PhD Dissertation

The Problems of Effective Forgetting in Blockchain Wallet Providers: A European Union Data Protection Perspective

Presented by

PhD Candidate:

MARIAM PILISHVILI

Supervisor:

Prof. Dr. habil. ILDIKÓ BARTHA, Ph.D.

Professor of Law

UNIVERSITY OF DEBRECEN

Marton Géza Doctoral School of Legal Studies

Debrecen, 2026

"*The Internet is the first thing that humanity has built that humanity doesn't understand, the largest experiment in anarchy that we have ever had*."[1]

"*The blockchain is going to change everything more than the Internet has*."[2]

Abstract

This dissertation investigates how blockchain wallet providers could operationalize compliance with European data protection law, focusing on the relationship between blockchain immutability and the rights specified in the GDPR. Wallet providers are essential access points for users interacting with blockchain networks, but their reliance on replication, immutability, and openness raises significant compliance concerns, especially in light of Article 17's right to erasure.

Two research questions structure the analysis. First, to what extent can wallet providers meaningfully accommodate the right to be forgotten, and should compliance be understood in terms of "effective forgetting" rather than absolute erasure? And second, how should controllership and accountability be allocated among custodial and non-custodial wallet providers, where traditional controller–processor distinctions are blurred by the technical and governance realities of decentralized systems?

In terms of methodology, this dissertation applies a doctrinal legal analysis grounded in the GDPR, CJEU jurisprudence, and regulatory guidance, strengthened by a socio-legal viewpoint that situates these regulations within operational and technical contexts. The findings reveal that compliance is not only a matter of legal interpretation but also of technical design and governance clarity. By proposing a structured compliance rubric for effective forgetting and a functional allocation model of controllership, the dissertation offers actionable frameworks to reconcile wallet-provider operations with GDPR obligations. This focused analysis positions wallet providers as a vital test case for comprehending how EU data protection law may adjust to decentralized infrastructures while maintaining individual rights.

[1] Schmidt, E. and Cohen, J. (2013). *The new digital age: reshaping the future of people, nations and business*. New York: Knopf, p. 294.
[2] Pierce, B. (2023). *Tweet: The blockchain is going to change everything more than the Internet has*. X (formerly Twitter). Available at: https://x.com/brockpierce/status/1722641939554525676 (Accessed: 25 July 2025).

PLAGIARISM DECLARATION

I, the undersigned ***Mariam Pilishvili*** by signing the present statement declare that the thesis, entitled ***The Problems of Effective Forgetting in Blockchain Wallet Providers: A European Union Data Protection Perspective*** is my individual work.

In the process of writing the thesis I have complied with the provisions of Act LXXVI of 1999 on Copyright and the regulations of the University of Debrecen regarding the principles of thesis writing, especially regarding references and citations.

I declare that I have not submitted a dissertation with the same content as the submitted dissertation for a doctoral degree at another university.

Furthermore, I declare that I did not mislead my supervisors in the course of the preparation of the thesis with regard to the condition of the individuality of my work.

I also declare that the thesis submitted in paper form and its electronic version are identical in all respects (see Rules and Regulations, Article 24, paragraph 8).

By signing this declaration, I acknowledge that the University of Debrecen has the right to refuse acceptance of the thesis and to take disciplinary measures against me if it can be proven that the thesis is not my intellectual creation and if there is a suspicion of copyright infringement. In this case, the refusal to accept the thesis and the disciplinary proceedings do not affect any other legal consequences caused by the copyright infringement.

Debrecen,
April 18, 2026

Signature
Mariam Pilishvili

SUPERVISORY OPINION

on Mariam Pilishvili's PhD dissertation to be submitted for preliminary defence

Debrecen, 20 April 2026

Mariam Pilishvili's PhD thesis provides a valuable contribution to legal discourse on the intersection between EU data protection law and recent technical innovations in the digital era, such as decentralised blockchain architectures. Specifically, it focuses on wallet providers as key intermediaries in the implementation of the right to be forgotten under Article 17 of the General Data Protection Regulation (GDPR).

The thesis addresses a complex and highly relevant legal issue: the feasibility of implementing Article 17 of the GDPR in custodial and non-custodial blockchain wallet ecosystems, and whether compliance should focus on effective 'forgetting' rather than absolute 'deletion'. This issue constitutes the main research question of the thesis and is further divided into coherent groups of doctrinal, governance, operational, and normative sub-questions, each of which is covered in a specific chapter. This structure enables the author to move from the conceptual clarification of effective forgetting and the interpretation of Article 17, through an examination of controllership in decentralised ecosystems, to the design of concrete compliance mechanisms and the assessment of the associated regulatory, governance, and policy implications.

The final conclusions of the research are based on a creative and comprehensive examination of the relevant regulatory environment and academic literature. The thesis's originality primarily lies in two interlinked contributions: an in-depth analysis of the concept of effective forgetting in blockchain environments, identifying its practical challenges in this context; and the development of a nuanced framework for functional controllership in wallet ecosystems.

Overall, Mariam's thesis demonstrates her ability to identify the main research problems of the examined topic, to conduct in-depth research and to communicate the findings to the scientific community in a professional manner. As the supervisor of the research, I support the acceptance of the dissertation for the final defence.

Dr. Ildikó Bartha, supervisor
Professor of Law
University of Debrecen

Acknowledgments

I would like to express my sincere gratitude to my supervisor, Professor Dr. Ildikó Bartha for her guidance, patience, and continuous support throughout my doctoral journey. Her scholarly insight and professionalism shaped the way I approached my research, and her encouragement, offered generously and without hesitation, made a real difference. I am deeply thankful for the time and trust she gave to my work and to my development as a researcher.

I am also sincerely grateful to all members of my preliminary defence committee and to those who provided valuable recommendations and scholarly feedback on my research. Your comments significantly contributed to improving the clarity, structure, and academic quality of this dissertation. Your expertise and thoughtful evaluation helped refine the arguments and strengthen the final work. I would particularly like to thank Dr. Mátyás Bencze, habil., Dr. Gábor Kecskés, Dr. Péter Bordás, and Dr. Dóra Lovas, for their professional opinions, constructive observations, and valuable recommendations provided during the preliminary defence process.

I would like to express my appreciation to Professor Dr. József Szabadfalvi, DSc, Head of the Doctoral School, Faculty of Law, University of Debrecen, and Dr. habil. Zaccaria Martin, Secretary of the Doctoral School, for their assistance and care throughout my four years of study. The administrative process progressed smoothly thanks to your clear guidance, prompt responses, and continuous support. I am also grateful to all lecturers and administrative staff of the Faculty of Law whose professionalism made this academic journey manageable and well-structured. A simple thank you may not fully reflect my appreciation, but I am truly thankful for your support.

I would also like to acknowledge Tempus Public Foundation, the University of Debrecen, and the Faculty of Law for the financial support that enabled me to pursue this PhD through scholarship funding. This support made it possible for me to fully dedicate myself to my research and academic development.

My appreciation also extends to my classmates, fellow international students, members of the Höök Mentor Network, members of Praetor Szakkollégium, my colleagues from the DOSZ Ambassador Program, and the broader academic community in Debrecen. You contributed to

creating a supportive and engaging academic environment, making my time at the University both productive and memorable.

My deepest gratitude belongs to my family, who made this achievement possible long before this dissertation began.

My Supermom, Naiza Shubladze, whose belief in education and unwavering support created opportunities that shaped my entire path. Your strength, sacrifice, and dedication laid the foundation for everything I have achieved. I consider myself incredibly fortunate to have a mother who invested so much in my future.

My father, Mogeli Pilishvili, who continues to guide me from another world. His values, strength, and influence remain a constant source of inspiration and direction in my life.

My better half, Iveri Kopaliani, whose continuous encouragement, understanding, and support strengthened my motivation throughout this journey. Your belief in my potential helped me remain focused and determined to become the best version of myself.

My aunt, Nargiza Shubladze, and my cousins Lika Khundadze and Levan Khundadze, who played an essential role in raising and supporting me. Your care, encouragement, and presence have shaped who I am today, and I am deeply grateful for everything you have done for me. My dear Emzo Tsindeliani, Tako Tsindeliani, and Achi Tsindeliani, thank you for always believing in my aspirations and encouraging me to aim higher.

I would also like to thank my close friends, whose support, encouragement, and belief in me gave me strength during demanding periods of this journey. Your presence made challenges easier and successes more meaningful. I am truly grateful to have such people in my life.

Finally, I would like to thank myself for perseverance, discipline, and determination. Completing this dissertation required consistency, resilience, and continuous self-development. This milestone represents only the closing of one small chapter in a much larger journey. I remain motivated to continue learning, growing, and contributing further.

ABBREVIATION

AEPD	Spanish Data Protection Agency (Agencia Española de Protección de Datos)
AML/CFT	Anti-Money Laundering / Countering the Financing of Terrorism
API	Application Programming Interface
Art.	Article
Breyer	Breyer v Germany (CJEU case)
BW / BWs	Blockchain Wallet / Blockchain Wallets
CETS	Council of Europe Treaty Series
CFREU	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
CNIL	Commission Nationale de l'Informatique et des Libertés
COVID-19	Coronavirus Disease 2019
DApp / dApp	Decentralised Application
DAO	Decentralised Autonomous Organisation
DeFi	Decentralised Finance
DPA	Data Protection Authority
DPbD	Data Protection by Design and by Default
DPC	Data Protection Commissioner
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DLT	Distributed Ledger Technology
EBSI	European Blockchain Services Infrastructure
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EEA	European Economic Area
ETH	Ether (cryptocurrency of Ethereum network)
EU	European Union
FATF	Financial Action Task Force
GCHQ	Government Communications Headquarters (United Kingdom)
GC and Others	GC and Others v CNIL
GDPR	General Data Protection Regulation
IoT	Internet of Things
IP	Internet Protocol
KYC	Know Your Customer
KYD	Know Your Data
LDH	Ligue des droits humains
MBS	Mortgage-Backed Securities
MiCA	Markets in crypto-assets
MiFID II	Directive 2014/65/EU on markets in financial instruments
NFT	Non-Fungible Token

NSA	National Security Agency (United States)
OAuth	Open Authorization (authorisation framework)
OECD	Organisation for Economic Co-operation and Development
OTP	One-Time Password
P2P	Peer-to-Peer
PNR	Passenger Name Record
PoS	Proof of Stake
PoW	Proof of Work
PRISM	PRISM surveillance programme operated by the NSA
RPC	Remote Procedure Call
RTBF	Right to Be Forgotten
SA	Supervisory Authority
SCC	Standard Contractual Clause
Schrems I	Schrems v Data Protection Commissioner
Schrems II	Data Protection Commissioner v Facebook Ireland
SPV	Simplified Payment Verification
TEMPORA	UK intelligence surveillance programme
TFEU	Treaty on the Functioning of the European Union
TFR	Transfer of Funds and Crypto-Assets Regulation
TU & RE	TU and RE v Google LLC
UI	User Interface
URL	Uniform Resource Locator
USD	United States Dollar
ZKP	Zero-Knowledge Proof

Table of Contents

Abstract ..... *i*

Chapter 1. Introduction *1*

1.1 Data in the Digital Age: From Hyperconnectivity to Blockchain **2**
1.1.1 Data as the Fabric of Everyday Life 2
1.1.2 Data as the Core of the Digital Economy 4
1.1.3 GDPR as a Response to the Data Economy 5
1.1.4 Key legal and technical concepts 8
1.1.5 The Evolution of Blockchain 13

1.2 Research Framework **14**
1.2.1 Problem Statement 14
1.2.2 Research Questions 16
1.2.3 Methodology 18
1.2.4 Novelty and Original Contribution 20

1.3 Structure of the Dissertation **21**

Chapter 2. Building the GDPR: Foundations for Data Protection in Blockchain Environments *23*

2.1 Foundations of European Data Protection **23**
2.1.1 European Treaties and Directives 23
2.1.2 Beyond Human Rights: GDPR as Internal Market Instrument 25
2.1.3 The Snowden catalyst 29
2.1.4 Landmark CJEU Rulings 29

2.2 Personal Data as the New Oil **33**
2.2.1 Defining Personal Data in a Networked Society 33
2.2.2 EU vs. Global Approaches 36
2.2.3 A Broader Digital Challenge 37

2.3 Legal Actors under the GDPR Framework **38**
2.3.1 Data Subjects as a Right-Holders 38
2.3.2 Data Controllers and Its Expanding Mandate 39
2.3.3 Data Processors and Joint Controllers 42
2.3.4 Supervisory Authorities and the EDPB 43

Chapter 3. The Right to Be Forgotten in Law and Blockchain-Based Architectures *45*

3.1 The RTBF as an Evolution of Article 8 Protections **46**

3.2 Right to Erasure under GDPR **48**
3.2.1 Article 17 of the GDPR 50
3.2.2 Grounds for Erasure 50

3.3 Case Law and Functional Interpretation of Erasure **54**
3.3.1 Methodological Relevance of Search Engine Case Law for Blockchain Wallet Providers 55
3.3.2 Google Spain v Spanish Data Protection Agency (AEPD) and Mario Costeja González 59
3.3.3 Google v CNIL 61
3.3.4 GC and Others v CNIL 63
3.3.5 TU, RE v Google 65
3.3.6 Additional CJEU Guidance on the Criteria and Responsibility for Erasure 69

3.4 Alternative Perspectives on the RTBF **72**

3.5 Concluding Remarks: Effective Forgetting and Erasure under EU Law **74**

Chapter 4. Blockchain Fundamental, Actors and Accountability Constraints *77*

4.1 Core Technical Concepts of Blockchain Relevant to This Dissertation **80**

4.2 Smart Contracts and Legal Automation **84**

4.3 From Satoshi to Satoshi: Historical Evolution of Blockchain Technology **87**
4.3.1 Origins of Bitcoin and the Double-Spending Solution 87
4.3.2 A Close Reading of Nakamoto's Whitepaper 90
4.3.3 Blockchain Beyond Bitcoin 91

4.4 Structural Anatomy of the Decentralized Ledger **94**
4.4.1 Public vs Private Chains 96
4.4.2 Ex Ante Compliance in Private Chains vs. Public Chains 97
4.4.3 Permissioned vs Permissionless Models 100
4.4.4 Peer-to-Peer Network and Consensus Mechanisms 102

4.5 Blockchain Actors and Accountability Frameworks **105**
4.5.1 Validators, Nodes, and Governance Entities 106
4.5.2 Developers and End-Users 108

Chapter 5. Effective Forgetting in Blockchain Systems: Wallet Providers as a Case Study ***110***

5.1 Wallet architectures and data processing roles **113**
5.1.1 Custodial Wallet Providers 114
5.1.2 Non-Custodial Wallet Providers 115
5.1.3 Hot, Cold, and Hybrid Wallet Models 117
5.1.4 Smart-Contract and Organisational Wallets 118

5.2 Controllership in Wallet Ecosystems **120**
5.2.1 On-Chain Personal Data and the Limits of Provider Influence 120
5.2.2 Off-Chain Personal Data and the Architecture of Provider Responsibility 121
5.2.3 Functional and Joint Controllership in Wallet Infrastructures 124

5.3 Technical Limits of Literal Erasure in Blockchain Systems **127**

5.4 From Erasure to Effective Forgetting **129**
5.4.1 Conceptual Foundations of Effective Forgetting 129
5.4.2 Off-Chain Erasure and Data Suppression 131
5.4.3 Delinking and the Neutralisation of Linkability 132
5.4.4 Interface-Level Mitigation and Contextual Decoupling 134
5.4.5 Metadata Minimisation and Infrastructure Adjustments 135
5.4.6 A Legal Test for Effective Forgetting under Article 17 GDPR 135
5.4.7 Proportionality in Architecture-Sensitive Compliance 138

5.5 Regulatory Implications of Effective Forgetting **139**

5.6 Technical and Industry Governance Mechanisms **143**

5.7 Multi-Stakeholder Allocation of Responsibility **146**

5.8 Practical Implementation Scenarios for Effective Forgetting **151**

5.9 Embedding Effective Forgetting in Protocol Design **152**

5.10 Limits, Risks, and Open Questions **157**

Chapter 6. Conclusion ***162***

References ***169***

"*A man without Privacy is a man without dignity*."[3]

"*We have elected to put our money and faith in a mathematical framework that is free of politics and human error*."[4]

Chapter 1. Introduction

In 1902, Charles Holland Duell, then Commissioner of the United States Patent Office, remarked, "*all previous advances in the various lines of invention will appear totally insignificant when compared with those which the present century will witness. I almost wish that I might live my life over again to see the wonders which are at the threshold*."[5] Duell's insightful analysis of the internet's development from its early phases makes one think back to a period when many were skeptical of its promise. In the modern era, the internet has grown to be an essential part of our everyday existence, even though some people still find it difficult to completely understand the underlying technology.[6] But just as the world began to settle into the rhythm of this new reality, another technological shift appeared on the horizon: blockchain.[7] While societies were still adapting to the transformative effects of the internet, blockchain emerged as a further technological paradigm shift, introducing architectures based on decentralised trust, cryptographic verification, and immutability. Blockchain is not just another tool; It is a fundamental reinvention of how we communicate, transact, and create digital systems, the "next internet" in a world still adjusting to the first.[8] Blockchain

[3] Cowan, Z. (1970). *The Private Man*. Institute of Public Affairs, Rev 26, see at Walters, R., Trakman, L. and Zeller, B. (2019). *Data Protection Law: A Comparative Analysis of Asia-Pacific and European Approaches*. Singapore: Springer, ISBN 978–981–13–8109–6, p. 4.

[4] Winklevoss, T. (2013). Tweet. Available at: https://x.com/gemini/status/1149483074356256768?lang=en, (Accessed: 26 July 2025).

[5] Mokyr, J. (2014). *The next age of invention: Technology's future is brighter than pessimists allow*. City Journal, Preface. Available at: https://bpb-us-e1.wpmucdn.com/sites.northwestern.edu/dist/3/1222/files/2016/06/The-Next-Age-of-Invention-Technologys-future-is-brighter-than-pessimists-allow-24f8u5v.pdf, (Accessed: 26 July 2025).

[6] Vladkov-Mirazchiyski, P. (2025). Con*temporary gaps in research on digital divide in education: A literature review*. Universal Access in the Information Society, 24, pp. 991–1008. Available at: https://www.researchgate.net/publication/385275226_Contemporary_gaps_in_research_on_digital_divide_in_education_a_literature_review, (Accessed: 29 July 2025).

[7] Hassan, F.U., Ali, A., Latif, S., Qadir, J., Kanhere, S., Singh, J. and Crowcroft, J. (2019). *Blockchain and the future of the internet: A comprehensive review*. pp. 1–17. Available at: https://www.researchgate.net/publication/331730251_Blockchain_And_The_Future_of_the_Internet_A_Comprehensive_Review, (Accessed: 29 July 2025).

[8] Langer, A.M. (2020). *Analysis and Design of Next-Generation Software Architectures: 5G, IoT, Blockchain, and Quantum Computing*. 1st ed. Cham: Springer International Publishing, ISBN 978-3-030-36898-2, pp. 44–46.

represents a significant example of innovation at this ever-changing nexus of connectivity and technology, giving current solutions and expanding the possibilities of what the internet can accomplish.

1.1 Data in the Digital Age: From Hyperconnectivity to Blockchain

Technological innovation has accelerated dramatically in the twenty-first century.[9] Blockchain, big data analytics, artificial intelligence, and the Internet of Things (IoT),[10] are fundamental infrastructures that are reshaping how societies function rather than merely being tools added to an existing system.[11] According to Luciano Floridi (2014), we have reached a hyperhistorical era in which information systems are now essential to social, economic, and political life rather than just supporting it.[12] Lev Manovich (2001) also notes that the emergence of "new media," in which all kinds of culture and knowledge are more subject to digital processing, modularity, and automation, is largely due to the convergence of computing and media technologies.[13]

1.1.1 Data as the Fabric of Everyday Life

People don't just use technology in our hyperconnected world; they inhabit it.[14] A steady stream of behavioural, geographic, and demographic data is produced by the widespread use of smartphones, wearables, social media, and smart environments or settings.[15] Michael Goodchild's (2007) concept of volunteered geographic information illustrates how individuals now function as passive "sensors" in a global data ecosystem.[16] Mark Andrejevic (2011) warns that such participation embeds individuals in infrastructures of commercial

[9] Greenfield, A., (2017). *Radical Technologies: The Design of Everyday Life*. Verso Books, ISBN-13: 978-1-78478-043-2, pp.17–36.

[10] Salazar, J. and Silvestre, S., (2017) *Internet of things*. PROJECT. ISBN 978-80-01-06232-6, p. 6. Available at: https://core.ac.uk/download/pdf/132530214.pdf, (Accessed: 25 July 2025); see also, Internet of Things, see at G. Nick. (2022). *How Many IoT Devices are there in 2025?* Techjury Blog. Available at: https://techjury.net/industry-analysis/iot/, (Accessed: 25 July 2025).

[11] Riahi, A., Challal, Y., Natalizio, E., Chtourou, Z. and Bouabdallah, A., (2013). *A systemic approach for IoT security*. In 2013 IEEE international conference on distributed computing in sensor systems (pp. 351–355). Available at: https://www.researchgate.net/publication/261075256_A_Systemic_Approach_for_IoT_Security (Accessed: 25 July 2025).

[12] Floridi, L. (2014). *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*. Oxford University Press, ISBN: 9780199606726, pp. 17–22.

[13] Manovich, L. (2001). *The Language of New Media*. Cambridge, MA: MIT Press, ISBN: 9780262632553, pp. 43–48.

[14] McLuhan, M. (1994). *Understanding media: the extensions of man.* Cambridge, MA: MIT Press, pp. 7–21. Available at: https://designopendata.wordpress.com/wp-content/uploads/2014/05/understanding-media-mcluhan.pdf, (Accessed: 26 July 2025).

[15] Lupton, D., (2016). *The Quantified Self*. Polity Press, ISBN-13: 978–1–5095–0059–8, pp. 94–112.

[16] Goodchild, M.F. (2007). *Citizens as sensors: the world of volunteered geography*. GeoJournal, 69(4), pp. 211–221, DOI 10.1007/s10708-007-9111-y.

surveillance, where data flows become sources of economic value often without meaningful user control.[17]

The result is an epochal shift.[18] Data is no longer episodically collected; it is continuously generated as a condition of everyday digital existence.[19] Browsing, purchasing, moving through cities, or even carrying a smartphone creates a stream of "digital exhaust"[20] that is captured by platforms and states alike.[21] This digital exhaust is converted by artificial intelligence systems into prediction models for employment, healthcare, law enforcement, and credit scoring.[22] The secrecy and power of algorithmic governance are increased by the speed and scale at which these systems operate.[23] Smart cities and infrastructures use sensors and automatic feedback loops to maximise efficiency and convenience,[24] but they also raise important issues about privacy, autonomy, and accountability.[25] The shift to smart nations, interconnected systems including public services, energy, transportation, and finance, is already in progress.[26] However, as critical scholars have pointed out, this vision often depends on the bulk capture and commercialisation of personal data, perpetuating current disparities under the pretence of advancement.[27] In addition to this, predictive systems do not merely reflect social realities, they participate in shaping them, categorising individuals, allocating resources, and producing outcomes that can be difficult to contest.[28] In this context,

[17] Andrejevic, M. (2011). *Surveillance and Alienation in the Online Economy*. Surveillance & Society, 8(3), pp. 278–287. Available at: https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/4164, (Accessed: 26 July 2025).
[18] Lyon, D. (2018). *The Culture of Surveillance: Watching as a Way of Life*. Cambridge: Polity Press, ISBN-13: 978-0-7456-7172-7, pp. 2–6.
[19] Mayer-Schönberger, V. and Cukier, K. (2013). *Big data: A revolution that will transform how we live, work, and think*. pp.40–48, 98–101.
[20] Zook, M. and Graham, M. (2007). *The creative reconstruction of the internet: Google and the privatization of cyberspace and DigiPlace*. GeoForum, 38(6), pp. 1322–1343. Available at: https://www.geographie.ens.psl.eu/IMG/pdf/zook2007.pdf, (Accessed: 26 July 2025).
[21] Beer, D. (2016). *Metric Power*. Basingstoke: Palgrave Macmillan, ISBN 978-1-137-55648-6, p. 148–156.
[22] Broussard, M. (2018). Artificial Unintelligence: How Computers Misunderstand the World. Cambridge, MA: MIT Press, pp. 7–18.
[23] Kitchin, R. (2016). *Thinking critically about and researching algorithms.* Information, Communication & Society, 20(1), pp. 1–14. Available at: https://www.researchgate.net/publication/297664844_Thinking_critically_about_and_researching_algorithms, (Accessed: 26 July 2025).
[24] Greenfield, A. (2013). *Against the Smart City*. New York: Do Projects, ISBN 978-0-9824383-1-2, pp. 8-19.
[25] Sadowski, J. (2020). *Too Smart: How Digital Capitalism is Extracting Data, Controlling Our Lives, and Taking Over the World*. Cambridge, MA: MIT Press, pp. 89–106.
[26] Townsend, A. (2013). Smart Cities: *Big Data, Civic Hackers, and the Quest for a New Utopia*. New York: W.W. Norton & Company, ISBN 978-0-393-08287-6, pp. 153-164.
[27] Eubanks, V. (2018). *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. New York: St. Martin's Press, pp. 1–30, 143–175.
[28] Rouvroy, A. and Berns, T. (2013). *Algorithmic Governmentality and Prospects of Emancipation*. Révues Multitudes, 1(1), ISSN 0751-7971, pp. 6–10.

data governance becomes not a technical issue but a democratic imperative, raising urgent questions about transparency, power, and control in the digital age.[29]

1.1.2 Data as the Core of the Digital Economy

Against this backdrop, data has become the defining resource of the contemporary economy. The shift from Know Your Customer (KYC) to Know Your Data (KYD)[30] exemplifies how identification and regulation increasingly rely on metadata, behavioral patterns, and algorithmic profiling.[31] As the Economist famously observed, "the world's most valuable resource is no longer oil, but data."[32] Internet giants such as Alphabet, Amazon, Apple, Facebook (now Meta), and Microsoft now surpass oil companies in market value, reflecting data's centrality to global capitalism.

Nonetheless, there are significant and weighty responsibilities that come with big data's opportunities. Boyd and Crawford (2012) argue that cultures routinely adopt data-driven insights without considering how the data was gathered, who stands to benefit, and what is neglected.[33] According to Kitchin (2014), data is shaped by the procedures and assumptions used to collect and understand it; it is not self-explanatory.[34] These disclosures and insights serve as a reminder that, while data promotes economic growth, it also requires ethical safeguards such as responsibility in decision-making, justice, and respect for privacy.[35]

The sheer scope of data collection also amplifies risk. Healthcare, finance, education, smart cities, entertainment, and supply chains are all saturated with data flows. This ubiquity means that breaches, leaks, or misuses can have cascading effects across domains of life. In networked data environments, informational harms rarely remain isolated, as interlinked

[29] Taylor, L., Floridi, L. and van der Sloot, B. (eds.) (2016). *Group Privacy: New Challenges of Data Technologies*. Dordrecht: Springer, pp. 57–60.
[30] Cohen, J.E. (2019). *Turning Privacy Inside Out*. Theoretical Inquiries in Law, 20(1), pp. 1–32. doi:10.1515/til-2019-0001, pp. 3-6. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3162178, (Accessed: 25 July 2025); see also, Ghosh, A. (2022). *RegTech: From KYC to KYD to … KYDL*. MEDIUM, Available at: https://medium.com/@avi900in/regtech-from-kyc-to-kyd-to-kydl-47e219e4a424, (Accessed: 25 July 2025).
[31] Pistor, K. (2019). *The Code of Capital: How the Law Creates Wealth and Inequality*. Princeton: Princeton University Press, pp. 210–213.
[32] The Economist, (2017). *The world's most valuable resource is no longer oil, but data*, The Economist. Available at: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data, (Accessed: 25 July 2025).
[33] Boyd, d. and Crawford, K. (2012). *Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon, Information, Communication & Society*. 15(5), pp. 662–679.
[34] Kitchin, R. (2014). *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences*. London: SAGE, pp. 27–30.
[35] O'Connell, A. and Frick, W. (2014). *You've Got the Information, But What Does it Mean? Welcome to "From Data to Action*." Harvard Business Review, p. 1.

processing infrastructures transform localised failures into systemic vulnerabilities. Recent controversies such as Cambridge Analytica,[36] the British Airways 2018 breach,[37] and the Finnish psychotherapy provider Vastaamo's catastrophic data leak[38] illustrate how failures in data governance imperil individuals and erode public trust.

1.1.3 GDPR as a Response to the Data Economy

The General Data Protection Regulation (GDPR) entered onto the legal stage in 2018 like a contemporary Prometheus, daringly opposing the current state of data capitalism in order to give the people some semblance of power.[39] The GDPR was introduced to harmonize data protection laws and enhance the rights of data subjects concerning the processing of their personal information. The GDPR provides uniform law across all member states, facilitating the free flow of personal data within the European Union.[40]

As the speed at which individuals themselves retain and share personal information has increased, data privacy laws have strengthened in parallel.[41] This technological revolution has not only transformed business and social life but has also made it easier to transfer personal data within the European Union and to other nations and international organizations.[42] However, the question of whether in the era of technological developments legally recognised rights are limited to paper or if they encompas adequate protections and maintains a high

[36] Boldyreva, E.L., Grishina, N.Y. and Duisembina, Y., (2018). *Cambridge Analytica: Ethics and online manipulation with decision-making process*. In: The European Proceedings of Social and Behavioural Sciences, 18th PCSF Conference, Future Academy, pp. 92–102.
Available at: https://www.europeanproceedings.com/article/10.15405/epsbs.2018.12.02.10, (Accessed: 25 July 2025); see also, Water, R., (2018). *Facebook sued by US regulator over Cambridge Analytica scandal*. Financial Times. Available at: https://www.ft.com/content/683554b2-03c2-11e9-99df-6183d3002ee1, (Accessed: 25 July 2025).

[37] Voss, W.G. (2021). *Airline Commercial Use of EU Personal Data in the Context of the GDPR, British Airways and Schrems II*. Colorado Technology Law Journal, 19(2), pp. 406–411. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3702223, (Accessed: 25 July 2025).

[38] Ghanbari, H. & Koskinen, K. (2024). *When data breach hits a psychotherapy clinic: The Vastaamo case*. Journal of Information Technology Teaching Cases, Vol. 0(0), pp. 1–9. Available at: https://journals.sagepub.com/doi/epdf/10.1177/20438869241258235, (Accessed: 25 July 2025).

[39] European Parliament and Council, (2016). Regu*lation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data,and repealing Directive 95/46/EC* (General Data Protection Regulation). Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj, (Accessed: 25 July 2025).

[40] Nyrén, O., Stenbeck, M. and Grönberg, H., (2014). *The European Parliament proposal for the new EU General Data Protection Regulation may severely restrict European epidemiological research*. European journal of epidemiology, 29(4), pp. 227–230. Available at:
https://www.researchgate.net/publication/262111577_The_European_Parliament_proposal_for_the_new_EU_General_Data_Protection_Regulation_may_severely_restrict_European_epidemiological_research, (Accessed: 25 July 2025).

[41] Kuner, C., Bygrave, L.A. and Docksey, C. (eds.) (2020). *The GDPR: General Data Protection Regulation (EU) 2016/679: Commentary*. Oxford: Oxford University Press, pp. 9–12. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3839645, (Accessed: 25 July 2025).

[42] *Ibid*, pp. 158-168.

level of privacy safeguards during rapid technological advancements remains a topic of concern.

Recital 6 explicitly recognizes that "rapid technological developments and globalization have brought new challenges for the protection of personal data."[43] Personal data began to be utilized by both governmental and private organizations on an unprecedented scale.[44] The GDPR sought to ensure that data protection remained independent of the methods employed and technologically neutral,[45] raising the question of whether its safeguards would apply across all forms of technology.

Nevertheless, enforcement has revealed both the power and the limits of the framework. Fines levied against Google (€50m, CNIL 2019;[46] €150m for cookie practices in 2022)[47] and Meta/Facebook (€1.2bn for unlawful transfers in 2022;[48] $270m for advertising coercion in 2023)[49] demonstrate that regulators are willing to sanction global tech firms. Yet large-scale exposures, such as the leak of 540 million Facebook records in 2019[50] or health data

[43] GDPR, Recital 6.
[44] Weingärtner, T., (2024). *Blockchain for Digital Identity*. In: Jaafar, F., Pierre, S., (eds), *Blockchain and Artificial Intelligence-Based Solution to Enhance the Privacy in Digital Identity and IoT*, CRC Press, pp. 9-14.
[45] GDPR, Recital 5.
[46] Commission Nationale de l'Informatique et des Libertés (CNIL), (2019). *Délibération SAN-2019-001 of 21 January 2019 against Google LLC for failure to comply with transparency and consent obligations under the GDPR*, CNIL, pp. 2–3, paras, 1–20. Available at: https://www.cnil.fr/sites/cnil/files/atoms/files/san-2019-001.pdf, (Accessed: 25 July 2025); see also, Porter, J., (2019). *Google fined €50 million for GDPR violation in France*. The Verge. Available at:https://www.theverge.com/2019/1/21/18191591/google-gdpr-fine-50-million-euros-data-consent-cnil, (Accessed: 25 July 2025).
[47] Commission Nationale de l'Informatique et des Libertés (CNIL), (2021). Deliberation of the restricted committee No. SAN-2021-023 of 31 December 2021 concerning Google LLC and Google Ireland Limited. CNIL, pp. 25–28, paras 143–161.
Available at: https://www.cnil.fr/sites/cnil/files/atoms/files/deliberation_of_the_restricted_committee_no._san-2021-023_of_31_december_2021_concerning_google_llc_and_google_ireland_limited.pdf, (Accessed: 25 July 2025).
[48] European Data Protection Board (EDPB), (2023). Bin*ding Decision 1/2023 on the dispute submitted by the Irish SA on data transfers by Meta Platforms Ireland Limited for its Facebook service (Art. 65 GDPR). pp. 61–* 63, 72–73; paras 220–230, 268–279. Available at: https://www.edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-12023-dispute-submitted_en, (Accessed: 25 July 2025); see also, Satariano, A., (2022). *Meta Fined $1.3 Billion for Violating E.U. Data Privacy Rules*. The New York Times. Available at: https://www.nytimes.com/2023/05/22/business/meta-facebook-eu-privacy-fine.html, (Accessed: 25 July 2025).
[49] Data Protection Commission. (2022). De*cision in the matter of LB v. Meta Platforms Ireland Limited (Facebook Service)*, IN-18-5-5. Dublin: Data Protection Commission; and Data Protection Commission (DPC), (2022). *Decision in the matter of TSA v. Meta Platforms Ireland Limited (Instagram Service)*. DPC Inquiry Reference: IN-18-5-7, Dublin: Data Protection Commission, pp. 153–154, paras, 10.43–10.45. Available at: https://www.dataprotection.ie/en/news-media/data-protection-commission-announces-conclusion-two-inquiries-meta-ireland, (Accessed: 25 July 2025).
[50] BBC, (2019). *Data on 540 million Facebook users exposed*. Available at: https://www.bbc.com/news/technology-47812470, (Accessed: 25 July 2025); see also, Whittaker, Z., (2019).

transmissions via smartphone apps,[51] suggest that structural vulnerabilities persist.[52] Even record penalties, such as the $5bn fine imposed on Facebook by the FTC in 2019,[53] have not decisively altered platform practices.[54]

The GDPR exemplifies the problem of regulation catching up with innovation. Technology is changing at an exponential rate, whereas law is changing linearly and frequently reactively. According to Sheila Jasanoff's (2004) theory of co-production, governance frameworks are formed by prevalent definitions of risk and political disputes over what knowledge counts. This serves as a reminder that law and science do not emerge in distinct domains.[55] Her analysis of GMO regulation in the United States demonstrates how narrow notions of "sound science" can marginalize public concerns.[56] The "incubation period"[57] that most new technologies go through may possibly be the reason for the reluctance to regulate too soon.[58] During this stage, it is difficult to predict whether an idea will become a pillar of everyday life or go away. The internet, long dismissed by some policymakers as an academic novelty, has evolved into the foundation of modern communication, commerce, and culture.[59] Regulating it too soon may have hindered its growth, while waiting too long allowed for monopolies, misinformation, and widespread privacy loss. Timing, it turns out, is more than just a technical issue; it is a political decision influenced by uncertainty and competing

---

Researchers find 540 million Facebook user records on exposed servers. Available at: https://techcrunch.com/2019/04/03/facebook-records-exposed-server/, (Accessed: 25 July 2025).

[51] CBS, (2019). *Facebook reportedly received users' sensitive health data from apps: "It's incredibly dishonest."* Available at: https://www.cbsnews.com/news/facebook-reportedly-received-sensitive-health-data-from-apps-without-consent/, (Accessed: 25 July 2025).

[52] UpGuard Team. (2019). Losing Face: Two More Cases of Third-Party Facebook App Data Exposure. Available at: https://www.upguard.com/breaches/facebook-user-data-leak, (Accessed: 25 July 2025).

[53] Kang, C., (2019). *F.T.C. Approves Facebook Fine of About $5 Billion*. The New York Times. Available at: https://www.nytimes.com/2019/07/12/technology/facebook-ftc-fine.html, (Accessed: 25 July 2025); see also, Gilbert, D., (2019). *Facebook Just Paid a $5 Billion Fine for Privacy Breaches. Now it Wants Access to Your Brain*. Available at: https://www.vice.com/en/article/facebook-just-paid-a-dollar5-billion-fine-for-privacy-breaches-now-it-wants-access-to-your-brain/, (Accessed: 25 July 2025).

[54] Carrie, J., (2019). *Hundreds of millions of Facebook records exposed on public servers–report*. The Guardian. Available at: https://www.theguardian.com/technology/2019/apr/03/facebook-data-public-servers-amazon, (Accessed: 25 July 2025)

[55] Jasanoff, S., (2004). *The idiom of co-production*. In: S. Jasanoff, ed. *States of Knowledge: The Co-Production of Science and Social Order*. London: Routledge, pp.1–12.

[56] Jasanoff, S., (2005). *Designs on Nature: Science and Democracy in Europe and the United States*. Princeton University Press, paperback ISBN-13: 978-0-691-13042-2, pp. 106–110.

[57] Phan, P.H., Mian, S.A. and Lamine, W. eds., (2016). *Technology entrepreneurship and business incubation: Theory, practice, lessons learned*. World Scientific, pp. 7–10.

[58] Rotolo, D., Hicks, D. and Martin, B.R. (2015). *What is an emerging technology?* Research Policy, 44(10), 1827–1843, pp. 5–15. doi:10.1016/j.respol.2015.06.006.
Available at: https://www.researchgate.net/publication/272164853_What_Is_an_Emerging_Technology, (Accessed: 26 July 2025).

