</sup> Landgericht Hamburg, 334 O 161/19, 23 July 2020, <https://www.landesrecht-hamburg.de/bsha/document/NJRE001442149>



## 3.6

### International transfers

International transfers to third countries outside the EEA are governed by Chapter V GDPR (Arts. 44–50). Where no adequacy decision exists, transfers require appropriate safeguards. Public blockchains are typically global; a broadcast can replicate to nodes in third countries.

This is not unique to blockchains; publication eliminates geographic control. In C–101/01 Lindqvist<sup>69</sup> the CJEU held that if the rules for third country transfers *were to be interpreted to mean that there is transfer of data to a third country every time that personal data are loaded onto an internet page, that transfer would necessarily be a transfer to all the third countries where there are the technical means needed to access the internet. The special regime provided for international data transfers would thus necessarily become a regime of general application, as regards operations on the internet. Accordingly, it must be concluded that [the uploading of data to a webserver does] not as such constitute a transfer of data to a third country. It is thus unnecessary to investigate whether an individual from a third country has accessed the internet page concerned or whether the server of that hosting service is physically in a third country.*

Although Lindqvist interpreted Directive 95/46/EC, the GDPR preserves the principles governing international governing international transfers - adequacy (Art. 45), appropriate safeguards (Art. 46, including SCCs and BCRs), derogations (Art. 49), and the specific rule on third country authority requests (Art. 48). Lindqvist therefore remains relevant for publication as such under the GDPR.

The EDPB Guidelines 05/2021<sup>70</sup> offer a three-element taxonomy for when Chapter V applies: (i) exporter subject to the GDPR; (ii) disclosure/making available to another controller/processor; (iii) importer in a third country. Such non-binding guidelines do not displace the rulings of the CJEU in Lindqvist. Thus, immediate, intentional publication to the public does not trigger Chapter V merely due to global accessibility or third country server location – even if the upload is targeted to such a server.

**69** Criminal proceedings against Bodil Lindqvist, Court of Justice of the European Union (CJEU), Judgment of 6 November 2003, Case C-101/01, ECLI:EU:C:2003:596, paras 69–70, <https://curia.europa.eu/juris/document/document.jsf?docid=48382&doclang=EN>

**70** EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, Version 2.0, 14 February 2023, [https://www.edpb.europa.eu/system/files/2023-02/edpb\\_guidelines\\_05-2021\\_interplay\\_between\\_the\\_application\\_of\\_art3-chapter\\_v\\_of\\_the\\_gdpr\\_v2\\_en\\_0.pdf](https://www.edpb.europa.eu/system/files/2023-02/edpb_guidelines_05-2021_interplay_between_the_application_of_art3-chapter_v_of_the_gdpr_v2_en_0.pdf)



By contrast, non-public disclosure to a determinable third country recipient (e.g., a private, permissioned blockchain with nodes in third countries) may constitute a transfer and, if so, must meet Chapter V requirements.

In *Lindqvist*, the CJEU recognised that, in a purely technical sense, uploading data online could amount to a transfer to third countries but declined to apply the rules on that basis, holding that publication does not constitute a transfer within the meaning of the EU data protection law. This reflects a fundamental-rights reading. While the rules for international data transfers aim to improve data protection worldwide and were largely successful in establishing the GDPR as an international “gold standard”, the GDPR also respects freedom of expression and information and Art. 85 GDPR requires Member States to provide by law exemptions and derogations to reconcile freedom of expression and information with data protection.

A strict application of the rules of Chapter V GDPR on publishing on the internet would severely impact activities on the internet. This is not limited to websites or social media but also includes public, permissionless blockchains. It should be noted that the European Court of Justice in *Lindqvist* not only excluded publication on the internet from being considered a transfer but also held that it did not matter where the server was located that served the website. Therefore, if data is sent to a node to be published on the Internet, Chapter V already does not apply to the data transfer to that node.

The EDPB, in its draft guidelines<sup>71</sup>, mentions in section 4.5 that blockchain will “often involve international data transfer” – particularly with non-EU nodes – and refers readers to other EDPB texts but does not discuss the *Lindqvist* publication rationale that publication is not considered a transfer to a third country even if a third country server is used).

71 EDPB, Guidelines 02/2025 on processing of personal data through blockchain technologies, Version 1.1, adopted on 8 April 2025 for public consultation, paras 74-75, [https://www.edpb.europa.eu/system/files/2025-04/edpb\\_guidelines\\_202502\\_blockchain\\_en.pdf](https://www.edpb.europa.eu/system/files/2025-04/edpb_guidelines_202502_blockchain_en.pdf)



## 3.7

### Data retention

The planned lifetime of blockchains is often unlimited and usually longer than data retention periods normally required by EU or member state law. However, unlimited data retention is not unprecedented. Qualified electronic ledgers in eIDAS do not have a retention limit (see 3.4.3.1). Books containing personal data do not have retention limits. Public archives often do not have retention limits either. While it is recommended to store personal data off-chain so that no personal data is stored on-chain (for the discussion of commitments see 3.2.6), there are also types of personal data where GDPR does not require a data retention limit, e.g., archiving in the public interest or long-term verification needs such as revocations of university diplomas (see 5.1).

If the law requires data retention to be limited, the responsibility lies with the entity that is sending the data to the blockchain. As has been discussed in 3.3.1, usually, there is no controller for a public permissionless blockchain. And as discussed in 3.4.3.1, the controller of a permissioned blockchain considered a qualified electronic ledger must not erase data on that qualified electronic ledger.



## Security and governance

Security of processing is an obligation for both controllers and processors and must reflect the state of the art, *the nature, scope, context and purposes of processing as well as the risks for data subjects* (Art. 32; Recital 83 GDPR).

Given the specifics of blockchains, the relevant state of the art can be found in community-based frameworks, technical papers and research reports such as:

- Bitcoin Core Security Advisories<sup>72</sup>,
- L2BEAT: Community framework aimed at Ethereum Layer 2<sup>73</sup>,
- Flashbots: Technical documentation regarding Ethereum Proof-of-Stake validation<sup>74</sup>,
- Security Alliance (SEAL 911): Community Log for cross-chain incident response for DeFi/bridges/smart-contracts; on-chain emergency coordination (whitehat rescue, playbooks)<sup>75</sup>,
- Smart Contract Weakness Classification (SWC) / EIP-1470 for Ethereum smart contracts<sup>76</sup>,
- Immunefi: Crypto Losses reports, research reports on empirical threat landscape across chains (Ethereum, BNB, etc.)<sup>77</sup> and
- D.U.C.K. – Distribution Utilization of Configurations and Knowledge, has the goal to equip node operators with open-source resources enhancing operations and mitigating risks in running staking infrastructure<sup>78</sup>.

Decentralised technologies apply different security measures and follow different governance and development models than centralised systems, which means that the relevant state of the art is reflected not in proprietary or centralised standards but in community-maintained frameworks, protocol specifications and research reports that govern blockchain operations and security.

72 BitcoinCore, Security Advisories, <https://bitcoincore.org/en/security-advisories/>

73 L2BEAT Research Team, "The Risk Rosette Framework," 8 Jun 2024, <https://gov.l2beat.com/t/the-risk-rosette-framework>

74 Flashbots, "MEV-Boost Risks and Considerations," 27 May 2025, <https://docs.flashbots.net/flashbots-mev-boost/architecture-overview/risks>

75 Security Alliance, SEAL 911, Incident Resolution Log, <https://www.securityalliance.org/seal-911>

76 Ethereum Foundation, "EIP-1470: Smart Contract Weakness Classification (SWC) and SWC Registry, 18 Sep 2018, <https://eips.ethereum.org/EIPS/eip-1470>

77 Immunefi Research, "Crypto Losses in Q1 2025," 1 Mar 2025, <https://assets.ctfassets.net/t3wqy70tc3bv/31xoJW2tdLXPuUoH2Z7fc2/3a639210ca1799a7e1cb8f-8cf5ce5f01/Immunefi-Crypto-Losses-in-April-2025.pdf>

78 D.U.C.K. - Distributed Utilization of Configurations and Knowledge Proposal, <https://research.lido.fi/t/d-u-c-k-distributed-utilization-of-configurations-and-knowledge-proposal/5848>, <https://duck-initiative.gitbook.io/d.u.c.k.-knowledge-base>





Security of processing is an obligation of controllers and processors pursuant to Art. 32 GDPR. Even if a data breach occurs after control has ended, controllers are responsible for means they have selected despite known security issues. In case a permissioned blockchain has been hacked, for example, it must be evaluated, whether proper security measures had been implemented.

Where a breach occurs after a controller's role has ended, liability is limited to past failures in choosing or implementing appropriate measures that were contrary to the then-applicable state of the art and risk; the assessment is *ex ante* (i.e., at the time of determination of means). Obligations need to be appropriate and are limited by the controller's possibility to determine the purposes and means of processing. A simple user has lesser and different obligations than a permissioned blockchain or the developer of a smart contract handling a large transaction load and high values.

Entities qualifying as current controllers may be obliged to notify data subjects (Art. 34 GDPR) and/or data protection authorities (Art. 33 GDPR) of data breaches that are likely to result in a high risk to the rights and freedom of natural persons. One of the reasons a controller may be exempted to inform data subjects directly is a disproportionate effort to inform the data subjects, for example, if the controller has no contact information. The obligation to inform the data protection authority and/or the data subjects only applies to current but not to former controllers.



## 3.9

### Data subject rights

Rights of data subjects can be limited if the processing does not require the identification of a data subject since the controller is not required to keep records to identify the data subjects for the sole purpose of complying with the GDPR according to Art. 11(1) GDPR. Arts. 15-20 GDPR, however, will apply if the data subject can provide the additional information enabling his or her identification (Art. 11(2) GDPR). Data subject rights as defined in Arts. 12-22 GDPR bind the current controller. A former data controller is not bound by these obligations and may only be liable due to actions he or she did or did not do when being the controller (see 3.3.6). According to Art. 23 GDPR, data subject rights may also be limited by way of legislative measure for a range of public interest grounds from national security to the protection of the judiciary.

GDPR applies to off-chain data in the usual way that will not be reflected in detail below. This paper is limited to on-chain data with a focus on public permissionless blockchains.

### 3.9.1

#### Information to be provided and right to access (Arts. 12-15 GDPR)

The controller has the obligation to inform the data subject (Arts. 12-14 GDPR). This does not depend on the technology used. In case the data is considered personal data but the controller is not able to identify the data subject, the controller may refuse to comply with the data subject's requests regarding their rights (Art. 12(2) GDPR).

The data subject also has a right to access the personal data (Art. 15 GDPR). In case of on-chain data on a public blockchain, this can be answered by a reference to the data. In case of off-chain data or data on private blockchains, this should not be different from non-blockchain scenarios.



### **Right to erasure (Art. 17 GDPR), withdrawal of consent (Art. 7(3) GDPR) and right to object (Art. 21 GDPR)**

The right to erasure – also called the right to be forgotten (Art. 17 GDPR) provides the data subjects with the right to request the deletion of personal data that relates to them. However, this right is excluded if there is a continuing legal basis for the storage of the data. If processing is required by law, the right to erasure is not available. Consent can be withdrawn but this does not impact the processing before the consent has been withdrawn (see 3.4.1). Processing on the basis of a legitimate interest can be objected to but not when there is compelling interest to continue the processing (see 3.4.4).

The right to erasure is not applicable, if there is no controller (see 3.3.1). The right to be forgotten, therefore, does not apply to public permissionless blockchains in most cases. eIDAS Regulation also excludes deletion for qualified electronic ledgers, which are often permissioned blockchains. For other electronic ledgers, there may be a compelling legitimate interest to continue the processing. Therefore, the applicability of Art. 17 GDPR to blockchains is very limited.

Additional reasons to prevent deletion may be found in Art. 17(3) GDPR (e.g., establishment/exercise/defence of legal claims, archiving/scientific or historical research in the public interest, freedom of expression and information).

Sometimes, the right may be fulfilled by deleting off-chain linkages (keys, look-up tables, references) if this renders information on the chain no longer personal data. The Austrian Datenschutzbehörde held that the right to erasure has been complied with when only the identification of the data with the data subject is removed and cannot be restored without disproportionate effort<sup>79</sup>. If simple delinking can be sufficient, methods like crypto-shredding (key-destruction), off-chain-dereferencing or ZK-rollups can be sufficient as well. While it is true, that some cryptographic functionality might be broken one day in the future and deleted data might be recovered, deletion under the GDPR does not require that even purely theoretical possibilities for recovery are excluded. Deletion is achieved if recovery of deleted data is impossible with all means reasonably likely to be used. Non-existing means are not likely to be used.