[59] Castells, M., (2001). The Internet Galaxy: Reflections on the Internet, Business, and Society. Oxford: Oxford University Press, ISBN 0–19–924153–8, pp. 9–33.

interests. But is delay always a symptom of confusion or caution? Not quite. Langdon Winner (1986) further reminds us that technologies are never neutral; they embody values and power structures.[60] Thus, when regulation is delayed, it is not mere oversight but often reflects the prioritization of market logics over public accountability. We've seen this play out before. When Facebook was still a college networking site,[61] few imagined it would reshape elections or redefine public discourse.[62] But regulation, like trust, often arrives too late, when the damage is already woven into the fabric of society.

Although the GDPR is written in technologically neutral language, its underlying assumptions of reversible processing, clearly identifiable controllers, and editable data repositories were designed with centralised systems in mind. Blockchain solutions, particularly wallet providers that act as the interface between users and decentralised ledgers, show the limitations of these assumptions with remarkable clarity.

1.1.4 Key legal and technical concepts

Because this dissertation operates at the intersection of law and technological architecture, conceptual clarity is essential. The GDPR-based legal interpretation of the key terminology used in this dissertation is necessary to be established before proceeding on to the technical and legal analysis. These terms and concepts are not self-evident to the wider public, and any legal analysis must begin by grounding its vocabulary in the applicable regulatory framework. The following definitions draw primarily from the GDPR and, where relevant, from guidance issued by the European Data Protection Board and the Article 29 Working Party.

Data and Personal Data. Any representation of facts, concepts, or instructions in a manner suitable for communication, interpretation, or processing by automated means is referred to as "data" in the digital environment.[63] The GDPR does not define "data" per se, but centers its scope on the narrower, legally operative category of "personal data." Under Article 4(1) GDPR, personal data means "any information relating to an identified or identifiable natural

[60] Winner, L., (2020). *The Whale and the Reactor: A Search for Limits in an Age of High Technology*. 2nd ed. Chicago: University of Chicago Press. pp. 37–44.
[61] Kirkpatrick, D. (2010). *The Facebook Effect: The Inside Story of the Company That Is Connecting the World*. New York: Simon & Schuster, pp. 30–52.
[62] Zuboff, S. (2019) The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs, pp. 110–121.
[63] International Organization for Standardization, (2015). ISO/IEC 2382:2015 Information technology—Vocabulary. Geneva: ISO. Available at: https://www.iso.org/obp/ui/ - iso:std:iso-iec:2382:ed-1:v2:en, (Accessed: 27 March 2026).

person ('data subject')." An identifiable person is one who can be identified, directly or indirectly, by reference to identifiers such as a name, identification number, location data, an online identifier, or factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.[64]

This definition is deliberately broad and technology-neutral, meaning that information qualifies as personal data not because of its format, but because it can reasonably be linked to an identifiable natural person.[65] The Court of Justice of the European Union has consistently interpreted identifiability expansively, confirming that the qualification of personal data depends on whether identification is reasonably likely, taking into account available means and contextual factors. In the blockchain context, public wallet addresses, transaction metadata, and IP addresses linked to node activity may constitute personal data where they enable the identification of a natural person, as reflected in guidance of the European Data Protection Board on blockchain and data protection.[66] Earlier case law such as Scarlet Extended (C-70/10) recognised that IP addresses constitute protected personal data where they enable user identification. By analogy, blockchain public keys may also qualify as personal data as persistent pseudonymous identifiers capable of linking transaction histories to individuals when combined with additional information.[67]

Data Processing. Under Article 4(2) GDPR, "processing" means any operation performed on personal data, including collection, recording, organisation, structuring, storage, retrieval, consultation, use, disclosure, restriction, erasure, or destruction.[68] The Court of Justice of the European Union has consistently interpreted the concept of processing broadly, confirming that even technical operations enabling the indexing, storage, or accessibility of information

[64] GDPR, Article 4(1).
[65] Court of Justice of the European Union, (2016). *Patrick Breyer v Bundesrepublik Deutschland* (*Case C-582/14, ECLI:EU:C:2016:779*, paras 32, 40–49. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62014CJ0582, (Accessed: 26 March 2026).
[66] European Data Protection Board, (2025). *Guidelines 02/2025 on processing of personal data through blockchain technologies*. Version 1.1, sections 3.2, 4.2. Available at: https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-022025-processing-personal-data_en, (Accessed: 27 March 2026); Article 29 Working Party, (2007). *Opinion 4/2007 on the concept of personal data*. 01248/07/EN, WP136, page 13–17. Available at: https://www.pdp.ie/docs/1030.pdf, (Accessed: 26 July 2025).
[67] Court of Justice of the European Union, (2011). S*carlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL, (SABAM) (C-70/10) ECLI:EU:C:2011:771,* para 51. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62010CJ0070, (Accessed: 27 March 2026).
[68] GDPR, Article 4(2).

online constitute processing of personal data.[69] Blockchain transactions involve the recording and storage of transaction-related data across distributed network nodes and therefore fall within the broad scope of processing activities regulated by the GDPR.[70] The decentralised architecture of blockchain infrastructures does not preclude qualification as processing but complicates the allocation of responsibility among participants involved in determining the purposes and means of processing operations.[71] Accordingly, assessing GDPR applicability in blockchain environments requires a functional analysis of the actors participating in transaction validation, propagation, and storage, consistent with the CJEU's jurisprudence on joint controllership.[72]

Controller and Processor. Article 4(7) GDPR defines the controller as the natural or legal person that determines the purposes and means of processing personal data, while Article 4(8) GDPR defines the processor as the entity that processes personal data on behalf of the controller.[73] In blockchain environments, determining controllership is particularly complex due to decentralised governance structures and the distributed validation of transactions.[74] Custodial wallet providers typically determine both the purposes and operational parameters of processing personal data connected to user accounts, thereby strongly indicating controller

[69] CJEU, (2014). *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*. Case C-131/12, ECLI:EU:C:2014:317, paras 21, 25–28, and 41. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0131, (Accessed: 26 March 2025); see also, Breyer v Bundesrepublik Deutschland, C-582/14, paras 38–45, 49.

[70] Finck, M., (2019). *Blockchain and the General Data Protection Regulation, Can distributed ledgers be squared with European data protection law?* European Parliamentary Research Service, pp. 29–33, 35–39. Available at: https://www.europarl.europa.eu/RegDzata/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf, (Accessed: 26 July 2025); Purtova, N., (2018). *The law of everything. Broad concept of personal data and future of EU data protection law*. Law, Innovation and Technology, 10(1), pp. 43–45, 54–55. Available at: https://www.studocu.com/en-gb/document/university-of-southampton/data-protection/purtova-the-law-of-everything-broad-concept-of-personal-data-and-future-of-eu-data-protection-law/59668268, (Accessed: 27 March 2026).

[71] European Data Protection Board, (2020). *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*. Version 2.1, pp. 50–55, 175–181. Available at: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en, (Accessed: 23 March 2026); see also, Article 29 Data Protection Working Party, (2010). *Opinion 1/2010 on the concepts of "controller" and "processor"*. 00264/10/EN, WP 169, pp. 10–12, 18–24. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf, (Accessed: 23 March 2026).

[72] Court of Justice of the European Union (CJEU), (2018). *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*. Case C-210/16, ECLI:EU:C:2018:388, para, 28–43. Available at: https://curia.europa.eu/juris/liste.jsf?num=C-210/16, (Accessed: 26 March 2026); see also, Court of Justice of the European Union, (2019). *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV*. Case C-40/17, Judgment of the Court (Second Chamber) of 29 July 2019, ECLI:EU:C:2019:629, paras 67–79. Available at: https://curia.europa.eu/juris/liste.jsf?num=C-40/17, (Accessed: 26 March 2026).

[73] GDPR, Articles 4(7)(8).

[74] Finck, 2019, pp. 41–49; see also, EDPB Guidelines 07/2020, pp. 9–13, 21–23, 54–58; WP169, Opinion 1/2010, 2010, pp. 14–17, 18–26.

qualification.[75] Non-custodial wallet providers, although exercising less direct control over private keys, may nevertheless qualify as controllers with respect to off-chain personal data processing, including user authentication, security monitoring, and analytics functions.[76]

Blockchain. EU law does not yet provide a single authoritative legal definition of "blockchain." However, Regulation (EU) 2022/858 on a pilot regime for market infrastructures based on distributed ledger technology (DLT Pilot Regulation) defines "distributed ledger technology" as "a type of technology that supports the distributed recording of encrypted data."[77] A distributed ledger may be understood as a shared repository of information in which transaction data is recorded, synchronised, and maintained across multiple network nodes using consensus mechanisms.[78] Blockchain constitutes a specific form of distributed ledger technology in which records are organised into cryptographically linked blocks, creating an append-only chronological structure secured through cryptographic validation.

In this dissertation, blockchain is understood as a decentralised distributed ledger in which transactions are recorded across multiple nodes, making stored data practically resistant to modification.[79] This functional understanding is legally relevant because it explains both the appeal of blockchain as an infrastructure for trust and transparency, and the structural tension it creates with GDPR obligations that presuppose the technical feasibility of data erasure and rectification.

---

[75] GDPR, Article 4(7); EDPB Guidelines 07/2020, pp. 13–15; Finck, 2019, pp. 13–19.

[76] GDPR, Article 4(7); EDPB Guidelines 07/2020, pp. 30–33; Finck, 2019, pp. 27–29; Purtova, 2018, pp. 48–49.

[77] European Union, (2022), *Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology*, Official Journal of the European Union, L 151, pp. 1–33. Article 2(1). Available at: https://eur-lex.europa.eu/eli/reg/2022/858/oj/eng, (Accessed: 27 March 2026).

[78] Jimenez-Gomez, B.S. (2023). Dist*ributed Ledger Technology in Financial Markets: The European Union Experiment*. Cuadernos de Derecho Transnacional, vol. 15, no. 2, pp. 667, 670–672. Available at: https://www.researchgate.net/publication/374967271_Distributed_Ledger_Technology_in_Financial_Markets_The_European_Union_Experiment, (Accessed: 27 March 2026).

[79] European Data Protection Board, (2020). *Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications*. Version 2, pp. 5–7. Available at: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012020-processing-personal-data-context_en, (Accessed: 27 March 2026); Von Hafe, F., Wagle, Y., Guede-Fernández, F., Giordano, A.P., Silva, L. and Azevedo, S., (2025). *Legal frameworks for blockchain applications: a comparative study with implications for innovation in Europe*. Frontiers in Blockchain, 8, pp. 1–12. Available at: https://www.researchgate.net/publication/394377041_Legal_frameworks_for_blockchain_applications_a_comparative_study_with_implications_for_innovation_in_Europe, (Accessed: 27 March 2026).

Blockchain Wallet. No binding EU legislative instrument presently defines "blockchain wallet" as a separate legal category. For regulatory purposes, the concept is most closely approximated by Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA), which addresses “crypto-asset service providers” and references “custody and administration of crypto-assets on behalf of clients” as a regulated service.[80]

A blockchain wallet, in the technical and operational sense used throughout this dissertation, refers to software or hardware that stores cryptographic keys enabling a user to interact with a blockchain network, initiate transactions, and exercise control over assets recorded on the distributed ledger. Crucially, the wallet does not hold the assets themselves; rather, the assets exist as entries recorded on the distributed ledger. The wallet stores the private cryptographic key that enables the user to access blockchain addresses and authorise transactions.[81] This distinction carries significant legal implications, as it influences the extent of the wallet provider’s control over data and, consequently, its potential qualification as a data controller or data processor under the GDPR.[82]

Blockchain Wallet Provider. A blockchain wallet provider is the natural or legal person that develops, operates, or makes available a blockchain wallet service to end users.[83] The legal significance of this concept varies depending on the degree of control exercised by the provider. Custodial wallet providers hold private keys on behalf of users and thus exercise direct control over the user’s on-chain access;[84] they typically collect, store, and process substantial off-chain personal data and are most likely to qualify as data controllers under

[80] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 *on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937, 2023, OJ L150/40* (MiCA Regulation), Articles 3(1)(17). Available at: https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng, (Accessed: 26 March 2026).

[81] European Banking Authority, (2019). *Report with Advice for the European Commission on Crypto-assets.* EBA Report, pp. 7–10. Available at: https://www.eba.europa.eu/sites/default/files/documents/10180/2545547/67493daa-85a8-4429-aa91-e9a5ed880684/EBA Report on crypto assets.pdf, (Accessed: 26 March 2026).

[82] GDPR, Articles 4(7), 4(8); Zafar, A., (2025). Reconciling blockchain technology and data protection laws: regulatory challenges, technical solutions, and practical pathways. Journal of Cybersecurity, 11(1), p.tyaf002, pp. 12–15. Available at: https://academic.oup.com/cybersecurity/article/11/1/tyaf002/8024082, (Accessed: 26 March 2026).

[83] Regulation (EU) 2023/1114, Article 3; European Banking Authority, (2020). *Annual Report 2019*. ISSN 1977-9046, ISBN 978-92-9245-659-7, Luxembourg: Publications Office of the European Union, 2020, pp. 7–10. Available at: https://www.eba.europa.eu/publications-and-media/press-releases/eba-publishes-its-2019-annual-report, (Accessed: 26 March 2026).

[84] Rauchs, M., Blandin, A., Klein, K., Pieters, G.C., Recanatini, M. and Zhang, B.Z., (2018). *2nd global cryptoasset benchmarking study.* Available at SSRN 3306125, pp. 30–33. Available at: https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/2nd-global-cryptoasset-benchmark-study/, (Accessed: 26 March 2026).

Article 4(7) GDPR.[85] Non-custodial wallet providers supply software through which users retain sole control of their private keys; such providers process less personal data directly, but may still qualify as controllers in respect of the off-chain data they handle.[86] The distinction between custodial and non-custodial providers is therefore not merely technical but carries direct legal consequences for the allocation of GDPR obligations, including those arising under Article 17's right to erasure.[87] The legal implications of this distinction are examined in greater depth in Chapters 4 and 5.

1.1.5 The Evolution of Blockchain

Blockchain joins an already tight regulatory landscape. Described as the "*trust protocol*," blockchain promises secure, transparent, and decentralized data storage and transfer,[88] by providing decentralized solutions.[89] Its evolution is typically characterized in three waves: Blockchain 1.0 (cryptocurrencies such as Bitcoin),[90] Blockchain 2.0 (smart contracts and programmable assets),[91] and Blockchain 3.0 (applications in governance, health, science, and culture).[92] By offering immutable, peer-validated records without intermediaries, blockchain challenges traditional models of trust and accountability.

Yet these same characteristics, immutability, replication, pseudonymity, bring blockchain into sharp tension with data protection law. The right to be forgotten under Article 17 GDPR presumes the possibility of erasure or modification,[93] while blockchain ledgers are designed

[85] GDPR, Article 4(7).
[86] Walch, A., (2019). *Deconstructing'decentralization': Exploring the core claim of crypto systems*. in Brummer (ed), Cryptoassets Cryptoassets: Legal, Regulatory, and Monetary Perspectives, Oxford University Press, pp. 23–24, 27–30. Available at: https://www.resistance.money/class/readings/deconstructing_decentralization.pdf, (Accessed: 26 March 2026).
[87] Zetzsche, D.A., Arner, D.W. and Buckley, R.P., (2020). *Decentralized finance. Journal of Financial Regulation*. 6(2), pp.139–147. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3539194, (Accessed: 26 March 2026).
[88] Tapscott, D., Tapscott, A. (2016) *Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World*. New York: Penguin, pp. 22–28.
[89] Mougayar, W. (2016). *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*. Hoboken, NJ: John Wiley & Sons, pp. 15–18; see also, King, M. (2016). *The End of Alchemy: Money, Banking, and the Future of the Global Economy*. New York: W. W. Norton, pp. 3–8.
[90] Badr, B., Horrocks, R. and Wu, X.B., (2018). *Blockchain By Example: A developer's guide to creating decentralized applications using Bitcoin, Ethereum, and Hyperledger*. Packt Publishing Ltd., pp. 8–12.
[91] Ayed, A.B. (2017). *A conceptual secure blockchain-based electronic voting system*. International Journal of Network Security & Its Applications, 9(3), pp. 01–09. Available at: https://doi.org/10.5121/ijnsa.2017.9301, (Accessed: 25 July 2025).
[92] Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). *Blockchain technology and its relationships to sustainable supply chain management*. International Journal of Production Research, 57(7), 2117–2135. doi: 10.1080/00207543.2018.1533261.
[93] GDPR, Article 17.

to resist alteration.[94] Similarly, GDPR presupposes identifiable controllers and processors who determine the purposes and means of processing,[95] whereas blockchain distributes decision-making across decentralised networks.[96] As John Mathews observes, "The GDPR was written on the assumption that you have centralized services controlling access rights to the user's data, which is the opposite of what a permissionless blockchain does."[97] The paradox is stark: is data recorded on blockchain still subject to GDPR? If so, how can its requirements be met without undermining the very properties that make blockchain distinctive?[98]

Yes, the GDPR applies, but not to the "blockchain" architecture, but to the object of its processing: personal data.[99] The moment personal data enters the ledger, be it in the form of public keys, transaction metadata, or hashed identifiers, the regulatory obligations are triggered. In other words: the law attaches to the data,[100] while the difficulty lies in the design.[101]

1.2 Research Framework

1.2.1 Problem Statement

The rapid adoption of blockchain technologies and the proliferation of blockchain wallets, both custodial and non-custodial, have fundamentally reshaped how personal data is generated, stored, and shared. Every wallet transaction leaves an immutable, publicly verifiable trail on the distributed ledger.[102] This technical feature, while essential for transparency and trust, creates an ecosystem of "remember-by-default" data, in stark contrast to the human brain's natural "forgetting-by-default" mechanism.[103]

This persistence of data raises several critical challenges.

---

[94] Ministry of Digital Affairs, DLT and Blockchain Working Group, (2019). *The GDPR and the blockchain technology*. Warsaw: Ministry of Digital Affairs, pp. 1–10.
[95] GDPR, Articles 4(7), 4(8), 26, 5(2), Recitals 79, 74, 81.
[96] DLT and Blockchain Working Group, *The GDPR and the blockchain technology*, 2019, pp. 1–10.
[97] Meyer, D., (2018). *Blockchain technology is on a collision course with EU privacy law*. International Association of Privacy Professionals Article, The Privacy Advisors. Available at: https://iapp.org/news/a/blockchain-technology-is-on-a-collision-course-with-eu-privacy-law, (Accessed: 29 July 2025).
[98] Finck, 2019, pp. 8–13.
[99] GDPR, Article 2(1).
[100] GDPR, Article 4(1).
[101] GDPR, Article 17.
[102] Casey, M. & Vigna, P. (2018). *The Truth Machine: The Blockchain and the Future of Everything*. New York: St. Martin's Press, pp. 71–78.
[103] Mayer-Schönberger, V., (2009). *Delete: The Virtue of Forgetting in the Digital Age*. Princeton University Press, 2009, pp. 1–15.

First, loss of control over personal data is inherent to the design. A user who interacts with a decentralized application (dApp) or sends funds using a wallet address cannot later retract that transaction history.[104] This is particularly problematic when addresses can be linked, even indirectly, to a real-world identity through on-chain analysis, leaks, or regulatory reporting requirements. a wallet address that was once used anonymously may eventually be deanonymized via analytics services or centralised exchange records, revealing years of historical activity.[105]

Second, there are significant contextual dangers associated with everlasting traceability.[106] Consider a scenario where a user experiments with a blockchain-based service that subsequently fails due to controversy or scandal. The user's wallet history is still publicly available years later, which could have an impact on job applications, legal disputes, or even personal and interpersonal relationships. Much like the digital traces left on social media platforms, immutable blockchain records can resurface in ways that users neither anticipate nor consent to.[107]

Third, self-censorship and participation chilling effects emerge. As users become more aware that every interaction is recorded permanently, they may avoid exploring innovative decentralized services or supporting causes that carry social or political sensitivity.[108] In this way, immutable design can inadvertently constrain user autonomy and freedom of expression.

The complicated role of wallet providers exacerbates these issues. Custodial wallets, which are frequently run by exchanges, are increasingly subject to AML/CFT regulations like the Transfer of Funds and Crypto Assets Regulation (EU) 2023/1113 and maintain a significant

[104] Antonopoulos, A.M. (2015). *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. 1st edn. Sebastopol, CA: O'Reilly Media, Incorporated, pp. 62–65.
[105] Greenberg, A. (2022). *Tracers in the Dark: The Global Hunt for the Crime Lords of Cryptocurrency*. 1st edn. New York: Knopf Doubleday Publishing Group, Chapter 14, pp. 99–104.
[106] Brin, D. (1998). *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?* ISBN : 978-0-465-02790-3, pp. 18–22.
[107] See most high-profile deanonymization cases, the Silk Road Takedown (2013), the Colonial Pipeline Ransomware Payment (2021), and Roman Sterlingov and Bitcoin Fog (2021), that have been used for legitimate and even critical law-enforcement purposes. However, this also raises concerns about privacy and surveillance, meaning, once a wallet is linked to a person, every past transaction becomes traceable.
[108] Kenyon, M. (2017). Jon Penney on the Chilling Effects of Online Surveillance. Available at: https://citizenlab.ca/2017/07/jon-penney-on-the-chilling-effects-of-online-surveillance/, (Accessed: 26 July 2025).

amount of off-chain data, such as IP logs and KYC records.[109] Despite being promoted as "privacy-preserving," non-custodial wallets frequently handle metadata or collaborate with outside analytics platforms, which raises concerns about functional responsibility and controllership.[110] Yet, current regulatory and technical frameworks do not clearly allocate responsibilities across this spectrum. This lack of conceptual clarity generates uncertainty regarding how GDPR obligations should be operationalised in decentralised infrastructures.

The legal tension with GDPR Article 17 (the "right to erasure") is acute. The principle of "effective forgetting," whether through de-referencing,[111] cryptographic deletion, or off-chain suppression,[112] remains underdeveloped in the blockchain context. To put it another way, providers cannot alter or erase the immutable on-chain records that unerpin blockchain operation, even while they can manage and remove off-chain data.[113] This challenge mirrors the inherent limitations of anonymization highlighted by the Article 29 Working Party, which notes that even the most robust techniques (e.g., noise addition, permutation, or k-anonymity) cannot guarantee irreversible de-identification where data remains linkable or inferable by reasonable means.[114] While guidance from authorities such as the CNIL and draft EDPB blockchain opinions urge off-chain storage of personal data and cryptographic techniques for access suppression, there is no coherent standard for what constitutes compliance when on-chain records are inherently indelible.

1.2.2 Research Questions

This dissertation examines whether the Right to be Forgotten (Article 17 GDPR) can be meaningfully implemented within blockchain-based wallet ecosystems, and whether

[109] European Parliament and of the Council. (2023). Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849, OJ L 150, 9.6.2023, pp. 1–39. Available at: https://eur-lex.europa.eu/eli/reg/2023/1113/oj/eng, (Accessed: 26 July 2025); see also, Jones Day. (2025). Crypto-Assets, CASPs and AML/CFT Compliance. Available at: https://www.jonesday.com/en/insights/2025/07/crypto-assets-casps-and-amlcft-compliance-the-new-european-regulatory-landscape-under-mica-and-amlr, (Accessed: 26 July 2025).

[110] Torres, C.F., Willi, F. and Shinde, S.,(2023). Is your wallet snitching on you? an analysis on the privacy implications of web3. In 32nd USENIX Security Symposium (USENIX Security 23), pp. 7–10, 10–14, 17–20. Available at: https://arxiv.org/abs/2306.08170, (Accessed: 26 July 2025).

[111] Court of Justice of the European Union (CJEU), (2019). *Google LLC v Commission nationale de l'informatique et des libertés (CNIL).* Case C-507/17, ECLI:EU:C:2019:772, para, 72. Available at: https://curia.europa.eu/juris/liste.jsf?language=en&num=C-507/17, (Accessed: 26 July 2025).

[112] Belen-Saglam, R., Altuncu, E., Lu, Y. and Li, S., (2023). *A systematic literature review of the tension between the GDPR and public blockchain systems*. Blockchain: Research and Applications, 4(2), p.100129. Available at: https://arxiv.org/pdf/2210.04541, (Accessed: 26 July 2025).

[113] Article 29 Data Protection Working Party, (2014). *Opinion 05/2014 on Anonymisation Techniques*. 0829/14/EN, WP216, pp. 5–11. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf, (Accessed: 26 July 2025).

[114] WP216, Opinion 05/2014, 2014, pp. 11–19.

compliance should be reframed through the concept of "effective forgetting," whereby personal data becomes practically inaccessible even if not technically erased. By doing so, the dissertation develops a framework that reconciles the operational realities of decentralised, immutable technological infrastructures with the legal requirements of EU data protection law.

To achieve this goal, this dissertation addresses the following research question:

> *To what extent can custodial and non-custodial wallet providers comply with the Right to be Forgotten under Article 17 GDPR, and should the compliance standard be reframed as "effective forgetting," meaning practical inaccessibility of personal data rather than absolute erasure?*

The following grouped sub-questions, reflecting the doctrinal, governance, operational, and normative aspects of compliance, are addressed in the dissertation in order to answer this primary research question.

Group A. Doctrinal and Interpretative Questions
(Answered primarily in Chapter 3)

- What constitutes "effective forgetting" in blockchain ecosystems, and can functional inaccessibility satisfy the substantive aims of Article 17 GDPR?
- To what extent can principles from CJEU jurisprudence, particularly Google Spain and Google v CNIL, be adapted to the unique architecture of blockchain networks?

Group B. Governance and Accountability Questions
(Answered primarily in Chapters 4 and 5)

- How should controllership and accountability be allocated in decentralized wallet ecosystems under the GDPR?

Group C. Operational and Compliance Questions
(Answered primarily in Chapter 5)

- What technical, regulatory, and contractual mechanisms could operationalize functional forgetting without undermining blockchain's operational integrity?

Group D. Normative and Policy Questions

(Answered primarily in Chapter 5)

- What are the normative and policy implications of embedding effective forgetting in blockchain governance frameworks?

1.2.3 Methodology

This dissertation's study technique provides a thorough examination of how blockchain wallet providers comply with European data protection regulation by combining socio-legal analysis and doctrinal legal research (the black-letter approach).

The doctrinal legal approach, sometimes referred to as the black-letter method,[115] focuses on analyzing primary legal sources, including:

- The General Data Protection Regulation (GDPR)
- Relevant CJEU judgments (such as Google Spain and Google v. CNIL)
- Guidance and opinions from the European Data Protection Board (EDPB)
- Supplementary EU legal instruments relating to privacy and data protection

This approach is supported by a thorough review of secondary legal sources, including scholarly articles, legal commentaries, and regulatory reports, to critically examine how Article 17 (Right to Erasure), data minimization, purpose limitation, and controllership principles are interpreted in legal and academic discourse.

The socio-legal component complements this analysis by considering the operational and technical context in which custodial and non-custodial wallet providers function.[116] Technical documentation, industry standards, white papers, and compliance frameworks are examined in order to situate legal obligations within the practical realities of blockchain-based systems. This combined methodological approach ensures t that the research addresses both the normative structure of EU data protection law and the technological constraints that shape the practical implementation of compliance measures.

[115] McConville, M. Chui, W., H., ed., (2017). *Research methods for law*. Edinburgh University Press. Second Edition, pp. 1–18. Available at: https://edinburghuniversitypress.com/pub/media/resources/9781474404259_Research_Methods_for_Law_-_Introduction_and_Overview.pdf, (Accessed: 26 July 2025).

[116] Schiff, D.N., 1976. Socio-legal theory: Social structure and law. The Modern Law Review, 39(3), pp.287–310. Available at: https://onlinelibrary.wiley.com/doi/10.1111/j.1468-2230.1976.tb01458.x, (Accessed: 26 July 2025).

In this dissertation, the term socio-legal is used in a law-and-technology sense rather than in the empirical sociological sense commonly associated with interviews, surveys, or behavioural observation of institutional actors. The socio-legal dimension refers instead to the analysis of how legal norms operate within concrete technological environments and institutional settings. The study examines how blockchain architectures, wallet infrastructures, and industry practices shape the practical conditions under which GDPR obligations can be implemented. In this respect, the research adopts an institutional and functional perspective, focusing on how technical design choices influence the allocation of responsibility, the feasibility of compliance, and the effective protection of fundamental rights.

The dissertation employs both normative and descriptive approaches:

- The descriptive approach[117] is used to map the legal and technical foundations of blockchain wallet ecosystems, describing how data is stored, processed, and replicated across systems.
- The normative approach[118] is applied to interpret the GDPR and related legal frameworks in the context of immutable ledgers, proposing pathways for "effective forgetting" and functional controllership allocation.
- A case-based lens is applied throughout, using real-world examples such as custodial wallets (e.g., Coinbase Wallet) and non-custodial solutions (e.g., MetaMask, Ledger) to ground the theoretical analysis in practical realities.

This combination of doctrinal legal research and socio-legal analysis enables the dissertation to develop a structured compliance rubric for "effective forgetting" tailored to wallet providers, build a functional controllership allocation model that clarifies accountability for both custodial and non-custodial wallets, and provide practical guidance for regulators and

[117] Van Hoecke, M. (ed.) (2011). Meth*odologies of legal research: Which kind of method for what kind of discipline?* Oxford: Hart Publishing, p. 8. Available at: https://www.academia.edu/70512862/Methodologies_of_legal_research_which_kind_of_method_for_what_kind_of_discipline, (Accessed: 26 July 2025); see also, Hutchinson, T., (2006). *Researching and writing in law*. Thomas Lawbook Co., ABN 64 058 914 668, p. 150.
[118] Van Hoecke, Methodologies of legal research, pp. 10–11.

industry actors on reconciling the immutable design of blockchain systems with the flexible but rigorous requirements of the GDPR.

The dissertation therefore proceeds in four analytical stages: doctrinal interpretation of Article 17 GDPR, examination of controllership structures in decentralised environments, development of operational compliance mechanisms, and assessment of the broader regulatory implications of effective forgetting for EU digital governance.

1.2.4 Novelty and Original Contribution

This dissertation makes three original contributions to European data protection scholarship in decentralised data environments.

First, the novelty of this research lies in its integration of legal, technical, and policy perspectives to conceptualize and operationalize the Right to be Forgotten within blockchain ecosystems. Rather than restating the well-known conflict between immutability and erasure, this dissertation develops a structured compliance rubric for effective forgetting tailored specifically to wallet providers. Existing scholarship has primarily focused on identifying incompatibilities between blockchain immutability and GDPR erasure, but has provided limited operational guidance on how compliance could be structured in practice. By mapping technical and governance controls, such as off-chain data deletion, address delinking,[119] and encryption strategies,[120] to GDPR standards, we provide a decision framework that helps custodial and non-custodial wallet providers identify proportionate RTBF measures. This practical, architecture-sensitive approach transforms a theoretical concept into actionable guidance for industry actors and regulators.

Second, by systematically analyzing custodial and non-custodial wallet architectures, this research introduces a nuanced framework for functional controllership allocation, mapping distributed decision-making to existing legal standards of accountability. Moreover, it draws on CJEU jurisprudence, including Google Spain, Google v CNIL, and

[119] Address delinking refers to the practice of reducing or removing the link between a blockchain address and a specific natural person by using techniques such as address rotation, hierarchical deterministic wallets, or off-chain identifiers. This reduces identifiability and supports pseudonymisation under GDPR (Recital 28). The practical implications of this approach for wallet providers will be explored in detail in Chapter 2.

[120] Encryption strategies use strong cryptography to make personal data on the blockchain unreadable without the right keys. While they don't remove the data, they help make it practically inaccessible, supporting the idea of "effective forgetting" under Article 17 GDPR. The practical use of these methods for wallet providers will be discussed in Chapter 3.

Wirtschaftsakademie,[121] to test how established doctrines can be adapted to decentralized systems, thus filling a critical gap in comparative and applied data protection scholarship.

Third, by combining privacy-enhancing technologies to protect confidentiality while facilitating compliance,[122] smart contractual governance mechanisms that codify consent and accountability,[123] regulatory sandboxes that provide operationally viable testing environments under supervision,[124] and selective de-anonymization frameworks that strike a balance between privacy and law enforcement requirements in a distributed, multi-party model, this dissertation further offers novel insights into the design of hybrid compliance models for blockchain wallets.[125] By situating these analyses within the broader normative framework of informational self-determination and the EU's constitutional commitment to fundamental rights, the study not only advances academic understanding but also offers practical guidance for regulators, developers, and policymakers navigating the tension between innovation and legal compliance.

1.3 Structure of the Dissertation

The dissertation opens with an Introduction that sets out the background, objectives, research questions, methodology, and scope.

In Chapter 2, the analysis traces the evolution of European data protection from the OECD Guidelines and Convention 108 through Directive 95/46/EC to the GDPR. It places the GDPR in the context of the EU's basic rights framework and describes the functions of the Article 29 Working Party and its successor, the EDPB. Along with significant CJEU decisions like Google Spain, Digital Rights Ireland, Schrems I/II, and Ligue des droits humains, which together influence the current legal system, the Snowden revelations are analyzed as a catalyst. The discussion then turns to defining "personal data" in practice, contrasting EU and

[121] Wirtschaftsakademie Schleswig-Holstein, Case C-210/16, para, 29.
[122] Joseph, S., (2024). *Balancing data privacy and compliance in blockchain-based financial systems*. Journal of Engineering Research and Reports, 26(9), pp.170–184.
Available at: https://journaljerr.com/index.php/JERR/article/view/1271/2577, (Accessed: 26 July 2025).
[123] Neisse, R., Steri, G. and Nai-Fovino, I., (2017). *A blockchain-based approach for data accountability and provenance tracking*. In Proceedings of the 12th international conference on availability, reliability and security, pp. 1–8. Available at: https://arxiv.org/pdf/1706.04507, (Accessed: 26 July 2025).
[124] Coinmetro, (2025). *Regulatory Sandboxes: Fostering Crypto Innovation Within Legal Frameworks*. Available at: https://www.coinmetro.com/learning-lab/regulatory-sandboxes, (Accessed: 26 July 2025).
[125] Sahu, N., Gajera, M., Chaudhary, A. and Ivey-Law, H., (2023). S*eDe: Balancing Blockchain Privacy and Regulatory Compliance by Selective De-Anonymization*. arXiv preprint arXiv:2311.08167, pp.1–12. Available at: https://arxiv.org/pdf/2311.08167, (Accessed: 26 July 2025).

non-EU approaches, and mapping the main legal actors: data subjects, controllers, processors, joint controllers, supervisory authorities, and the EDPB.

The Right to Be Forgotten (RTBF) in law and technology is the main topic of Chapter 3. After a thorough discussion of Article 17 GDPR and its grounds for deletion, the doctrinal foundation of the RTBF is constructed as a development of Article 8 safeguards. Key case law, including Google Spain, Google v CNIL, GC and Others, and TU & RE v Google, illustrates how "effective forgetting" functions through limiting accessibility rather than deleting lawful content. The discussion incorporates alternative perspectives from scholarship, such as Koops' emphasis on retrievability and reuse, and considers the implications of these insights for blockchain ecosystems.

The topic of blockchain principles and the function of wallet providers is covered in Chapter 4. Custodial and non-custodial wallets are distinguished, and fundamental blockchain designs and data flows are described. The analysis maps how personal data are processed on-chain and off-chain, highlights the functions of block explorers and analytics vendors, and identifies the points at which issues of identifiability, pseudonymisation, and profiling arise.

Chapter 5 constitutes the central analytical contribution of the dissertation by developing the concept of effective forgetting as a functional interpretation of Article 17 GDPR in decentralised environments. Building on the doctrinal and technical analysis developed in the previous chapters, the chapter proposes a structured compliance framework tailored to custodial and non-custodial wallet providers. The framework demonstrates how erasure obligations may be operationalised through measures such as off-chain deletion, delinking of identifiers, interface-level suppression, metadata minimisation, and privacy-preserving architectural design. The chapter further examines the governance implications of distributed data processing and evaluates how responsibilities may be allocated among wallet providers and related infrastructure actors in order to maintain the effectiveness of data subject rights within immutable ledger environments.

Chapter 6 presents the conclusion of the dissertation. It synthesises the doctrinal and technical findings of the research and argues that Article 17 GDPR can remain normatively effective in decentralised technological systems when interpreted through the concept of effective forgetting. The conclusion emphasises that blockchain architectures do not render data protection law inapplicable, but rather require context-sensitive interpretation aligned with

technological realities. It also highlights the broader implications of the research for the future development of EU data protection law, decentralised governance, and privacy-preserving system design.

Chapter 2. Building the GDPR: Foundations for Data Protection in Blockchain Environments

While this chapter examines the historical and doctrinal development of the GDPR, its purpose within this dissertation is to establish the legal foundations necessary to assess data protection challenges arising in blockchain-based systems.

2.1 Foundations of European Data Protection

The Organisation for Economic Co-operation and Development (OECD) established a set of recommendations in 1980 on the transmission of personal data across borders and the protection of privacy.[126] These guidelines identified disparities in national data protection regulations as barriers to cross-border data flows and, consequently, as impediments to economic growth.[127] To balance the benefits of data use with the need for privacy protection, the recommendations emphasised risk assessment, the implementation of security measures, and the promotion of interoperability between privacy frameworks. They also encouraged countries to simplify cross-border cooperation in privacy law enforcement.[128]

2.1.1 European Treaties and Directives

In line with the OECD's recommendations, the Council of Europe adopted the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108),[129] an international treaty establishing binding standards for data protection. Building on this foundation, the European Commission adopted Directive 95/46/EC in 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data,[130] aiming to address the disparities among Member States' data

[126] OECD (1980, amended 2013). Re*commendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*. OECD Legal Instruments, OECD/LEGAL/0188. Available at: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188, (Accessed: 26 July 2025).
[127] OECD, 1980, amended 2013, Preamble.
[128] *Ibid*, Articles 15, 20–23.
[129] Council of Europe (COE), (1981). *Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data*, ETS 108.
Available at: https://www.refworld.org/legal/agreements/coe/1981/en/31908, (Accessed: 26 July 2025).
[130] European Parliament and Council, (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the

protection laws.[131] The independent advisory board Article 29 Working Party was established under the Data Protection Directive.[132] Under this Directive, the independent advisory body known as the Article 29 Working Party was established, tasked with examining issues related to the Directive's national implementation and providing expert guidance and opinions on data protection matters across the EU.[133]

The EU and the Council of Europe have adopted legal instruments safeguarding both rights to privacy and data protection of personal data. Article 8 of the European Convention on Human Rights (ECHR), an international treaty of the Council of Europe, guarantees the right to respect private and family life.[134] Similarly, Article 16 of the Treaty on the Functioning of the European Union (TFEU) ensures the protection of personal data.[135] Furthermore, the Charter of Fundamental Rights of the European Union (EU Charter) recognises the rights to privacy and data protection as distinct rights under Articles 7 and 8, setting more detailed rules for the processing of personal data and the transparency required for such processing.[136] Unlike the TFEU, the Charter set more detailed guidelines for the processing of personal data and the necessary levels of transparency.[137]

The Data Protection Directive (European Parliament and Council, 1995) did not apply directly in the Member States but required transposition into national law. As a result, Member States' implementation and interpretation differed greatly, creating a fragmented regulatory environment throughout the EU.[138] The Directive's main goal of harmonising data protection rules inside the internal market may be undermined as a result, since some data

---

free movement of such data (Data Protection Directive). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri46, (Accessed: 26 July 2025).