If deletion or delinking of specific on-chain entries is infeasible or would disproportionately affect the integrity or the rights of others, deletion could violate GDPR itself. Deletion is itself a form of processing. If a controller cannot properly delete a record because of design choices that prevent separation of records, the consequence is often not – as the EDPB suggests – the deletion of a whole blockchain, but no deletion.

<sup>79</sup> Datenschutzbehörde Austria, DSB-D123.270/0009-DSB/2018, 5.12.2018, [https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT\\_20181205\\_DSB\\_D123\\_270\\_0009\\_DSB\\_2018\\_00/DSBT\\_20181205\\_DSB\\_D123\\_270\\_0009\\_DSB\\_2018\\_00.html](https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20181205_DSB_D123_270_0009_DSB_2018_00/DSBT_20181205_DSB_D123_270_0009_DSB_2018_00.html)



The right to be forgotten does not justify the deletion of unrelated records that would affect the rights of other data subjects that are only connected due to technical constraints. If there is a liability for this situation, it may not be carried by the controller of the blockchain who is unable to comply with the GDPR obligations of several data subjects at the same time, but by the controller who chose the wrong means of processing a choice potentially constituting a breach of GDPR obligations, for example *Art. 25 GDPR (privacy by design/default)*. For the discussion of the liability of former controllers see 3.3.6. This liability might be excluded if the data subject explicitly consented to the processing on a blockchain (see 3.4.1).

### 3.9.3

#### **Right to rectification (Art. 16 GDPR)**

Similarly to the right to erasure, the application of the right to rectification is limited. Public permissionless blockchains usually do not have a controller. Only the current controller, however, has to comply with the right to rectification.

In general, rectification can be done through replacing or deleting information, or by adding information, such as by tombstoning. Courts have decided in many cases that adding a rectification note is sufficient for rectification under the GDPR. Only in some cases courts have decided that the old data needs to be deleted.

In case of qualified electronic ledgers, the controller must ensure immutability of the ledger (see 3.4.3.1). This means, corrections are only possible through adding an additional record.

Not every faulty or undesired personal data is inaccurate and can be a basis for the right to rectification. When a faulty statement is recorded like the erroneous answer in an exam, the answer might be incorrect, but the record of the answer given is accurate<sup>80</sup>. Similarly, when a phishing mail fraudulently asked for a payment to a wrong address or when assets have been transferred with a stolen private key, the outcome may be the undesirable result of a crime, but the record accurately notes the transactions performed. There may be a civil claim to do a reverse transaction against the criminal recipient, but not against the blockchain nodes on the grounds of Art. 16 GDPR.

Non-reversible payments are not limited to blockchains. Cash payments and even some bank payments cannot be reversed but only compensated by reverse payments. Where irreparable damage results from a breach of duty, liability for damages may arise.

<sup>80</sup> Peter Nowak v Data Protection Commissioner, Court of Justice of the European Union (CJEU), Judgment of 20 December 2017, Case C-434/16, ECLI:EU:C:2017:994, para 52, <https://curia.europa.eu/juris/document/document.jsf?docid=198059&doclang=EN>



### 3.9.4

#### Right to restriction of data processing (Art. 18 GDPR)

As with the right to erasure, only a current controller has to comply with the right to restriction of data processing. This excludes in most cases public permissionless blockchains. For permissioned blockchains, the right may apply in general.

The right to restriction of data processing applies to data where the legality of the processing is contested, where the accuracy of the data is contested, where data only needs to be preserved for the establishment, exercise or defence of legal claims or the data subject prefers the restriction of processing to erasure of unlawfully processed data.

The right to restriction of processing is excluded, when the processing is needed for the protection of the rights of other natural or legal persons or for reasons of important public interest. For qualified electronic ledgers there is a public interest in the availability of the ledger. The Annex of the draft implementing act<sup>81</sup> makes reference to ETSI EN 319 401<sup>82</sup> in 3(a) and ISO 23257-2022<sup>83</sup> in 3(c). ETSI EN 319 401 lists availability as REQ-7.3.2-03X, REQ-7.3.2-04X and REQ-7.14.2-13X. ISO 23257-2022 lists the availability of the DLT system in Principle 8 in 4.2.8. Restriction of processing for a qualified electronic ledger would mean that it is mostly unavailable. Even if only small parts of the ledger were unavailable, the integrity could no longer be verified. Therefore, for qualified electronic ledgers the restriction of processing should be excluded. For other permissioned blockchains, a case-by-case assessment must determine whether important public interests or the rights of others preclude restricting the processing.

**81** Annex to the Draft Commission Implementing Regulation (EU) ... laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards reference standards and specifications for qualified electronic ledgers, Ref. Ares(2025)7285493, 05 Sep 2025, unadopted draft, [https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=PL\\_COM:Ares\(2025\)7285493](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=PL_COM:Ares(2025)7285493)

**82** ETSI EN 319 401 V3.1.1 (2024-06), Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers, [https://www.etsi.org/deliver/etsi\\_en/319400\\_319499/319401/03.01.01\\_60/en\\_319401v030101p.pdf](https://www.etsi.org/deliver/etsi_en/319400_319499/319401/03.01.01_60/en_319401v030101p.pdf)

**83** ISO/TS 23635 2022-02, Blockchain and distributed ledger technologies – Guidelines for governance, <https://cdn.standards.itih.ai/samples/76480/6cbc6ced3ed3460d8c6feba44aec30b4/ISO-TS-23635-2022.pdf>



### 3.9.5

#### **Right to data portability (Art. 20 GDPR)**

Public blockchains and open standards can offer data portability by design. They offer data in a structured and commonly used, machine-readable format. Smart contracts and bridges allow for the integration of existing data and assets into different eco systems. Therefore, data portability does not pose a substantive challenge, as the data is inherently available.

The right to data portability is a right that the current controller has to comply with. It is therefore not available when there is no current controller as with most public permissionless blockchains. It is also limited to cases where the current processing is based on consent (see 3.4.1) or on a contract (see 3.4.2). Therefore, the right to data portability rarely applies and if it applies, it is not particularly difficult for the controller to comply with it.



## Automated decision-making (Art. 22 GDPR)

Art. 22(1) GDPR grants the right not to be subject to a decision based solely on automated processing that produces legal effects concerning the data subject or similarly significantly affects them. As under the GDPR generally, Art. 22(1) GDPR operates as a prohibition subject to exceptions in Art. 22(2) GDPR (necessity for a contract; Union/Member State law with safeguards; explicit consent). Where an exception is relied upon, Art. 22(3) GDPR obligations apply (meaningful information about the logic involved, the right to obtain human intervention, to express one's view, and to contest the decision).

A simple crypto-asset transfer executes code that reallocates control over assets and may involve high values. However, does this execution constitute a "decision" or is it purely mechanical accounting without any room for a real decision? Recital 71 lists examples of rather complex scenarios, making predictions concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements. Finck does not see a rationale in the creation process of the GDPR that could explain how to define the minimal threshold of "decision" in Art. 22 GDPR and awaits clarification from the CJEU on this question<sup>84</sup>. The WP29 did not discuss this either in their paper on automated decision-making. However, WP29 lists some examples, mostly including profiling and higher complexity but also the example of the automatic issuing of a speeding ticket<sup>85</sup>. Seeing this example, Finck argues that at least some smart contracts should be considered automated decision-making. The CJEU, in its SCHUFA judgment, clarified that the decisive factor is the automated step that determines the outcome: where an upstream automated result usually dictates the downstream contractual decision, that upstream computation may qualify as the automated decision under Art. 22(1) GDPR<sup>86</sup>. By analogy, for a plain blockchain transfer - or when submitting a transaction to a smart contract - the effective decision will usually lie with the party that decides to invoke the transparent, deterministic mechanics of a blockchain smart contract; the mechanical execution is not, by itself, the Art. 22 GDPR decision. So, generally, blockchain smart contracts cannot be regarded as automated decision-making.

<sup>84</sup> Finck, Michèle, Smart Contracts as a Form of Solely Automated Processing Under the GDPR (January 8, 2019). Max Planck Institute for Innovation & Competition Research Paper No. 19-01, pp. 7-9, <https://ssrn.com/abstract=3311370>

<sup>85</sup> Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 6 February 2018, p. 8, <https://ec.europa.eu/newsroom/article29/redirection/document/49826>

<sup>86</sup> SCHUFA Holding (Scoring), Court of Justice of the European Union (CJEU), Judgment of 7 December 2023, Case C-634/21, ECLI:EU:C:2023:957, para 50, <https://curia.europa.eu/juris/document/document.jsf?docid=280426&doclang=EN>



Art. 22 GDPR will also typically not apply where the data subject controls and executes the transaction themselves. When a smart contract relies on an external oracle, the effective decision might shift to the oracle that provides a complex value comparable to the Schufa score. When the oracle is automated and only supplies neutral and simple data like weather data, exchange rates or similar data, the oracle should not be regarded as an automated decision-making.

If blockchain smart contracts were to become substantially more complex and incorporate advanced logic or even artificial intelligence, Art. 22 GDPR could apply. This would also require that the automated step alone allocates or denies a right, or otherwise produces legal or similarly significant effects for the data subject. In such cases the controller must ensure that one of Art. 22(2) GDPR exceptions is met and that the Art. 22(3) GDPR safeguards are implemented.

The EDPB's draft guidelines only state that the execution of a smart contract may fall into the scope of Article 22 but fail to provide any criteria or example for that<sup>87</sup>. Given our result that currently most smart contracts are clearly out of the scope of Art. 22 GDPR, this vague statement unnecessarily increases legal uncertainty.

**87** EDPB, Guidelines 02/2025 on processing of personal data through blockchain technologies, Version 1.1, adopted on 8 April 2025 for public consultation, para 107, [https://www.edpb.europa.eu/system/files/2025-04/edpb\\_guidelines\\_202502\\_blockchain\\_en.pdf](https://www.edpb.europa.eu/system/files/2025-04/edpb_guidelines_202502_blockchain_en.pdf)



### Data protection impact assessments (Art. 35 GDPR)

Where planned processing is likely to result in a high risk to the rights and freedoms of natural persons, particularly where innovative blockchain technology is used or data become publicly accessible, a data protection impact assessment (DPIA) is required (Art. 35(1) GDPR). Even when not formally required, DPIAs can help ensure compliance and help reduce compliance risks.

The requirement to perform a DPIA depends on the novelty of the technology used. The requirement to perform a DPIA is not meant to put a special burden on some types of processing. Data protection authorities will whitelist use cases that already have been verified as technology is established and no longer new. If there already exists a DPIA for an identical use case with an identical technical implementation, controllers may reference it or use it as a template.

A DPIA must describe the processing, assess necessity and proportionality, identify and evaluate risks for data subjects, and define measures to address them (Art. 35(7) GDPR). Blacklists/whitelists provided by data protection authorities should be checked. If there is a data protection officer, it must be involved (Art. 35(2) GDPR); data subjects or their representatives may be consulted where appropriate (Art. 35(9) GDPR). If a high residual risk remains, the controller must conduct prior consultation with the supervisory authority (Art. 36 GDPR). Data protection authorities provide tools for DPIAs. For example, the French CNIL offers a DPIA tool<sup>88</sup> and the British ICO a template<sup>89</sup>.

Guidelines should positively list use cases of privacy-preserving technology in the blockchain context to encourage their use. Guidelines could also provide templates for addressing blockchain-specific risks in DPIAs.

<sup>88</sup> CNIL, PIA software: <https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment>

<sup>89</sup> ICO, DPIA template: <https://ico.org.uk/media2/migrated/2553993/dpia-template.docx>



## Result

The EDPB draft guidelines, in our assessment, differ in several important respects from the GDPR and the jurisprudence of the European Court of Justice. This begins with a too broad definition of personal data. The draft does not expressly reference certain relevant jurisprudence (e.g., Lindqvist), currently gives limited consideration to related EU law such as eIDAS, and does not fully reflect the decentralised nature of public permissionless blockchains, where a factual evaluation may not qualify nodes/miners/verifiers as controllers.

The reasoning could, in our view, place greater emphasis on the principle of proportionality, a cornerstone of EU fundamental rights law. Mandating the deletion of an entire blockchain because of a single record processing personal data in violation of the GDPR would generally infringe far more upon individual rights and freedoms than not deleting the record. If courts were to follow the draft guidelines of the EDPB without substantial refinement, this could significantly limit a number of useful, legitimate and privacy-preserving use cases. There is a good chance that courts would rather follow the jurisprudence of the European Court of Justice, which is anchored in proportionality and contextual interpretation providing a more balanced framework. We hope this paper can assist courts and regulators in that assessment.