[131] Voigt, P. and Von dem Bussche, A., (2017). The EU General Data Protection Regulation (GDPR). A practical guide, 1st ed., Cham: Springer International Publishing, 10(3152676), p. 2. Available at: https://link.springer.com/book/10.1007/978-3-031-62328-8, (Accessed: 26 July 2025).

[132] Recital 65 and Article 29 of the Data Protection Directive.

[133] Data Protection Directive, Article 29.

[134] Council of Europe, (1950). *European Convention for the Protection of Human Rights and Fundamental Freedoms*. ETS 5, 4, Article 8. Available at: https://www.refworld.org/legal/agreements/coe/1950/en/18688, (Accessed: 26 July 2025).

[135] Conference of the Representatives of the Governments of the Member States, (2007). *Consolidated version of the Treaty on the Functioning of the European Union*. 2008/C 115/01, Article 16. Available at: https://www.refworld.org/legal/agreements/eu/2007/en/97880, (Accessed: 26 July 2025).

[136] European Union, (2007). Charter of Fundamental Rights of the European Union, C 303/1, Articles 8, 9. Available at: https://www.refworld.org/legal/agreements/eu/2007/en/19131, (Accessed: 26 July 2025).

[137] EU Charter, Article 8.

[138] Kuner, C., (2007). *European data protection law: corporate compliance and regulation*. Oxford University Press, ISBN 978-0-19-928385-9, pp. 50–57.

processing operations may be lawful in one jurisdiction while breaching the law in another.[139] The General Data Protection Regulation (GDPR), which sought to establish a directly applicable, uniform framework more suited to the shortcomings,[140] of contemporary data-driven economy, replaced the Directive in 2016 after it was found to have these flaws.

The GDPR, in contrast to the Data Protection Directive, is directly applicable in every EU member state, removing the requirement for national transposition and guaranteeing a consistent legal framework throughout the Union.[141] With its adoption, the former Article 29 Working Party was replaced by the European Data Protection Board (EDPB), tasked with ensuring consistent interpretation and application of the Regulation.[142]

The GDPR's primary objectives are to protect natural persons' rights, privacy, and freedoms while also lowering obstacles to the free flow of personal data across the internal market, which will facilitate company business operations throughout Member States.[143] Under this framework, individuals are granted a range of enforceable rights, while data controllers and processors are bound by strict obligations to ensure lawful, transparent, and secure data processing.[144]

2.1.2 Beyond Human Rights: GDPR as Internal Market Instrument

Most scholarship on the GDPR begins from the premise that we are dealing with a human rights instrument. There are good reasons for this. The Regulation explicitly grounds itself in Articles 7 and 8 of the Charter of Fundamental Rights, its recitals emphasise the protection of natural persons, and the Court of Justice has consistently characterised data protection as a fundamental right deserving of high-level protection.[145] But there is a problem with stopping the analysis there. The EU is not the Council of Europe. Its constitutional order was not built primarily to constrain state power in relation to individuals, it was built to create a common market.[146] Data protection law in the EU has always existed within that larger project, and

[139] Bygrave, L.A., (2014). *Data privacy law: an international perspective*. Oxford University Press, ISBN 978–0–19–967555–5, pp. 190–195.
[140] Voigt and Von dem Bussche, 2017, p. 2.
[141] Voigt and Von dem Bussche, 2017, page 2.
[142] GDPR, Article 68; Voigt and Von dem Bussche, 2017, page 197.
[143] IT Governance Privacy Team, (2020). *EU General Data Protection Regulation: An Implementation and Compliance Guide*. Fourth Edition, IT Governance Publishing, (IT Privacy Team), page 13.
[144] *Ibid*, page 16.
[145] Lynskey, 2015, pp. 8–9.
[146] Craig, P. and de Búrca, G., (2020). *EU Law: Text, Cases, and Materials.* 7th edn. Oxford: Oxford University Press, ch 3 ('The Development of European Integration'), pp. 302–314.

this institutional context has consequences that scholarship focused solely on rights protection tends to overlook.

Article 16 TFEU provides the legal basis for EU data protection legislation. What is striking about this provision is that it explicitly links two objectives: protecting individuals with regard to the processing of personal data, and ensuring the free movement of such data within the Union.[147] The drafters could have separated these into distinct legal bases; one for rights protection, another for market regulation. The legislative history suggests this was deliberate.[148] Member States had developed widely divergent approaches to data protection through the 1970s and 1980s, and by the time serious work began on what would become the 1995 Data Protection Directive, it had become clear that these differences were creating friction for businesses attempting to operate across borders.[149] Some Member States had strict rules, others had virtually none. Companies faced uncertainty about which rules applied when data moved between jurisdictions, and this uncertainty was seen as an obstacle to the development of cross-border services.

The GDPR inherited this dual character from the Directive, but if anything it intensifies the market dimension. Recital 13 is explicit about this. It states that differences in the level of protection of the rights and freedoms of natural persons in relation to the processing of personal data in the Member States may prevent the free movement of data throughout the Union, and that such differences 'may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law.'[150] This is not incidental language tucked away in the preamble. It articulates one of the core justifications for harmonisation at EU level. The problem being addressed is not just that some Member States protect rights inadequately, it is that variation as such creates market distortions.

Translated into regulatory design, the GDPR grants data subjects enforceable rights grounded in Articles 7 and 8 of the Charter of Fundamental Rights; rights to protection of personal data and privacy that carry the force of primary EU law.[151] Its direct applicability across all

[147] TFEU, Article 16; GDPR, Recitals 1,9 and 13.
[148] Lynskey, 2015, ch 2–3.
[149] Craig et al., 2020, pp. 302–314.
[150] GDPR, Recital 13.
[151] EU Charter, Articles 7, 8.

Member States, the central coordinating role of the European Data Protection Board, and the one-stop-shop principle for supervisory jurisdiction all serve to eliminate the regulatory arbitrage opportunities that would otherwise emerge from fragmented[152] national regimes.[153] These are not incidental features but rather deliberate instruments designed to enable data-driven business models that depend on processing at scale across territorial boundaries.

The increasing interaction between data governance and financial regulation further illustrates the EU's technologically adaptive regulatory approach. Directive 2014/65/EU (MiFID II), together with subsequent developments in distributed ledger technology regulation (DLT), reflects the Union's recognition that emerging digital infrastructures, including blockchain-based financial services, must be accommodated within existing internal market frameworks.[154] These developments demonstrate that EU law increasingly adopts technologically neutral regulatory approaches capable of integrating innovative data architectures while maintaining regulatory coherence and legal certainty.[155]

This economic aspect is made clear in the Commission's policy discourse. The Commission presented data as an essential component for innovation, economy growth, and competitive advantage in global markets in its 2017 Communication Building a European Data Economy.[156] The framing is instructive: data privacy laws are described as enabling circumstances for long-term engagement in digital marketplaces rather than as restrictions on economic activity. The reasoning behind the argument is founded on trust: without strong data protection guarantees, people won't use digital services, which will limit the growth of data-driven industries. Whether this causal claim accurately describes user behaviour remains

[152] By "fragmented national regimes", we refer to the legal, institutional, and enforcement divergences that arose under Directive 95/46/EC as a consequence of national transposition, producing obstacles to cross-border data flows and uneven regulatory burdens within the internal market, see CJEU, Judgment of 6 November 2003, Bodil Lindqvist, C-101/01, EU:C:2003:596, para 41. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62001CJ0101, (Accessed: 10 January 2026).
[153] TFEU, Article 288; GDPR, Recital 10.
[154] European Parliament and of the Council, (2014). *Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014, on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (recast) Text with EEA relevance, L 173/349*. Available at: https://eur-lex.europa.eu/eli/dir/2014/65/oj/eng, (Accessed: 10 January 2026).
[155] Walch, A., (2016). *The path of the blockchain lexicon (and the law)*. Review of Banking & Financial Law, 36, pp. 735–736, 745–746. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2940335, (Accessed: 10 January 2026); see also, EU Blockchain Observatory and Forum, 2018, pp. 4, 6–8, 28–30.
[156] European Commission, (2017). *Building a European Data Economy (Communication) COM*. pp. 2–3. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0009, (Accessed: 10 January 2026).

contested in the empirical literature, but its prevalence in policy documents reveals how market-building considerations shape institutional understandings of the GDPR's purpose.

The GDPR's dual nature is important because the difficulties presented by blockchain technology and other decentralised systems cannot be adequately evaluated using a purely normative lens that merely enquires as to whether specific rights are upheld in theory.[157] Blockchain wallet providers, like other market participants, operate within competitive environments structured by incentives toward scalability, cost efficiency, and cross-border reach. The economic and technical constraints they face are not external to legal analysis but rather constitute part of the regulatory context in which compliance obligations must function.[158] This becomes particularly salient for requirements such as the right to erasure or the broader obligation to enable "effective forgetting"; provisions whose feasibility depends not only on normative commitments but on how those commitments interact with the material properties of distributed ledger architectures in competitive market settings within the internal market framework.[159]

The analytical task, then, requires holding both dimensions in view simultaneously: acknowledging the GDPR as an instrument of fundamental rights protection while also recognising how its operation within the internal market project structures the practical meaning of those protections.[160] This is not to suggest that economic considerations should override rights commitments, but rather to insist that effective legal analysis must account for how these objectives interact, and occasionally tension, in specific technological contexts.[161] For blockchain-based services, this dual framework proves particularly revealing, as it exposes gaps between the Regulation's formal requirements and the structural realities of decentralised systems operating in cross-border digital markets.

Institutional engagement with these challenges is reflected in the work of the EU Blockchain Observatory and Forum, established by the European Commission to analyse legal,

[157] CJEU, (2014). *Joined Cases C-293 & C-594/12, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others, and Kärntner Landesregierung and Others*. ECLI:EU:C:2014:238, paras 38–40. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0293, (Accessed: 26 July 2025). see also, Lynskey, 2015, ch 3.
[158] Finck, 2019, pp. 8–14.
[159] EU Blockchain Observatory and Forum, 2018, pp. 24–31.
[160] GDPR, Recitals 1, 9, 13; Lynskey, 2015, ch 3.
[161] Digital Rights Ireland, C-293/12 and C-594/12, paras 38–40; Schrems II, C-311/18, paras 96–98.

regulatory, and technological developments associated with distributed ledger technologies. The Observatory emphasises the need for governance models capable of balancing innovation with fundamental rights protection, particularly in areas such as data protection, interoperability, and cross-border regulatory coordination.[162]

2.1.3 The Snowden catalyst

The 2013 Edward Snowden disclosures revealed widespread surveillance activities by the National Security Agency (NSA) of the United States. These revelations showed that the NSA had access to information from millions of private individuals, including data from significant US internet technology companies like Apple, Google, and Facebook.[163] One of the first publicly acknowledged surveillance programmes, PRISM, granted the NSA direct access to communications and internet traffic handled by these corporations, including data belonging to millions of European users.[164] The revelations further showed that vast amounts of communication data were incidentally captured through transatlantic fibre-optic cables linking the US and Europe. Through its TEMPORA programme, the UK's Government Communications Headquarters (GCHQ) was also able to intercept and store a significant share of global internet traffic transmitted via these cables.[165] The Snowden revelations did more than spark outrage; they reshaped Europe's approach to data protection, exposing the fragility of existing safeguards. This heightened scrutiny paved the way for landmark CJEU rulings that strengthened individual rights and redefined the balance between privacy, innovation, and cross-border data flows.

2.1.4 Landmark CJEU Rulings

Over time, a series of significant rulings by the Court of Justice of the European Union reshaped both the legal landscape and the European Union's perception of citizens' rights to online privacy. In Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González (commonly referred to as the "right to be forgotten" case), the plaintiff, Mario Costeja González, requested that Google be barred from displaying a link

---

[162] Lyons, T., Courcelas, L. and Timsit, K., (2019). *Legal and regulatory framework of blockchains and smart contracts.* In The European Union Blockchain Observatory and Forum. Available at: https://blockchain-observatory.ec.europa.eu/publications/legal-and-regulatory-framework-blockchains-and-smart-contracts_en, (Accessed: 26 March 2026).

[163] Macaskill, E., Dance, G., (2013). *NSA Files: Decoded, What the revelations mean for you*. theguardian. Available at: https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded - section/1, (Accessed: 26 July 2025).

[164] Gellman, B., Poitras, L., (2013). *U.S., British Intelligence mining data from nine U.S. Internet companies in broad secret program*. The Washington Post. Available at: https://www.washingtonpost.com/investigations/2013, (Accessed: 26 July 2025).

[165] Shubber, K., (2013). *A simple guide to GCHQ's internet surveillance programme Tempora*. WIRED. Available at: https://www.wired.co.uk/article/gchq-tempora-101, (Accessed: 26 July 2025).

to a 1998 newspaper article detailing his past financial difficulties, which had long been resolved.[166] The CJEU held that individuals have the right to request the removal of links to personal information from search engine results where the information is "inadequate, irrelevant or no longer relevant,"[167] and further determined that Google acts as a "data controller" in this context.[168] The "right to be forgotten," which gives people the ability to ask for links to websites holding their personal data to be removed, was established as a result of this ruling.[169] The case affected the global availability and flow of information online, with major ramifications for search engines and Internet intermediaries, however it doesn't entail total "forgetting," since more targeted searches may still display results with links to the content.[170]

In 2014, in Digital Rights Ireland,[171] the Court of Justice of the European Union (CJEU) invalidated Directive 2006/24/EC on data retention.[172] The Directive, adopted in response to the terrorist attacks in Madrid and London,[173] required the retention of communications data[174] for law enforcement and investigative purposes, aiming to harmonise Member States' laws.[175] The CJEU held that the Directive failed to meet the principle of proportionality, as it excessively interfered with fundamental rights and lacked clear safeguards regarding data access, retention periods, and oversight mechanisms.[176] This landmark ruling underscored the

[166] Google Spain, Case C-131/12, para 14.
[167] Google Spain, Case C-131/12, paras 92–97.
[168] Google Spain, Case C-131/12, paras 33–34.
[169] Google Spain, Case C-131/12, para 85.
[170] Hoffman, D., Bruening, P., Carter, S., (2016). *The Right to Obscurity: How We Can Implement the Google Spain Decision*. 17 N.C. J.L. & Tech. 437, pp. 457–459. Available at: https://scholarship.law.unc.edu/ncjolt/vol17/iss3/2, (Accessed: 26 July 2025).
[171] Digital Rights Ireland, C-293/12 and C-594/12, paras 65–71.
[172] European Parliament and Council, (2006). *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC*. OJ L 105/54. Available at: https://eur-lex.europa.eu/eli/dir/2006/24/oj, (Accessed: 26 July 2025).
[173] Turégano-Fuentes, F., Caba-Doussoux, P., Jover-Navalón, J.M., Martín-Pérez, E., Fernández-Luengas, D., Díez-Valladares, L., Pérez-Díaz, D., Yuste-García, P., Guadalajara Labajo, H., Ríos-Blanco, R. and Hernando-Trancho, F., (2008). I*njury patterns from major urban terrorist bombings in trains: the Madrid experience.* World journal of surgery, 32(6), pp.1168–1175, Available at: DOI 10.1007/s00268-008-9557-1, (Accessed: 26 July 2025).
[174] Communication data refers to information generated, transmitted, or exchanged during the process of electronic communications, including metadata such as sender and recipient details, time stamps, routing information, and technical identifiers. It generally excludes the content of the communication itself but may reveal patterns of interaction and relationships between parties. Available at: Law Insider, https://www.lawinsider.com/dictionary/communication-data, (Accessed: 26 July 2025).
[175] Data Retention Directive, Recital 10.
[176] Digital Rights Ireland, C-293/12 and C-594/12, paras 64–66.

privacy risks inherent in large-scale data collection,[177] and highlighted the ongoing difficulty of balancing national security objectives with the protection of personal data.

In the Schrems I Decision, Austrian national Maximillian Schrems challenged the Irish Data Protection Commissioner's refusal to investigate Facebook's transfer of personal data to the United States.[178] In light of the revelations regarding the NSA's extensive surveillance practices, Schrems argued that his personal data, even under the EU–US "Safe Harbour" framework,[179] lacked adequate protection.[180] The Court of Justice of the European Union (CJEU) found that US law permitted the indiscriminate collection and storage of personal data, with the Safe Harbour principles applying only to US corporations and not to public authorities. This framework, therefore, allowed national security and law enforcement priorities to override data protection guarantees.[181] The CJEU concluded that the Safe Harbour agreement lacked the safeguards, legal remedies, and proportionality required under EU law, and thus failed to ensure an "adequate level of protection" equivalent to that afforded within the Union. Consequently, the Court invalidated the Safe Harbour framework as incompatible with the fundamental rights enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.[182]

In the Schrems II Decision,[183] delivered on 16 July 2020, the Court of Justice of the European Union (CJEU) issued a preliminary ruling that invalidated the European Commission's Decision (EU) 2016/1250, which had established the EU–U.S. Privacy Shield framework.[184] The case arose from a complaint by Austrian lawyer Maximilian Schrems, who argued before

[177] Digital Rights Ireland, C-293/12 and C-594/12, para 27.
[178] CJEU, (2015). *Judgment of the Court (Grand Chamber) of 6 October 2015, Maximillian Schrems v Data Protection Commissioner*. Case C-362/14, ECLI:EU:C:2015:650. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362, (Accessed: 26 July 2025).
[179] European Commission, Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbor Privacy Principles and related frequently asked questions issued by the US Department of Commerce, OJ L 215, 25.8.2000, p. 7–47. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT, (Accessed: 26 July 2025).
[180] Schrems I, Case C-362/14, paras 27–29.
[181] Schrems I, Case C-362/14, paras 94–98.
[182] Schrems I, Case C-362/14, paras 98–106, 94.
[183] CJEU, (2020). *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems.* (Case C-311/18), ECLI:EU:C:2020:559. Available at: https://curia.europa.eu/juris/document/document, (Accessed: 26 July 2025).
[184] The Decision allowed the free flow of data to organizations recognized in the US under the Privacy Shield; Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176) (Text with EEA relevance), (the EU-U.S. Privacy Shield Decision), Document 32016D1250, L 207/1, 2016. Available at: https://eur-lex.europa.eu/legal-content/EN, (Accessed: 26 July 2025).

the Irish Data Protection Commissioner that Facebook Ireland's reliance on Standard Contractual Clauses (SCCs)[185] for data transfers to its U.S. headquarters failed to provide adequate protection of personal data, given the possibility of access by U.S. intelligence authorities during both the transmission and storage of that data.[186] Importantly, the CJEU found that the Privacy Shield framework failed to ensure an equivalent level of protection for EU residents' personal data, particularly in light of disproportionate U.S. surveillance practices and the absence of effective judicial redress mechanisms.[187] Consequently, the Privacy Shield was declared invalid for breaching the principles of proportionality and judicial protection under Articles 7, 8, and 47 of the Charter of Fundamental Rights of the European Union.[188]

The case Ligue des droits humains v Conseil des ministres[189] concerned the incorporation of the Passenger Name Record Directive (PNR Directive) into domestic law.[190] The PNR Directive mandates the systematic processing of large volumes of passenger name record (PNR) data for extra-EU flights,[191] with optional extension to intra-EU flights under Article 2, to prevent terrorist offences and serious crime.[192] Following Belgium's transposition of the directive, the Ligue des droits humains (LDH) sought annulment of the national law,[193] alleging infringements of the rights to privacy and data protection under Belgian and EU law.[194] The Court of Justice of the European Union (CJEU) found that the directive entailed significant interferences with Articles 7 and 8 of the EU Charter of Fundamental Rights, describing it as establishing "a surveillance regime that is continuous, untargeted and systematic, including the automated assessment of the personal data of everyone using air

[185] Contractual provisions guaranteeing adequate data protection measures may be used to justify data transfers from the EU to third countries in accordance with the General Data Protection Regulation. See at: Pilishvili, M, (2024). *How Schrems II Judgment Affected the Personal Data Flow between the European Union and Third Countries*. Public Goods Journal, DOI 10.21868/PGnG.2025.1.2., p. 3. Available at: https://publicgoodsjournal.eu/wp-content/uploads/2025/06/PGG_2025-1_MariamPilishvili.pdf, (Accessed: 26 July 2025).
[186] Schrems II, C-311/18, para 52.
[187] Schrems II, C-311/18, paras 168–185.
[188] Schrems II, C-311/18, paras 196–199.
[189] Judgement of the European Court of Justice (Grand Chamber), (2022). Li*gue des droits humains v Conseil des ministers*, (Case C-817/19, ECLI:EU:C:2022:63.
Available at: https://curia.europa.eu/juris/document/document.jsf, (Accessed: 26 July 2025).
[190] European Union, (2016). *Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (PNR Directive)*. Official Journal of the European Union, L 119/132, 4 May. Available at: https://eur-lex.europa.eu/eli/dir/2016/681/oj, (Accessed: 26 July 2025).
[191] PNR Directive, Article 1(1)(a).
[192] PNR Directive, Article 2(1).
[193] Ligue des droits humains, Case C-817/19, paras 51–52.
[194] Ligue des droits humains, Case C-817/19, paras 53–54.

transport services."[195] However, the Court recognised that these rights are not absolute[196] and that the directive's objective of combating terrorism and ensuring national security could justify such intrusions, provided that adequate safeguards and proportionality are observed.[197]

The discussed rulings illustrate the Court of Justice's consistent effort to balance the protection of personal data against competing interests through a functional and proportionality-based approach. This interpretive stance prompts concrete questions as to how the GDPR concepts of erasure, identifiability, and controllership should be applied in emerging technological contexts, including blockchain systems, where data persistence, decentralised structures, and distributed governance challenge assumptions of data alterability and centralised control.

2.2 Personal Data as the New Oil

In 1963, during the height of the Space Race, President John F. Kennedy declared that even though technology had advanced significantly, "man is still the most extraordinary computer of all."[198] Little did he know that, decades later, it would not be man but his data that would become the most valuable resource of all, the "new oil" of the digital age. These days, every click, movement, and interaction powers enormous digital ecosystems, turning personal data into a catalyst for economic growth and innovation. However, this enormous value carries risks and obligations, just like with oil. To fully utilise personal data, ethical, inclusive, and publicly accountable governance is required in addition to technical governance.

2.2.1 Defining Personal Data in a Networked Society

At the outset of this research, it is essential to clarify what constitutes an individual's personal data, why safeguarding its confidentiality is of critical importance, and the reasons and mechanisms through which states seek to protect their citizens' personal information. It is equally important to examine the significance of ensuring the security of personal data and how different countries have progressively developed frameworks to address this need.

[195] Ligue des droits humains, Case C-817/19, paras 110–111.
[196] Ligue des droits humains, Case C-817/19, paras 113–115.
[197] Ligue des droits humains, Case C-817/19, paras 121–122.
[198] Kennedy, J. F. (1963). *Man is still the most extraordinary computer of all*. In John F. Kennedy Quotes. Today in Science. Available at: https://todayinsci.com/K/Kennedy_John/KennedyJohn-Quotations.htm, (Accessed: 15 January 2025).

The notion of personal data serves not only as a definitional threshold for the application of the GDPR but also as a source of significant legal and theoretical complexity. Article 4(1) GDPR defines personal data as.

> '…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…'[199]

However, this seemingly simple term hides a number of interpretive difficulties, especially when used in relation to contemporary digital infrastructures, metadata, and networked information systems. These definitions, however, closely resemble those found in the 1995 Directive, where Article 2(a) stressed that consideration should be given to the means likely to be used to identify an individual and defined personal data as related to a "identifiable natural person."[200]

The breadth of the term "relating to" has been consistently interpreted expansively by EU institutions. The Article 29 Working Party, in its seminal Opinion 4/2007, proposed a tripartite test to determine when data "relates to" an individual:

i. where the content is about the individual,
ii. when the purpose of the data processing is to evaluate or treat the person in a certain way, or
iii. when the result of the processing has an impact on the rights or interests of the individual.[201]

This relational reading moves beyond formal identifiability and introduces a substantive dimension that draws the boundaries of personal data not only based on reference, but also function and effect.

[199] GDPR, Article 4(1).
[200] Data Protection Directive, Article 2(a).
[201] WP 136, Opinion 4/2007, page 6.

A second axis of analysis focusses on identifiability. Given that identifiability can be either direct or indirect, the GDPR requires an assessment of "all the means reasonably likely to be used" to identify the individual.[202] This idea requires a contextual and relative evaluation, moving away from both a rigid data taxonomy and an absolute anonymity requirement. In Breyer v. Germany, the CJEU adopted similar reasoning, holding that dynamic IP addresses could be regarded as personal data when third parties, such as internet service providers, have the legal and practical capacity to re-identify the data subject.[203] The Court's approach shows a practical understanding: identifiability is determined by whether the controller currently possesses the information needed for identification, not by whether it is practically possible within the existing legal and technological framework.[204]

A functional and risk-oriented understanding of personal data is the end outcome. Bygrave points out that rather than having a rigid, ontological definition, EU data protection law employs a regulatory lens in which the idea of personal data serves as a catalyst for protective obligations.[205] This strategy makes it possible for the legal system to continue being flexible in the face of swift advancements in technology. As a result, depending on the actual chance of identification and the risks to the subject, the same piece of information may be considered personal data in one situation but not in another.

The explicit inclusion of "online identifiers," such as IP addresses, cookie identifiers, or device IDs, as personal data is a significant improvement of the GDPR since they may identify individuals even in the absence of traditional identifiers. Recital 30 further clarifies that these identifiers, when combined with other information, can lead to the identification of a natural person.[206] This marks a clear departure from the 1995 Data Protection Directive's narrower focus on identifiers like names and registration numbers, as it acknowledges that modern technologies and pervasive tracking mechanisms, e.g., cookies and IP logging, can suffice to re-identify individuals.[207] By broadening the concept of what constitutes personal

[202] GDPR, Recital 26.
[203] Breyer v Bundesrepublik Deutschland, C-582/14, paras 49–52.
[204] Breyer v Bundesrepublik Deutschland, C-582/14, para 49.
[205] Bygrave, 2014, pp. 62–64.
[206] GDPR, Recital 30.
[207] Papadogiannakis, E., Kourtellis, N., Papadopoulos, P., & Markatos, E. P. (2021). *User tracking in the post-cookie era: How websites bypass GDPR consent to track users*. In Proceedings of the Web Conference 2021, pp. 2130–2141). Available at: https://doi.org/10.1145/3442381.3450056, (Accessed: 26 July 2025);

data, the GDPR strengthens the protections afforded to data subjects, extending enforceable rights over a wider array of digital identifiers.

2.2.2 EU vs. Global Approaches

It is also crucial to acknowledge that the EU approach differs greatly from more restrictive definitions used in other countries, like the US, where clear identifiers typically prioritised over inferred or indirect identifiability.[208] By contrast, as stated in Article 8 of the Charter of basic Rights of the European Union (CFREU), the EU framework represents a constitutional commitment to privacy as a basic right.[209] Under this approach, interpretive focus shifts from what the data is to what the data does, its connection to an individual's private life, autonomy, and exposure to risk. The interpretive emphasis is thus placed not on what the data is, but on what it does, its relationship to an individual's private life, autonomy, and exposure to risk.[210]

This is a precautionary model from a doctrinal standpoint. If there is still a plausible chance of re-identification, even pseudonymized material, where direct identifiers have been eliminated, may still be considered personal data.[211] This cautious approach is consistent with the GDPR's overall design, which prioritises ex-ante safeguards over ex-post remedies and incorporates the accountability principle throughout the whole data processing lifecycle.

The concept of informational self-determination, which has its roots in the German constitutional tradition, has also evolved concurrently with the extent of "personal data."[212] This idea has had a significant impact on the broad and person-centric orientation of EU data protection jurisprudence, although not being expressly stated in EU law. This is evident in both the CJEU's case law and the EDPB's interpretive guidelines. Consequently, the GDPR does more than regulate the mechanics of data transactions; it establishes a normative

[208] Bygrave, 2014, pp. 23–28.
[209] European Union (2012) Charter of Fundamental Rights of the European Union. 2012/C 326/02. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT, (Accessed: 26 July 2025); see
[210] Digital Rights Ireland, C-293/12 and C-594/12, paras 29, 33, and 47.
[211] GDPR, Recital 26; see also Kuner, C., (2011). *Regulation of Transborder Data Flows Under Data Protection and Privacy Law: Past, Present, and Future*. OECD Digital Economy Papers No. 187, pp. 10–18. Available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2011/12/regulation-of-transborder-data-flows-under-data-protection-and-privacy-law_g17a2074/5kg0s2fk315f-en.pdf, (Accessed: 26 July 2025).
[212] BVerfG, (1983). Judgment of 15 December 1983 – 1 BvR 209/83 (Volkszählungsurteil). Available at: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html, (Accessed: 26 July 2025); see also Hornung, G., Schnabel, C., (2009). *Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination*. Computer Law & Security Review, 25(1), pp. 84–88. Available at: https://www.researchgate.net/publication/257101753_Data_protection_in_Germany_I_The_population_census_decision_and_the_right_to_informational_self-determination, (Accessed: 26 July 2025).

framework through which individuals are empowered to exercise control over the digital representations of their identity.

Hence, the GDPR's definition of personal data is intentionally broad, grounded in the constitutional and normative commitments embedded in EU law. It is operationalised through a combination of legal tests, contextual interpretation, and risk-based analysis, ensuring that the protection of fundamental rights remains effective in an increasingly complex and evolving data environment.

2.2.3 A Broader Digital Challenge

Today, the concept of personal data has expanded significantly with the rapid growth of the internet. People routinely provide personal information to various platforms and applications, often without careful consideration or review of privacy policies, allowing websites to store and process their data without informed consent. That being said, our data is accessible everywhere. One of the most difficult impediments facing humanity today is the challenge of keeping track of data and making meaningful sense of it.[213] This leads us to one of the most pressing questions of our time: could personal data become the world's first digital weapon?[214] Specifically, in an interconnected world, where capacity to track and comprehend data continues to become increasingly complicated. When data is transmitted across national boundaries without interruption, protection of personal data has become critical.[215] Rapid technology improvements have made it easier for economies around the world to integrate, but this has also made strong frameworks necessary to protect people's right to privacy while allowing data to be exchanged that is necessary for economic activity.[216]

The breadth of the concept of personal data has particular relevance for blockchain environments, where transaction metadata, wallet identifiers, and public keys may indirectly

[213] Zuboff, *The Age of Surveillance Capitalism*, pp. 158–169.
[214] Pace, R.M. and Coelho, E.R. (2022). Infor*mation as a weapon of mass disruption: From information disorder to cognitive warfare*. Revista da Escola de Guerra Naval, 28(3), pp. 708–717. Available at: https://portaldeperiodicos.marinha.mil.br/index.php/revistadaegn/article/view/3866, (Accessed: 26 July 2025); see also, Staton, W. (2015). *Information as a Weapon: The Real Threat of Privacy & Data in 2015*. Medium. Available at: https://medium.com/@WStaton85/information-as-a-weapon-63ef60b8ee96, (Accessed: 26 July 2025); see also, Torreblanca, J.I. (2015). *Digital weapons, Digital vulnerability is a great concern for governments and companies*. European Council on Foreign Relations. Available at: https://ecfr.eu/article/digital_weapons3012/, (Accessed: 26 July 2025).
[215] Mercurio, B. and Yu, L. (2023). *Regulating Cross-Border Data Flows*. Cambridge: Cambridge University Press, pp. 9–18.
[216] *Ibid*.

enable identification of natural persons.[217] This interpretive flexibility becomes central to the analysis of effective erasure in decentralised architectures developed in later chapters.

2.3 Legal Actors under the GDPR Framework

The GDPR's architecture is grounded in a sophisticated legal framework that defines the roles and responsibilities of key actors central to the enforcement and compliance mechanisms of EU data protection law.[218] These actors, the data subject, the data controller, the data processor, and the supervisory authorities, function within a relational model that seeks to balance competing interests: the autonomy of the individual, the accountability of organisations, and the public interest in the lawful and proportionate use of personal data.[219]

2.3.1 Data Subjects as a Right-Holders

At the core of the GDPR lies the figure of the data subject, defined in Article 4(1) GDPR as the "identified or identifiable natural person" to whom personal data relates.[220] However, this seemingly simple definition reflects a significant legal evolution: the data subject is now an active rights-holder with enforceable claims based on primary EU law, including the EU Charter of Fundamental Rights, rather than a passive recipient of regulatory protections. This paradigm shift from administrative oversight to individual empowerment places the data subject at the centre of the data governance ecosystem.[221]

Data subjects frequently provide their personal information online in the current era of rapid technological advancement and widespread internet use, sometimes with full awareness and other times without. This fact emphasises the need for strong security measures that provide individuals more control over how their personal data is processed and used. The GDPR gives data subjects a wide range of rights intended to protect their privacy and increase their autonomy in order to meet this demand. The primary rights consist of:

a) Right of Access:[222] to know whether personal data is processed and to obtain a copy, enabling transparency.

[217] WP 136, Opinion 4/2007, page 16–22.
[218] GDPR, Articles 4, 24–28, and 51–59. Kuner et al., 2020, pp. 37–42.
[219] Kuner et al., 2020, pp. 87–138, 457–530.
[220] GDPR, Article 4(1).
[221] Fuster, G.G., (2014). *The emergence of personal data protection as a fundamental right of the EU*. Vol. 16. Springer Science & Business, p. 159.
[222] GDPR, Article 15.

b) Right to Rectification:[223] to correct inaccurate or incomplete data, reflecting the accuracy principle under Art. 5(1)(d).
c) Right to Erasure ("Right to be Forgotten"):[224] to request deletion in certain cases, subject to limits balancing other fundamental rights.
d) Right to Restriction of Processing:[225] to limit processing, for example during disputes over accuracy or lawfulness.
e) Right to Data Portability:[226] to receive personal data in a portable format, fostering interoperability and competition.
f) Right to Object:[227] to oppose processing based on legitimate interests or direct marketing.
g) Rights Related to Automated Decision-Making and Profiling:[228] to avoid decisions based solely on automated processing with significant effects, ensuring human oversight.

Additionally, the rights to access and rectify one's personal data are safeguarded under Article 8(2) of the Charter of Fundamental Rights of the European Union. The data subject, therefore, is not merely an object of data processing regulation, but the normative anchor of the entire legal framework. As Lynskey argues, this elevation "transforms the individual from a legal recipient to an active subject of digital constitutionalism."[229]

2.3.2 Data Controllers and Its Expanding Mandate

If the data subject is the normative centre of the GDPR, the data controller is its legal pivot. Defined in Article 4(7) as the natural or legal person who determines the "purposes and means" of the processing of personal data, the controller bears primary responsibility for compliance with the GDPR's principles and obligations:

> '...the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal

[223] GDPR, Article 16.
[224] GDPR, Article 17.
[225] GDPR, Article 18.
[226] GDPR, Article 20.
[227] GDPR, Article 21.
[228] GDPR, Article 22.
[229] Lynskey, O., (2015). *The Foundations of EU Data Protection Law*. Oxford Studies in European Law, pp. 1–9. Available at: https://api.pageplace.de/preview/DT0400.9780191028069_A26234784/preview-9780191028069_A26234784.pdf, (Accessed: 26 July 2025).

data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law...'[230]

This concept mirrors that of the 1995 Directive,[231] whose interpretation became pivotal in Google Spain. There, despite Advocate General Jääskinen's view that search engines were merely intermediaries, the CJEU held that Google was a controller because it determined how personal data was indexed and displayed.[232] This reasoning, reaffirmed in NT1 and NT2 v Google, expanded the scope of controllership to ensure that powerful intermediaries could not evade accountability for their role in shaping access to personal data.[233]

The Court of Justice of the European Union (CJEU) has adopted an expansive interpretation of the notion of "controller" under EU data protection law. In Jehovah's Witnesses, the Court clarified that the determination of the purposes and means of processing need not be exclusive to a single entity.[234] Rather, joint controllership may arise even where an actor exercises only partial influence over the relevant processing activities.[235] This interpretation signals a clear departure from traditional binary models of responsibility, reflecting a functional and context-driven understanding of modern data ecosystems, where roles and responsibilities are often diffuse, overlapping, and interdependent.

Similarly, in Wirtschaftsakademie Schleswig-Holstein, the Court of Justice held that the administrator of a Facebook fan page could be considered a joint controller. Taken together, these judgments underscore the Court's functional and context-sensitive approach to the concept of controllership, ensuring that data governance responsibilities are attributed in a manner consistent with the practical realities of complex, multi-actor digital ecosystems, and preventing entities from evading regulatory accountability through formalistic distinctions.[236]

[230] GDPR, Article 4(7).
[231] Data Protection Directive, Article 2(d).
[232] Google Spain, Case C-131/12, para 85.
[233] High Court of Justice of England and Wales (2018) NT1 and NT2 v Google LLC [2018] EWHC 799 (QB), paras 9–10, 29, 33, 59–60. Available at: https://www.judiciary.uk/wp-content/uploads/2018/04/nt1-Nnt2-v-google-2018-Eewhc-799-QB.pdf, (Accessed: 26 July 2025).
[234] Court of Justice of the European Union (2018) *Tietosuojavaltuutettu v Jehovan todistajat — uskonnollinen yhdyskunta*(Case C-25/17, ECLI:EU:C:2018:551, Judgment of the Court (Grand Chamber) of 10 July 2018), para 65. Available at: https://curia.europa.eu/juris/document/document.jsf?docid=203822&doclang=EN, (Accessed: 26 July 2025).
[235] Jehovan todistajat, Case C-25/17, paras 68–69.
[236] Wirtschaftsakademie Schleswig-Holstein, Case C-210/16, paras 29, 36–40.

Taken together, these rulings highlight the Court's functional and context-sensitive approach to the idea of controllership, ensuring that data governance responsibilities are assigned in a way that is consistent with the practical realities of intricate, multi-actor digital ecosystems and stopping entities from using formalistic distinctions to avoid regulatory accountability.

This construction reinforces the principle of accountability enshrined in Article 5(2) GDPR, which requires that controllers not only comply with the Regulation but also demonstrate such compliance through the implementation of appropriate technical and organisational measures. This is a paradigm shift from "reactive enforcement to proactive governance," as noted by De Hert and Papakonstantinou. Instead of just reacting to violations after they occur, controllers are required to include compliance procedures into their organisational structures. This proactive model enhances regulatory effectiveness by fostering a culture of continuous risk assessment, documentation, and demonstrable adherence to data protection obligations, thereby operationalising the GDPR's broader objective of preventive and adaptive governance in the digital environment.[237]

Controllers also function as the primary interface between data subjects and the broader regulatory framework. They bear explicit legal obligations to respond to subject access requests,[238] facilitate the exercise of rights,[239] conduct Data Protection Impact Assessments (DPIAs), and, where applicable, appoint Data Protection Officers.[240] The failure to fulfil these duties not only triggers administrative penalties under Article 83, but may also amount to a breach of fundamental rights under the CFREU.[241]

This functional understanding of controllership provides a doctrinal foundation for allocating responsibility in decentralised and multi-actor environments, where no single entity exercises exclusive control over data processing.

[237] De Hert, P. and Papakonstantinou, V. (2012). *The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals*. Computer Law & Security Review, 28(2), pp. 130–142. Available at: https://www.researchgate.net/publication/257101611_The_proposed_data_protection_Regulation_replacing_Directive_9546EC_A_sound_system_for_the_protection_of_individuals, (Accessed: 26 July 2025).
[238] GDPR, Article 15.
[239] GDPR, Articles 16–21
[240] GDPR, Article 37.
[241] GDPR, Article 83.

2.3.3 Data Processors and Joint Controllers

A data processor is any entity that processes personal data on behalf of a controller.[242]

> '...any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction...'[243]

The GDPR imposes direct obligations on processors, such as following documented instructions, maintaining records of processing, and implementing security measures.[244] The scope of "processing" under Article 4(2) extends beyond obvious data-handling activities.[245] This broad definition captures diverse functions, including the organisation and dissemination of personal data on social media platforms, where hosts curate user homepages and distribute uploaded content. Such activities demonstrate that entities facilitating or structuring data flows may fall within the GDPR's framework, and in cases of data breaches or misuse, could be held liable for non-compliant processing.[246]

Similarly, joint controllers[247] arise where two or more entities jointly determine the purposes and means of processing.[248] This creates a shared responsibility framework that requires clear delineation of obligations.[249] The scope of joint controllership was further clarified by the CJEU in Fashion ID. The Court held that a website embedding Facebook's "Like" button was a joint controller with Facebook for the collection and transmission of user data,[250] despite having no control over the subsequent processing.[251] This decision underscores that even limited influence over the purposes or means of data collection can trigger joint controllership and shared responsibility under the GDPR.

---

[242] GDPR, Article 4(8); see also, Kuner et al., 2020, pp. 41–42.
[243] GDPR, Article 4(2).
[244] GDPR, Articles 28, 32; Voigt and von dem Bussche, 2017, pp. 73–76.
[245] GDPR, Article 4(2).
[246] See Wirtschaftsakademie Schleswig-Holstein, Case C-210/16.
[247] GDPR, Article 26.
[248] Wirtschaftsakademie Schleswig-Holstein, Case C-210/16, paras 28–30.
[249] Kuner et al., 2020, pp. 123–125.
[250] Fashion ID, Case C-40/17, paras 78–79.
[251] Fashion ID, Case C-40/17, paras 80–81.

2.3.4 Supervisory Authorities and the EDPB

The European Data Protection Board (EDPB) and supervisory authorities (SAs) are the final institutional actors in the GDPR framework. Each Member State is required by Chapter VI of the GDPR to set up an independent SA that is in charge of monitoring compliance, handling complaints, and imposing sanctions.[252]

The Court of Justice of the European Union (CJEU) has repeatedly upheld the necessity of genuine independence for national supervisory authorities. In Commission v Hungary,[253] the Court ruled that an early termination of a national data protection commissioner's mandate breached EU law,[254] underscoring the need for both structural and functional independence.[255] The Court underlined that independence must be both structural and functional, including operational autonomy and freedom from outside influence.[256]

The EDPB, which was established under Article 68 GDPR,[257] is crucial for maintaining consistency and cooperation amongst jurisdictions at the European level. Unlike its predecessor, the Article 29 Working Party, the EDPB is endowed with binding powers under the consistency mechanism,[258] enabling it to issue decisions in cross-border disputes between national authorities.[259] This mechanism was notably exercised in the Meta Platforms enforcement proceedings, where objections from several supervisory authorities to the Irish DPC's draft decision triggered a formal referral to the EDPB, resulting in a harmonised resolution.[260]

The GDPR establishes a multi-level governance system through these participants, reaching a balance between centralised coordination and decentralized enforcement.[261] Similar multi-level governance considerations are reflected in technological policy initiatives such as the

[252] GDPR, Article 51.
[253] Court of Justice of the European Union, (2014). *European Commission v Hungary, Case C-288/12, Judgment of the Court (Grand Chamber)*. Available at: https://curia.europa.eu/juris/liste.jsf?language=en&num=C-288/12, (Accessed: 26 July 2025).
[254] European Commission v Hungary, Case C-288/12, paras 53–54.
[255] European Commission v Hungary, Case C-288/12, para 48.
[256] European Commission v Hungary, Case C-288/12, para 48 and 53.
[257] GDPR, Article 68.
[258] GDPR, Article 65.
[259] GDPR, Articles 63–65.
[260] EDPB Binding Decision 1/2023, paras 7, 11, 12–23, 261.
[261] GDPR, Articles 51–63; see also EDPB, (2023). *Report of the Work Undertaken by the Supervisory Authorities within the 101 Task Force*. Available at: https://www.edpb.europa.eu/our-work-tools/support-cooperation-and-enforcement/gdpr-cooperation-and-enforcement_en, (Accessed: 31 March 2026).

European Blockchain Services Infrastructure (EBSI), a joint initiative of the European Commission and the European Digital Infrastructure Consortium aimed at supporting cross-border digital public services through blockchain-based infrastructures.[262] EBSI illustrates how distributed ledger technologies may operate within structured regulatory environments designed to ensure trust, legal certainty, and compliance with fundamental rights, including data protection requirements.[263] The regulatory structure remains inherently pluralistic: Member States retain procedural autonomy, yet remain bound by overarching principles of EU law, including effectiveness, equivalence, and proportionality.[264]

Complementing these developments, the Pan-European Blockchain Regulatory Sandbox provides a coordinated framework in which regulators, supervisory authorities, and blockchain developers jointly explore legal uncertainties associated with distributed ledger technologies.[265] The sandbox contributes to harmonised supervisory approaches across Member States and facilitates practical assessment of how existing legal frameworks, including GDPR obligations, can be applied within decentralised technological systems.[266]

The doctrinal foundations of EU data protection law are established in this chapter and serve as the basis for the analysis that follows. It offers the legal basis for evaluating the viability of effective forgetting and functional responsibility in blockchain wallet ecosystems by following the development of personal data, erasure, and controllership through legislation and CJEU jurisprudence.[267]

---

[262] European Commission, European Blockchain Services Infrastructure (EBSI), (2023). Available at: https://digital-strategy.ec.europa.eu/en/policies/european-blockchain-services-infrastructure, (Accessed: 31 March 2026).

[263] Lyons et al., 2019, pp. 5–7, 9–10, 19–21.

[264] Court of Justice of the European Union, (1976). *Rewe-Zentralfinanz eG and Rewe-Zentral AG v Landwirtschaftskammer für das Saarland (Case 33/76)*, EU:C:1976:188, European Court Reports 1976, p. 1989, para 5. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:61976CC0033, (Accessed: 31 March 2026). Court of Justice of the European Union, (1976). C*omet BV v Produktschap voor Siergewassen (Case 45/76)*, EU:C:1976:191, European Court Reports 1976, p. 2043, paras 13–16. Available at: https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX:61976CJ0045, (Accessed: 31 March 2026).

[265] European Commission, European Blockchain Regulatory Sandbox (2023). Available at: https://blockchain-observatory.ec.europa.eu/european-blockchain-sandbox_en - paragraph_119, (Accessed: 31 March 2026).

[266] Geus, M., Waterman, R., G., Mohr, Q., (2026). European Commission. The European Blockchain Sandbox Report. Final Best Practices Report (3rd cohort). Chapter 3, and conclusions section. Available at: https://www.twobirds.com/en/insights/2026/the-european-blockchain-sandbox-report, (Accessed: 31 March 2026).

[267] GDPR, Articles 4, 17; Google Spain, Case C-131/12, paras 4–5, 32–38, 70–72.

Chapter 3. The Right to Be Forgotten in Law and Blockchain-Based Architectures

This chapter examines how the Right to Be Forgotten has been interpreted in EU law and considers whether Article 17 GDPR can operate effectively in technological environments characterised by decentralisation and technical persistence. While the analysis is grounded in doctrinal developments within EU data protection law, its purpose within this dissertation is to establish the legal framework necessary to assess the application of the right to erasure in blockchain-based systems. It argues that the jurisprudence of the Court of Justice increasingly supports a functional understanding of erasure, according to which the protection of data subjects may be achieved through limiting accessibility, visibility, or linkability of personal data, even where complete deletion is not technically feasible.

With the rapid pace of technological progress, the processing of personal data has become an integral part of everyday life. In such a reality, it seems reasonable that each person should be able to control how much of their personal information is accessible to the public and have the option to block or remove it when needed. This protection is especially important in a time when widespread surveillance can undermine personal autonomy, as Orwell warned.[268]

One of the most contentious and theoretically complex features of contemporary data protection regulation is the so-called right to be forgotten (RTBF). It gives data subjects the right of requesting for the removal of personal information that data controllers have acquired and maintained. It has historically been linked to data deletion.[269] As a mechanism of

[268] See Orwell, G. (1949). 1984.
[269] Li, T., Villaronga, E.F. and Kieseberg, P., (2018). *Humans forget, machines remember: Artificial intelligence and the right to be forgotten*. Boston University School of Law Faculty Scholarship, pp. 1–19. Available at: https://scholarship.law.bu.edu/faculty_scholarship/817/, (Accessed: 29 August 2025).

control,[270] the RTBF reinforces the principle of informational self-determination, viewed as the active dimension of privacy.[271] It ensures that individuals retain the power to determine how their personal data is used and disseminated, preserving their autonomy in an era of pervasive data processing.

This interpretation provides the doctrinal foundation for the concept of "effective forgetting" developed in Chapter 5.

3.1 The RTBF as an Evolution of Article 8 Protections

As mentioned earlier, the European Convention on Human Rights and the Charter of Fundamental Rights of the European Union (the Charter) serve as the cornerstones of European privacy legislation. Together, these texts lay the theoretical groundwork for contemporary data protection regulations, such as the Right to Be Forgotten.

The ECHR, through Article 8,[272] guarantees the right to respect for private and family life. Over decades, the European Court of Human Rights (ECtHR) has interpreted this provision expansively, adapting it to new contexts, including the publication and digital dissemination of personal information. Importantly, Article 10 ECHR,[273] which safeguards freedom of expression, has required courts to develop balancing mechanisms to ensure that neither privacy nor expression is afforded absolute primacy.

Complementing this, the Charter codifies parallel but more explicit protections: Article 7 mirrors Article 8 ECHR by guaranteeing respect for private and family life, while Article 8 introduces a distinct right to the protection of personal data, including access and rectification rights:

> '...Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified...'[274]

[270] Lynskey, 2015, *The foundations of EU data protection law*, pp. 9–13.
[271] Frosio, G.F. (2017). *Right to be forgotten: Much ado about nothing*. Colorado Technology Law Journal, 15(2), pp. 308–315. Available at: https://www.researchgate.net/publication/319585053_Right_to_Be_Forgotten_Much_Ado_About_Nothing, (Accessed: 29 August 2025).
[272] ECHR, Article 8.
[273] ECHR, Article 10.
[274] EU Charter, Article 8(2).

The Charter does not specifically create a right to erasure similar to the RTBF, even though it acknowledges rectification. The formalization of a right to erasure emerged only with Article 17 GDPR, expanding the data subject's autonomy and control over personal information in ways that the Charter and ECHR had only implicitly envisioned.

The ECtHR's jurisprudence under Article 8 ECHR has been pivotal in shaping the principles that underpin the RTBF. Key cases illustrate how privacy rights are balanced against competing interests:

- **Von Hannover v. Germany (No. 1)**[275] established that public figures retain a core right to privacy against intrusive media exposure, especially where the information is of no public interest.
- **Lillo-Stenberg and Sæther v. Norway**[276] reaffirmed that the unauthorized publication of personal images, even in public settings, can violate Article 8, particularly where the intent is commercial or sensational rather than public interest.
- **Peck v. United Kingdom**[277] highlighted that the unauthorized dissemination of personal data or images can constitute a disproportionate interference with privacy.

The proportionality and balance tests that later influenced CJEU jurisprudence[278] in evaluating when the erasure of personal data might supersede conflicting rights like the public interest or freedom of expression were established by these viewpoints.

Thus, it is possible to view the Right to Be Forgotten as a natural evolution of Article 8 protections. It translates the ECHR's Article 8 right to privacy and the Charter's Article 8 right to data protection into mechanisms that may be enforced online. At the same time, it incorporates the proportionality test developed through ECtHR jurisprudence, ensuring that

[275] European Court of Human Rights (ECtHR), (2004). *Von Hannover v Germany (No. 1)*. Application No. 59320/00, paras 63–65, 76–78, 80. Available at: https://hudoc.echr.coe.int/eng - {"itemid":["001-61853"]}, (Accessed: 29 August 2025).
[276] ECtHR, (2014). *Lillo-Stenberg and Sæther v. Norway*. Application no. 13258/09, paras 26–27, 30, 39–43.
[277] European Court of Human Rights (ECtHR), (2003). *Peck v. United Kingdom*. Application no. 44647/98, paras 57–63, 76–87. Available at: https://hudoc.echr.coe.int/eng - {"itemid":["001-60898"]}, (Accessed: 29 August 2025).
[278] See Google Spain (Case C-131/12), Schrems II (C-311/18), and European Court of Justice (Grand Chamber), (2019). GC and Others v Commission nationale de l'informatique et des libertés (CNIL), Case C-136/17, Judgment of 24 September 2019, ECLI:EU:C:2019:773.
Available at: https://curia.europa.eu/juris/liste.jsf?num=C-136/17, (Accessed: 29 August 2025).

freedom of expression under Article 10 ECHR[279] and considerations of public interest remain integral to the assessment. Moreover, it provides individuals, under Article 17 GDPR, with a concrete mechanism to challenge the perpetual storage, replication, and dissemination of their data, a challenge that earlier privacy frameworks had not anticipated.[280] This doctrinal continuity underscores that the RTBF is not an isolated innovation but rather a logical extension of Europe's long-standing commitment to dignity, autonomy, and informational self-determination.[281]

3.2 Right to Erasure under GDPR

With the adoption of the GDPR in 2018, the Right to Erasure was formally incorporated into European legislation. This was not an entirely new development, as the concept had already been formulated in the Data Protection Directive:

> '...Member States shall guarantee every data subject the right to obtain from the controller as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data...'[282]

When the inclusion of this right was first proposed in the draft version of the GDPR, it attracted significant public attention and criticism.[283] Opponents, particularly from U.S. Media,[284] argued that the provision risked enabling online "censorship," posed serious practical challenges for implementation, and could undermine the principle of freedom of expression.[285] Part of the reason the right attracted so much attention was that many EU citizens were unaware that the 1995 Data Protection Directive already included an erasure

[279] ECtHR, (2012). *Axel Springer AG v Germany*. App no 39954/08, paras 85–95. Available at: https://hudoc.echr.coe.int/fre - {"itemid":["001-109034"]}, (Accessed: 29 August 2025). This case established the structured proportionality test balancing Article 8 privacy rights with Article 10 freedom of expression, particularly emphasizing the role of public interest in the assessment.
[280] Kuner et al., 2020, pp. 285–289.
[281] Fuster, G.G., 2014, pp. 115–118.
[282] Data Protection Directive, Article 12(b).
[283] Hoven, M., (2012). *Balancing privacy and speech in the right to be forgotten*. Harvard Journal of Law & Technology. Available at: https://jolt.law.harvard.edu/digest/balancing-privacy-and-speech-in-the-right-to-be-forgotten, (Accessed: 29 August 2025).
[284] Thierer, A, (2012). *Europe's 'Right to Be Forgotten': Privacy as Internet Censorship*. THE TECHNOLOGY LIBERATION FRONT, Available at: https://techliberation.com/2012/01/23/europes-right-to-be-forgotten-privacy-as-internet-censorship/, (Accessed: 29 August 2025).
[285] Kulk, S. and Zuiderveen Borgesius, F., (2019). Pri*vacy, freedom of expression, and the right to be forgotten* in Europe. In: R. Leenes, R. van Brakel, S. Gutwirth and P. De Hert, eds. *Data Protection and Privacy: The Internet of Bodies*. Oxford: Hart Publishing, pp. 301–321.

mechanism.[286] In the landmark Google Spain case, the CJEU clarified this by relying on Article 12 of the Directive to establish the scope of that deletion right,[287] a case that will be discussed in detail later.

It is important to note that the GDPR's provisions apply only to data processing activities that fall within its material scope,[288] typically those of a commercial, professional, or institutional nature. Data collected and processed by individuals for exclusively personal or household purposes, such as maintaining a private address book or managing a personal email account, remains outside its scope.[289] Equally significant is the underlying rationale of the Right to Be Forgotten: it is not intended to rewrite history or censor lawful expression but to promote fairness, transparency, and proportionality in data processing practices.[290]

Everyday digital interactions, from streaming music on Spotify during a commute, to binge-watching a new series on Netflix, to updating a LinkedIn profile, quietly generate vast amounts of personal data. These platforms build intricate behavioural profiles by analysing what we view and buy, what we search for, and how long we engage with items, often combined with contextual signals like location or timing.[291] This information is then monetised, whether to refine recommendation algorithms, optimise advertising, or develop new products. Yet, users often have only a superficial understanding of how deeply their data is collected, analysed, and shared with third parties.[292] Such asymmetry in knowledge and control underscores the protective ambitions of the GDPR, and particularly Article 17, which seeks to ensure that individuals can reclaim agency over their personal information once it is no longer necessary for its original purpose or when consent is withdrawn.

Furthermore, the GDPR seeks to ensure that the exercise of the Right to Erasure is not merely theoretical but practical and accessible. Recital 59 explicitly calls for clear, user-friendly

[286] Herrmann, D., & Lindemann, J. (2016). *Obtaining personal data and asking for erasure: Do app vendors and website owners honour your privacy rights?* arXiv preprint. Available at: https://arxiv.org/pdf/1602.01804, (Accessed: 29 August 2025).
[287] Google Spain, Case C-131/12, paras 88–94.
[288] GDPR, Article 2(1); Recital 14.
[289] GDPR, Article 2(2)(c); Recital 18.
[290]GDPR, Recitals 65–66.
[291] Mayer-Schönberger, V. and Cukier, K., 2013, pp. 74–90.
[292] *Ibid*, 49–51.

mechanisms for data subjects to request erasure, thereby reducing procedural barriers and reinforcing individuals' control over their digital footprint.[293]

3.2.1 Article 17 of the GDPR

The Right to Be Forgotten (RTBF) is grounded in core principles of privacy, data protection, and personal autonomy.[294] It also embodies the value of human dignity by safeguarding individuals from comm if consent is withdrawn and no other legal basis applies, erasure is requiredercial exploitation by data processors, which increasingly risk treating people as objects rather than as autonomous subjects.[295]

In March 2014, amendments to the GDPR retitled Article 17 from "Right to be forgotten and to erasure" to "Right to erasure."[296] Accordingly, the data subject is entitled to obtain from the controller the erasure of his or her personal data without undue delay.[297] This right applies where the data are no longer necessary for the purposes for which they were collected.[298] Where processing is based on consent, that consent may be withdrawn at any time;[299] following withdrawal, the controller must erase the data if no other legal basis applies,[300] subject to the exceptions.[301]

3.2.2 Grounds for Erasure

Article 17(1) sets out the substantive grounds under which a data subject may invoke the RTBF. These include:

a) the personal data are **no longer necessary** in relation to the purposes for which they were collected or otherwise processed;
b) the data subject **withdraws consent** on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

[293] GDPR, Recital 59.
[294] Vrabec, H., U., (2021). *Data Subject Rights Under the GDPR*. With a Commentary through the Lens of the Data- driven Economy. Oxford University Press, ISBN 978– 0– 19– 886842– 2, pp. 131–139,
[295] Tsesis, A., 2014. *The right to erasure: Privacy, data brokers, and the indefinite retention of data*. Wake Forest Law Review, 49, pp.101–103.
[296] European Parliament, (2014). *Protection of individuals with regard to the processing of personal data (European Parliament legislative resolution of 12 March 2014 on COM(2012)0011 — 2012/0011(COD)*. Available at: https://www.europarl.europa.eu/doceo/document/TA-7-2014-0212_EN.html?redirect, (Accessed: 29 August 2025).
[297] GDPR, Article 17(1).
[298] GDPR, Article 17(1)(a).
[299] GDPR, Article 7(3).
[300] GDPR, Article 17(1)(b).
[301] GDPR, Article 17(3).

c) the data subject **objects to the processing pursuant to Article 21(1)** and **there are no overriding legitimate grounds for the processing,** or the data subject objects to the processing pursuant to Article 21(2);
d) the personal data have been **unlawfully** processed;
e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).[302]

While Article 17(1)(a) GDPR grants individuals the right to erasure when personal data is "no longer necessary" for its original purpose, scholars have debated its practical effectiveness, noting that such rights often place unrealistic burdens on data subjects.[303] A straightforward interpretation suggests that erasure should occur when consent has lapsed or when a once-legitimate purpose has ceased to apply over time. However, as Sartor argues, this interpretation may not fully account for data uses that are ancillary or complementary to the initial purpose; a situation particularly relevant in today's data ecosystems where profiling, enrichment, and tailored targeting are common.[304] For instance, customer purchase histories initially collected solely for billing and order-fulfillment purposes are later repurposed for secondary activities, such as targeted advertising or training algorithmic recommendation systems.

In the modern data economy, where personal data is frequently continuously repurposed across platforms and third parties, this tension is exacerbated.[305] Consider the case of fitness applications that gather data for personalised health recommendations but later integrate those datasets into broader analytics services for insurers or research partners. In such contexts, controllers could argue that the data remain “relevant,” effectively eroding the

[302] GDPR, Article 17(1)(a)–(f).
[303] Solove, D., J., (2023). *The Limitations of Privacy Rights*. 98(3) Notre Dame Law Review 977, 983–985. Available at: https://ndlawreview.org/wp-content/uploads/2023/03/NDL301_Solove_Cropped.pdf, (Accessed: 29 August 2025).
[304] Sartor, G., (2015). *The Right to Be Forgotten in the Draft Data Protection Regulation*. International Data Privacy Law, vol. 5, no. 1, 2015, pp. 64–72.
Available at: https://academic.oup.com/idpl/article/5/1/64/622968?login=true - no-access-message, (Accessed: 29 August 2025).
[305] Choo, M. and Findlay, M., 2021. *Data Reuse and Its Impacts on Digital Labour Platforms*. SMU Centre for AI & Data Governance Research Paper, (13), pp. 28–33.
Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3957004, (Accessed: 29 August 2025).

erasure right and undermining the GDPR's principle of purpose limitation.[306] This underscores the importance of interpreting Article 17(1)(a) in light of the foundational principles of purpose limitation[307] and data minimisation,[308] ensuring that the right to erasure functions as a meaningful check against the perpetual retention and proliferation of personal information in digital ecosystems.

Withdrawal of consent under Article 17(1)(b) GDPR triggers the right to erasure where consent was the sole lawful basis for processing and no alternative ground exists.[309] Once consent is revoked, the controller loses its legal justification to continue processing, and the data must be erased.[310] The provision is most relevant in contexts where processing relies exclusively on consent. For example, in clinical research, if a participant withdraws consent for their health data to be used in a study, and there is no overriding public interest or legal obligation, the controller must erase the data. Similarly, wellness apps or targeted marketing campaigns that process sensitive health or behavioural data based solely on explicit consent must comply with an erasure request once that consent is withdrawn.

However, its practical impact in the wider digital ecosystem is limited. Large platforms and data-driven services, such as social media networks or recommendation engines, often rely on legitimate interests[311] or contractual necessity,[312] allowing them to continue processing even after a withdrawal. In these cases, an erasure request may fail unless the individual demonstrates that their privacy interests clearly outweigh those asserted by the controller.[313]

---

[306] Koops, B.J., (2011). For*getting footprints, shunning shadows: A critical analysis of the right to be forgotten in big data practice*. SCRIPTed, Volume 8, Issue 3, pp. 242–255. Available at: https://script-ed.org/wp-content/uploads/2011/12/koops.pdf, (Accessed: 29 August 2025).
[307] GDPR, Article 5(1)(b).
[308] GDPR, Article 5(1)(c).
[309] Vrabec, H., U., 2021, 142–143.
[310] Court of Justice of the European Union, (2020). *Orange Romania SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), Case C-61/19, ECLI:EU:C:2020:901*. C-61/19 - Orange Romania, paras 32–45. Orange România (C-61/19) clarifies that consent must be valid and freely given, it supports the principle that once such consent is withdrawn or invalidated, the controller loses its lawful basis, triggering the right to erasure under Article 17(1)(b) GDPR. Available at: https://curia.europa.eu/juris/liste.jsf?num=C-61/19&language=en, (Accessed: 29 August 2025).
[311] GDPR, Article 6(1)(f).
[312] GDPR, Article 6(1)(b).
[313] GDPR, Recital 49; see also, CJEU, (2019). *Case C-673/17, Planet49 GmbH v. Verbraucherzentrale Bundesverband eV*. ECLI:EU:C:2019:801, paras 54–56, clarifying that consent must be freely given, specific, informed, and unambiguous, which underscores why many platforms instead rely on other lawful bases that are not revocable through withdrawal.

Despite these drawbacks, Article 17(1)(b) is nonetheless powerful tool in contexts where consent is the main legal basis, strengthening personal data control for individuals and supporting the GDPR's focus on accountability and autonomy.

Article 17(1)(c) GDPR empowers data subjects to request erasure when they object to processing under Article 21 GDPR and the controller cannot demonstrate overriding legitimate grounds to continue.[314] This provision shifts the burden of proof to the controller: once an objection is raised, the controller must justify the necessity of continued processing, or else erase or at least restrict public access to the data.[315] This mechanism is especially relevant in contexts such as targeted advertising, behavioural profiling, or algorithmic recommendations, where personal data is often processed beyond its original purpose.[316] For example, a user who objects to their geolocation data being used for behavioural advertising would be entitled to erasure unless the controller could show a compelling security or compliance reason for retaining that information.[317]

Under Article 17(1)(d) GDPR, individuals may request erasure where their personal data has been unlawfully processed. This covers situations where the data was collected or used without a valid legal basis or in breach of key GDPR principles such as fairness, transparency, or purpose limitation.[318] Examples include the unauthorised publication of sensitive data or the sharing of personal information with third parties without consent. In such instances, controllers are under a positive obligation to remove the data unless another overriding legal basis for its retention exists.

---

[314] European Data Protection Board, (2020). *Guidelines 05/2020 on consent under Regulation 2016/679*. Version 1.1, paras 8–10. Available at: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf, (Accessed: 29 August 2025).

[315] Kuner et al., 2020, pp. 87–138, 464–467.

[316] European Data Protection Board, (2021). *Guidelines 8/2020 on the targeting of social media users.* Version 2.0, paras 34–40. Available at: https://www.edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf, (Accessed: 29 August 2025); see also, Moerel, L. and Prins, C., (2016). *Privacy for the homo digitalis: Proposal for a new regulatory framework for data protection in the light of Big Data and the internet of things*. International Data Privacy Law, pp. 68, 74–77. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2784123, (Accessed: 29 August 2025).

[317] European Data Protection Board, (2019). *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, paras 25–28. Available at: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf, (Accessed: 29 August 2025).

[318] GDPR, Recital 39; see also, Kuner et al., 2020, pp. 469–472.

Article 17(1)(e) provides an additional ground, requiring erasure where it is necessary for the controller to comply with a legal obligation under Union or Member State law.[319] This typically arises in sectors with strict data retention limits, such as financial services, telecommunications, or health care, where retention periods are legally prescribed.[320] Once those periods lapse, controllers must securely erase or anonymise the data to remain compliant, reinforcing the GDPR's principle of storage limitation, , as emphasised by the CJEU in Rijkeboer (Case C-553/07).[321]

3.3 Case Law and Functional Interpretation of Erasure

The following analysis does not apply these principles to blockchain directly, but extracts the doctrinal logic that later informs that application.

The selection of cases analysed in this section follows a doctrinal and functional methodology. The core jurisprudence examined, including Google Spain, Google v CNIL, GC and Others, and TU & RE v Google, was selected because these judgments provide the most developed articulation of how Article 17 GDPR operates in technologically mediated environments where personal data cannot always be removed at its source, but where intermediaries influence accessibility, visibility, or linkage of information. These cases establish the key doctrinal criteria relevant for assessing the concept of effective forgetting, including proportionality balancing, functional controllership, contextual limitation of accessibility, and the distinction between deletion and de-referencing.

Additional decisions, including Manni (C-398/15), Újpesti Polgármesteri Hivatal (C-46/23), and IP v Quirin Privatbank AG (Case C-655/23), are included to demonstrate that the Court consistently applies a contextual and functional approach to erasure obligations beyond search engine contexts. These judgments confirm that Article 17 GDPR does not operate as an absolute right to deletion, but requires a case-by-case assessment of competing interests, technical feasibility, and the role of different actors in enabling or limiting access to personal data. The selected cases therefore represent the most doctrinally relevant foundation for

[319] GDPR, Article 17(1)(e); Recital 65; see also GDPR, Article 5(1)(e).
[320] EDPB Guidelines 07/2020, paras 11–16.
[321] CJEU, (2009). *College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer*. Case C-553/07, EU:C:2009:293, paras 47–53.
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62007CJ0553, (Accessed: 29 August 2025). In this case, the Court held that retaining personal data for longer than necessary undermines both the principle of storage limitation and the effectiveness of data subject rights, rejecting national rules that allowed indefinite limitation of access rights to data older than one year.

analysing how erasure obligations may be interpreted in decentralised technological environments such as blockchain systems.

The development of the Right to Be Forgotten (RTBF) has been shaped less by legislative text and more by judicial interpretation. Although Article 17 GDPR provides the legal foundation for erasure rights, its scope and limitations have been clarified through a series of landmark judgments. The following section examines the most influential decisions that have defined the RTBF, beginning with its recognition in Google Spain and extending to subsequent jurisprudence that refines its application in different contexts.

3.3.1 Methodological Relevance of Search Engine Case Law for Blockchain Wallet Providers

There is an immediate objection to drawing on search engine jurisprudence when analysing blockchain wallet providers: the two have little in common technologically. Google and other search engines operate centralised platforms with direct control over indexing and ranking algorithms. They process content that exists on third-party servers, presenting it through search results that they can modify at will.[322] Blockchain wallet providers interact with fundamentally different systems. The networks are decentralised, records are immutable by design, and no single actor, including wallet providers themselves, exercises control over the underlying infrastructure.[323] Given these differences, it may be questioned whether case law developed for search engines can meaningfully inform the analysis of blockchain intermediaries. However, the Court of Justice's approach in its right to be forgotten jurisprudence has focused less on specific technical architectures than on the functional relationships between actors and personal data.[324] It is this functional orientation that makes the case law relevant to blockchain contexts, despite the obvious technological disparities.

The CJEU's Right to Be Forgotten jurisprudence is grounded in a functional understanding of data processing and responsibility. Rather than focusing on who created the data or where it is stored, the Court consistently emphasises who determines the modalities of access, visibility,

[322] Google Spain, Case C-131/12, paras 35–41.
[323] Finck and Moscon, 2019, pp. 82–85; see also, see also, Herian R, (2018). *Legal Recognition of Blockchain Registries and Smart Contracts.* Research Handbook on the Law of Emerging Technologies (EE Elgar, forthcoming), pp. 1–5, 9–14, 25–31. Available at: https://www.researchgate.net/publication/329715394_Legal_Recognition_of_Blockchain_Registries_and_Smart_Contracts, (Accessed: 10 January 2026).
[324] Google Spain, Case C-131/12, paras 33–38.

and linkage of personal data.[325] In Google Spain and subsequent cases, search engine operators were qualified as controllers not because they authored the content at issue, but because their indexing activity structured the conditions under which personal data became visible and actionable within the information environment, and the Court held that those consequences generated responsibility.

This logic matters for blockchain ecosystems because it shifts the focus from technical control over data storage to practical control over data visibility.[326] Wallet providers lack the technical capacity to delete records that are embedded on an immutable blockchain.[327] But they often have considerable control over how those records become meaningful to users and third parties. For instance, wallet providers query the blockchain, retrieve transaction histories, and present them in structured formats that shape how information is perceived and interpreted. Some wallets link addresses to identity information.[328] Some display transaction graphs that make patterns visible.[329] Block explorers take this further by aggregating data across the network and making it searchable by address, by transaction hash, by time period. Analytics platforms go even further, clustering addresses, tracing fund flows, attempting to deanonymise pseudonymous activity.[330] None of these actors can alter what's written on the blockchain. But they determine whether an ordinary user can easily access that information, how it is presented, what context surrounds it, and whether it gets linked to a person's real-world identity.

The analogy to search engines is therefore functional rather than technological. Both involve actors who mediate access to information they didn't create and can't directly modify.[331] Both

[325] Google Spain, Case C-131/12, paras 33–41, 80–88.
[326] Koops, 2011, pp. 9–12, 16–18.
[327] Mittelstadt, B.D., Allo, P., Taddeo, M., Wachter, S. and Floridi, L., (2016). *The ethics of algorithms: Mapping the debate*. Big data & society, 3(2), p.2053951716679679. Available at: https://journals.sagepub.com/doi/10.1177/2053951716679679, (Accessed: 10 April 2026).
[328] Rauchs et al., 2nd Global Cryptoasset Benchmarking Study, Section 5.2.1, Section 5.4.3–5.4.4.
[329] Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G.M. and Savage, S., (2016). *A fistful of bitcoins: characterizing payments among men with no names*. In Proceedings of the 2013 conference on Internet measurement conference, pp. 2-3. Available at: https://dl.acm.org/doi/10.1145/2896384, (Accessed: 12 December 2025).
[330] Meiklejohn et al., 2016, pp. 9-11; Narayanan A., Bonneau J., Felten E., Miller A., Goldfeder S., (2016). *Bitcoin and cryptocurrency technologi*es. Princeton University Press, pp. 53–60. Available at: https://www.lopp.net/pdf/princeton_bitcoin_book.pdf, (Accessed: 7 April 2026).
[331] Cohen, Julie E., (2019). *Between Truth and Power: The Legal Constructions of Informational Capitalism.* Oxford University Press, ISBN 9780190246693, pp. 63–68. Available at: https://www.researchgate.net/publication/336780917_Between_Truth_and_Power_The_Legal_Constructions_of_Informational_CapitalismThe_Legal_Constructions_of_Informational_Capitalism, (Accessed: 8 April 2026).

exercise influence through presentation and aggregation rather than through control of the underlying data source.[332] And crucially, both can profoundly affect whether data subjects remain burdened by their historical personal data.[333]

Another aspect of the search engine jurisprudence is relevant for the analysis of immutable ledgers. The Court has progressively moved away from treating erasure as requiring physical deletion of data at its source.[334] Early reactions to Google Spain often described it as establishing a 'right to be forgotten' that would force information to be removed from the internet. However, this interpretation overstates the scope of the ruling. Google was ordered to de-index the links to the newspaper articles, to remove them from search results, but the articles themselves remained online and accessible at their original source.[335] The Court accepted this distinction. What mattered was the reduction of the practical visibility of the information, thereby decreasing the likelihood that searches conducted using the data subject's name would immediately reveal the relevant material.[336] The objective was not absolute deletion as such, but effective protection of the data subject's rights.[337]

Subsequent cases have reinforced this. The Court has indicated that effective compliance with data subject rights might be achieved through measures that attenuate accessibility, disrupt linkages between data and identifiers, or contextualise information in ways that change its impact.[338] This is a significant doctrinal move because it opens up conceptual space for

[332] Pasquale, F., (2015). *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge, MA: Harvard University Press. Available at: https://raley.english.ucsb.edu/wp-content/Engl800/Pasquale-blackbox.pdf, (Accessed: 8 April 2026).
[333] Ohm, P., (2010). *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*. UCLA Law Review, Vol. 57, p. 1701, U of Colorado Law Legal Studies Research Paper No. 9-12, pp. 1716–1720. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006, (Accessed: 8 April 2026).
[334] Mantelero, A., (2014). *The future of consumer data protection in the EU Re-thinking the "notice and consent" paradigm in the new era of predictive analytics.* Computer Law & Security Review, 30(6), pp. 643–660. Available at: https://www.sciencedirect.com/science/article/pii/S026736491400154X, (Accessed: 8 April 2026).
[335] Google Spain, Case C-131/12, paras 83–88.
[336] Frantziou, E., (2014). *Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos*. Human Rights Law Review, 14(4), pp. 761–777. Available at: https://academic.oup.com/hrlr/article/14/4/761/644686, (Accessed: 11 April 2026).
[337] Floridi, L., (2005). *The ontological interpretation of informational privacy*. Ethics and information technology, 7(4), pp. 185–200. Available at: https://www.researchgate.net/publication/226949294_The_Ontological_Interpretation_of_Informational_Privacy, (Accessed: 11 April 2026).
[338] Google Spain, Case C-131/12, paras 80–88, 93; Carnegy-Arbuthnott, H.M., (2023). *Privacy, publicity, and the right to be forgotten*. Journal of Political Philosophy, Volume 31, Issue 4, pp. 494–516. Available at: https://onlinelibrary.wiley.com/doi/10.1111/jopp.12308, (Accessed: 11 April 2026).

compliance strategies that don't require literal deletion.[339] In blockchain architectures where on-chain records are immutable, this consideration has direct legal consequences. It suggests that the relevant legal inquiry concerns whether proportionate measures can mitigate the risks arising from continued accessibility of personal data, rather than whether the underlying data can be technically erased.[340] Those are different questions, and the second one admits of a wider range of possible answers.[341]

For these reasons, the CJEU's jurisprudence on the Right to Be Forgotten in search engine cases provides a particularly suitable analytical framework for assessing the challenges of effective forgetting in blockchain wallet ecosystems.[342] It supplies the criteria, balancing logic, and functional conception of responsibility necessary to translate Article 17 GDPR into technological contexts defined by decentralisation, persistence, and distributed governance.