Applying GDPR to decentralised systems is undeniably complex, but a detailed analysis shows GDPR can be applied to blockchains better than initially thought. Many of the perceived obstacles arise not from the GDPR itself, but from interpretations that may be perceived as rigid and that do not yet fully take into account certain technical realities. While full legal certainty remains elusive, a contextual and technologically informed application of GDPR leads to results far more consistent and workable than the current draft guidelines of the EDPB.

When personal data is stored off-chain and the blockchain only contains perfectly hiding commitments, the on-chain data do not qualify as personal data and the GDPR does not apply to the blockchain. Node operators of public permissionless blockchains are not considered controllers and therefore not subject to the GDPR. Permissioned ledgers can be subject to the GDPR when they store personal data, but at least in the case of qualified electronic ledgers eIDAS mandates immutability, an obligation the GDPR respects. If processing of personal data on a blockchain is needed for compliance reasons to trade coins or provide other crypto-asset services, there is a legitimate interest in writing the pseudonymous transaction data including the blockchain addresses on-chain.

Alternatively, explicit consent may serve as a lawful basis where individuals are fully informed about the storage on a blockchain. Contractual necessity can also serve as justification when, for example, a contract involves crypto-asset transactions.



Still, blockchain and GDPR compliance remain a nuanced field: Writing personal data on-chain should be avoided unless it is necessary and justified. Even metadata and verification data should be minimised on-chain. Hash values of personal data should not serve as identifiers or indexes on-chain. A data protection impact analysis (DPIA) may be required to document necessity, proportionality and risk mitigation measures.



Blockchains have evolved and continue to evolve since the start of Bitcoin in 2009, offering new ways to reconcile decentralisation, transparency and data protection. Recent advances in privacy-preserving blockchain architectures demonstrate how these objectives can be achieved within existing legal frameworks by embedding privacy and auditability directly in the protocol design. New blockchain architectures offer different consensus mechanisms and data-visibility properties that integrate privacy-preserving technologies (such as zero-knowledge proofs and perfectly hiding commitments) at the base layer. These architectures are designed such that validators, or any other consensus participants, are able to access only information that is required to verify state transitions and not content (payload) or transaction metadata. In such designs, the validators' role is limited to verifying mathematical proofs (cryptographic proofs of correctness) that state transitions follow protocol rules, meaning that base-layer participants only interact with verification artefacts rather than transactional content or metadata. In privacy-preserving designs, this ensures that validators do not access information relating to an identifiable natural person. This separation between system integrity and user identity further reinforces GDPR's principles of data minimisation and allows base-layer participants to provide assurance of credible neutrality, because they do not access any transaction data nor process personal data.

Assumptions about data visibility, controllership and identifiability at the consensus layer no longer hold true for emerging blockchain architectures that embed privacy-by-design directly at the base layer. Modular stacks decouple consensus, data availability and execution; execution environments - ranging from lightweight, permissionless settings to sovereign rollups - host decentralised applications and user transactions, while the base layer verifies succinct, non-revealing mathematical proofs.

Such technological developments do not replace the arguments made for a more proportionate reading of the GDPR by the EDPB in this paper and, in fact, are aligned with this approach. Actors on the blockchain level of traditional public permissionless blockchains, like miners, validators or block producers, may not be controllers under the GDPR because these actors do not determine the purposes and means of processing personal data. Privacy-preserving blockchain architectures go a step further by restructuring the consensus function so that the base layer participants operate only on cryptographic artefacts that prove protocol correctness. This substantially reduces - and, in some implementations, eliminates - the handling of personal data at the consensus layer.



While not qualifying as a controller protects actors from GDPR obligations even if personal data are written on a traditional blockchain, privacy-preserving blockchain architectures can, by design, minimise or remove personal data from the base layer and hence reduce the likelihood that GDPR will be applicable to consensus participants.

Technically, privacy-preserving blockchain architectures can be designed to calibrate almost any balance between transparency and confidentiality across its modular layers. They achieve verifiable integrity of the network by providing only mathematical proofs and verification artefacts which confirm protocol correctness without revealing underlying data. Such artefacts do not contain information about natural persons and should, therefore, in our view, not be considered personal data. The “Digital Package of Simplification” proposes to amend Art. 4(1) GDPR to turn the definition of personal data into a purely relative definition where blockchain actors as well as other trust service providers that are processing data without the means to identify natural persons, will no longer be considered processing personal data<sup>90</sup>.

As regulatory understanding about blockchain architectures matures, it will be important to re-emphasise the distinction between “data about identifiable natural persons” and technical “data about protocol integrity”. The draft guidelines of the EDPB, however, extend the scope of personal data to verification artefacts in a way that, in our reading, is not sufficiently grounded in the text of the GDPR or in the jurisprudence of the CJEU. Revising the draft in this regard could remove uncertainties about how such technologies are viewed under the GDPR and could further encourage adoption of technologies that align technical design with the principles of data protection by design and data minimisation under the GDPR.

**90** The Digital Omnibus package proposes to amend Art. 4(1) GDPR as follows: ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; **Information relating to a natural person is not necessarily personal data for every other person or entity, merely because another entity can identify that natural person. Information shall not be personal for a given entity where that entity cannot identify the natural person to whom the information relates, taking into account the means reasonably likely to be used by that entity. Such information does not become personal for that entity merely because a subsequent recipient has means reasonably likely to be used to identify the natural person to whom the information relates.** European Commission, Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus) COM (2025) 837 final



This also directly aligns with EDPB's own endorsement of the use of *different privacy enhancing technologies to provide sufficient levels of data protection for data subjects*.<sup>91</sup> Existing blockchain technology already furthers the goals of the GDPR through data minimisation, integrity, accountability, and meaningful user control.

Privacy-preserving architectures exemplify an evolution of blockchain infrastructure by reducing exposure on public infrastructure while preserving verifiability. Existing blockchains demonstrate that decentralised design and data protection can coexist in practice, emerging privacy-preserving architectures aim to embed these same guarantees directly into infrastructure. In this regard, regulations and regulators should support this direction, as it clearly aligns with the GDPR's purpose of protecting data subjects.