In decentralised ledger environments, the tension between persistence and data subject protection is particularly pronounced. Blockchain networks are designed to ensure data integrity through replication across multiple nodes and resistance to modification.[343] These architectural characteristics do not remove personal data from the scope of the GDPR, but rather complicate the modalities through which compliance may be achieved.[344] The functional reasoning developed in search engine jurisprudence therefore becomes analytically valuable, as it demonstrates that data protection law does not require technical impossibilities, but instead requires proportionate measures capable of effectively safeguarding data subjects'

[339] Kamarinou, D., Millard, C., Singh, J. and Leenes, R., (2017). *Machine learning with personal data*. Queen Mary School of Law Legal Studies Research Paper No. 247/2016, Oxford: Hart Publishing, pp. 89–114. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2865811, (Accessed: 11 April 2026).
[340] Wardaningsih, A.D., (2025). *PERSONAL DATA AS A COMMODITY IN THE DIGITAL ECONOMY*. Berumpun: International Journal of Social, Politics, and Humanities, 8(1), pp. 54–66. Available at: https://www.researchgate.net/publication/394110286_PERSONAL_DATA_AS_A_COMMODITY_IN_THE_DIGITAL_ECONOMY, (Accessed: 11 April 2026).
[341] Brownsword, R., (2016). *Technological management and the rule of law*. Law, Innovation and Technology, 8(1), pp.6–8, 12–13. Available at: https://kclpure.kcl.ac.uk/ws/portalfiles/portal/116705661/Technological_management_and_the_Published_online_22_April_2016_GREEN_AAM.pdf, (Accessed: 11 April 2026).
[342] Ausloos, J., (2020). *The right to erasure in EU data protection law*. Oxford University Press, pp. 172–178.
[343] Glaser, F., (2017). *Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain enabled System and Use Case Analysis*. Proceedings of the 50th Hawaii International Conference on System Sciences, pp. 1543–1552. Available at: https://publikationen.bibliothek.kit.edu/1000073702, (Accessed: 17 April 2026).
[344] Pisa, M. and Juden, M., (2017). *Blockchain and economic development: Hype vs. reality.* Center for global development policy paper, 107(150), pp.1–42. Available at: https://www.cgdev.org/sites/default/files/blockchain-and-economic-development-hype-vs-reality_0.pdf, (Accessed: 17 April 2026).

rights within the constraints of a given technological environment.[345] In this sense, the doctrinal shift from absolute erasure toward functional inaccessibility provides a conceptual bridge between traditional intermediary liability and decentralised data infrastructures.

Taken together, the jurisprudence demonstrates that the right to erasure has never been interpreted as requiring literal deletion in all circumstances, but rather as requiring controllers to adopt measures proportionate to technological and institutional constraints; an interpretive logic that supports the doctrinal feasibility of effective forgetting in decentralised architectures.

3.3.2 Google Spain v Spanish Data Protection Agency (AEPD) and Mario Costeja González

The modern Right to be Forgotten emerged from the CJEU's landmark decision in Google Spain SL and Google Inc. v AEPD and Mario Costeja González. The dispute originated when La Vanguardia, a Spanish newspaper, lawfully published notices in 1998 concerning the forced sale of property linked to Mr González's social security debts. Although the debts were resolved years later, searches of Mr González's name through Google continued to prominently display links to these outdated announcements.[346] Mr González argued that the persistent association of his name with these outdated proceedings infringed his rights to privacy and data protection, and requested that both the newspaper and Google remove the material. The Spanish Data Protection Agency rejected the request against La Vanguardia on the ground that the original publication was lawful, but upheld the complaint against Google.[347]

In its judgment, the CJEU held that search engine operators qualify as "controllers" of personal data under Directive 95/46, since they determine the purposes and means of indexing and displaying results.[348] Accordingly, they may be obliged, in certain circumstances, to remove links to personal data that is "inadequate, irrelevant, or no longer relevant, or excessive in relation to the purposes of the processing."[349]

[345] Calo, R., (2013). *Digital market manipulation*. Geo. Wash. L. Rev., 82, pp. 1024–1031. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2309703, (Accessed: 17 April 2026).
[346] Google Spain, Case C-131/12, paras 14–16.
[347] *Ibid*, paras 17–18.
[348] *Ibid*, paras 41.
[349] *Ibid*, para 93.

In this way, the judgment established that the Right to be Forgotten under EU data protection law could operate at the level of de-referencing, rather than requiring the erasure of original publications, thereby laying the doctrinal foundation for Article 17 GDPR.[350] Importantly, this obligation applied even where the underlying content remained lawfully published and accessible at its original source.[351] In effect, the Court distinguished between erasure of the source and suppression of accessibility through de-referencing, thereby reframing the RTBF not as an absolute right to deletion but as a functional restriction on visibility.

The Court also underscored the necessity of a proportionality test. It required balancing the rights to privacy and data protection under Articles 7 and 8 CFREU against the public's right to access information under Article 11 CFREU.[352] While the public interest may justify continued accessibility in cases where the data subject plays a role in public life, information may, with the passage of time, lose its relevance to that interest.[353]

The CJEU has consistently emphasised that the right to erasure is not absolute, but must be balanced against competing fundamental rights and legitimate societal interests, including freedom of expression and access to information under Article 11 of the Charter. This balancing logic remains relevant in blockchain environments, where data transparency may serve functions linked to financial accountability, fraud prevention, and market integrity. Article 17(3) GDPR therefore operates as an internal limitation ensuring that erasure obligations do not undermine legally protected interests requiring continued data availability.

From a doctrinal perspective, the significance of Google Spain lies in its recognition that effective protection of personal data does not always require literal erasure but may be achieved by attenuating accessibility through intermediaries that structure visibility.[354] This reasoning provides a conceptual bridge to blockchain ecosystems. Just as Google could not delete the La Vanguardia articles but was nonetheless obliged to suppress their discoverability, blockchain wallet providers cannot alter immutable on-chain records but may

[350] *Ibid*, paras 97–99.
[351] *Ibid*, paras 83–84, 88, 94
[352] *Ibid*, paras 81, 97
[353] *Ibid*, paras 96–98.
[354] Uncular, S., (2019). *The right to removal in the time of post-Google Spain: myth or reality under general data protection regulation?*. International Review of Law, Computers & Technology, 33(3), pp. 309–329. Available at: https://www.researchgate.net/publication/328340387_The_right_to_removal_in_the_time_of_post-google_Spain_myth_or_reality_under_general_data_protection_regulation, (Accessed: 17 April 2026).

be expected to ensure functional inaccessibility.[355] This could take the form of cryptographic suppression of access, off-chain delinking, layered permissioning, or contractual restrictions imposed on analytics firms.

Equally important is the Court's expansion of "controllership." Search engines were deemed controllers not because they created the content, but because they determined the modalities of access.[356] By analogy, custodial wallet providers, exchanges, and blockchain analytics firms may be regarded as controllers insofar as they shape how on-chain personal data is linked, aggregated, or exposed to third parties. Even where they cannot erase blockchain entries, they exercise decisive influence over accessibility, and therefore carry compliance duties under Article 17 GDPR.

3.3.3 Google v CNIL

The scope of the Right to be Forgotten was tested further in Google LLC v Commission nationale de l'informatique et des libertés. The dispute arose after CNIL, the French data protection authority, ordered Google to apply de-referencing not only on EU domain names (e.g., google.fr, google.de) but across all of its global search domains.[357] Google contested the order, arguing that EU law could not impose worldwide obligations. After a penalty was threatened, Google sought annulment of CNIL's decision before the Conseil d'État, which referred the question to the CJEU.[358]

The CJEU confirmed that search engine operators are controllers under EU law and may be required to de-reference results following a valid request under Articles 12(b) and 14 of Directive 95/46 (as reinterpreted through Google Spain) and now Article 17 GDPR.[359] However, the Court declined to impose a global obligation. It held that EU law requires de-referencing to be carried out on all EU domain versions of the search engine and, crucially, to be configured in such a way that users searching from within the EU cannot access de-

[355] Kaminski, M., E., (2019). Bi*nary Governance: Lessons from the GDPR's Approach to Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability.* 92 S. CAL. L. REV. 1529, pp. 1529–1595. Available at: https://scholar.law.colorado.edu/faculty-articles/1265/, (Accessed: 17 April 2026); see also, Hoofnagle, C.J., Van Der Sloot, B. and Borgesius, F.Z., (2019). *The European Union general data protection regulation: what it is and what it means.* Information & communications technology law, 28(1), pp. 65–98. Available at: https://www.tandfonline.com/doi/full/10.1080/13600834.2019.1573501, (Accessed: 17 April 2026).
[356] Google Spain, Case C-131/12, para 41.
[357] Google v CNIL, Case C-507/17, paras 36–38.
[358] *Ibid*, para 39.
[359] *Ibid*, para 40.

referenced results regardless of the domain used.[360] The Court justified this territorial limitation by reference to the need to balance fundamental rights: the rights to privacy and data protection against the freedom of expression and information.[361] Imposing global de-referencing could create conflicts with third-country legal regimes, and therefore the EU's duty was to ensure a "high level of protection" within its own territory.[362]

This functional understanding is reinforced by Advocate General Szpunar's Opinion in Google v CNIL, which argued that the right to be forgotten should not be implemented as worldwide de-referencing, but should reflect territorial limits and the need for effective technical measures, such as geo-blocking, to protect EU users, while remaining consistent with proportionality and the balancing of rights.[363]

From a doctrinal perspective, Google v. CNIL clarified the territorial scope of the effective forgetting concept. While the RTBF may not extend globally, providers must implement technical measures that ensure robust protection within the EU, such as geoblocking and filtering mechanisms.[364] This approach acknowledges the necessity of proportionality in a pluralistic legal setting as well as the practical constraints of enforcement.

For blockchain ecosystems, this reasoning highlights the need to define the operational perimeter of compliance duties. Immutable ledgers are, by design, global in scope, but the Court's reasoning suggests that compliance can be territorially constrained: actors subject to EU jurisdiction (e.g., EU-based wallet providers, exchanges, or analytics firms) may be required to implement measures that suppress accessibility for EU users, even if data remains visible elsewhere in the world.[365] As with de-referencing, the focus shifts from altering the global data record to controlling its accessibility within the EU's normative space.[366]

---

[360] *Ibid*, paras 64–66.
[361] *Ibid*, paras 68–70.
[362] *Ibid*, paras 54–59, 72.
[363] Opinion of Advocate General Szpunar (2019) in Case C- 507/ 17, Google Inc. v Commission nationale de l'informatique et des libertés (CNIL), (ECLI:EU:C:2019:15), paras 33–36, 46–50, 58–63. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62017CC0507, (Accessed: 29 August 2025).
[364] Google v CNIL, Case C-507/17, *para 70.*
[365] Svantesson, D.J.B., (2017). *Solving the Internet Jurisdiction Puzzle*. IRL Press Oxford University Press, Oxford Scholarship Online, ISBN: 9780198795674, pp. 63–69; Goldsmith, J., (2007). *Who controls the Internet? Illusions of a borderless world.* Strategic Direction, 23(11). Available at: https://jost.syr.edu/wp-content/uploads/who-controls-the-internet_illusions-of-a-borderless-world.pdf, (Accessed: 17 April 2026).
[366] Bradford, A., (2020). *The Brussels effect: How the European Union rules the world*. Oxford University Press. 107 NW. U. L. REV. 1, pp. 54–61. Available at: https://www.almendron.com/tribuna/wp-content/uploads/2018/08/the-brussels-effect.pdf, (Accessed: 17 April 2026).

The implications for controllership are equally significant. Just as Google was responsible for ensuring territorial effectiveness through technical design, custodial wallet providers or blockchain analytics firms could be expected to configure their services to ensure that deanonymised transaction histories or personal identifiers are not accessible to EU data subjects when they invoke Article 17 rights.[367] Measures might include jurisdiction-based access restrictions, smart contract layers that suppress visibility, or contractual obligations imposed on downstream processors.[368]

In this way, Google v CNIL demonstrates that the RTBF does not demand universal erasure but rather the maximisation of effective forgetting within the scope of EU law. For blockchain governance, the lesson is that Article 17 compliance can be operationalised through territorial and technical mechanisms, without requiring the impossible, alteration of the global ledger itself.

This functional and territorially bounded understanding of erasure is reinforced by the jurisprudence of the European Court of Human Rights. In Węgrzynowski and Smolczewski v Poland, the Court rejected an obligation to delete lawfully published material from online archives, favouring contextual safeguards over removal. The judgment confirms that privacy protection does not require the erasure of historical records as such, but may be achieved through limits on accessibility and reuse.[369]

3.3.4 GC and Others v CNIL

The CJEU refined the contours of the Right to be Forgotten in GC and Others v CNIL, where the issue was whether search engines must give heightened protection to special categories of personal data under Article 9 GDPR.

---

[367] Celeste, E., (2022). *Digital constitutionalism: The role of internet bills of rights*. Routledge, pp. 118–123. Available at: https://researchrepository.ucd.ie/server/api/core/bitstreams/c33cb42c-7fc2-4b2d-bb65-4383c5ae573e/content, (Accessed: 17 April 2026); see also, Helberger, N., Pierson, J. and Poell, T., (2018). *Governing online platforms: From contested to cooperative responsibility*. The information society, 34(1), pp. 5–9. Available at: https://www.tandfonline.com/doi/full/10.1080/01972243.2017.1391913, (Accessed: 17 April 2026).

[368] Finck, M., (2019). *Smart contracts as a form of solely automated processing under the GDPR*. International Data Privacy Law, 9(2), pp. 78–94. Available at: https://academic.oup.com/idpl/article/9/2/78/5488488, (Accessed: 17 April 2026).

[369] European Court of Human Rights, (2013). Case of Węgrzynowski and Smolczewski v. Poland. Application no. 33846/07, paras 59, 65–66. Available at: https://hudoc.echr.coe.int/fre - {"itemid":["001-122365"]}, (Accessed: 29 August 2025).

The proceedings arose from several individuals in France who requested that Google remove links to web pages containing sensitive information, including details of criminal convictions and, in one case, intimate aspects of private life such as sexual orientation.[370] Google refused to grant the requests, and the CNIL declined to order de-referencing. The case was referred to the CJEU for clarification on how the prohibition on processing sensitive data under Article 9 should interact with the RTBF.[371]

The CJEU confirmed that search engines are controllers and thus subject to the GDPR prohibition on processing special categories of data.[372] It held that when assessing RTBF requests concerning such data, operators must conduct a case-by-case proportionality assessment. This involves:

- Recognising that the sensitive nature of the data requires particular weight in favour of the data subject's privacy rights.[373]
- Applying the balancing test between the rights to privacy/data protection (Articles 7–8 CFREU) and freedom of expression/information (Article 11 CFREU), but with a stricter threshold given the heightened risk of harm.[374]
- Considering exceptions where publication serves an overriding public interest, particularly in journalistic, academic, or artistic contexts.[375]

The significance of GC and Others lies in the Court's insistence that the character of the data itself may recalibrate the RTBF balance. This principle is highly relevant in blockchain ecosystems, where immutable transaction histories can indirectly reveal sensitive attributes:

- Donations to political movements may reveal political opinions.
- On-chain interactions with health-related dApps may reveal health data.
- Transfers linked to LGBTQ+ charities may disclose sexual orientation.

Just as the CJEU required search engines to adopt a more protective stance when sensitive data is implicated, wallet providers and blockchain analytics firms may be required to

[370] GC and Others, C-136/17, paras 28–31.
[371] *Ibid*, paras 32–35.
[372] *Ibid*, paras 34–35.
[373] *Ibid*, paras 44–46.
[374] *Ibid*, paras 67–68.
[375] *Ibid*, paras 53–55.

implement heightened suppression mechanisms where deanonymised data exposes such categories.

The analogy demonstrates that the effective forgetting model should not treat all blockchain data equally. Instead, particular weight must be given to transaction histories that reveal or infer special categories of data. Mechanisms such as differential privacy layers, selective disclosure protocols, or contractual restrictions on analytics providers could function as the blockchain analogue of the stricter RTBF obligations articulated in GC and Others.

This case reinforces the dissertation's central claim: effective forgetting can be conceptualised as functional inaccessibility rather than deletion.[376] It also suggests that in blockchain governance, the compliance standard may need to be graduated, with more rigorous measures where sensitive data is at stake.[377] By drawing on GC and Others, the dissertation situates effective forgetting within a rights-based hierarchy that mirrors CJEU doctrine.

3.3.5 TU, RE v Google

The proceedings arose from requests by two investment professionals who sought the de-referencing of links on Google that led to articles criticising their past business practices. They claimed that ongoing references violated their rights under Article 17 GDPR and that the articles contained false material.[378] Google declined the requests, citing the need to preserve public access to the contested information, particularly given the applicants' professional role in financial markets.[379]

The CJEU clarified that the right to erasure under Article 17(1)(d) GDPR extends to situations where the personal data is inaccurate.[380] Crucially, the Court held that individuals requesting de-referencing are not required to obtain a judicial declaration of inaccuracy

[376] Irion, K. and Luchetta, G., (2013). *Online personal data processing and EU data protection reform*. In CEPS Task Force Report of the CEPS Digital Forum, ISBN 978-94-6138-302-0. Available at: https://pure.uva.nl/ws/files/2562572/166448_IRION_LUCHETTA_2013_Online_personal_data_processing.pdf (Accessed: 31 March 2026).
[377] Ducato, R., (2020). *Data protection, scientific research, and the role of information*. Computer Law & Security Review, 37, pp. 1–16. Available at: https://www.sciencedirect.com/science/article/pii/S0267364920300170, (Accessed: 31 March 2026).
[378] CJEU, Grand Chamber, (2022). *TU and RE v Google LLC*. Case C-460/20. ECLI:EU:C:2022:962. paras 15–20. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62020CJ0460, (Accessed: 29 August 2025).
[379] TU and RE v Google LLC, C-460/20, paras 21–23.
[380] *Ibid*, para 72.

before search engines act.[381] Instead, data subjects must provide evidence that, "in light of all the circumstances of the case," the content is manifestly inaccurate or no longer reliable.[382]

The Court reiterated that de-referencing must adhere to Article 11 CFREU while weighing this against freedom of expression and information. The search engine must, however, either eliminate the disputed links or provide search results in a manner that indicates the current disagreement in cases where the accuracy cannot be established.[383] This reflects a flexible approach: the public's interest in accessing information may still be served, but without compromising the individual's right to fair and accurate representation.

The ruling in TU, RE v. Google is noteworthy for articulating effective forgetting as a graded requirement rather than a binary one, in addition to validating the applicability of inaccuracy as a basis for erasure.[384] The Court acknowledged that the protection of data subjects' rights does not necessarily require the complete removal of contested information from search results.[385] Where the accuracy of information cannot be definitively established, compliance with Article 17 GDPR may instead require search engines to adopt contextual measures that modify how information is presented.[386] These may include displaying results in a manner that reflects the existence of an ongoing dispute or signalling that the reliability of the information is contested.[387] In this way, the Court accepted that proportionality may be achieved through design choices that mitigate harm without suppressing information entirely.[388]

The other aspect of TU and RE that deserves attention involves how the Court treated photographs. The judgment held that displaying thumbnail images alongside search results constitutes a separate processing operation requiring independent assessment.[389] At first this looks like a technical point about how to categorise different elements of a search result. But the Court's reasoning reveals something more substantive about how visual and textual information are understood to affect data subjects differently. Images, the Court observed,

[381] *Ibid*, paras 73–74.
[382] *Ibid*.
[383] *Ibid*, paras 75–77.
[384] *Ibid*, paras 52–54.
[385] *Ibid*, paras 57–59.
[386] *Ibid*, paras 60–63.
[387] *Ibid*, paras 65–66.
[388] *Ibid*, paras 68–70.
[389] *Ibid*, paras 101–105.

attract attention more readily than text. They create stronger mental associations. A photograph can intensify reputational damage in ways that a textual description of the same events might not.[390] There is empirical support for this; studies on information processing suggest that visual content is encoded and recalled more effectively than textual content, and that images shape impressions more powerfully than equivalent verbal descriptions.

Because visual and textual presentations have different impacts, the Court held they require separate balancing under Articles 7, 8, and 11 of the Charter.[391] A search engine cannot simply decide that a particular news story justifies including links in search results and then assume that any accompanying images are automatically justified as well. Even where textual links remain appropriate, because they serve freedom of expression or public interest in information, the photographs might create disproportionate harms that require their separate suppression. This complicates the balancing exercise considerably. Search engines must now assess not just whether information should appear in results, but in what forms it should appear.

For blockchain wallet providers and related intermediaries, this evolution in the Court's thinking opens up possibilities that would not exist under a strict deletion paradigm. Interface-level remedies become conceptually available: flagging disputed information, modifying visual presentations, limiting the prominence of certain associations, disabling specific features that amplify privacy harms.[392] These are measures that actors who cannot modify blockchain ledgers might nonetheless implement through their control over how data is accessed and displayed.[393] Whether such measures would be deemed sufficient to satisfy Article 17 in particular cases would depend on various factors, the nature of the contested data, the severity of the harm, the availability of alternative means of protection, the interests

[390] *Ibid*, para 107; see also, Childers, T.L. and Houston, M.J., (1984). C*onditions for a picture-superiority effect on consumer memory.* Journal of consumer research, pp. 643-654. Available at: https://www.researchgate.net/publication/239278291_Conditions_for_a_Picture-Superiority_Effect_on_Consumer_Memory, (Accessed: 10 January 2026); and, Paivio, A., (1990). *Mental representations: A dual coding approach*. Oxford Psychology Series, N9, Oxford university press, ISBN 0-19-503936-X, pp. 176–201.

[391] TU and RE v Google LLC, C-460/20, paras 108–111.

[392] Balkin, J.M., (2015). *Information fiduciaries and the first amendment*. UCDL Vol., 49, No 4:1183, pp. 1205–1212. Available at: https://law.yale.edu/sites/default/files/area/center/isp/documents/930am_49-4_balkin.pdf, (Accessed: 10 April 2026).

[393] Suzor, N.P., (2019). *Lawless: The secret rules that govern our digital lives*. Cambridge University Press, pp. 142, 214–221.

that continued visibility serves.[394] But TU and RE at minimum establishes that effective forgetting is not synonymous with deletion, and that design choices about presentation can themselves constitute compliance mechanisms.

Finally, this judgment marks an important expansion of the RTBF: it establishes that the right extends not only to information that is outdated, irrelevant, or excessive (Google Spain), or sensitive (GC and Others), but also to information that is demonstrably inaccurate. In doctrinal terms, the Court emphasised that the RTBF protects not only privacy but also informational integrity; the right not to be misrepresented by distorted or false data.[395]

For blockchain ecosystems, the analogy is significant. Once recorded, on-chain data (e.g., wallet addresses linked to alleged fraud, or mislabeled transfers) cannot be corrected or erased, even if later proven inaccurate.[396] According to TU, RE v. Google, functional remedies would be required in such cases: custodial wallet providers, block explorers, and analytics firms could be obliged to flag disputed records, contextualise them, or suppress their visibility, rather than perpetuating inaccuracies indefinitely.[397] Just as Google was required to acknowledge disputes in search outputs, blockchain intermediaries may need to develop mechanisms that prevent inaccurate or misleading associations from continuing to harm individuals.

The RTBF is progressively expanded from literal deletion to functional inaccessibility by the CJEU's jurisprudence. This change directly affects blockchain wallet providers: they can regulate how personal data is disclosed, connected, or aggregated through off-chain logs, analytics, and interfaces, but they are unable to remove immutable on-chain records. In this way, the case law provides a normative basis for reframing compliance in wallet ecosystems as a duty to ensure effective forgetting, not impossible erasure.

[394] Barocas, S. and Selbst, A.D., (2016). *Big data's disparate impact*. Calif. L. Rev., 104, pp. 694–698. Available at: https://www.cs.yale.edu/homes/jf/BarocasSelbst.pdf, (Accessed: 10 April 2026).
[395] TU and RE v Google LLC, C-460/20, paras 73–74.
[396] Koulu, R., (2016). *Blockchains and online dispute resolution: smart contracts as an alternative to enforcement*. SCRIPTed, Vol. 13 No. 1, pp. 41–69. Available at: https://journals.ed.ac.uk/script-ed/article/view/11491, (Accessed: 10 April 2026).
[397] Binns, R., (2018). *Fairness in machine learning: Lessons from political philosophy*. Proceedings of the 1st Conference on Fairness, Accountability and Transparency, PMLR 81, pp. 149–159. Available at: https://proceedings.mlr.press/v81/binns18a.html, (Accessed: 10 April 2026).

3.3.6 Additional CJEU Guidance on the Criteria and Responsibility for Erasure

The search engine cases provide the most developed body of CJEU jurisprudence on the right to be forgotten, but they are not the only relevant decisions. Several other judgments have addressed erasure requests in different regulatory contexts, and while these cases do not always involve digital intermediaries or online platforms, they help clarify the structural boundaries of erasure rights and how responsibility for ensuring those rights gets allocated across multiple actors. The principles that emerge from these cases apply beyond their immediate factual contexts.

Case C-398/15 Manni involved a request to erase personal data from a public commercial register in Italy.[398] Salvatore Manni had been listed as a director of a company that went into liquidation. Years later, he sought removal of this historical information from the register, arguing that its continued accessibility harmed his reputation and served no legitimate purpose given the passage of time.[399] The Court rejected an absolute right to erasure, emphasising that continued accessibility could be justified by overriding interests in legal certainty, transparency, and the protection of third parties. However, it did not characterise the continued publication of information as falling outside data protection law's scope entirely. Rather, the Court treated it as a proportionality question within the scope of data protection regulation.[400]

Specifically, commercial registers carry out crucial public functions, including facilitating creditor risk assessment, ensuring transparency in corporate structures, and providing reliable records for legal and regulatory proceedings. Significant interest in keeping thorough and historically accurate records is generated by these functions. In Manni, the Court of Justice recognised that such interests may justify refusing erasure requests, provided that a proper balancing exercise is conducted which takes account of the specific circumstances of the data subject.[401] Hence, this judgment demonstrated that the Right to Be Forgotten is not unconditional and that certain data may justifiably remain accessible where strong countervailing interests exist.

---

[398] European Court of Justice, (2017), Case C-398/15 Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni. ECLI:EU:C:2017:197. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62015CJ0398, (Accessed: 10 January 2026).
[399] *Ibid*, 14–19.
[400] *Ibid*, 54–58.
[401] *Ibid*, 39–45, 51–60.

This reasoning is relevant for data infrastructures that serve comparable transparency or accountability functions. Blockchain systems, for example, are frequently justified by reference to their capacity to create tamper-resistant audit trails and transparent transaction records. The logic of Manni suggests that these functions may constitute legitimate interests capable of justifying resistance to erasure requests, although any such conclusion would necessarily depend on the nature of the personal data at issue and the extent of the harm arising from its continued accessibility.

More recently, Újpesti Polgármesteri Hivatal Case C-46/23 has provided additional clarification on how erasure requests should be assessed procedurally and substantively.[402] The case arose after the Hungarian supervisory authority investigated a municipal COVID-19 support scheme and ordered the municipality to erase personal data it found to have been processed unlawfully.[403] The CJEU held that Article 58(2)(d) and (g) GDPR empower supervisory authorities to order the erasure of unlawfully processed personal data even where no request has been made by the data subject under Article 17(1).[404] In reaching that conclusion, the Court emphasised that Article 17(1) contains two independent dimensions: (i) a right of the data subject to obtain erasure, and (ii) a standalone obligation on the controller to erase personal data where a ground in Article 17(1) applies, irrespective of any request.[405] The Court also confirmed that this corrective power does not depend on the origin of the data: it may apply both to data collected from the data subject and to data obtained from other sources.

This emphasis on context-specific assessment reinforces a pattern visible across the Court's data protection jurisprudence. The Court consistently rejects bright-line rules in favour of balancing exercises that account for particular factual circumstances. For Google Spain, this meant that de-indexing decisions had to consider the data subject's role in public life, the nature of the information, and the time elapsed. For TU and RE, it meant separately assessing textual and visual content based on their differing impacts. For Case C-46/23, it means examining the specific processing context rather than applying categorical outcomes. The

[402] Court of Justice of the European Union, (2024), Case C-46/23 Budapest Főváros IV. Kerület Újpest Önkormányzat Polgármesteri Hivatala v Nemzeti Adatvédelmi és Információszabadság Hatóság., ECLI:EU:C:2024:239. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62023CJ0046, (Accessed: 10 January 2026).
[403] Budapest Főváros IV. Kerület, Case C-46/23, paras 13–17.
[404] *Ibid*, paras 35–36.
[405] *Ibid*, paras 37–38.

implication for blockchain systems is that one cannot simply assert 'erasure is technically impossible on blockchain, therefore Article 17 does not apply.' Instead, the analysis must proceed case-by-case, considering what data is at issue, what harm its continued accessibility causes, what legitimate interests support retention, and what alternative measures might provide adequate protection.

Similarly, the case C-655/23 concerned an unauthorised disclosure of personal data during recruitment; specifically, a bank employee used a professional networking platform's messaging service and sent a message intended for the applicant to an uninvolved third party, who then forwarded it to the applicant; the message included salary expectations and failed negotiations.[406] The referring court asked whether the GDPR itself gives a data subject a preventive remedy, a prohibitory injunction ordering the controller to refrain from future unlawful processing, even when the data subject has not requested erasure.[407]
The Court held the GDPR does not itself provide a standalone right to obtain such a preventive prohibitory injunction in that situation, and it cannot be derived from Article 17 or Article 18.[408] But the GDPR does not prevent Member States from offering that kind of injunction under national law, because the GDPR did not exhaustively harmonise remedies and Article 79 operates "without prejudice" to other remedies.[409]

This reasoning is relevant for distributed systems such as blockchains, where several actors influence the visibility and use of personal data without controlling the underlying ledger. Case C-655/23 confirms that GDPR obligations are linked to the effectiveness of data subject rights rather than to exclusive or absolute control over data. Although the Court did not address decentralised technologies, its approach indicates that responsibility may arise where an actor's conduct contributes materially to unlawful processing or its continuation.

Taken together, these cases beyond the core search engine jurisprudence establish several points that matter for understanding Article 17 in complex data ecosystems. First, erasure rights are not absolute and must be balanced against legitimate interests in transparency, auditability, and legal certainty (Manni). Second, controllers cannot apply categorical rules

[406] European Court of Justice, (2025), Case C-655/23 Quirin Privatbank, ECLI:EU:C:2025:655, paras 23–24, 28. Available at: https://curia.europa.eu/juris/liste.jsf?language=en&num=C-655/23, (Accessed: 10 January 2026).
[407] *Ibid*, paras 29–31, 35–36.
[408] *Ibid*, paras 42, 52.
[409] *Ibid*, paras 46–51, 52.

but must conduct individualised, context-sensitive assessments (Case C-46/23). Third, responsibility for enabling erasure may attach to multiple actors who collectively determine data accessibility, not just to controllers who host or create data (Case C-655/23). These principles do not resolve all questions about how Article 17 applies to blockchain systems, but they provide the doctrinal framework within which those questions must be addressed.

3.4 Alternative Perspectives on the RTBF

Although its underlying rationale goes beyond legal texts, the Right to be Forgotten is frequently examined in doctrinal terms. In basic terms, the RTBF addresses the risks of "digital permanence," which refers to a individual's inability to stay away from outdated or irrelevant information that nevertheless has an impact on their life long after its value to society has decreased.. This broader perspective highlights that the RTBF is not simply about deleting data, but about preserving individual autonomy, dignity, and the capacity for renewal.[410]

Several thinkers frame forgetting as essential for human flourishing. Mayer-Schönberger emphasises that the ability to move beyond the past is a prerequisite for moral growth and self-determination.[411] In a similar vein, Velleman conceptualises the self as an evolving project that must remain free from perpetual external definition.[412] When digital systems endlessly preserve personal information, they threaten to “freeze” individuals in time, denying them the space to reinvent themselves.

Another line of thought is contextual. Nissenbaum’s theory of contextual integrity suggests that privacy is not secrecy but the appropriateness of information flows within social settings.[413] The problem of perpetual records, whether on search engines or blockchains, is that they collapse these boundaries: disclosures made in one context, such as resolving a debt or experimenting with a new technology, become permanently available in others, such as job applications or reputational assessments, producing distortion and harm.

[410] Koops, 2011, pp. 229–236.
[411] Mayer-Schönberger, 2009, pp. 169–171.
[412] Velleman, J., D., (2001). *The Genesis of Shame*. Philosophy & Public Affairs, Vol. 30, No. 1, pp. 35–37. Available at: https://www.jstor.org/stable/3558019?seq=1, (Accessed: 29 August 2025).
[413] Nissenbaum, H., (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* Stanford University Press, JC596.2.U5N57 2010, 323.44’80973—dc22, pp. 180–186.

The jurisprudence of the Court of Justice of the European Union (CJEU) in Google Spain may be read as implicitly embracing these perspectives. By requiring de-referencing rather than deletion, the Court signalled that the right to be forgotten is not absolute but functional, restoring control by limiting accessibility rather than by erasing lawful content.[414] This doctrinal move reflects a deeper normative idea: identity protection is achieved not through historical erasure but through constraining the ways in which information is retrieved and reused.

The European Court of Human Rights (ECtHR) emphasised that privacy protection must be weighed against long-term public interests in M.L. and W.W. v. Germany, reiterating that the simple passage of time does not automatically justify the deletion of lawfully disclosed material.[415] The judgment confirms that European privacy law does not require the erasure of historical records as such, but instead permits the use of contextual safeguards to mitigate ongoing harm. This further supports a model of functional forgetting rather than absolute erasure.

For blockchain wallet providers, this alternative perspective is particularly pertinent. The immutability of blockchain records makes literal erasure impossible. Blockchain records cannot be literally erased since they are immutable. However, when financial histories are permanently connected to real-world identities, the problems noted in RTBF scholarship, such as reputational stagnation, contextual distortion, and the suppression of self-expression, become more severe.[416] As Koops has argued, the real problem of digital memory lies less in the persistence of data than in its retrievability and reusability, suggesting that "functional forgetting," restricting access and contextual reuse, is more significant than literal deletion.[417] Wallet providers, exchanges, and analytics partners therefore face not only compliance questions under the GDPR but also a broader responsibility to safeguard the conditions of human autonomy in a digital economy built on indelible traces.[418]

---

[414] Lynskey, O., (2015). *Control over Personal Data in a Digital Age: Google Spain v AEPD and Mano Costeja Gonzalez*. The Modern Law Review, Vol. 78, No. 3, pp. 526–527, 529. Available at: https://www.jstor.org/stable/43829127, (Accessed: 29 August 2025).
[415] European Court of Human Rights, (2018). M.L. and W.W. v. Germany. Applications nos. 60798/10 and 65599/10, paras 100–105, 116.
[416] Koops, 2011, pp. 233–234, 244–246, 252–254.
[417] *Ibid*, 244–246.
[418] Werro, F., (2009). *The Right to Inform v the Right to be Forgotten: A Transatlantic Clash*. A Colombi Ciacchi and others (eds), Liability in the Third Millennium, Nomos, pp. 287–298.

According to this viewpoint, the normative core of the RTBF may be captured by the standard of "effective forgetting," which is defined as rendering data practically inaccessible even if it is not technically erased.[419] If the law's concern is that individuals should not be indefinitely judged by past data once it loses relevance, then mechanisms such as access suppression, contextual decoupling, and privacy-preserving wallet architectures can be seen as functional equivalents of forgetting.[420] This interpretation bridges the apparent tension between GDPR and blockchain immutability by shifting the emphasis from erasure to control over discoverability.[421]

This understanding does not dilute the Right to Be Forgotten, but reflects the Court's consistent emphasis on effectiveness, proportionality, and contextual control over data use.

3.5 Concluding Remarks: Effective Forgetting and Erasure under EU Law

This chapter has demonstrated that the Right to Be Forgotten, as developed in the jurisprudence of the Court of Justice of the European Union, is grounded in concepts of effective forgetting and functional accessibility rather than in the literal deletion of personal data. The case law confirms that Article 17 GDPR must be interpreted in light of the realities of digital information flows and applied through a proportionality-based balancing of the data subject's rights to privacy and data protection against competing interests in freedom of expression and information, rather than as an absolute erasure obligation.

A clear distinction must be drawn between the right to erasure as codified in the GDPR and the "right to be forgotten" as developed through judicial interpretation, particularly in the context of search engine delisting.[422] The right to erasure constitutes a concrete statutory entitlement under Article 17 GDPR, subject to expressly defined grounds and exceptions, and may require the deletion of personal data where processing is unlawful, no longer necessary for its original purpose, inaccurate, or otherwise incompatible with the requirements of the

[419] Floridi, L., (2015). *The Right to be Forgotten: A Philosophical View*. Section III, Availability vs. Accessibility of Information, pp. 526–527. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3853478, (Accessed: 29 August 2025).
[420] Finck, M., (2018). *Blockchains and Data Protection in the European Union*. European Data Protection Law Review, Volume 4, Issue 1, Pages 23–29, 31–33. Available at: https://edpl.lexxion.eu/article/edpl/2018/1/6, (Accessed: 29 August 2025).
[421] Kuner et al., 2020, pp. 92–96.
[422] GDPR, Article 17; Google Spain, Case C-131/12; European Data Protection Board, (2019). *Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR*. Version, 2.0, Introduction. Available at: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201905_rtbfsearchengines_afterpublicconsultation_en.pdf, (Accessed: 10 January 2026).

Regulation.[423] By contrast, the right to be forgotten does not operate as an autonomous or independent legal right, but functions as an interpretive framework through which the right to erasure, and, where relevant, the right to object under Article 21 GDPR, is applied in digital environments characterised by persistence, searchability, and the amplified dissemination of personal data via search engines.[424]

The jurisprudence of the Court of Justice of the European Union makes clear that the effective protection of data subjects does not necessarily require the deletion of personal data at its source. Instead, measures such as de-referencing, contextualisation, and the limitation of name-based visibility may be sufficient to neutralise ongoing harm arising from disproportionate exposure through search engines.[425] Accordingly, effective forgetting operates as a functional standard aimed at reducing excessive accessibility and impact, rather than as a guarantee of complete or permanent oblivion.

However, the Court has also established clear limits. The right to be forgotten is not absolute. It yields when confronted with sufficiently strong countervailing interests. Freedom of expression, public interest in accessing information, legal requirements for record-keeping, protection of third parties, all of these can justify refusing erasure requests or limiting their scope.[426] The Manni judgment made this particularly clear in the context of commercial registers, holding that transparency and legal certainty could justify continued publication of historical company information despite privacy harms. The search engine cases consistently emphasise balancing: whether someone is a public figure, whether information concerns their professional activities, how much time has passed, whether the information remains relevant to public debate. Article 17 itself contains explicit exceptions for processing necessary for exercising freedom of expression and information, for compliance with legal obligations, for archiving purposes in the public interest, and for establishment, exercise, or defence of legal claims.

What emerges from all of this is that effective forgetting operates as a contextual and proportional standard. It is contextual because what counts as adequate protection depends on the specific circumstances; the nature of the data, who the data subject is, what legitimate

[423] GDPR, Article 17(1), (3); EDPB, Guidelines 5/2019, paras 13–16.
[424] Google Spain, Case C-131/12, paras 80–88; EDPB, Guidelines 5/2019, paras 5–7, 13–16.
[425] EDPB, Guidelines 5/2019, paras 7–11.
[426] GDPR, Article 17(3).

interests support continued accessibility, what technical measures are available. It is proportional because it requires balancing privacy rights against competing interests rather than treating erasure as categorically superior. And it is functional in the sense that it focuses on practical outcomes, whether data subjects remain exposed to ongoing harm, rather than on formal compliance with deletion requirements.

The foundation for analysing blockchain systems in later chapters is provided by this framework. Blockchain compliance becomes unfeasible if effective forgetfulness necessitates the literal erasure of data at the source; the technology is intended to prohibit changes to previous records. However, compliance solutions become feasible if effective forgetting can be accomplished by controls over display, accessibility, and contextualisation while maintaining underlying records. Can blockchain data be deleted?" is no longer the question. Regarding "can blockchain intermediaries implement measures that adequately protect data subjects from ongoing harm caused by the persistent accessibility of transaction records?" The Court did not have blockchain systems in mind when it developed these principles, thus the Court's jurisprudence does not directly address this subject. However, it creates the framework for analysis that must be used to address the question. Whether that framework can be successfully applied to immutable distributed ledgers is what the remainder of this thesis examines.

Chapter 4. Blockchain Fundamental, Actors and Accountability Constraints

Lehman Brothers declared bankruptcy in September 2008, claiming assets of about USD 639 billion and liabilities of USD 619 billion,[427] making it the fourth-largest investment bank in the United States at that time. This event constituted the largest bankruptcy in American history,[428] surpassing those of WorldCom and Enron. Although the 2008 financial crisis brought on by subprime mortgages was the direct reason of Lehman's demise, further research showed that the company's vulnerability had been made worse by years of bad accounting methods.[429]

Eighteen months after the failure, the bankruptcy examiner's investigation revealed that Lehman Brothers had routinely used accounting tricks to hide the real amount of its debt. Specifically, the firm made extensive use of repurchase agreements (repos)[430] with Cayman Islands banks. Although repos are a common financial instrument, the classification of these transactions as sales rather than loans departed from conventional accounting treatment. In practice, the mechanism allowed Lehman to transfer mortgage-backed securities (MBS)

[427] Jeffers, A., (2011). *How Lehman Brothers Used Repo 105 to Manipulate Their Financial Statements*. Article, Department of Accounting and Finance Faculty Scholarship and Creative Works. 9., pp. 44–45. Available at: https://digitalcommons.montclair.edu/cgi/viewcontent.cgi, (Accessed: 7 September 2025).

[428] Azadinamin, A., (2013). *The Bankruptcy of Lehman Brothers: Causes of Failure & Recommendations Going Forward*. Article in Social Science Research, DOI:10.2139/ssrn.2016892, page 3–5. Available at: https://www.researchgate.net/publication/230687440_The_Bankruptcy_of_Lehman_Brothers_Causes_of_Failure_Recommendations_Going_Forward, (Accessed: 7 September 2025).

[429] Jeffers, 2011, pp. 45–46.

[430] Repurchase agreements (repos) are contractual arrangements in which securities are temporarily transferred as collateral for short-term borrowing, with the borrower committing to repurchase them at maturity together with interest. see at Le Maux, J. and Morin, D., (2011). *Black and white and red all over: Lehman Brothers' inevitable bankruptcy splashed across its financial statements.* International Journal of Business & Social Science, 2(20), pp. 39–65, at p. 43, quoting Valukas, A., (2010). *Lehman Brothers Holdings Inc*. Chapter 11 Proceedings Examiner's Report. Volume 7, p. 76.
Available at: https://ijbssnet.com/journals/Vol_2_No_20_November_2011/6.pdf, (Accessed: 7 September 2025).

temporarily,[431] with the commitment to repurchase them at a later date, thereby removing large volumes of troubled assets from its balance sheet.

The relevance of these developments extends beyond financial stability concerns. They illustrate how the design of record-keeping systems influences the allocation of responsibility among actors who generate, validate, or rely upon information. Questions concerning transparency, verification, and institutional trust therefore form an important conceptual background for understanding the emergence of distributed ledger technologies.

The examiner identified three major instances of "balance sheet manipulation" between late 2007 and early 2008. In the first of these instances, the amount of debt that was concealed totaled USD 50.4 billion, which is an enormous sum by any measure. The second instance involved hiding USD 49.1 billion in obligations. The third episode concealed USD 38.6 billion.[432] These transactions, taken together, had the effect of obscuring what was actually a rising and increasingly dangerous exposure on the part of the firm to various risks. At the same time, they misrepresented Lehman's true financial position and condition to the various parties who had a stake in understanding the firm's real situation, this included regulatory authorities who were supposed to be monitoring the firm's safety and soundness, as well as investors who had put their money into the institution.[433] Lehman Brothers' eventual collapse had far-reaching effects on the entire world, starting a domino effect that exacerbated the financial crisis and led to an unprecedentedly deep and severe economic downturn.[434]

Repurchase agreements were a major factor in the events leading up to Lehman Brothers' demise. The company gave investors, analysts, and the general public an artificially strong

[431] In the static model of trade in illiquid assets, financial intermediaries (banks) fund investment either through cash reserves or by selling assets, with mortgage-backed securities serving as the main illiquid assets that generate adverse selection problems. see at House, L., C., Masatlioglu, Y., (2015). *Managing markets for toxic assets*. Journal of Monetary Economics, 70, pp. 84–87. Available at: http://econweb.umd.edu/~masatlioglu/Toxic.pdf, (Accessed: 7 September 2025).

[432] Lenzner, R., (2010). *Lehman Lies But Nobody's In Jail*. Forbes. Available at: https://www.forbes.com/consent/ketch. (Accessed: 7 September 2025).

[433] Valukas, R., A., (2010). *Lehman Brothers Holding Inc. Chapter 11 Proceedings Examiner's Lehman Brothers Holding Inc. Chapter 11 Proceedings Examiner's Report*. Volume 1, YPFS Resource Library, pp. 1–13. Available at: https://elischolar.library.yale.edu/cgi/viewcontent.cgi?article=11989&context=ypfs-documents, (Accessed: 7 September 2025).

[434] Gyntelberg, J., Fender, G., (2008). *Overview: global financial crisis spurs unprecedented policy actions*. BIS Quarterly Review, pp. 1–2, 6–8, 9–17, 20–24. Available at: https://www.bis.org/publ/qtrpdf/r_qt0812a.pdf, (Accessed: 7 September 2025).

balance sheet by incorrectly defining repos as sales rather than loans.[435] Although senior executives denied knowledge of these practices, the bankruptcy examiner concluded that they amounted to negligence rather than fraud, and thus did not constitute criminal conduct under applicable law.[436] The collapse ultimately led to the loss of thousands of jobs and wiped out trillions of dollars in global market value.

The events surrounding the financial crisis revealed structural weaknesses in systems dependent upon centralised intermediaries responsible for maintaining and verifying transactional records. Where institutional actors exercise exclusive control over information flows, asymmetries of knowledge may arise that complicate both regulatory supervision and accountability allocation. These dynamics are directly relevant to contemporary discussions concerning decentralised digital infrastructures, where the distribution of informational authority across multiple actors challenges traditional legal assumptions regarding responsibility for data processing activities.

In the aftermath of this systemic breakdown, the anonymous figure Satoshi Nakamoto published the Bitcoin white paper in November 2008, outlining the first peer-to-peer electronic cash system designed to operate without reliance on traditional financial intermediaries.[437] This innovation marked the beginning of blockchain technology as a new paradigm in finance.

The emergence of blockchain technology introduced an alternative model of record validation in which informational control is distributed across network participants rather than concentrated within a single institutional intermediary. This shift has significant implications for the allocation of legal responsibility under EU data protection law, particularly in determining which actors may qualify as controllers or joint controllers where personal data is processed within decentralised technological environments.

---

[435] Valukas, R., A., (2010). L*ehman Brothers Holding Inc. Chapter 11 Proceedings Examiner's Lehman Brothers Holding Inc. Chapter 11 Proceedings Examiner's Report*. Vol. 3, Section III.A.4 'Repo 105'. United States Bankruptcy Court, Southern District of New York. Chicago & New York: Jenner & Block LLP, pp. 768–775. Available at: https://www.jenner.com/a/web/obFa233r8auoB6xdtZXE7C/4k1Wwn/VOLUME 3.pdf, (Accessed: 7 September 2025).

[436] *Ibid*, pp. 914–918.

[437] Nakamoto, S., (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Available at: https://bitcoin.org/bitcoin.pdf, (Accessed: 7 September 2025).

4.1 Core Technical Concepts of Blockchain Relevant to This Dissertation

Because blockchain technology relies on a specialised technical vocabulary, a brief clarification of its core structural features is necessary before turning to the legal analysis.[438] This section does not seek to provide an exhaustive or instructional account of blockchain systems. Instead, it introduces only those technical characteristics that are essential for understanding the challenges posed by blockchain architectures to data protection law, particularly in relation to erasure, functional accessibility, and the allocation of responsibility under the GDPR.

Distributed Ledger

At its core, a blockchain is a form of distributed ledger technology in which records are maintained across a decentralised network of participants rather than by a single central authority. Transactions are recorded in discrete data structures known as blocks, which are sequentially linked in chronological order through cryptographic techniques.[439] Each block contains a set of validated transactions together with a cryptographic reference, typically a hash, to the preceding block, thereby forming a continuous and append-only chain of records.[440] Since any effort to change a previously recorded block would necessitate matching changes to all subsequent blocks and consensus from the distributed network, this architecture guarantees the integrity and immutability of the ledger.[441]

Immutability and its Implementation

A defining characteristic of blockchain systems is immutability, meaning that data written to the ledger is designed to be permanent and resistant to modification once confirmed.[442] After a block is validated and appended, altering its contents would compromise the internal coherence of the chain and require coordinated intervention across the distributed network.[443]

---

[438] Baker, H.K. and Kim, H.J. (2021). *A glossary of blockchain terms*. In: H.K. Baker, E. Kiymaz and G. Smith (eds.) *Blockchain applications in finance.* Bingley: Emerald Publishing, pp. 373–381. Available at: https://www.emerald.com/books/edited-volume/13510/chapter/84150828/A-Glossary-of-Blockchain-Terms, (Accessed: 7 September 2025).
[439] Nakamoto, 2008.
[440] Narayanan et al., pp. 15–21.
[441] Nakamoto, 2008.
[442] Pilkington, M., (2016). *Blockchain Technology: Principles and Applications. Research Handbook on Digital Transformations, edited by F. Xavier Olleros and Majlinda Zhegu*. Edward Elgar. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2662660, (Accessed: 10 January 2026).
[443] Gervais, A., Karame, G.O., Wüst, K., Glykantzis, V., Ritzdorf, H. and Capkun, S., (2016). *On the security and performance of proof of work blockchains*. In Proceedings of the 2016 ACM SIGSAC conference on computer and communications security, pp. 3-16. Available at: https://eprint.iacr.org/2016/555.pdf, (Accessed:

This immutability underpins key functional advantages of blockchain systems, including resistance to tampering, reliable audit trails, and trust generation among participants in the absence of centralised governance.[444] At the same time, immutable data structures conflict with fundamental data protection principles that assume the feasibility of rectification and erasure of personal data, thereby creating a structural tension with the GDPR that lies at the centre of this dissertation's analysis.[445]

Some scholars have argued that blockchains aren't truly immutable because a sufficiently powerful actor could theoretically rewrite the chain if they controlled enough computational power or stake.[446] This is technically accurate, the so-called '51% attack', but it misses the practical point. For major blockchain networks, executing such an attack would be economically irrational and would immediately destroy trust in the network, making any gains from the attack worthless. For our purposes, immutability can be treated as a functional reality of blockchain systems even if it is not an absolute physical impossibility.

Cryptographic Keys and Wallets

Users interact with blockchains through pairs of cryptographic keys: a private key and a public key.[447] The public key functions like an account number or address, it is what others use to send you cryptocurrency or identify your transactions on the blockchain. It is derived mathematically from the private key but can't be used to reverse-engineer the private key. The private key is what proves ownership and authorizes transactions. Anyone who possesses your private key can control the assets associated with your public key, which is why losing private keys means losing access to cryptocurrency holdings permanently.

---

10 January 2026); see alos, Huang, H., Yin, Z., Yang, Q., Li, T., Luo, X., Zhou, L. and Zheng, Z., (2024). *Scalability and Security of Blockchain-empowered Metaverse: A Survey*. IEEE Open Journal of the Computer Society, pp. 648–649. Available at: https://www.computer.org/csdl/journal/oj/2024/01/10695094/20yDjfh9vm8, (Accessed: 10 January 2026).

[444] Yli-Huumo, J., Ko, D., Choi, S., Park, S. and Smolander, K., (2016). *Where is current research on blockchain technology?—a systematic review*. PloS one, 11(10), p.e0163477, pp. 1–3. Available at: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0163477, (Accessed: 10 January 2026).

[445] GDPR, Articles 16–17.

[446] Moerel, L., (2019). *Blockchain & Data Protection… and Why They Are Not on a Collision Course*. European Review of Private Law 6-2019, 825–852, Kluwer Law International BV, The Netherlands, pp. 848–849. Available at: https://assets.contentstack.io/v3/assets/blt5775cc69c999c255/bltec64345cb0bd32d9/191019-blockchain-data-protection.pdf, (Accessed: 10 January 2026).

[447] Diffie, W. and Hellman, M., (1976). *New Directions in Cryptography*. Vol. IT-22, N6 IEEE Transactions on Information Theory, pp. 644–654. Available at: https://ee.stanford.edu/~hellman/publications/24.pdf, (Accessed: 10 January 2026).

Wallets are software (or sometimes hardware devices) that manage these cryptographic keys.[448] They don't 'store' cryptocurrency in the way a physical wallet stores cash. The cryptocurrency exists as entries on the blockchain. What wallets store are the private keys that prove ownership of those entries. Wallet providers become relevant to data protection analysis because, although they can't modify blockchain data, they control interfaces through which users access that data. They decide what information to display, how to aggregate transaction histories, whether to link addresses to identities, and what analytical tools to provide. This intermediary role creates potential leverage points for implementing data protection measures even where the underlying blockchain remains immutable.

Wallet providers may also play a legally relevant role in the allocation of responsibility under the GDPR. The distinction between custodial and non-custodial wallet providers, introduced in Section 1.1.4, illustrates how varying degrees of control over cryptographic keys and associated off-chain personal data may influence qualification as controller or processor. This issue is examined in greater detail in Chapter 5.

Hashing and Data Representation

Hashing is fundamental to how blockchains work. A hash function takes input data of any size and produces a fixed-size output (the hash) that's unique to that input.[449] Even a tiny change to the input produces a completely different hash. The function works only in one direction, you can't reconstruct the original data from its hash. This one-way property is what makes hashing useful for blockchain security. Blocks are linked by including the hash of the previous block, transaction integrity is verified by hashing transaction data, and miners in PoW systems compete to find hashes with particular properties.

For data protection purposes, hashing has been debated as a potential anonymization technique. If you hash personal data before putting it on a blockchain, does it still count as

[448] Walch, A. (2019) 'In Code(rs) We Trust: Software Developers as Fiduciaries in Public Blockchains', in Dimitropoulos, G., Eich, S., Hacker, P. and Lianos, I. (eds.) The Blockchain Revolution: Legal and Policy Challenges. Oxford: Oxford University Press. Available at: https://commons.stmarytx.edu/cgi/viewcontent.cgi?article=1612&context=facarticles, (Accessed: 11 January 2026).

[449] WP216, Opinion 05/2014, 2014, pp. 20–22; see also, Sevin, A., Osman Mohammed, A.A., (2024). *Comparative Study of Blockchain Hashing Algorithms with a Proposal for HashLEA*. Applied Sciences, 14(24), p.11967, pp. 2–3. Available at: https://www.researchgate.net/publication/387330149_Comparative_Study_of_Blockchain_Hashing_Algorithms_with_a_Proposal_for_HashLEA, (Accessed: 11 January 2026).

personal data? The GDPR defines personal data as information relating to an identified or identifiable person.[450] Whether hashed data remains 'identifiable' depends on whether someone could reasonably re-identify individuals from the hash. The Article 29 Working Party (now the European Data Protection Board) has taken the position that hashing alone generally doesn't constitute anonymization, particularly where the original data might be available to allow comparison, or where the input space is limited enough that hashing can be reversed through brute force.[451] This interpretation suggests that simply hashing personal data before blockchain storage wouldn't necessarily avoid GDPR obligations.

These technical characteristics, distributed architecture, immutability, decentralized consensus, cryptographic verification, are what make blockchain attractive for certain applications. They create trust without requiring trusted intermediaries, enable transparent record-keeping, and resist censorship or single points of failure. But these same characteristics create friction with data protection law's assumptions about controllers who can modify data, individuals who can exercise rights against identified responsible parties, and the possibility of erasure as a remedy for privacy harms. The legal analysis in subsequent chapters builds from this technical foundation to examine whether and how these tensions might be resolved.

From a legal perspective, hashing and public key identifiers typically constitute pseudonymisation rather than anonymisation, as the underlying data may still be attributed to an identifiable natural person through the use of additional information.[452] Under Recital 26 GDPR, data remains personal data where identification is reasonably possible through additional information. The Court of Justice of the European Union has confirmed that online identifiers may constitute personal data where the controller or another party has legal or practical means enabling identification.[453] Legal scholarship further emphasises that pseudonymisation reduces the linkability of data but does not remove the possibility of identification where auxiliary datasets or contextual information exist.[454] Because blockchain

[450] GDPR, Article 4(1).
[451] WP216, Opinion 05/2014, 2014, pp. 20–22.
[452] GDPR, Recitals 26, 28.
[453] Breyer v Bundesrepublik Deutschland, C-582/14, paras 43, 44–45; see also, Court of Justice of the European Union, (2017). *Peter Nowak v Data Protection Commissioner (C-434/16 Nowak)*. ECLI:EU:C:2017:994, paras 31, 34–35, 40. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62016CJ0434, (Accessed: 31 March 2026).
[454] WP216, Opinion 05/2014, 2014, pp. 26, 28–30; Purtova, 2018, pp. 49–50, 52–54.

addresses are persistent identifiers that can often be linked to individuals through exchanges, IP logs, or analytics services, they frequently remain within the scope of personal data under EU data protection law.[455] Consequently, technical measures such as hashing, encryption, or key abstraction do not automatically exclude blockchain data from the material scope of the GDPR but instead affect the likelihood and risk of re-identification, which remains central to the legal assessment under Recital 26.[456]

In decentralised blockchain environments, allocation of responsibility cannot be assessed independently of the technological mechanisms through which processing occurs, particularly smart contracts, which may autonomously determine the execution and persistence of data operations.

4.2 Smart Contracts and Legal Automation

Smart contracts are programs deployed on blockchains that automatically execute agreed rules, moving assets, recording outcomes, and updating state, without a human intermediary at execution time.[457] In other words, Smart contracts are programs stored on a blockchain that execute automatically when predefined conditions are met. Ethereum introduced this capability, though other platforms have implemented it as well. A smart contract might say: 'If address A sends 1 ETH to this contract, automatically transfer ownership of digital asset X to address A.' Once published, they have their own address, balance, and storage, and every consensus node re-executes the same code to reach the same result. In practice, most general-purpose smart contracts today target Ethereum's virtual machine, which deliberately aims for deterministic execution so that all nodes agree on state transitions.[458]

Two traits make smart contracts powerful and risky at once. First, immutability: after deployment, the code and state history are locked into the blockchain consensus, and correcting errors typically means deploying a new contract (or using a proxy indirection). As

[455] Finck, 2019, 29–33; WP216, Opinion 05/2014, 2014, pp. 9–13.
[456] European Data Protection Board, (2020). *Guidelines 4/2019 on Data Protection by Design and by Default*. Article 25, Version 2.0, paras 8–13. Available at: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en, (Accessed: 31 March 2026); see also, Gürses, S., Troncoso, C. and Diaz, C., (2011). *Engineering privacy by design*. Computers, Privacy & Data Protection, 14(3), pp. 3–7. Available at: https://software.imdea.org/~carmela.troncoso/papers/Gurses-CPDP11.pdf, (Accessed: 31 March 2026).
[457] Szabo, N., (1996). *Smart Contracts: Building Blocks for Digital Markets*. pp. 1–11. Available at: https://www.truevaluemetrics.org/DBpdfs/BlockChain/Nick-Szabo-Smart-Contracts-Building-Blocks-for-Digital-Markets-1996-14591.pdf, (Accessed: 17 September 2025).
[458] Antonopoulos , 2015, pp. 159–170.

Werbach notes, every Ethereum node executes the same bytecode deterministically, so bugs or inefficiencies propagate across the network with no way to patch them directly.[459] This makes outcomes tamper-resistant but also makes mistakes permanent and costly.[460] Second, autonomy: encoded preconditions (the "if") trigger on-chain effects (the "then") whenever a transaction supplies inputs that satisfy the logic, no clerk, bank, or platform operator is asked for permission.[461]

Because contracts execute in a public environment, technical pitfalls surface quickly. Common logic and security hazards include re-entrancy, mishandled exceptions, timestamp and transaction-ordering dependencies, and gas-related edge cases; tools and methods such as static analyzers, formal verification, and gas-usage linters help, but cannot substitute for sound design.[462] Privacy is another challenge: base-layer transactions and storage are broadly observable, so privacy-preserving constructions and authenticated "oracle" bridges are used when contracts must consume external data or hide inputs/outputs.[463] Performance also constrains design: most platforms process contract calls sequentially, limiting throughput; proposals for parallel execution work only when state conflicts can be ruled out.[464]

Smart contracts already underpin real systems, decentralized exchanges and lending, machine-to-machine payments in IoT, automated royalty splits, escrow and fair-exchange, and are increasingly packaged as open libraries and domain-specific languages to lower error rates.[465] Still, important non-technical limits remain. Code is not a complete substitute for

[459] Werbach, 2018, Section 3 More than Money.
[460] Wright, Filippi, 2018, pp. 72–76.
[461] Bashir, I., (2017). *Mastering blockchain*. Distributed ledger technology, decentralization, and smart contracts explained, Second Edition, ISBN 978-1-78883-904-4, Packt Publishing Ltd., pp. 95–103. Available at: https://users.cs.fiu.edu/~prabakar/cen5079/Common/textbooks/Mastering_Blockchain_2nd_Edition.pdf, (Accessed: 17 September 2025).
[462] Luu, L., Chu, D., Olickel, H., Saxena, P., Hobor, A., (2016). *Making Smart Contracts Smarter*. CCS '16: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pp. 254–269. Available at: https://eprint.iacr.org/2016/633.pdf, (Accessed: 17 September 2025).
[463] Chen, T. et al., (2017). *Under-optimized Smart Contracts Devour Your Money*. Conference: SANER(IEEE International Conferece on Software Analysis, Evolution, and Reengineering). Available at: https://www.researchgate.net/publication/314157173_Under-Optimized_Smart_Contracts_Devour_Your_Money, (Accessed: 17 September 2025); see also, Kosba, A. et al., (2016). IEEE Symposium on Security and Privacy (SP), ISSN: 2375-1207. Available at: https://eprint.iacr.org/2015/675.pdf, (Accessed: 17 September 2025).
[464] Vukolić, M., (2017). *Rethinking permissioned blockchains*. In Proceedings of the ACM workshop on blockchain, cryptocurrencies and contracts. Available at: https://vukolic.com/rethinking-permissioned-blockchains-BCC2017.pdf, (Accessed: 17 September 2025).
[465] Alharby, M., Aldweesh, A., Van Moorsel, A., (2018). *Blockchain-based smart contracts: A systematic mapping study of academic research*. In 2018 International Conference on Cloud Computing, Big Data and

contract law: unforeseen events, unconscionable terms, consumer protections, or force-majeure scenarios are difficult to encode exhaustively. And anonymous or pseudonymous deployment complicates accountability and remedies when things go wrong.[466]

These challenges also raise questions about the human actors behind smart contracts. Smart contract developers occupy an ambiguous but increasingly important role in crypto ecosystems, with contract logic capable of shifting core incentives in ways that affect network stability.[467] These actors write and deploy the code that executes transactions on-chain without further human intervention. Although technically passive once deployed, the act of creating and publishing the smart contract may constitute a form of pre-determined processing, as the contract itself encodes the purposes and means of subsequent operations.[468] According to this perspective, developers can be considered joint controllers in cases where the contract handles personal data or restricts how it can be used by others. This interpretation is consistent with the functional approach to controllership under EU data protection law, which prioritises an actor's control over processing over their official legal authority.[469]

In this sense, software architecture itself may constitute a determination of the "means of processing," as design decisions concerning data structures, storage logic, and transaction visibility directly shape how personal data is processed within decentralised environments.[470] Legal scholarship confirms that technical configurations embedded in digital infrastructures may influence the conditions under which personal data is collected, accessed, and disseminated, thereby contributing to the determination of the essential means of processing

Blockchain (ICCBB) (pp. 1-6). IEEE. Available at: https://arxiv.org/pdf/1710.06372, (Accessed: 17 September 2025).

[466] Kerikmäe, T. and Särav, S., (2017). *Paradigms for automatization of logic and legal reasoning. Law and Logic: Contemporary Issues*. Duncker & Humblot, pp. 205–222. Available at: https://www.researchgate.net/publication/319069131_Paradigms_for_Automatization_of_Logic_and_Legal_Reasoning, (Accessed: 17 September 2025).

[467] Delmolino, K., Arnett, M., Kosba, A., Miller, A., Shi, E., (2016). *Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab. In International conference on financial cryptography and data security*. pp. 3–4, 8-11. Available at: https://eprint.iacr.org/2015/460.pdf, (Accessed: 17 September 2025).

[468] Reijers, W., Wuisman, I., Mannan, M., Orgad, L., et al., (2021). *Now the Code Runs Itself: On-Chain and Off-Chain Governance of Blockchain Technologies*. Topoi 40(1), pp. 1–6. Available at: https://www.researchgate.net/publication/329656620_Now_the_Code_Runs_Itself_On-Chain_and_Off-Chain_Governance_of_Blockchain_Technologies, (Accessed: 17 September 2025).

[469] Finck, 2019, pp. 37–44.

[470] EDPB Guidelines 07/2020, paras 20–21, 38–39, 40–44; Wirtschaftsakademie Schleswig-Holstein, Case C-210/16, paras 29, 35, 38–41; Fashion ID, Case C-40/17, paras 67–69, 74, 79.

within the meaning of Article 4(7) GDPR.[471] In blockchain-based systems, protocol design choices, including consensus mechanisms, key management structures, and transaction transparency parameters, may therefore constitute relevant elements in assessing whether an actor exercises factual influence over the means of processing personal data.[472] The technological characteristics of smart contracts also demonstrate why the practical implementation of Article 17 GDPR cannot always depend on literal deletion of data. Because blockchain systems typically operate as append-only infrastructures, information embedded within smart contract logic may remain permanently recorded even where its accessibility can be limited. This architectural rigidity supports the interpretation that effective compliance with erasure obligations may require functional approaches that reduce the practical identifiability, accessibility, or linkage of personal data, rather than requiring the physical removal of all traces of information from distributed ledgers.

This chapter does not seek to resolve questions of GDPR compliance or to allocate definitive legal responsibility, but rather to map the technical and organisational conditions that shape how controllership and accountability must be approached in decentralised blockchain systems.

4.3 From Satoshi to Satoshi: Historical Evolution of Blockchain Technology

4.3.1 Origins of Bitcoin and the Double-Spending Solution

Although the true identity of Satoshi Nakamoto remains unknown, and it is unclear whether he or she is an individual, a company, or a group of individuals, the pseudonymous author is credited with writing the Bitcoin white paper in 2008.[473] Until roughly 2010, Nakamoto remained actively involved in Bitcoin's software development and governance, after which he seemingly vanished from public view.[474]

[471] GDPR Commentary 2020, pp. 90–92, 103–106; Hijmans, 2016, pp. 147–150, 153–156; De Caria, R., (2020). *Blockchain and smart contracts: Legal issues and regulatory responses between public and private economic law*. Italian LJ, 6, p.363, pp. 29–35. Available at: https://iris.unito.it/retrieve/e27ce431-2b39-2581-e053-d805fe0acbaa/363 DE CARIA.pdf, (Accessed: 31 March 2026);
[472] Finck, 2019, pp. 41–48.
[473] Ducrée, J., (2022). Sat*oshi Nakamoto and the Origins of Bitcoin -- Narratio in Nomine, Datis et Numeris*. School of Physics Sciences, Dublin City University, Abstract. Available at: https://www.researchgate.net/publication/361456322_Satoshi_Nakamoto_and_the_Origins_of_Bitcoin_--_Narratio_in_Nomine_Datis_et_Numeris, (Accessed: 7 September 2025).
[474] *Ibid*, introduction.

While Nakamoto did not originate the general idea of "cryptocurrencies," he addressed a key problem that prevented their practical viability: double-spending.[475] This refers to the possibility that the same digital token could be copied or spent more than once. Nakamoto solved this through the blockchain verification system, which ensures a consensus among network participants without requiring a centralized authority.[476]

Bitcoin's underlying blockchain database was first implemented with the launch of Bitcoin, beginning with the mining of the genesis block on January 3, 2009.[477] As the first peer-to-peer electronic cash system, Bitcoin allowed value to be transferred directly between parties without financial institutions or traditional intermediaries. Utilizing a decentralized peer-to-peer network, users can transact without knowing or trusting each other, because cryptographic techniques and distributed consensus allow nodes to automatically verify and record transactions without the need for human intervention, a central point of control, or third parties (such as governments, banks, financial institutions, or other organisations).[478]

Many of the mathematical breakthroughs used in the Bitcoin white paper were not discovered by Nakamoto. Most of the technological elements behind Bitcoin originated in academic research conducted during the 1980s and 1990s, such as David Chaum's work on digital cash and blind signatures,[479] Stefan Brands' restrictive blind signatures,[480] and research into Byzantine fault tolerance and timestamping systems.[481] These earlier contributions

[475] Chohan, W., U., (2021). *The Double Spending Problem and Cryptocurrencies*. pp. 1–11. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3090174, (Accessed: 7 September 2025). See also, Hayes, A., Rasure, E., Perez, Y., (2023). *Who is Satoshi Nakamoto?* Investopedia. Available at: https://www.investopedia.com/terms/s/satoshi-nakamoto.asp, (Accessed: 7 September 2025).
[476] Bolfing, A., (2021). C*ryptographic Primitives in Blockchain Technology: A mathematical introduction*. Oxford University Publishing, ISBN 978–0–19–886284–0, pp. 225–234.
[477] Bitcoin Wiki, (2025). *Genesis block*. Available at: https://www.blockchain.com/explorer/blocks/btc/, (Accessed: 7 September 2025).
[478] Atzori, M., (2017). *Blockchain Technology and Decentralized Governance: Is the State Still Necessary?* Journal of Governance and Regulation, Volume 6, Issue 1, pp. 58–59. Available at: https://virtusinterpress.org/BLOCKCHAIN-TECHNOLOGY-AND.html, (Accessed: 7 September 2025).
[479] Chaum, D. (1983). *Blind signatures for untraceable payments*. In Chaum, D., Rivest, R.L. and Sherman, A.T. (eds.) *Advances in cryptology: Proceedings of CRYPTO 82*. Santa Barbara, CA, 23–25 August 1982. New York: Springer, pp. 199–203. Available at: https://link.springer.com/chapter/10.1007/978-1-4757-0602-4_18, (Accessed: 7 September 2025).
[480] Brands, S., (1995). *Restrictive Binding of Secret-Key Certificates*. In: L.C. Guillou and J.-J. Quisquater, eds. *Advances in Cryptology – EUROCRYPT '95: International Conference on the Theory and Application of Cryptographic Techniques*. Saint-Malo, France, May 21–25, 1995. Proceedings. Lecture Notes in Computer Science, vol. 921. Berlin, Heidelberg: Springer, pp. 231–248.
[481] Driscoll, K.R., (2010). *Murphy Was an Optimist*. In: E. Schoitsch, ed. *Computer Safety, Reliability, and Security*. SAFECOMP 2010: 29th International Conference, Vienna, Austria, September 14–17, 2010. Proceedings. Lecture Notes in Computer Science, vol. 6351. Berlin, Heidelberg: Springer, pp. 481–482; see

demonstrated how digital signatures could establish ownership, how cryptographic hashing could protect data integrity, and how consensus could be achieved among distributed actors even in adversarial settings.[482]

Not diminishing Nakamoto's accomplishments, it has often been emphasized that he was "standing on the shoulders of giants."[483] Nakamoto's true breakthrough was not in creating an entirely new mathematical system, but rather in ingeniously combining pre-existing concepts; such as Merkle trees for data verification, proof-of-work for consensus, and distributed timestamp servers into a cohesive architecture that resolved the double-spending problem without reliance on a trusted third party.[484] This explains why the creation of Bitcoin took so long: the building blocks had existed for decades, but no one had yet devised a system that assembled them in this precise way.

Nakamoto ultimately succeeded in his goal of developing a decentralized transactional system by allowing payments to be completed in low-trust environments without the need for a reliable intermediary. His method rests on cryptographic proof rather than interpersonal trust, transforming the way value can be exchanged across digital networks.[485]

Although Bitcoin is today synonymous with the word "blockchain", Nakamoto himself never used this term in the 2008 white paper. Instead, the document speaks of a "proof-of-work chain," "blocks are chained," or "a chain of blocks," reflecting the descriptive language of the time.[486] Only until 2011 did the term "blockchain" become popular in the industry's discourse. For example, the Bitcoin wallet service blockchain.info, one of the first popular platforms to visualize Bitcoin transactions in real time, debuted in August 2011 and played a significant role in spreading the terminology.[487]

---

also, Narayanan, A., Clark, J., (2017). *Bitcoin's Academic Pedigree*. Communications of the ACM, Volume 60, Issue 12, pp. 36–42. Available at: https://dl.acm.org/doi/pdf/10.1145/3132259, (Accessed: 7 September 2025).

[482] Lamport, L., Shostak, R. and Pease, M., (1982). *The Byzantine generals problem*. ACM Transactions on Programming Languages and Systems (TOPLAS), 4(3), pp. 382–401. Available at: https://dl.acm.org/doi/pdf/10.1145/357172.357176, (Accessed: 7 September 2025).

[483] Chohan, 2021, sections "Earlier Advances" and "Accounting & Accountability Issues."

[484] Nakamoto, 2008, pp. 2–4, 7–8.

[485] Rosenfeld, M., (2012). *Analysis of hashrate-based double-spending*. arXiv, pp. 2–13. Available at: https://arxiv.org/abs/1402.2009, (Accessed: 7 September 2025).

[486] Nakamoto, 2008, pp. 1–7.

[487] Burniske, C., Tatar, J., (2017). Cryp*toassets: The Innovative Investor's Guide to Bitcoin and Beyond.* McGraw-Hill Education, ISBN: 978-1-26-002668-9, pp. 61–65; see also, Karjian, R., (2024). *A timeline and history of blockchain technology*. TechTarget. Available at: https://www.techtarget.com/whatis/feature/A-timeline-and-history-of-blockchain-technology, (Accessed: 7 September 2025).

It was only by 2015 that the term blockchain had become widely used across cryptocurrency companies, venture capital circles, and eventually mainstream media, by which time it began to designate not only the ledger underlying Bitcoin, but also a general class of distributed ledger technologies (DLT).[488] This semantic shift signaled the broadening of interest from Bitcoin itself toward applications of its underlying architecture.

In the meantime, the alternative cryptocurrency ecosystem started to grow. The goal of Litecoin's 2011 creation was to increase Bitcoin's scalability and transaction speed.[489] In an effort to lessen reliance on electricity, Peercoin, which debuted in 2012, invented the proof-of-stake consensus process.[490] Ethereum, launched in 2015, expanded blockchain's scope from digital money to decentralized applications and smart contracts, laying the foundation for today's DeFi and NFT ecosystems.[491] These projects illustrate how, although Nakamoto provided the original framework, the terminology and applications of blockchain evolved rapidly beyond his work.

4.3.2 A Close Reading of Nakamoto's Whitepaper

Nakamoto's whitepaper sets out a peer-to-peer electronic cash system that replaces trust in intermediaries with cryptographic proof and an open, append-only ledger maintained by network participants.[492] It begins by diagnosing the drawbacks of trust-based online payments, chargebacks, mediation costs, and reliance on third parties, and argues for direct transactions verified by the network rather than by financial institutions.[493]

Sections 2 and 3 introduce "coins" as chains of digital signatures: each owner transfers value by digitally signing a hash of the previous transaction and the recipient's public key, creating a verifiable ownership trail. To avoid double-spending without a central authority, all participants share a public history of transactions that is secured by a timestamp server: nodes

[488] Burniske and Tatar, 2017, pp. 57–66.
[489] Krückeberg, S., Scholz, P. (2019). *Cryptocurrencies as an Asset Class*. In Goutte, S., Guesmi, K., Saadi, S. (eds) *Cryptofinance and Mechanisms of Exchange: The Making of Virtual Currency*. Cham: Springer Nature Switzerland AG, pp. 5–6.
[490] King, S., Nadal, S., (2012). PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. Semantic Scholar. Available at: https://www.semanticscholar.org/paper/PPCoin%3A-Peer-to-Peer-Crypto-Currency-with-King-Nadal/0db38d32069f3341d34c35085dc009a85ba13c13, (Accessed: 7 September 2025).
[491] Krückeberg and Scholz, 2019, pp. 4–5.
[492] Nakamoto, 2008, para 1.
[493] Nakamoto, 2008, para 2.

batch transactions into blocks and timestamp them by hashing the block; each block includes the previous block's hash, forming a chain.[494]

Sections 4–6 specify the technical engine: proof-of-work (PoW) makes blocks hard to alter by requiring nodes to discover a nonce that yields a block hash below a target; difficulty adjusts over time to target a stable block interval. The network protocol is simple: broadcast transactions, assemble them into blocks, find valid PoW, and accept the longest (most-work) chain. Incentives come from a block subsidy and fees, aligning miners' economic interests with honest behavior.[495]

Sections 7–11 refine the design. Disk space is reclaimed via Merkle-tree pruning: since a block header commits to a Merkle root, old spent transactions can be discarded while preserving block validity. Simplified Payment Verification (SPV) lets light clients verify inclusion using headers plus a Merkle path, while full nodes remain the trust anchor. The system supports combining/splitting value via multi-input/multi-output transactions, preserves practical privacy through pseudonymous keys (with cautions about linkage), and quantifies double-spend risk, showing the attacker's catch-up probability decays exponentially with confirmations when honest hash power is in the majority.[496]

Overall, the paper provides a compact but comprehensive blueprint for a permissionless ledger: security emerges from economic incentives and probabilistic finality on the longest-work chain, rather than from institutional trust.[497]

4.3.3 Blockchain Beyond Bitcoin

Blockchain's potential is undeniable. In the next five to ten years, digital assets, which are based on blockchains, will likely pose a serious threat to existing fiat currencies,[498] according to over 76% of respondents in Deloitte's 2021 Global Blockchain Survey.[499] By 2025, the business value added by blockchain is expected to reach just over $176 billion; by 2030, it is

[494] Nakamoto, 2008, paras 3–4.
[495] Nakamoto, 2008, paras 4–6.
[496] Nakamoto, 2008, paras 7–11.
[497] Nakamoto, 2008, para 12.
[498] Fiat money refers to legal tender established by government decree, typically coins and paper notes not redeemable for gold or silver, whose face value exceeds any commodity value. The Editors of Encyclopaedia Britannica, (2014). "Fiat money," Encyclopaedia Britannica. Available at: https://www.britannica.com/money/fiat-money, (Accessed: 7 September 2025).
[499] Deloitte Insights, (2021). *Deloitte's 2021 Global Blockchain Survey: A new age of digital assets*. pp 5–6. Available at: https://bitcoinke.io/wp-content/uploads/2021/08/Deloitte-2021-Global-Blockchain-Survey.pdf, (Accessed: 7 September 2025).

expected to exceed $3.1 trillion.[500] Cryptocurrencies are currently one of the most salient use cases for blockchain technology in a rapidly changing world, and this will likely remain the case for some time. Non-fungible tokens (NFTs),[501] in contrast, point to an even more expansive future for blockchain applications.[502] In March 2021, NFT sales totaled around $400 million, a 400% increase over the previous month.[503]

Blockchain technology can revolutionise multiple sectors by adding security, efficiency, and transparency to existing processes. However, broad adoption will likely require regulatory clarity, industry collaboration, and sustained innovation to overcome current obstacles and realise its full benefits.[504]

Most people understandably associate blockchain with Bitcoin. Bitcoin, the first decentralised, permissionless, peer-to-peer payments system, is both a cryptocurrency and a protocol. More broadly, blockchain is a type of distributed ledger technology (DLT): a decentralised, peer-to-peer network that maintains a shared digital ledger of transactions.[505] Put simply, it organises data into cryptographically linked "blocks" that are recorded sequentially across a distributed, global network of computers.