### **Towards scalable privacy as public infrastructure**

A complementary yet often overlooked dimension of privacy-preserving blockchain design is its role in broadening accessibility and institutional participation in public, permissionless networks. When privacy is embedded as a foundational infrastructure layer rather than retrofitted through add-ons or intermediated layers, it transforms public blockchains from open exposure systems into compliant, trustable, and enterprise-ready digital commons. For regulated actors, including financial institutions, corporates, and public administrations, this shift lowers the compliance barrier to participation by ensuring that data-protection obligations are met by design, not by ex-post contractual or procedural mitigation. In essence, the evolution toward privacy-native, modular architectures establishes a new category of digital infrastructure that combines the sovereignty of computation with lawful data boundaries. By decoupling consensus, execution, and data availability, and embedding advanced cryptographic techniques including zero-knowledge architecture, fully homomorphic encryption (FHE), and partially homomorphic encryption (PHE), systems can validate correctness without disclosing underlying data.

This approach not only secures sensitive information but also optimises network performance. Smaller, proof-based payloads reduce bandwidth and storage requirements, allowing faster block confirmation, lower energy consumption, and more efficient data propagation across nodes.

The result of this evolution is an ecosystem in which privacy and scalability reinforce each other. Decentralisation becomes operationally lighter, and compliance ceases to be a constraint on openness.

<sup>91</sup> EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, 7 July 2021, para 77, [https://www.edpb.europa.eu/system/files/2023-10/EDPB\\_guidelines\\_202007\\_controllerprocessor\\_final\\_en.pdf](https://www.edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf)



Such architectures enable diverse actors (private, public, and civil) to engage with public ledgers under a shared governance model rooted in confidentiality, verifiability, and efficiency.

It is therefore essential that regulatory guidance, particularly that of the EDPB evolves in parallel with these technological developments. Extending the scope of “personal data” to include purely mathematical verification artefacts that perfectly hide the information they are verifying, risks deterring the adoption of privacy-enhancing infrastructures that in fact advance the objectives of the GDPR.

Data protection guidance should encourage privacy-optimised designs. The interpretation of the GDPR must be risk based, aligned with the text of the GDPR and the jurisprudence of the CJEU. Expansive readings of “personal data” may not always promote better privacy in practice, and risk discouraging privacy innovation, reinforcing less secure intermediated models, and making it harder for Europe to maintain leadership in trust infrastructure. The EDPB could provide constructive, interpretative guidance for the emerging modular privacy preserving architectures so that Europe’s legal framework continues to drive higher levels of data protection through decentralised, privacy preserving scalable public ledgers as a public good.



## 5 Use cases

### 5.1 Certifying diplomas through a smart contract on a public blockchain

#### 5.1.1 Description of the use case

Academic diplomas are issued as electronically sealed documents (qualified electronic seals under eIDAS). Qualified electronic seals are time-limited and non-revocable (only the certificates can be revoked prospectively). To ensure long-term validation, it must be proven that the certificate was valid when the seal was created<sup>92</sup> and that the diploma was not revoked in the meantime. This verification must be possible independently of the issuer since a diploma remains valid, even when the issuer ceases to exist.

#### 5.1.2

##### Data stored on a blockchain

A smart contract stores a hash of the diploma<sup>93</sup>. In case of revocation, a flag is added to the smart contract.

#### 5.1.3

##### Does this data qualify as personal data? If so, how is this justified?

In this design, without revocation, the on-chain hash serves solely as a verification artefact. By itself it reveals no information related to a natural person and is not personal data for neutral observers. For parties holding the diploma, the hash merely functions as a verification artefact. In case of a revocation, however, the hash value functions as a lookup key to the revocation flag. This does add personal content on-chain. This is justified, because it optimally minimises access to the revocation information. A diploma needs to remain verifiable for a long time even after the issuing institution ceases to exist. Independent verifiability ensures the credibility of the diploma, which is in the interest of the data subject. At the same time, access to the revocation information is limited to those who can demonstrate possession of a copy of the diploma. It also protects those to whom a revoked diploma might be presented to.

**92** Although qualified electronic seals are time stamped by default, time stamps are also based on certificates that expire. To maintain legal validity of the qualified electronic seal over time, additional periodical time stamps are required. A yearly qualified electronic timestamp of the hash of a recent block is recognised as a qualified electronic timestamp of all prior information on the blockchain as shown by Christoph Sorge and Maximilian Leicht, Blockchain-based electronic time stamps and the eIDAS regulation: The best of both worlds" (2022) 19:1 SCRIPTed 61 <https://script-ed.org/?p=4017>, DOI: 10.29666/scrip.190122.61

**93** It is ensured that the diploma has enough entropy before being hashed, otherwise additional noise (salt) is added. Adding a secret key ("pepper") would not provide any privacy advantage since that key would always be communicated together with the diploma.



## 5.1.4

### **How does the use case support fundamental rights of the data subjects?**

The approach enables independent and durable verification without central dependence on the issuer, while shielding revocation details. It supports accuracy (updatable status), integrity (tamper-evident anchoring), and data minimisation.

The revocation flag informs those and only those that have a copy of the diploma that the appearance is not correct.

Verification using a blockchain allows verification without leaving a trace at a centralised institution. By contrast, centralised revocation registries would enable the tracing how often diplomas are verified by which IP addresses.

## 5.2

### **Proof of reserves**

#### 5.2.1

##### **Description of the use case**

Exchanges and other crypto-asset service providers have custody of their customers' funds. Some exchanges went bankrupt after customer funds were misappropriated (e.g. FTX, QuadrigaCX, Thodex etc.). Bundling customer funds reduces transaction fees and the environmental impact of crypto transactions but provides limited transparency about the existence of reserves covering all the assets a crypto-asset service provider has custody for its clients. To provide transparency about the existence of reserves, some exchanges offer a "proof of reserves".

#### 5.2.2

##### **Data stored on a blockchain**

There are different implementations of "proof of reserves". Binance hashes the individual account balances as liabilities and creates a Merkle tree based on them. A zero-knowledge proof is then constructed to prove the sum of all liabilities without disclosing individual account balances. The zero-knowledge proof and the link to the account holding the bundled reserves are added to the Merkle tree, the Merkle tree is published off-chain. The Merkle root hash could potentially be stored on a blockchain to ensure that the proof is not adjusted on the fly.