Blockchain is a highly sophisticated technology that is briefly described as a growing list of records, called blocks, which are linked using cryptography.[506] A blockchain is essentially a distributed, synchronized digital database, kept up to date across multiple nodes (computers that each hold a local copy of the database) and governed by a consensus method. Because

[500] Lovelock, D., Reynolds, M., Granetto, B., Kandaswamy, R., (2017). *Forecast: Blockchain Business Value, Worldwide, 2017-2030*. GARTNER. Available at: http://www.gartner.com/doc/3627117, (Accessed: 7 September 2025).
[501] Unlike fungible assets such as Bitcoin or dollar bills, which have a fixed value per unit, NFTs (non-fungible tokens) represent a unique class of cryptoassets. Because each NFT is distinct, they can be used to verify ownership of digital goods such as music records, artwork, virtual real estate, and even digital pets, see at: Coinbase, (2025). *What Is a Non-fungible Token (NFT)?* Available at: https://www.coinbase.com/en-gb/learn/crypto-basics/what-are-nfts, (Accessed: 7 September 2025).
[502] The European Business Review, (2021). *Future of Blockchain: How will it revolutionize the world in 2022 and Beyond*. Available at: https://www.europeanbusinessreview.com/future-of-blockchain, (Accessed: 7 September 2025).
[503] *Ibid.*
[504] Tews, S., (2024). *Beyond Bitcoin: Unlocking Blockchain's Potential*. AEIdeas. Available at: https://www.aei.org/technology-and-innovation/beyond-bitcoin-unlocking-blockchains-potential/, (Accessed: 7 September 2025).
[505] Dewey, J., N., (2018). *Global legal insights: Blockchain & cryptocurrency regulation 2019 (1st ed.)*. Global Legal Group Ltd, pp. 5–8.
Available at: https://www.acc.com/sites/default/files/resources/vl/membersonly/Article/1489775_1.pdf, (Accessed: 7 September 2025).
[506] Narayanan et al., 2016, pp. 4–18.

replication is intended to provide durability, many parties are frequently involved in database upkeep. Each node can independently update the database and maintains an integrated copy of it. In practice, coordination and validation occur continuously across the participating network peers worldwide. Such systems use decentralized approaches for collecting, storing, and processing data.[507]

A blockchain can be defined as "a shared and distributed ledger or database that maintains a continuously growing list of blocks".[508] To build a decentralized, trustworthy, inclusive, secure, and egalitarian digital economy, blockchain is recognized as a powerful instrument. Hence, blockchain is often referred to as a public ledger. The term blockchain reflects its operational mechanism; specifically, the blocks are sequentially and linearly arranged to form a chain of linked blocks. Each block contains data, whether it is factual information, transaction records, or other types of data.[509] Blocks containing transaction data are arranged according to their uniquely generated hash,[510] a digital fingerprint. Importantly, the hash information from the previous block is also included in each block.[511] A chain of transactions may occur since each new block can attest to the legitimacy of the preceding block in this way.

Since blockchain technology is still relatively new, there is no fixed definition for it in EU laws or regulations. According to the CNIL's recommendation, a blockchain can be defined as follows: "A blockchain is a database in which data is stored and distributed to a large number of computers and in which all entries, called 'transactions', are visible to all users. A blockchain is not, in itself, a data processing operation with its own purpose: it is a technology which can serve in a diverse range of processing operations."[512]

---

[507] Finck, STOA Report, 2019, pp. 1–5.

[508] Drescher, D. (2017). *Blockchain Basics: A Non-Technical Introduction in 25 Steps*. Quoted in Fenwick, M., Vermeulen, E.P.M. (2019). *A primer on blockchain, smart contracts & crypto-assets*. pp. 3–4. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3379443, (Accessed: 7 September 2025).

[509] Fenwick, 2019, pp. 2–3.

[510] Scaling Parrots, (2025). *Blockchain Hash: what is it and what is it for*. Available at: https://www.scalingparrots.com/en/blockchain-hash-what-is-it/ - :~:text=A Blockchain hash is a,a previously generated hash value., (Accessed: 7 September 2025).

[511] Sater, S., (2017). Bl*ockchain and the European Union's General Data Protection Regulation: A Chance to Harmonize International Data Flows*. SSRN Electronic Journal, page 19–22. Available at: https://www.researchgate.net/publication/323979226_Blockchain_and_the_European_Union's_General_Data_Protection_Regulation_A_Chance_to_Harmonize_International_Data_Flows, (Accessed: 7 September 2025).

[512] Commission Nationale de l'Informatique et des Libertés, (CNIL), (2018). *Solutions for a responsible use of the blockchain in the context of personal data*. Available at: https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data, (Accessed: 7 September 2025).

On the official website of the European Union, the EU's "Blockchain Strategy" policy is outlined, aiming to position the EU as a leader in blockchain technology. The European Union seeks to promote blockchain innovation and establish itself as a central location for major blockchain platforms, businesses, and applications.[513] A "gold standard" for blockchain technology has been set by the Commission, and it includes cybersecurity, data protection, and environmental sustainability. The minimum specifications that blockchain technologies in Europe must follow are described in this standard. Crucially, it places strong emphasis on compliance with the EU's strict data protection requirements, ensuring that blockchain implementations respect individuals' right to privacy and adhere to data protection legislation.[514]

4.4 Structural Anatomy of the Decentralized Ledger

Software systems can be implemented in a variety of ways. However, when putting a system into execution, one of the most significant decisions concerns its architecture, which refers to how its parts are assembled and linked to one another. The two main types of software systems are centralizd and distributed architectures.[515]

In a centralized design, every component is connected to a single central component, and all decision-making flows through that component. Such a design is sometimes called subordinated because the peripheral units or subsystems are dependent on the central controller.[516] For example, a traditional banking system is centralized, as every transaction is routed through a core server.

In a distributed architecture, no component is directly connected to every other component; instead, connections are established indirectly through peer-to-peer communication.[517] This

[513] European Commission, (2025). *Blockchain and web3 strategy*. *Shaping Europe's digital future, Blockchain Strategy*. Available at: https://digital-strategy.ec.europa.eu/en/policies/blockchain-strategy, (Accessed: 7 September 2025).
[514] *Ibid*.
[515] Tanenbaum, A., S., Steen, M., V., (2006). *Distributed systems:principles and paradigms*. Upper Saddle River, NJ: Pearson Prentice Hall, ISBN: 0-13-239227-5, pp. 33–36. Available at: https://vowi.fsinf.at/images/b/bc/TU_Wien-Verteilte_Systeme_VO_%28Göschka%29_-_Tannenbaum-distributed_systems_principles_and_paradigms_2nd_edition.pdf, (Accessed: 15 September 2025).
[516] Mosleh, M., Dalili, K. and Heydari, B., (2016). *Distributed or monolithic? A computational architecture decision framework*. IEEE Systems journal, 12(1), pp.125–136. Available at: https://arxiv.org/pdf/1608.00944, (Accessed: 15 September 2025).
[517] Drescher, D., (2017). *Blockchain Basics: A Non-Technical Introduction in 25 steps*. Apress, ISBN 978-1-4842-2603-2, see sections, *Two Types of Software Architecture*, and *Distributed Peer-to-Peer Systems*.

improves scalability and resilience but introduces coordination complexity. An example is peer-to-peer file sharing, such as BitTorrent, where users exchange file pieces without relying on a single server.[518]

This paper will discuss public permissionless blockchains, which allow anyone to read, write, and create transactions. These systems are a form of distributed architecture, as no single entity has authority over the entire network. For instance, Bitcoin and Ethereum are public blockchains where any participant can propose transactions and help validate them.[519]

It is important to distinguish between different blockchain types. Public blockchains are open networks where anyone can participate in maintaining and accessing the ledger. Private blockchains restrict participation to a single organization or consortium, limiting who can read and write transactions.[520] For example, a supply chain consortium may implement a private blockchain where only approved firms can add or verify data.

Between these two extremes, there are permissioned or consortium blockchains, which combine features of both models. They allow controlled participation but still distribute trust across multiple organizations.

Blockchains of the public, permissionless kind enable all participants to read, write, and create transactions without requiring approval from a central authority. This openness distinguishes them from private or subordinated architectures, where control is concentrated in one entity.

Illustrated software systems[521]

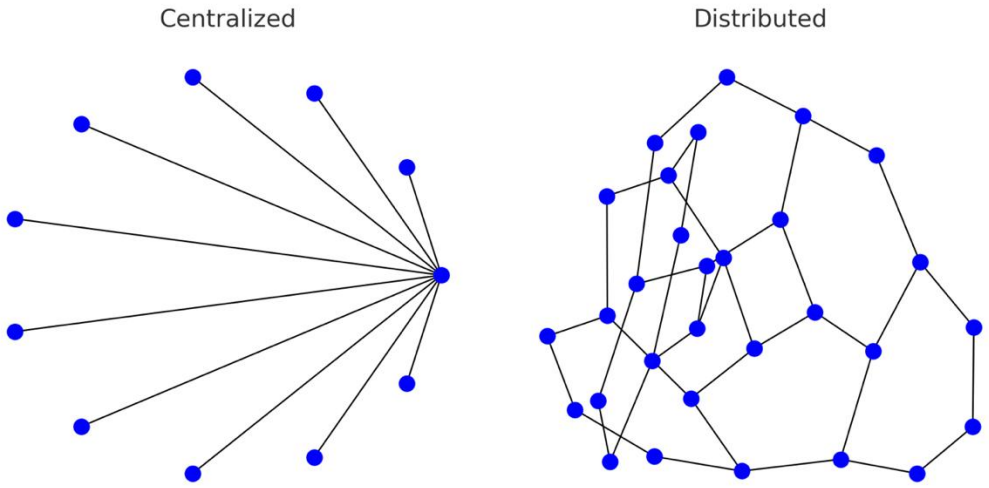
Available at: https://lib.zu.edu.pk/ebookdata/Engineering/Cyber Security/Blockchain basics_ a non-technical introduction in 25 steps by Drescher, Daniel -Apress (2017).pdf, (Accessed: 15 September 2025).

[518] Pouwelse, J., Garbacki, P., Epema, D. and Sips, H., (2005). *The bittorrent p2p file-sharing system: Measurements and analysis*. In International workshop on peer-to-peer systems. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 205–216. Available at: https://www.researchgate.net/publication/221160480_The_Bittorrent_P2P_File-Sharing_System_Measurements_and_Analysis

[519] Seira, A., Allen, J., Watsky, C. and Alley, R., (2024). *Governance of permissionless blockchain networks*. FEDS Notes. Washington: Board of Governors of the Federal Reserve System, February 09, 2024. Available at: https://doi.org/10.17016/2380-7172.3443, (Accessed: 15 September 2025).

[520] Drescher, 2017, Section 2, Two Types of Software Architecture.

[521] Figure generated by the author using Python (matplotlib + networkx).



4.4.1 Public vs Private Chains

Blockchains can be categorized as private (where a single entity operates the platform) or public (where no specific entity manages the platform).[522] One of the main distinctions between public and private blockchains lies in who can join the network, participate in the consensus protocol, and maintain the shared ledger.[523]

Anyone can submit transactions and read the ledger;[524] block creation is handled collectively through consensus; this type of network is known as a public blockchain.[525] Each user has the ability to perform transaction procedures and read data from the system. Anyone can participate at any time; it is not limited to specific public blockchain users. As a result, anybody can access the ledger, make changes to it, and use the transaction mechanisms.[526] Bitcoin and Ethereum can be used as examples of public blockchains. They are well-known for being decentralized and not requiring any central network infrastructure.[527] In contrast to public blockchains, private blockchains are not available to the public and can only be

[522] Ganne, E., (2018). *Can Blockchain revolutionize international trade?* World Trade Organization, pp. 8–12. Available at: https://www.ibm.com/downloads/documents/us-en/10c31775a1540303, (Accessed: 15 September 2025).
[523] Godfrey-Welch, D., Lagrois, R., Law, J., Anderwald, R.S. and Engels, D.W., (2018). *Blockchain in payment card systems*. SMU Data Science Review, 1(1), pp. 3–7. Available at: https://scholar.smu.edu/datasciencereview/vol1/iss1/3/, (Accessed: 15 September 2025).
[524] *Ibid*.
[525] Herath, H.M.A.D., M.J. Sabani, A., Shafana, M.S., (2021). Id*entifying Suite Type of Blockchain for Application: Public and Private*. Department of Information and Communication Technology, pp. 180–188. Available at: http://ir.lib.seu.ac.lk/bitstream/123456789/5786/1/26 P_ICST2021 Final v11_win_Done_sec_p197-205.pdf, (Accessed: 15 September 2025).
[526] *Ibid*.
[527] Godfrey-Welch et al., 2018, pp. 7–9; see also, Herath et al., 2021, pp. 182–183.

accessed by specific individuals. They rely on trust to function and are usually used by businesses for internal networking needs. For entry, authorization is mandatory.[528]

Consortium-managed blockchain is a type of private blockchain where decisions are not made by a single individual but rather by a selected group of people representing the member companies.[529] It can be described as a partially decentralised platform with a limited number of participants.[530] In a consortium blockchain, a predefined group of nodes is chosen to oversee the consensus process, unlike in a purely private blockchain where one entity retains full control.[531] This governing group decides who is granted access to the ledger, who is authorised to participate, and whether the blockchain should be publicly accessible or restricted to approved members. Typically, consortium blockchains are permissioned systems, widely used in international trade, where many participants prefer to keep their business information private and secure.[532]

4.4.2 Ex Ante Compliance in Private Chains vs. Public Chains

Can the distinction between private and public blockchain affect implementation of the GDPR? Indeed yes. The GDPR is expected to have a major impact on the architecture and governance structure of a private blockchain created by a particular organisation. This is due to the fact that private blockchains usually function under a more conventional governance framework, where data controllers are assigned certain duties. Consequently, more stringent adherence to the GDPR's ex ante[533] components, such as the idea of Data Protection by Design and by Default (DPbD),[534] is anticipated.[535] Rigorously, the emphasis on ex ante mechanisms, such as "data protection by design and by default," Data Protection Impact

[528] Herath et al., 2021, pp. 182–183.
[529] Boucher, P., Nascimento, S., Kritikos, M., (2017). *How blockchain technology could change our lives*. STOA, ISBN 978-92-846-0549-1, pp. 5–6. Available at: https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf, (Accessed: 15 September 2025).
[530] Solanki, A., Singh, A.K. and Tanwar, S. eds., (2023). *Blockchain Technology for IoE: Security and Privacy Perspectives*. CRC Press, ISBN: 978- 1- 032- 43174- 1 (hbk), pp. 47–48.
[531] *Ibid*.
[532] Buterin, V., (2015). *On Public and Private Blockchains*. Ethereum Blog. Available at: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains, (Accessed: 15 September 2025).
[533] Ex ante regimes rely on a system of prior approval by a regulatory authority.
[534] GDPR, Article 25; Recitals 78, 108.
[535] Yeung, K. and Bygrave, L.A., (2022). *Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship*. Regulation & Governance, 16(1), pp.137–155. Available at: https://www.researchgate.net/publication/351311905_Demystifying_the_modernized_European_data_protection_regime_Cross-disciplinary_insights_from_legal_and_regulatory_governance_scholarship, (Accessed: 15 September 2025).

Assessments (DPIAs),[536] and prior consultations with Data Protection Authorities (DPAs),[537] may require organisations to establish solid control and compliance management systems prior to initiating data processing activities for private blockchains, which frequently operate under more centralised governance structures.[538]

For permissionless public blockchains, the absence of a clearly identifiable controller can make compliance with the GDPR's ex-ante obligations, such as DPIAs,[539] data protection by design and by default,[540] and prior consultation,[541] operationally challenging, since these duties presuppose an accountable controller (or defined joint controllers) to perform them.[542] Furthermore, as required by the GDPR, determining whether particular processing operations constitute a "high risk" to fundamental rights may be difficult given the open and transparent character of public blockchains.[543]

The technical distinction between public and private blockchains forms a critical fault line when applied to the GDPR's regulatory framework. While private chains allow for well-defined governance, user access control, and accountability mechanisms,[544] public chains present a starkly different landscape: decentralised, pseudonymous, and governed by consensus rather than contract.[545] This divergence raises the question of whether traditional concepts of controllership and legal responsibility are adequate for distributed ledger technologies.[546]

[536] GDPR, Article 35.
[537] GDPR, Article 36.
[538] Finck, STOA Report, 2019, pp. 1–7.
[539] GDPR, Article 35.
[540] GDPR, Article 25.
[541] GDPR, Article 36.
[542] Article 29 Data Protection Working Party, (2017). G*uidelines on Data Protection Impact Assessment (DPIA) and determining whether*. WP 248 rev.01, pp. 6–7, 14–15, 18–19. Available at: https://ec.europa.eu/newsroom/article29/items/611236, (Accessed: 15 September 2025).
processing is "likely to result in a high risk" for the purposes of Regulation 2016/679
[543] Finck, M. Pallas, F. (2020). *They Who Must Not Be Identified — Distinguishing Personal from Non-Personal Data under the GDPR*. International Data Privacy Law, Volume 10, Issue 1, pp. 12–16. Available at: https://academic.oup.com/idpl/article/10/1/11/5802594, (Accessed: 15 September 2025).
[544] Finck, STOA Report, 2019, 1–7.
[545] Mulligan, C., Scott, J.Z., Warren, S. and Rangaswami, J.P., (2018). *Blockchain beyond the hype: A practical framework for business leaders*. In white paper of the World Economic Forum, pp. 3–8. Available at: https://www.weforum.org/publications/blockchain-beyond-the-hype/, (Accessed: 15 September 2025).
[546] Finck, Pallas, 2020, pp. 3–7.

Under GDPR, a controller is the entity that determines the purposes and means of processing personal data.[547] In private blockchains, this role typically falls to the central operator or the consortium governing the chain.[548] These entities often set the system parameters, define participation rules, and oversee data architecture.[549] They are thus capable of fulfilling GDPR duties such as providing data subject information,[550] conducting Data Protection Impact Assessments,[551] and embedding data protection by design and by default.[552]

In contrast, public permissionless chains lack a central governance body. No individual actor or node determines the purposes or means of data processing in a comprehensive way. The processing is collective, automated, and decentralised.[553] This raises the "many hands" problem: who is accountable when no one is fully in control? The European Data Protection Board has emphasised that decentralisation does not relieve actors of responsibility, yet it remains unclear how compliance duties can be operationalised when validator nodes, developers, and users all contribute to data processing without a formal or contractual hierarchy.[554]

Moreover, the immutability of public chains challenges core data protection rights; particularly the right to erasure under Article 17 GDPR. Once personal data (or pseudonymous data later deemed identifiable) is written to the ledger, erasure becomes practically impossible without breaking chain integrity. Legal scholars have questioned whether GDPR compliance is even achievable in such systems without significant governance or architectural innovation.[555] While private chains may align more readily with GDPR's accountability model, public chains remain a legal grey zone, necessitating a rethinking of compliance strategies and perhaps even regulatory adaptation.

[547] GDPR, Article 4(7).
[548] EDPB Guidelines 07/2020, pp. 27–33.
[549] Beck, R., Mueller-Bloch, C., (2018). *Governance in the Blockchain Economy: A Framework and Research Agenda*. Journal of the Association for Information Systems, 19(10):1020-1034, pp. 7–17. Available at: https://www.researchgate.net/publication/323689461_Governance_in_the_Blockchain_Economy_A_Framework_and_Research_Agenda, (Accessed: 15 September 2025).
[550] GDPR, Article 13.
[551] GDPR, Article 35.
[552] GDPR, Article 25.
[553] Werbach, K., (2018). *The Blockchain and the New Architecture of Trust*. The MIT Press. ISBN 9780262038935, Section 7, Blockchain Governance.
[554] Royakkers, L. and Sjoerd D.. Zwart, (2015). *Moral responsibility and the problem of many hands*. Routledge. ISBN: 978-1-138-83855-0 (hbk), pp. 50–62.
[555] Finck, 2018, pp. 17–19, 26–32.

The principle of data minimisation under Article 5(1)(c) GDPR requires that personal data be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.[556] This principle presents particular challenges in public blockchain environments, where transaction data is replicated across multiple distributed nodes in order to ensure integrity, transparency, and resilience of the ledger.[557] The Court of Justice of the European Union has consistently emphasised that EU data protection principles must be interpreted broadly in order to ensure effective protection of fundamental rights under Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.[558]

Once personal data is included in a blockchain transaction payload, it may be propagated and stored across numerous network participants, increasing both the volume and persistence of processed data and potentially conflicting with the requirement that personal data remain limited to what is necessary for the intended processing purpose.[559] Legal scholarship highlights that distributed ledger technologies inherently favour redundancy and immutability, characteristics which may complicate compliance with the principle of data minimisation where personal data is recorded directly on-chain.[560] Consequently, the inclusion of personal data in blockchain transaction structures may create tensions with Article 5(1)(c) GDPR, particularly where replication across nodes results in increased exposure, persistence, and potential re-identification risks.[561]

4.4.3 Permissioned vs Permissionless Models

A blockchain is considered “permissionless” when all nodes are unknown. It is referred to as a consortium blockchain or “permissioned” when every writing node is known.[562] Complementary to public blockchains, private blockchains allow for the immutable sharing and storing of data in the order in which it is generated. Solely, the method used to reach a

[556] GDPR, Article 5(1)(c), Recital 39;
[557] Finck, 2019, pp. 35–39; EU Blockchain Observatory and Forum, (2019). *Blockchain and digital identity*. Luxembourg: Publications Office of the European Union, pp. 12–14, 15–18. Available at: https://blockchain-observatory.ec.europa.eu/publications/blockchain-and-digital-identity_en, (Accessed: 31 March 2025).
[558] Digital Rights Ireland, C-293/12, para 38; see also, Court of Justice of the European Union, (2016). *Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Watson*. ECLI:EU:C:2016:970, paras 96–103, 108–111. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62015CJ0203, (Accessed: 31 March 2026).
[559] WP216, Opinion 05/2014, 2014, pp. 10–13; EDPB Guidelines 07/2020, pp. 18–21.
[560] Zetzsche et al., 2020, Decentralized Finance, pp. 12–15, 17–18. Haque Bappy, F., Cheon, E. and Islam, T., (2025). *Centralized Trust in Decentralized Systems: Unveiling Hidden Contradictions in Blockchain and Cryptocurrency*. arXiv e-prints, arXiv-2505, ACM ISBN 979-8-4007-1482-5/25/06, pp. 7–10. Available at: https://dl.acm.org/doi/pdf/10.1145/3715275.3732130, (Accessed: 31 March 2026).
[561] EDPB Guidelines 07/2020, pp. 18–21.
[562] Solanki et al., 2023, pp. 48–49.

consensus is different.[563] Permissioned blockchains have the potential to outperform missionless blockchains in terms of performance and operating costs, but it is typically believed that this comes at the expense of transaction security, particularly in low-trust contexts.[564]

The permission structure of a blockchain network is more than a matter of performance or architecture, it is legally decisive in determining how the GDPR applies.[565] In permissioned systems, participants are typically known in advance, and access to writing or validating blocks is restricted by governance rules.[566] These features allow for more traditional forms of controllership under Article 4(7) GDPR, since the consortium or managing entity can often be identified as determining the "purposes and means" of processing.[567] In such cases, a specific legal person or group of actors may bear full responsibility for GDPR compliance, including transparency obligations, legitimate basis for processing, and mechanisms for redress.

By contrast, permissionless blockchains, which lack central administration and allow unrestricted participation, challenge the GDPR's underlying assumption that a centralised or at least identifiable controller must exist.[568] In such networks, no single entity initiates, structures, or directs the processing in a manner that would traditionally qualify as "determining the purposes and means of processing" under Article 4(7) GDPR.[569] Instead, each participant, whether node operator, user, or miner, plays only a partial technical role, and no one actor exercises comprehensive control.[570] This dispersion of agency undermines the accountability principle enshrined in Article 5(2) GDPR and epitomises the classic "problem of many hands": how can legal responsibility be allocated when decision-making and control are simultaneously shared, fragmented, and fluid?

[563] Godfrey-Welch et al., 2018, pp. 3–7.
[564] Bakos, Y., Halaburda, H., (2021). *Tradeoffs in Permissioned vs Permissionless Blockchains: Trust and Performance*. pp. 1–4. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3789425, (Accessed: 15 September 2025); see also, Strehle, E., (2020). *Public Versus Private Blockchains*. Blockchain Research Lab, BRL Working Paper Series No. 14, pp. 1–8. Available at: https://www.blockchainresearchlab.org/wp-content/uploads/2020/05/BRL-Working-Paper-No-14-Public-vs-Private-Blockchains.pdf, (Accessed: 15 September 2025).
[565] Finck, 2018, pp. 22–23.
[566] Finck, STOA Report, 2019, pp. 28–30.
[567] EDPB Guidelines 07/2020, paras 15–41.
[568] Finck, 2018, pp. 17–19, 27.
[569] EDPB Guidelines 07/2020, paras 15–41.
[570] Finck, STOA Report, 2019, pp. 44–47.

Furthermore, there are significant differences between the two models' legal foundations for processing. Under Article 6(1)(b) and (f) GDPR, permitted blockchains may rely on contractual necessity or justifiable interest as long as the necessary precautions are taken.[571] However, in permissionless environments, users typically do not have a direct relationship with data subjects and therefore cannot satisfy the standard conditions for valid consent under Article 6(1)(a) GDPR.[572] In cases where personal data is processed, such as wallet identifiers that may later be linked to real-world identities, it becomes increasingly difficult to demonstrate any lawful basis for on-chain activities.[573]

4.4.4 Peer-to-Peer Network and Consensus Mechanisms

4.4.4.1 Peer-to-Peer (P2P) Network Architecture

In a peer-to-peer (P2P) network, participants communicate and transact directly, eliminating the need for intermediaries to manage confirmation or verification processes.[574] A P2P network is a distributed system composed of individual computers referred to as nodes. These nodes make their computational resources (such as processing power and storage) available to other participants.[575] In terms of their rights and functions inside the system, nodes are equal to one another. Without any kind of coordination or control, every node in these totally distributed P2P networks carries out the same functions, serving as both a providers and a consumer of resources and services.[576] Given that the P2P system employs Blockchain as a mechanism to attain and preserve integrity in a trustless environment, P2P and Blockchain are linked.[577]

The peer-to-peer (P2P) nature of blockchain networks introduces profound structural challenges to data protection law, particularly with regard to the attribution of legal

[571] Kuner et al., 2020, pp. 45–48.
[572] *Ibid*.
[573] Werbach, 2018, Section 6, Centralized Edge Providers.
[574] Drescher, 2017, Section 2, Distributed Peer-to-Peer Systems.
[575] Werbach, K. and Cornell, N., (2017). *Contracts ex machina*. Duke Law Journal, Vol: 67:313, p.327. Available at: https://scholarship.law.duke.edu/dlj/vol67/iss2/2/, (Accessed: 15 September 2025).
[576] Schollmeier, R., (2001). *A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications.* In Proceedings first international conference on peer-to-peer computing, IEEE, pp. 101–102, IEEE. Available at: https://www.researchgate.net/publication/3940901_A_Definition_of_Peer-to-Peer_Networking_for_the_Classification_of_Peer-to-Peer_Architectures_and_Applications, (Accessed: 15 September 2025).
[577] Raskin, M., Yermack, D. (2016) *Digital Currencies, Decentralized Ledgers, and the Future of Financial Services*. New York: NYU Stern, pp. 474–477, in Conti-Brown, P., Lastra, R.M. (eds.) Raskin, M., Yermack, D. (2016) *Digital Currencies, Decentralized Ledgers, and the Future of Financial Services*. New York: NYU Stern, pp. 474–477, in Conti-Brown, P., Lastra, R.M. (eds.) Research Handbook on Central Banking. Cheltenham: Edward Elgar Publishing.

responsibility.[578] Unlike client-server models, where a single entity can typically be designated as the controller under Article 4(7) GDPR, P2P networks rely on a multiplicity of autonomous nodes that independently validate, broadcast, and store transactions.[579] Each node is simultaneously a consumer and provider of services, with no formal hierarchy or central coordination.[580] In legal terms, this architecture creates what some scholars describe as a "polycentric" processing environment, one in which control over data is fragmented and fluid.[581]

This technical decentralisation clashes with the GDPR's normative structure, which presupposes centralised accountability and purposive processing.[582] The European Data Protection Board has repeatedly stated that the designation of a data controller depends not on formal status but on who determines the purposes and means of processing.[583] In a P2P blockchain, however, this question is exceptionally difficult to answer. Validators and full nodes process data as part of a protocol rather than a conscious legal choice, and their actions are automated by consensus mechanisms rather than determined by human intent.[584] This raises the question of whether processing can occur in the absence of a clearly accountable actor, and if so, whether the GDPR can apply at all in such contexts.[585]

4.4.4.2 Consensus Mechanisms in Blockchain Networks

Because blockchains are distributed across many nodes without central authority, the network needs some way to agree on what the valid state of the ledger is. This is what consensus mechanisms do. The two most common approaches are Proof of Work (PoW) and Proof of Stake (PoS), though variations and hybrid models exist.

[578] Werbach, Cornell, 2017, pp. 378–380.
[579] Kuner et al., 2020, pp. 37–40.
[580] Beck, Mueller-Bloch, 2018, pp. 6–12.
[581] European Data Protection Board, (2019). *Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities*. paras 37–47, 63–70, 79–85.
[582] Finck, 2018, pp. 17–18, 26–27, 32–33.
[583] EDPB Guidelines 07/2020, para 14.
[584] Werbach, Cornell, 2017, pp. 420–425.
[585] Zetzsche, D., A., Buckley, R., P., Arner, D., W., (2019). T*he ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators*. Volume, 60. Number 2. Harvard International Law Journal, pp. 279–293. Available at: https://journals.law.harvard.edu/ilj/wp-content/uploads/sites/84/3_ICO_60.2.pdf, (Accessed: 15 September 2025); see also, WP169, Opinion 1/2010, 2010, pp. 17–25.

Proof of Work, used by Bitcoin and formerly by Ethereum, requires nodes called miners to compete to solve computationally difficult puzzles.[586] The first miner to find a valid solution gets to add the next block to the chain and receives a reward (newly created cryptocurrency plus transaction fees). Other nodes verify the solution and accept the new block. This mechanism makes it expensive to attack the network because you'd need enormous computational resources. But it also consumes vast amounts of electricity, which has prompted substantial environmental criticism and regulatory concern.[587]

Proof of Stake, which Ethereum now uses, takes a different approach. Instead of computational puzzles, validators are selected to propose new blocks based on how much cryptocurrency they've locked up (their 'stake').59 The more you stake, the higher your chances of being selected. If you propose an invalid block or act maliciously, you lose part of your stake. This is much more energy-efficient than PoW but introduces different security considerations. For legal purposes, the main point is that both mechanisms achieve the same outcome: they enable a distributed network to agree on a single version of the ledger without requiring any central coordinator. This means there's no entity with unilateral power to modify or delete data from the blockchain, which is precisely what creates problems for data protection compliance.

Moreover, distributed consensus mechanisms, while critical for trustless validation, further obscure the locus of legal authority. In Proof-of-Work or Proof-of-Stake systems, the selection of block validators is probabilistic or algorithmic, meaning that data processing responsibilities rotate unpredictably among pseudonymous actors.[588] This undermines the predictability and stability required for effective regulatory oversight.[589] Data subjects cannot easily identify which node processed their personal data, nor can they exercise their rights under Articles 15–22 GDPR if no contact point exists.[590]

Some scholars suggest that all nodes in a permissionless blockchain should be treated as joint controllers, a view that draws support from the Court of Justice of the European Union in

[586] Nakamoto, 2008, 3–4.
[587] De Vries A., (2018). *Bitcoin's Growing Energy Problem*. Joule, 2(5), pp. 801-809. Available at: https://www.researchgate.net/publication/325188032_Bitcoin's_Growing_Energy_Problem, (Accessed: 10 January 2026).
[588] Narayanan et al., 2016, pp. 151–155.
[589] Finck, 2018, pp. 26–27.
[590] EDPB Guidelines 07/2020, paras 18–21.

Wirtschaftsakademie Schleswig-Holstein[591] and Fashion ID case,[592] which interpreted joint controllership broadly to include actors that merely influence data processing without full control. Yet this approach has significant drawbacks: it risks overextending liability to individuals or entities with no real decision-making power, thereby discouraging participation in open-source or decentralised networks.[593]

Others advocate for technical mitigations, such as off-chain processing, data minimisation, or strong encryption of on-chain entries, to reduce the identifiability of personal data.[594] However, these approaches remain experimental and provide only limited relief in highly transparent systems, where even pseudonymous identifiers can become personal data once linked with auxiliary datasets.[595]

In conclusion, while P2P systems enable decentralised innovation and data integrity, they expose critical gaps in the GDPR's accountability regime. Without a recognisable controller or processor, enforcement becomes impractical, and data subjects may be left without effective remedies. This suggests the need for either regulatory innovation or judicial interpretation that can adapt legal norms to polycentric infrastructures; a theme that will be explored further in subsequent sections.

4.5 Blockchain Actors and Accountability Frameworks

The distributed ledger is stored by nodes, which are the component of the blockchain network that enable validation of the single immutable ledger dispersed over numerous local storage facilities.[596] Typically, nodes are numerous and dispersed throughout a large geographic area.[597] Although there is considerable overlap between users and nodes, not every user downloads the entire ledger since permissionless blockchains usually have high download sizes.[598] This fragmentation and decentralisation of network participation presents a

[591] Wirtschaftsakademie Schleswig-Holstein, Case C-210/16, paras 35–43.
[592] Fashion ID, Case C-40/17, paras 68–75.
[593] Kuner et al., 2020, pp. 221–226.
[594] Edwards, L., Veale, M. (2017). *Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For*. Duke Law & Technology Review, Volume 16, Number 1, pp. 77–80. Available at: https://scholarship.law.duke.edu/dltr/vol16/iss1/2/, (Accessed: 15 September 2025).
[595] GDPR, Recital 26, Article 4(1)(5); Breyer v Bundesrepublik Deutschland, C-582/14, paras 43–49; see also, WP216, Opinion 05/2014, 2014, pp. 7–12, 20–21.
[596] Mougayar, 2016, pp. 1–3; see also, Drescher, 2017, Section 2, Distributed Peer-to-Peer Systems.
[597] Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. Sebastopol: O'Reilly Media, sections d. What Is the Blockchain? and e. The Connected World and Blockchain: The Fifth Disruptive Computing Paradigm.
[598] BitcoinCore, (2025). *Running A Full Node. Support the Bitcoin network by running your own full node.* Available at: https://bitcoin.org/en/full-node - setup-a-full-node, (Accessed: 15 September 2025); see also,

significant challenge for data protection law, particularly regarding the attribution of responsibility.[599] To evaluate the legal position of blockchain actors under the GDPR, it is necessary to distinguish between key functional roles: full nodes, miners/validators, end-users, smart contract developers, and, potentially, governance entities.

4.5.1 Validators, Nodes, and Governance Entities

Full nodes are actors who store a complete and up-to-date copy of the blockchain and participate in the validation of transactions.[600] In Proof-of-Work systems like Bitcoin, these are often miners;[601] in Proof-of-Stake systems, they function as validators or staking entities.[602] Their primary legal significance lies in their role in endorsing and preserving personal data on the ledger.[603]

If a transaction contains personal data, whether directly or by way of pseudonymous identifiers, then storing and verifying that data may constitute processing under Article 4(2) GDPR.[604] As such, full nodes arguably qualify as data processors, or potentially joint controllers, depending on their level of autonomy and coordination with other actors.[605]

YCHARTS, (2025). *Bitcoin Blockchain Size (I:BBS)*. Available at: https://ycharts.com/indicators/bitcoin_blockchain_size, (Accessed: 15 September 2025); see also, Newman, D., (2025). *Light vs Full vs Archive Ethereum Nodes*. GETBLOCK, Available at: https://getblock.io/blog/light-vs-full-vs-archive-ethereum-nodes, (Accessed: 15 September 2025).

[599] Beck, Mueller-Bloch, 2018, pp. 33–36.

[600] Glaser, 2017, Pervasive Decentralisation of Digital Infrastructures, pp. 1545–1546.

[601] Wörner, D., Von Bomhard, T., Schreier, Y.P. and Bilgeri, D., (2016). *The bitcoin ecosystem: Disruption beyond financial services?* Twenty-Fourth European Conference on Information Systems (ECIS), İstanbul,Turkey, pp. 2–4. Available at: https://www.resvearchgate.net/publication/317304739_The_Bitcoin_Ecosystem_Disruption_Beyond_Financial_Services, (Accessed: 17 September 2025).