#### 5.2.3

##### **Does this data qualify as personal data? If so, how is this justified?**

Individual account balances of identifiable natural persons constitute personal data and are only communicated to the individual customer. A hash of this data, provided the data has sufficient entropy, cannot be used to reconstruct the original data. The Merkle root hash, potentially stored on a blockchain, cannot be used to relate information to a natural person.



The account information communicated only to the respective clients can, however, be used to verify that the amount is included in the sum of liabilities and that these liabilities are covered by the on-chain reserves. Without the account information, the Merkle tree can be used to verify that the total of all accounts is covered by on-chain reserves. Therefore, the Merkle root as well as the Merkle tree are only a verification artefacts as discussed above in 3.2.6 and do not constitute personal data.

#### 5.2.4

##### **How does the use case support fundamental rights of the data subjects?**

The approach allows to ensure that funds held by data subjects are covered. At the same time, no information about the account holders, not even their account balances, are disclosed.

An alternative would be to have an authority or auditor manually verify liabilities and reserves held by the exchange. This, however, would only be done in regular intervals, has a longer delay and exposes personal data to auditors and/or authorities.

### 5.3

#### **TRISA travel rule data exchange for crypto-asset service providers**

#### 5.3.1

##### **Description of the use case**

Crypto-asset service providers (CASPs), in particular exchanges, must exchange originator and beneficiary data under the "travel rule" (FATF Rec. 16; in the EU: Regulation (EU) 2023/1113, the Transfer of Funds Regulation, TFR). To implement this, open messaging protocols such as the Travel Rule Information Sharing Architecture (TRISA) and the Travel Rule Protocol (TRP) are used. Although the protocols are distinct, interoperability bridges exist so that CASPs using either protocol can exchange the required data; most solutions serialise payloads using the IVMS 101 data model.

#### 5.3.2

##### **Data stored on a blockchain**

On-chain transaction data typically includes transaction identifiers, timestamps, amounts and wallet/public-key addresses. By itself, such data does not directly identify natural persons but may permit linkage of past and subsequent transactions. As discussed in 3.4.4, CASPs rely on on-chain data, combined with off-chain KYC records, to meet anti-money laundering and crypto-regulatory obligations (e.g., screening, tracing), while travel-rule identity data is exchanged off-chain via protocols such as TRISA/TRP.



### 5.3.3

#### **Does this data qualify as personal data? If so, how is this justified?**

On-chain addresses and related metadata qualify as personal data only where they are reasonably linkable to an identified or identifiable natural person (e.g., via a CASP's KYC). Role allocation depends on the contractual arrangement: a CASP may act as controller for compliance processing; in other constellations data processing may be done as a processor for a client. Lawful bases under Art. 6(1) GDPR include:

- Art. 6(1)(c) GDPR (legal obligation) for travel-rule transmissions and AML/CFT compliance (in the EU: TFR obligations applicable as of 30 December 2024);
- Art. 6(1)(b) GDPR where processing is necessary to perform the contract with the customer to transfer the crypto-assets; and
- Art. 6(1)(f) GDPR (legitimate interests) for measures not directly mandated as legal obligations but required to provide the service as well as additional risk controls proportionate to the service.

Processing must satisfy the principles of necessity and proportionality. Regarding data minimisation, storage-limitation and security measures there is limited choice regarding the on-chain transaction data but one measure is not to re-use Bitcoin addresses, for example.

### 5.3.4

#### **How does the use case support fundamental rights of the data subjects?**

The setup enables lawful transfers initiated by data subjects while minimising personal-data exposure: identity data is exchanged off-chain and limited to fields required by the travel rule/AML law; on-chain publication remains pseudonymous and limited to what is technically required to perform the transaction and also serves as a basis for legally required transaction analysis. TRISA/TRP provide mutually authenticated, encrypted transport and a field-minimised structured payload (e.g. IVMS 101), which implements privacy by design. Where Chapter V GDPR regarding third-country transfers applies, SCCs are agreed upon bilaterally – where required. Transfer Risk or Impact Assessments (TRA/TIA) ensure the minimisation of the risk to data subjects.



## 6

# Proposed amendments to the GDPR

The GDPR was adopted in 2016. While Bitcoin started in 2009, the significance of distributed ledger technology in general and of blockchain as a trust service in particular became apparent to a wider public only over the following decade. Amendments to the Recitals set out below are based on EU legislation and case-law and intended to clarify how the GDPR should be interpreted in the context of blockchain technology.

### 6.1

## Motivations for amendments

#### 6.1.1

### Trust services

As discussed in 3.4.3 and 3.4.4 qualified trust service providers for qualified electronic ledgers are required to ensure the integrity of records on the ledger which includes ensuring immutability as clarified in the draft implementing acts. For other ledgers there may be a legitimate interest in doing so, because manipulations on the contents of a blockchain could undermine the legal recognition and evidential value afforded under eIDAS.

#### 6.1.2

### Crypto-asset service providers

As discussed in 3.4.3.2 and 3.4.4 crypto-asset service providers are obliged to analyse the transaction history of crypto-assets they admit for trading, custody or transfer. Where transaction history is no longer accessible, e.g. certain privacy coins, providers may not be able to meet their compliance obligations or are even expressly banned from providing services. This means, there is a legal obligation to process the on-chain transaction history and a legitimate interest to store this history for compliance reasons.

#### 6.1.3

### Verification artefacts

The reasoning of EDPS v Single Resolution Board (SRB) and its risk-based reading in 3.2.1 support a relative concept of identifiability. Based on that decision, Recital 26 needs to be read as excluding certain pseudonymous data from a subjective definition of personal data. This interpretation, for example, excludes the source of the data where the source would not gain additional information by relating the data to identifiable natural persons. This would also clarify that all perfectly hiding verification artefacts are not considered personal data for those not having access to the verified information.



The “Digital Package of Simplification” proposes to amend Art. 4(1) GDPR to render the definition of personal data purely relative<sup>94</sup>. If adopted, regardless of whether verification artefacts can be considered personal data at all, their qualification as personal data will apply, if at all, at most for those actors who are able to use them.

#### 6.1.4 Explicitly integrate Lindqvist

Already in 2003, the CJEU found that applying the rules on third-country transfers to internet publishing would disproportionately impose greater restrictions on internet publication than on publication in other forms, such as on paper. The Recitals should reflect that exception:

## 6.2 Proposed amendments to Recitals for the GDPR

### 6.2.1 Recital 65: Right of Rectification and Erasure

In a sixth sentence, trust services and processing of transaction histories shall be added as an exception to the right of rectification and erasure:

<sup>1</sup>A data subject should have the right to have personal data concerning him or her rectified and a ‘right to be forgotten’ where the retention of such data infringes this Regulation or Union or Member State law to which the controller is subject. <sup>2</sup>In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation. <sup>3</sup>That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet.

**94** The Digital Omnibus package proposes to amend Art. 4(1) GDPR as follows: ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; **Information relating to a natural person is not necessarily personal data for every other person or entity, merely because another entity can identify that natural person. Information shall not be personal for a given entity where that entity cannot identify the natural person to whom the information relates, taking into account the means reasonably likely to be used by that entity. Such information does not become personal for that entity merely because a subsequent recipient has means reasonably likely to be used to identify the natural person to whom the information relates.** European Commission, Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus) COM (2025) 837 final



<sup>4</sup>The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child. <sup>5</sup>However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims. <sup>6</sup>This includes, in particular, situations where obligations under Union or Member State law governing trust services – including electronic ledgers within the meaning of Regulation (EU) No 910/2014 as amended by Regulation (EU) 2024/1183 and its implementing acts – require the immutability of records to ensure integrity over time and unique sequential chronological ordering; and situations where controllers subject to Union frameworks on anti-money-laundering, and on information accompanying transfers of funds and certain crypto-assets, and to market-integrity frameworks for financial instruments, including crypto-assets, are required to retain and analyse transaction and order histories, including those derived from distributed-ledger systems.

## 6.2.2

### **Recital 47: Overriding Legitimate Interest**

To clearly allow the processing of transaction histories for fraud prevention, the following sentence should be inserted after the 6th sentence.

<sup>1</sup>The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. <sup>2</sup>Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. <sup>3</sup>At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. <sup>4</sup>The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing. <sup>5</sup>Given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks.



<sup>6</sup>The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. <sup>7</sup>Similarly, processing that is strictly necessary and proportionate to prevent fraud, market abuse or the circumvention of restrictive measures in relation to crypto-assets and financial instruments - including the storage of transaction histories, risk-based screening, on-chain analytics and surveillance of the transaction and order data - may constitute a legitimate interest of the controller. <sup>8</sup>The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.

### 6.2.3

#### **Recital 49: Network and Information Security and Trust Services as Overriding Legitimate Interest**

A third sentence shall be added to highlight the legitimate interest of trust service providers of electronic ledgers:

<sup>1</sup>The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. <sup>2</sup>This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems. <sup>3</sup>Similarly, the processing of personal data that is strictly necessary and proportionate to ensure the integrity and immutability of electronic ledgers as trust services within the meaning of Regulation (EU) No 910/2014 may constitute a legitimate interest of controllers.



## 6.2.4

### **Recital 45: Fulfilment of Legal Obligations**

The processing of on-chain transaction histories shall be listed as an example of legal obligations for data processing:

<sup>1</sup>Where processing is carried out in accordance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, the processing should have a basis in Union or Member State law. <sup>2</sup>This Regulation does not require a specific law for each individual processing. <sup>3</sup>A law as a basis for several processing operations based on a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority may be sufficient. <sup>4</sup>It should also be for Union or Member State law to determine the purpose of processing. <sup>5</sup>Furthermore, that law could specify the general conditions of this Regulation governing the lawfulness of personal data processing, establish specifications for determining the controller, the type of personal data which are subject to the processing, the data subjects concerned, the entities to which the personal data may be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing. <sup>6</sup>It should also be for Union or Member State law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or, where it is in the public interest to do so, including for health purposes such as public health and social protection and the management of health care services, by private law, such as a professional association. <sup>7</sup>This includes, in particular, obligations under Union law on the prevention of money laundering and terrorist financing, and on information accompanying transfers of funds and certain crypto-assets, requiring crypto-asset service providers to collect, retain and analyse originator/beneficiary information and transaction histories of crypto-assets.



## 6.2.5

### **Recital 26: Not Applicable to Anonymous Data**

The CJEU has decided on pseudonymous data where only the data source was able to identify the data subject. The “Digital Omnibus” proposes to amend Art. 4(1) GDPR to turn the definition of personal data into a relative one. If accepted, this takes a slightly different approach and would - in some cases - go further than the amendments in Recital 26 proposed here.

<sup>1</sup>The principles of data protection should apply to any information concerning an identified or identifiable natural person. <sup>2</sup>Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. <sup>3</sup>To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. <sup>4</sup>To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. <sup>5</sup>Where the identifiability of pseudonymous data “by another person” is considered, only such other persons shall be taken into account for whom, given the means reasonably likely to be used by them, the information in question would provide additional information beyond the identified information to which they already have lawful access. <sup>6</sup>Where such a person already has lawful access to information relating to that natural person, linking the data in question to a subset of that identified information does not provide that person with any additional information about the data subject and does not increase the risk to the rights and freedoms of the data subject associated with identification. <sup>7</sup>The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered pseudonymous in such a manner that the controller or another person who is not in possession of the original non-pseudonymised data, cannot reasonably likely identify the pseudonymous data with the natural person to whom the information relates. <sup>8</sup>This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.



## 6.2.6

### **Recital 101: General Principles for International Data Transfers**

The CJEU ruling in the Lindqvist case that the rules for publishing take precedence over the rules for third country transfers shall be clarified in Recital 101:

<sup>1</sup>Flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation. <sup>2</sup>The increase in such flows has raised new challenges and concerns with regard to the protection of personal data. <sup>3</sup>However, when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation. <sup>4</sup>In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation. <sup>5</sup>A transfer could take place only if, subject to the other provisions of this Regulation, the conditions laid down in the provisions of this Regulation relating to the transfer of personal data to third countries or international organisations are complied with by the controller or processor. <sup>6</sup>For the avoidance of doubt, the mere fact that personal data are made publicly available on a website or other publicly accessible online interface in the Union – including where such data can be accessed from third countries, and irrespective of the physical location of the servers used to make the content publicly available – does not in itself constitute a transfer to a third country under this Regulation.





**Blockchain For Europe**

Rue Montoyer 47  
B-1000 Brussels  
Belgium

[secretariat@blockchain4europe.eu](mailto:secretariat@blockchain4europe.eu)  
[www.blockchain4europe.eu](http://www.blockchain4europe.eu)