[602] Tschorsch, F., Scheuermann, B., (2016). *Bitcoin and beyond: A technical survey on decentralized digital currencies*. IEEE Communications Surveys & Tutorials, 18(3), pp. 2084–2123. Section 6.3 Proof of Stake—Towards Solving Incentive Problems. Available at: https://eprint.iacr.org/2015/464.pdf, (Accessed: 17 September 2025).

[603] Finck, 2018, pp. 18–20.

[604] GDPR, Article 4(2); see also,

[605] Michalski, R., Dziubałtowska, D., Macek, P., (2020). *Revealing the character of nodes in a blockchain with supervised learning*. Ieee Access, 8, pp. 109639-109647. Available at: https://www.researchgate.net/publication/342112597_Revealing_the_Character_of_Nodes_in_a_Blockchain_With_Supervised_Learning, Accessed: 17 September 2025); see also, Conte de Leon, D., Stalick, A.Q., Jillepalli, A.A., Haney, M.A., Sheldon, F.T., (2017). *Blockchain: properties and misconceptions*. Asia Pacific Journal of Innovation and Entrepreneurship, 11(3), pp. 286–300.
Available at: https://www.researchgate.net/publication/321811785_Blockchain_properties_and_misconceptions, (Accessed: 17 September 2025).

However, node operators typically lack meaningful control over the inclusion or erasure of data.[606] Their activity is automated and governed by consensus protocols, not individual choice.[607] This raises the question of whether responsibility under GDPR should attach even in the absence of purposive processing.[608] The accountability regime of GDPR, according to some commentators, requires a centralised actor with discretionary power, which is difficult to achieve in decentralised systems.[609]

Nevertheless, the right to erasure is in direct opposition to the immutability of the ledger, which is a key characteristic of blockchain technology.[610] Prior blocks cannot be removed by validators without rendering the chain invalid.[611] Therefore, it would seem that either (a) technical solutions like off-chain storage and encryption-based "erasure" or (b) a fundamental rethinking of GDPR application to decentralised systems are required for legal compliance.[612]

Despite the decentralisation rhetoric, many blockchain networks include governance entities, such as foundations, DAOs (Decentralised Autonomous Organisations),[613] or core development teams.[614] These bodies may steer protocol updates, coordinate marketing, allocate funding, or act as public faces of the network.[615]

Where such bodies exercise de facto control over network operations, for example, by maintaining repositories, managing validator permissions, or controlling treasury functions,

[606] Zhou, R., (2023). *Research on the Development of the Digital Economy based on Blockchain Technology*. Iris Online Journal of Arts and Social Sciences, Volume 1, Issue 2, ISSN: 2837-4509, pp. 1–9. Available at: https://www.researchgate.net/publication/370759632_Research_on_the_Development_of_the_Digital_Economy_based_on_Blockchain_Technology, (Accessed: 17 September 2025); see also, Nakamoto, 2008, Bitcoin: A Peer-to-Peer Electronic Cash System.
[607] Werbach, 2018, Introduction: The Parable of the Tree.
[608] Kuner et al., 2020, pp. 195–200.
[609] Wright, A., Filippi, P., D., (2018). *Blockchain and the Law. The Rule of Code*. Harvard Universtity Press, ISBN 9780674976429, pp. 89–94.
[610] GDPR, Article 17; see also, Pollicino, O., De Gregorio, G. & Bassini, M. (2021). *Blockchain and Public Law: Global Challenges in the Era of Decentralisation*. Edward Elgar, ISBN 978 1 83910 079 6, pp. 1–11.
[611] Raskin, Yermack, 2016, pp. 476–477.
[612] Zyskind, G., Nathan, O., (2015). *Decentralizing privacy: Using blockchain to protect personal data*. In 2015 IEEE security and privacy workshops (pp. 180-184). IEEE. Available at: https://ieeexplore.ieee.org/document/7163223, (Accessed: 17 September 2025).
[613] A DAO is a blockchain-based governance structure where rules are encoded in smart contracts, and decisions (e.g., funding allocations or protocol changes) are typically made collectively by token-holders through on-chain voting. DAOs are designed to operate without centralized management, though in practice their effectiveness and degree of decentralisation vary.
[614] These are groups of software developers who maintain and improve the underlying blockchain protocol. They may propose updates, fix vulnerabilities, and guide the technical roadmap. While they often lack formal legal authority, their technical expertise and control over reference implementations give them significant influence within the ecosystem. See Wright, Filippi, 2018, pp. 133–145, 146–155.
[615] Werbach, 2018, Section 3 More than Money.

they may be designated as data controllers or joint controllers under GDPR.[616] This interpretation is supported by the functional approach endorsed by the CJEU in Jehovah's Witnesses and Wirtschaftsakademie, which emphasised that controller status can be shared and need not be based on formal legal authority.[617]

However, identifying and enforcing obligations against such entities may be constrained by their legal form. DAOs often lack corporate personality and operate across jurisdictions with unclear legal accountability.[618] The absence of legal personhood complicates the application of administrative fines under Article 83 GDPR and challenges the practical reach of data protection authorities.[619]

4.5.2 Developers and End-Users

At the other end of the chain are end-users: individuals or entities that initiate transactions, interact with smart contracts, or send or receive tokens.[620] Depending on the use-case, these users may input personal data into the blockchain, intentionally (e.g., digital identity platforms) or incidentally (e.g., wallet addresses that can be tied to natural persons).[621] As discussed in Section 4.1, wallet providers may themselves qualify as controllers where they influence the processing of associated off-chain personal data.

A key legal issue here is the controller status of users. If a natural or legal person determines the purposes and means of data processing, for instance, by deploying a smart contract that records others' data;[622] they may qualify as a data controller under Article 4(7) GDPR.[623] The

[616] Cirone, E., (2021). *Blockchain and the General Data Protection Regulation: an irreconcilable regulatory approach?* Queen Mary Law Journal, Collections 38 and 51, pp. 29–30, 30–31. Available at: https://qmro.qmul.ac.uk/xmlui/handle/123456789/73939, (Accessed: 17 September 2025).
[617] Wirtschaftsakademie Schleswig-Holstein, Case C-210/16, paras 35–39; see also, Kuner et al., 2020, pp. 37–40.
[618] Hacker, P., Thomale, C., (2018). *Crypto-securities regulation: ICOs, token sales and cryptocurrencies under EU financial law*. European Company and Financial Law Review, 15(4), pp. 10–12. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3075820, (Accessed: 17 September 2025).
[619] GDPR, Article 83; see also, Finck, 2018, pp. 26–29.
[620] Schär, F., (2021). *Decentralized Finance: On Blockchain- and Smart Contract-based Financial Markets*. SSRN, pp. 1–3, 6–12. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3571335, (Accessed: 17 September 2025).
[621] Finck, STOA Report, 2019, pp. 1–5.
[622] Fischer, M.J., Lynch, N.A., Paterson, M.S., (1985). *Impossibility of distributed consensus with one faulty process*. Journal of the ACM (JACM), 32(2), pp. 374-382. Available at: https://groups.csail.mit.edu/tds/papers/Lynch/jacm85.pdf, (Accessed: 17 September 2025).
[623] GDPR, Article 4(7).

EDPB has emphasised that technical neutrality does not exempt actors from liability: the legal status depends on functional behaviour, not the underlying technology.[624]

That said, where individuals use blockchain in a purely personal or household capacity (e.g., peer-to-peer payments), they may benefit from the household exemption under Article 2(2)(c) GDPR.[625] However, the exemption is narrow, and does not apply where the processing is made public or affects others' rights.[626] In decentralised systems, where transparency is foundational, this exemption may rarely apply in practice.[627]

EU data protection law adopts a functional approach to controllership, meaning that qualification does not depend on formal legal designation but on the factual influence exercised over the purposes and means of processing.[628] The Court of Justice of the European Union has consistently emphasised that controllership may arise where an actor exerts practical influence over data processing operations, even where such influence is indirect or shared among multiple participants.[629] The Court has further clarified that joint controllership may exist where several actors participate in determining the conditions under which processing takes place, even if their levels of involvement differ.[630] Legal scholarship confirms that the GDPR deliberately adopts a broad notion of control in order to ensure effective protection of fundamental rights in complex technological ecosystems characterised by distributed decision-making structures.[631]

This functional interpretation is particularly relevant in decentralised blockchain environments, where technical architecture, consensus mechanisms, and governance protocols may influence how personal data is validated, stored, and made accessible, even in

[624] WP169, Opinion 1/2010, 2010, pp. 3–9.
[625] GDPR, Article 2(2)(c).
[626] Jehovan todistajat, Case C-25/17, paras 41–43.
[627] Wachter, S., Mittelstadt, B., (2019). *A right to reasonable inferences: re-thinking data protection law in the age of big data and AI*. Columbia Business Law Review, Volume 2019, Issue 2, pp. 59–69. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829, (Accessed: 17 September 2025).
[628] GDPR, Article 4(7); EDPB Guidelines 07/2020, paras 20–28.
[629] Wirtschaftsakademie Schleswig-Holstein, Case C-210/16, paras 28–30, 35, 43; Fashion ID, Case C-40/17, paras 67–70, 74, 79; Jehovan todistajat, Case C-25/17, paras 66–71.
[630] Wirtschaftsakademie Schleswig-Holstein, Case C-210/16, paras 29–30, 35, 38, 40, 43; Fashion ID, Case C-40/17, paras 67–69, 74,79.
[631] GDPR Commentary, pp. 102–105; Lynskey, 2015, pp. 79–88; see also, Hijmans, H., (2016). *The European Union as Guardian of Internet Privacy*. The Story of Art 16 TFEU. Law, Governance and Technology Series 31, Volume 31, ISBN 978-3-319-34090-6, pp. 147–152.

the absence of traditional hierarchical organisational structures.[632] Accordingly, actors participating in the design or operation of blockchain-based systems may qualify as controllers where they exercise factual influence over the determination of processing purposes or essential technical means, including decisions embedded in software architecture or protocol governance.[633]

The analysis above demonstrates that decentralised architectures do not eliminate legal responsibility but instead redistribute factual influence across multiple actors and technical layers. This redistribution complicates the application of traditional GDPR categories, particularly in relation to the right to erasure under Article 17. Chapter 5 therefore examines whether the concept of effective forgetting can provide a legally coherent interpretation of erasure obligations in blockchain-based processing environments.

Chapter 5. Effective Forgetting in Blockchain Systems: Wallet Providers as a Case Study

This chapter addresses the dissertation's first research question by: (i) distinguishing wallet architectures and their associated processing operations; (ii) identifying where controllership attaches in practice; and (iii) translating Article 17 into an architecture-sensitive rubric of "effective forgetting" measures.

This chapter advances the central doctrinal contribution of the dissertation by proposing the concept of effective forgetting as a legally coherent method for operationalising Article 17 GDPR within decentralised technological environments. While prior scholarship has frequently described blockchain architectures as structurally incompatible with the right to erasure, this chapter demonstrates that the apparent incompatibility arises primarily from an overly literal interpretation of deletion. By distinguishing between the persistence of on-chain

[632] De Caria, 2020, pp. 29–34; Gstrein, O.J. and Kochenov, D., (2020). *Digital identity and distributed ledger technology: Paving the way to a neo-feudal brave new world?*. Frontiers in Blockchain, Blockchain for Good, Volume 3, pp. 1–8.
Available at: https://www.frontiersin.org/journals/blockchain/articles/10.3389/fbloc.2020.00010/full, (Accessed: 31 March 2026); see also, Atzori, 2017, pp. 6–11.
[633] EDPB Guidelines 07/2020, paras 20–21, 38–44, 48–55; Finck, 2019, pp. 41–47.

records and the controllability of off-chain and interface-level data processing, the analysis shows that erasure can be functionally realised through measures that reduce identifiability, accessibility, and linkability of personal data. Wallet providers are examined as the primary operational actors through which such measures can be implemented in practice, but the doctrinal implications extend more broadly to the interpretation of controllership and erasure obligations across decentralised data ecosystems. The chapter therefore establishes an architecture-sensitive framework capable of preserving the normative objectives of EU data protection law despite the technical constraints of distributed ledger systems. Beyond its operational dimension, the framework also contributes to ongoing discussions concerning the adaptation of EU data protection law to decentralised technological environments, particularly with regard to how legal responsibility may be distributed across actors who collectively influence the accessibility and interpretability of personal data.

Over the past decade, payment methods have shifted dramatically alongside broader economic change and rapid digitisation.[634] Among the most consequential developments is the rise of cryptocurrencies.[635] Since Bitcoin's 2008 debut, a succession of cryptoassets has emerged, expanding well beyond simple payments to programmable functionality and new financial primitives.[636] Business models that scarcely existed ten years ago now operate at scale, illustrating a wider trend of digitalisation across sectors. In payments specifically, cryptocurrencies moved from a niche idea to a global phenomenon within just a few years.[637] For most people, Bitcoin remains the defining reference point in cryptocurrency: from its early days, it has shaped the market, with long-term holders often reaping significant wealth through multiple market cycles, much like the guests at Morehead's house,[638] where Bitcoin's potential to transform wealth and disrupt the status quo was already evident, despite the skepticism and crises it faced along the way.[639]

[634] Casey et al., 2018, pp. 9–15.
[635] Burniske et al., 2017, pp. 32–35.
[636] *Ibid*.
[637] McDonald, O., (2021). *Cryptocurrencies: MONEY , TRUST AND REGULATION*. ISBN 978-1-78821-420-9, Agenda Publishing, Chapter 2, New cryptocurrencies and new developments.
[638] The reference is to Dan Morehead, founder of Pantera Capital, one of the earliest and most influential Bitcoin investment firms. In Digital Gold (2015), Nathaniel Popper describes a gathering at Morehead's house in California, where a number of early Bitcoin adopters, investors, and entrepreneurs met during Bitcoin's formative years.
[639] Popper, N., (2015). Digital gold : *Bitcoin and the inside story of the misfits and millionaires trying to reinvent money*. New York, NY : Harper, an Imprint of HarperCollins Publishers, pp. 4–10. Available at: http://repo.darmajaya.ac.id/4146/1/Digital Gold_ Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money %28 PDFDrive %29.pdf, (Accessed: 12 October 2025).

Cryptocurrency networks are accessed through blockchain-based wallets (BWs); software or hardware tools that let users send and receive cryptocurrencies, digital assets, and tokens.[640] These wallets supply the secure interface to the chain: they generate and manage private keys that are cryptographically linked to public keys/addresses.[641] Public keys (or their encoded hashes) serve as addresses for receiving value, while private keys authorise control via digital signatures.[642] Because blockchains maintain an immutable, distributed ledger of transactions, BWs differ fundamentally from traditional, centrally managed digital wallets: they operate without a single controlling authority and interact directly with decentralised networks.[643]

The chapters that follow position wallet providers as the user-facing access layer; distinct from protocol actors through which keys are generated, transactions are authorised, and dApps are reached.[644] As hybrid entities, they are both technical gateways and legal subjects, making them the "low-hanging fruit" for oversight in polycentric systems.[645] The discussion proceeds by mapping their anatomy, custodial versus non-custodial, hot versus cold, and across web, mobile, desktop, hardware, smart-contract, and organisational variants, and analysing how each manages personal data; and, where applicable, KYC/AML datasets. The study advances the notion of effective forgetting for blockchain wallets and outlines a compliance framework that situates wallet providers as key agents of accountable privacy. This focus reflects the broader governance question of how compliance obligations may be allocated in polycentric technical environments where multiple actors influence the lifecycle of personal data through layered infrastructural design.

---

[640] Antonopoulos , 2015, pp. 84–89.

[641] Koch, R., (2024). *Cryptocurrency Basics for Litigators*. TECHNOLOGY IN THE LAW PRACTICE, pp. 18–21. Available at: https://cl.cobar.org/wp-content/uploads/2024/08/SeptOct2024-Tech.pdf, (Accessed: 12 October 2025).

[642] Jokić, S., Cvetković, A., S., Adamović, S., Ristić, N., Spalević, P., (2019). *Comparative Analysis of Cryptocurrency Wallets vs Traditional Wallets*. ISSN 0350-137X, EISSN 2334-9190, UDK 338 (497,1), pp. 66–67. Available at: https://www.researchgate.net/publication/336871260_Comparative_analysis_of_cryptocurrency_wallets_vs_traditional_wallets, (Accessed: 12 October 2025).

[643] Bandara, T., (2024). *Blockchain Technology in International Trade: Legal and Regulatory Implications.* ResearchGate, pp. 1–2. Available at: https://www.researchgate.net/publication/381461735_Blockchain_Technology_in_International_Trade_Legal_and_Regulatory_Implications, (Accessed: 12 October 2025).

[644] Kersic, V., Vidovic, U., Vrecko, A., Domajnko, M. and Turkanovic, M., (2023). *Orchestrating digital wallets for on-and off-chain decentralized identity management*. IEEE access, 11, pp. 1–9. Available at: https://www.researchgate.net/publication/372662346_Orchestrating_Digital_Wallets_for_On-_and_Off-chain_Decentralized_Identity_Management, (Accessed: 12 October 2025).

[645] Deloitte Touche Tohmatsu Limited, (2022). *Blockchain: Legal implications, questions, opportunities and risks*. CoRe Creative Services. RITM1153882., pp. 3, 6–7, 14. Available at: https://www.deloitte.com/content/dam/assets-shared/legacy/docs/dttl-tax-global-blockchain-wp-sept-20221.pdf, (Accessed: 12 October 2025).

Crucially, this section positions wallet providers as the primary point at which the Right to be Forgotten can be operationalised in decentralised systems. While blockchain protocols cannot alter or delete on-chain entries, controllership under the GDPR attaches to the actors who deploy applications, rather than to the underlying infrastructure.[646] Drawing on Moerel's argument that controllership depends on a technology's specific deployment, wallet providers are the entities that structure, associate, retain, and present personal data to users.[647] Their proximity to the end-user and their control over off-chain data flows render them the only actors able to implement measures approximating erasure.[648] The analysis therefore illustrates how effective forgetting operates not only as a technical compliance strategy, but also as a doctrinal framework capable of guiding the interpretation of controllership within distributed data ecosystems.

5.1 Wallet architectures and data processing roles

This section fulfils the first analytical step of the chapter by distinguishing wallet architectures according to their technical design and associated personal data processing operations.

Blockchain wallets are commonly understood as cryptographic tools for key generation and transaction authorisation.[649] Yet, within the legal and regulatory context of the GDPR, they must be conceptualised not merely as software artefacts but as organisational actors whose technical design determines the nature, extent, and legal classification of personal data processing.[650] Accordingly, this section develops a typology of wallet providers that distinguishes custodial from non-custodial architectures,[651] active key management from passive interface provision, and online from offline storage models. This typology is essential

[646] Moerel, L. (2020). *Blockchain and data protection*. In L. A. DiMatteo, M. Cannarsa, & C. Poncibò (Eds.), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*. pp. 217–218. Cambridge University Press.
[647] *Ibid*.
[648] Narayanan et al., 2016, pp. 112–114.
[649] Huang, K., Budorin, D., Tan, L. JY., Ma, W. & Zhang, Z. W. (eds.) 2023. *A Comprehensive Guide for Web3 Security. From Technology, Economic and Legal Aspects.* Chapter 3.2 How Blockchain Wallets Work. Future of Business and Finance. Springer Nature Switzerland. ISBN 978-3-031-39287-0. Available at: https://doi.org/10.1007/978-3-031-39288-7, (Accessed: 11 November 2025).
[650] Guri, M. 2018. *BeatCoin: Leaking private keys from air-gapped cryptocurrency wallets*. arXiv:1804.08714 arXiv. Available at: https://arxiv.org/pdf/1804.08714, (Accessed: 11 November 2025).
[651] Cryptopedia Staff, 2025. *Custodial vs. Non-Custodial Wallets*. Cryptocurrency Wallets. Available at: https://www.gemini.com/en-GB/cryptopedia/crypto-wallets-custodial-vs-noncustodial, (Accessed: 11 November 2025).

to analysing the extent to which different wallet designs can support a standard of "effective forgetting," given that each model entails distinct data flows, degrees of controllership, and technical constraints.

5.1.1 Custodial Wallet Providers

Custodial wallets are operated by centralised service providers, typically exchanges or payment platforms, that generate, store, and manage users' private keys on their behalf.[652] In this model, the user does not exercise exclusive control over the cryptographic credentials; rather, the provider functions as a digital fiduciary, maintaining full access to the private keys that authorise blockchain transactions.[653] As Narayanan et al. observe, custodial systems reproduce the traditional trust model of the Internet by re-introducing a central authority that mediates access to decentralised networks.[654]

From a data protection perspective, custodial wallet providers are best understood as data controllers within the meaning of Article 4(7) GDPR, since they centrally determine the purposes and means of processing both on-chain–adjacent and off-chain data, such as KYC/AML information and transactional records, linked to blockchain addresses.[655] In practice, this typically extends to transaction metadata, IP logs, device identifiers and records of user interactions. Their legal position is reinforced by the EU AML/CFT regime, particularly the Transfer of Funds and Crypto-Assets Regulation (TFR), which mandates the collection, retention, and disclosure of identifiable personal data.[656] Because custodial providers determine the purposes and means of these processing activities, they bear the full spectrum of GDPR obligations, including those associated with erasure under Article 17.[657]

The implication for "effective forgetting" is twofold. First, custodial providers possess substantial control over off-chain repositories and can implement erasure, suppression, or

[652] Seymour, T., Goodell, G., (2024). *Custodial and Non-Custodial Wallets*. Manuscript. arXiv. Available at: https://arxiv.org/pdf/2409.15389, (Accessed: 11 November 2025).
[653] Zetzsche, D.A., Nikolakopoulou, A. 2024. *Crypto Custody and Crypto Wallets – An Empirical Assessment*. FutureFinTech Working Paper Series, SSRN, pp 12–13. http://dx.doi.org/10.2139/ssrn.4769396. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4769396&download=yes, (Accessed: 11 November 2025).
[654] Narayanan et al., 2016, pp. 112–1161.
[655] Cirone, 2021, pp. 22–29.
[656] Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 (Text with EEA relevance). Available at: https://eur-lex.europa.eu/eli/reg/2023/1113/oj/eng, (Accessed: 11 November 2025).
[657] Finck, 2019, pp. 43–52.

decoupling measures directly.[658] Second, however, they remain structurally unable to delete the on-chain artefacts that record each transaction.[659] This asymmetry positions custodial providers as highly capable yet inherently limited agents of erasure: they can meaningfully reduce the accessibility of personal data but cannot alter the immutable ledger that underlies their services.

5.1.2 Non-Custodial Wallet Providers

Non-custodial wallets, also called self-custody or user-controlled wallets, operate on fundamentally different principles. The provider generates or facilitates the generation of private keys but does not store them; the user retains full, exclusive control.[660] As is well-expressed within the crypto community, this model reflects the foundational ethos of decentralisation, often summarised in the maxim "not your keys, not your coins."[661]

This structural separation from key management has direct implications for data protection. Because non-custodial providers are technically unable to access or authorise transactions on behalf of the user, their role in the processing of personal data is, in principle, considerably narrower than that of custodial intermediaries.[662] Nevertheless, they still process off-chain network data arising from the operation of the system, notably IP addresses and transaction-relay metadata associated with user connections, as well as information produced when wallet software relies on provider-hosted nodes or APIs to broadcast transactions and query blockchain state.[663] In practice, many non-custodial wallet implementations also incorporate additional off-chain processing of device-level identifiers, application telemetry, and interaction data with embedded services. As Troncoso et al. observe in their systematisation of decentralised architectures, decentralisation does not remove the need for application-layer

[658] Finck, 2019, pp. 75–78; see also, CNIL, 2018, pp. 4–6.
[659] CNIL, 2018, pp. 8–10; Finck, 2019, 84–88;
[660] Mangipudi, E. V., Desai, U., Mondal, M., Minaei, M., and Kate, A. 2023. *Uncovering Impact of Mental Models towards Adoption of Multi-device Threshold Crypto-Wallets*. CCS '23: Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security, p. 2. Available at: https://eprint.iacr.org/2022/075.pdf, (Accessed: 11 November 2025).
[661] Ledger Academy, (2020). *Not Your Keys, Not Your Coins: Explained*. Available at: https://www.ledger.com/academy/not-your-keys-not-your-coins-why-it-matters, (Accessed: 25 November 2025).
[662] Narayanan et al., 2016, pp. 103–107.
[663] Koshy, P., Koshy, D., McDaniel, P., (2014). *An analysis of anonymity in bitcoin using p2p network traffic. In International conference on financial cryptography and data security*. (pp. 1-16). Pennsylvania State University, University Park, PA 16802, USA. Available at: https://www.ifca.ai/fc14/papers/fc14_submission_71.pdf, (Accessed: 25 November 2025).

processing and may, in fact, expand the range of metadata handled outside the core cryptographic protocol.[664]

The scope of this processing becomes more legally salient when the wallet relies on the provider's own infrastructure to interface with the blockchain.[665] A well-known example is MetaMask's default use of Infura as a remote procedure call (RPC) endpoint.[666] In such configurations, the provider may engage in sufficient factual influence over the means and purposes of processing to qualify as a data controller, or even a joint controller, within the meaning of the GDPR.[667] As the CJEU and its commentators emphasise, the GDPR adopts a functional approach to controllership: responsibility attaches wherever an actor exerts factual influence over the purposes or means of processing, even where that influence is partial, distributed, or embedded in a decentralised architecture.[668] Therefore does not extinguish legal responsibility; it merely redistributes it across those who shape the processing environment.

These distinctions have particular relevance for the interpretation of the right to erasure under Article 17 GDPR. Non-custodial providers face even more stringent technical constraints than custodial intermediaries, as their lack of access to private keys renders them incapable of modifying, removing, or otherwise suppressing on-chain records or user-controlled crypto-assets.[669] Consequently, their erasure obligations pertain almost exclusively to the off-chain data that they themselves have generated or stored, as well as to any adjustments they can make at the interface level to limit the visibility of residual information.[670] This considerably

[664] Troncoso, C., Isaakidis, M., Danezis, G. and Halpin, H., (2017). *Systematizing decentralization and privacy: Lessons from 15 years of research and deployments*. Proceedings on Privacy Enhancing Technologies ; 2017 (4), pp. 307–329. Available at: http://carmelatroncoso.com/papers/Troncoso-PETS17.pdf, (Accessed: 25 November 2025).
[665] Finck, M., (2019). *Blockchain Regulation and Governance in Europe*. Cambridge University Press, ISBN: 9781108465458, 214 PP, & Werbach, K., (2019). *The Blockchain and the New Architecture of Trust*. ISBN: 9780262038935, 344 PP.
Reviewer: J Savirimuthu. Available at: https://livrepository.liverpool.ac.uk/3096584/, (Accessed: 25 November 2025).
[666] Consensys, MetaMask: Privacy Policy and Technical Architecture (2022), documenting default RPC routing through Infura. Available at: https://consensys.io/privacy-notice, (Accessed: 25 November 2025).
[667] Kuner et al., 2020, pp. 37–40.
[668] *Ibid*.
[669] Wang, K., (2025). *Regulating Cryptocurrency Non-Custodial Service Providers Through the Bank Secrecy Act*. The University of Chicago Business Law Review. Rev., 4:2, pp. 344–347. Available at: https://businesslawreview.uchicago.edu/sites/default/files/2025-10/Kai Wang_0.pdf, (Accessed: 25 November 2025).
[670] Savirimuthu, 2019; see also, Finck, M., Moscon, V., (2019). *Copyright Law on Blockchains: Between New Forms of Rights Administration and Digital Rights Management 2.0*. IIC - International Review of Intellectual

narrows, but does not entirely extinguish, the scope for what might be considered an "effective" form of forgetting within non-custodial architectures.

5.1.3 Hot, Cold, and Hybrid Wallet Models

A further dimension of the typology concerns the mode by which cryptographic keys are stored and accessed.[671] Wallets can function as "hot" wallets, which are constantly linked to the internet via desktop programs, mobile apps, or browser extensions. Conversely, "cold" wallets produce and store keys on offline media, usually in the form of specialised hardware devices or, occasionally, paper-based storage mechanisms.[672] Hardware wallets that connect with companion apps like Ledger Live are an example of the expanding class of hybrid systems that fall between these two extremes, combining offline key storage with online transaction interfaces.[673]

This distinction affects the type and scope of personal data processing and is not just taxonomical. Due to their frequent interactions with online infrastructures, hot wallets produce a large amount of metadata, including as IP addresses, device fingerprints, application telemetry, and network request logs.[674] These data flows result from the client application's architecture and the communication channels it uses, not from blockchain operations per se.[675] In comparison, cold wallets handle relatively little personal information. Data processing is mostly limited to firmware upgrades, initial device configuration, and optional diagnostic submissions due to its offline nature.[676] Hybrid wallets represent a middle

---

Property and Competition Law, Vol 50, pp. 90-99 (discussing blockchain immutability, the impossibility of modifying on-chain data, and the need for off-chain and interface-level control mechanisms). Available at: https://link.springer.com/article/10.1007/s40319-018-00776-8, (Accessed: 25 November 2025).

[671] Dowsley, R.B., Farias, M.C., Larangeira, M., Nascimento, A.C. and Virdee, J., (2022). *A spendable cold wallet from QR video*. In International Conference on Security and Cryptography, pp. 283-290. Scitepress. Available at: https://researchmgt.monash.edu/ws/portalfiles/portal/468554595/430334621_oa.pdf, (Accessed: 25 November 2025).

[672] Larangeira, M., (2025). *Secure and Practical Cold (and Hot) Staking*. In Proceedings of the 22nd International Conference on Security and Cryptography (SECRYPT), pages 339-346, ISBN: 978-989-758-760-3; ISSN: 2184-7711. CC license (CC BY-NC-ND 4.0). DOI: 10.5220/0013458200003979. Available at: https://www.scitepress.org/Papers/2025/134582/134582.pdf, (Accessed: 25 November 2025).

[673] Ledger Live introduced a hybrid wallet architecture by pairing the Ledger Nano™ Gen5 Signer, an offline hardware device that generates and stores private keys within a secure element, with the Ledger Wallet™ app, an online interface that retrieves account data, broadcasts signed transactions, and connects to networked services; the architecture is "hybrid" because key custody remains entirely offline while transactional interaction and metadata processing occur online. Available at: https://shop.ledger.com/pages/ledger-nano-gen5, (Accessed: 25 November 2025).

[674] Torres et al., 2023, pp. 2, 4, 6–12.

[675] *Ibid.*

[676] Antonopoulos, 2015, pp. 235–236.

ground: the online interface generates behavioural and system-level metadata through regular program use, while the offline component reduces the visibility of cryptographic content.[677]

The divergence in data intensiveness across these models bears directly upon the feasibility of operationalising "effective forgetting."[678] Cold wallets, by virtue of their limited engagement with personal data, present fewer challenges for compliance but simultaneously afford fewer opportunities for remedial action, as there is comparatively little that can be erased or suppressed.[679] On the other hand, hot and hybrid wallets produce larger data footprints, especially when it comes to off-chain metadata.[680] This expands the domain in which erasure, delinking, or contextual suppression techniques can be applied, but it also raises the risk surface for identifiability and profiling. The architecture of key storage thus serves as a material determinant of both the scope and the limits of Article 17 compliance within wallet ecosystems.

5.1.4 Smart-Contract and Organisational Wallets

Recent developments have expanded the wallet landscape to include smart-contract wallets, also called account-abstraction wallets,[681] and multi-signature or organisational wallets used by companies, DAOs, and investment funds. These systems distribute control across multiple signatories or encode governance logic directly into smart contracts.[682] As Robert Herian argues, such programmable infrastructures reconfigure legal responsibility by embedding operational decisions into automated rules.[683]

---

[677] Mahmoud, Q.H., Lescisin, M. and AlTaei, M., (2019). *Research challenges and opportunities in blockchain and cryptocurrencies*. Internet Technology Letters 2(2):e93, John Wiley & Sons, Ltd, pp. 1–6. Available at: https://www.researchgate.net/publication/330917374_Research_Challenges_and_Opportunities_in_Blockchain_and_Cryptocurrencies, (Accessed: 7 December 2025).

[678] Politou, E., Alepis, E., Virvou, M., Patsakis, C., (2022). *Privacy and Data Protection Challenges in the Distributed Era*. Learning and Analytics in Intelligent Systems, Vol 26, ISBN 978-3-030-85442-3, Springer, pp. 31–35.

[679] Antonopoulos, 2015, pp. 235–236.

[680] Torres et al., 2023, pp. 1–3.

[681] Coinbase, (2025). Crypto Glossary. Available at: https://www.coinbase.com/en-gb/learn/crypto-glossary/what-is-account-abstraction-and-why-is-it-important, (Accessed: 7 December 2025).

[682] Napieralska, A., Kępczyński , P., (2024). *Redefining accountability: navigating legal challenges of participant liability in decentralized autonomous organizations*. Networking and Internet Architecture (cs.NI); General Economics (econ.GN). arXiv preprint arXiv:2408.04717. Available at: https://arxiv.org/abs/2408.04717, (Accessed: 7 December 2025); see also, Kolber, A.J., (2018). *Not-so-smart blockchain contracts and artificial responsibility*. Stan. Tech. L. Rev., 21, p.198. Available at: https://law.stanford.edu/wp-content/uploads/2018/09/Kolber_LL_20180910.pdf, (Accessed: 7 December 2025); see also, Werkheiser, B., (2024). How do ERC-4337 smart contract wallets work? Alchemy. Available at: https://www.alchemy.com/overviews/how-do-smart-contract-wallets-work, (Accessed: 7 December 2025).

[683] Herian, R., (2019). *Regulating blockchain: Critical perspectives in law and technology*. Routledge, ISBN: 978-1-138-59276-6 (hbk), pp. 20–22, 58–64.

Smart-contract wallets introduce new complexities for erasure. Their logic is executed on-chain and visible to all nodes, which makes modification or deletion virtually impossible without deploying new contract versions.[684] Homoliak and Perešini show that many modern wallet schemes, especially custodial and co-signing arrangements, combine blockchain-verified signatures with additional off-chain authentication factors (passwords, OTPs, biometrics, OAuth identities). In organisational or shared-control wallets, these mechanisms typically require maintaining extra off-chain user and device data while the underlying on-chain transaction and immutability model remains unchanged.[685]

Taken together, these wallet designs show that technical complexity is increasing faster than the law's ability to adapt. As wallets gain new functions, we also need more precise ways of describing their role in processing personal data under the GDPR.

5.1.5 Implications for "Effective Forgetting"

This typology reveals that wallet providers cannot be treated as a homogeneous category for the purposes of GDPR analysis. Different wallet types process personal data in different ways, resulting in different levels of controllership, accountability, and erasing capacity. While non-custodial, cold, and smart-contract wallets offer more limited but nonetheless legally significant ways to reduce retrievability and contextual linking, custodial providers enable the widest range of effective amnesia due to their substantial control over off-chain data.

This chapter's analysis maps this terrain to pinpoint the exact locations within each architecture where functional forgetting can be operationalised and where structural constraints are still intractable. Thus, the typology serves as the foundation for the compliance framework that is created in the sections that follow, elucidating the possibilities and constraints of Article 17 in blockchain wallet ecosystems.

---

[684] Atzei, N., Bartoletti, M. and Cimoli, T., (2017). *A survey of attacks on ethereum smart contracts (sok)*. In International conference on principles of security and trust, pp. 1–22. Berlin, Heidelberg: Springer Berlin Heidelberg. Available at: https://eprint.iacr.org/2016/1007.pdf, (Accessed: 7 December 2025); see also, Wood, G., (2014). *Ethereum: A secure decentralised generalised transaction ledger*. Ethereum project yellow paper, 151(2014), pp.1-32. Available at: https://ethereum.github.io/yellowpaper/paper.pdf, (Accessed: 7 December 2025).

[685] Homoliak, I., Perešíni, M., (2024). So*K: Cryptocurrency wallets–A security review and classification based on authentication factors*. In 2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) (pp. 1-8). IEEE. Available at: https://arxiv.org/pdf/2402.17659, (Accessed: 7 December 2025).

5.2 Controllership in Wallet Ecosystems

Building on this architectural distinction, this section addresses the second analytical step by examining how controllership and joint controllership attach in practice across wallet infrastructures.

The legal characterisation of blockchain wallets cannot be confined to their cryptographic function. They create, modify, and arrange personal data in ways that are essential to the implementation of the GDPR, even if they also serve as the interface via which private keys function on decentralised networks. Their data-processing role is layered: the wallet software, its supporting infrastructure, and any auxiliary services incorporated into the interface provide considerable off-chain metadata that coexists with on-chain identifiers generated as a result of blockchain transactions.[686] To assess the feasibility of erasure and the contours of "effective forgetting," it is necessary to disaggregate these forms of processing and to identify the actors who determine their purposes and means. This section therefore offers a structured account of (i) the distinction between on-chain and off-chain personal data, (ii) the legal basis of controllership in wallet ecosystems, and (iii) the implications of distributed controllership for Article 17 GDPR.

5.2.1 On-Chain Personal Data and the Limits of Provider Influence

Blockchain systems record a set of identifiers and transactional artefacts that, while pseudonymous, constitute personal data whenever they can be linked to an identifiable natural person. Public keys, hashed addresses, transaction histories, contract interactions, and temporal markers together form a persistent and searchable record of a user's activity. As the Article 29 Working Party and subsequent scholarship have emphasised, pseudonymisation does not remove information from the scope of data protection law when re-identification is reasonably possible,[687] a position later confirmed in CJEU jurisprudence adopting an actor-relative assessment based on the means reasonably likely to be used for identification.[688] In blockchain environments, re-identification may occur through multiple pathways: the use of centralised exchanges that maintain legally mandated identity files, blockchain analytics

[686] Augusto, A., Belchior, R., Correia, M., Vasconcelos, A., Zhang, L. and Hardjono, T., (2024). *SoK: security and privacy of blockchain interoperability [extended version]*. Authorea Preprints. Available at: https://oaklandsok.github.io/papers/augusto2024.pdf, (Accessed: 7 December 2025).
[687] WP216, Opinion 05/2014, pp. 15–18.
[688] Breyer v Bundesrepublik Deutschland, C-582/14, para 42–44, 46–48; Court of Justice of the European Union (2025), EDPS v SRB (Notion de données à caractère personnel), Case C-413/23 P, ECLI:EU:C:2025:645, paras 78–82, 84–85. Available at: https://curia.europa.eu/juris/liste.jsf?num=C-413/23, (Accessed: 10 December 2025).

capable of clustering addresses, or network-level identifiers such as IP addresses that accompany the transmission of signed transactions.

This form of data is distinctive because wallet providers do not mediate its persistence. Once broadcast to the network and incorporated into a block, the data becomes embedded in the consensus mechanism of the chain and replicated across nodes. Providers have no factual or technical capacity to delete or modify it. From the standpoint of Article 17, this immutability defines the structural limit of erasure: controllers cannot fulfil an obligation that is technically impossible within the protocol. Nevertheless, the immutable character of on-chain data does not negate the applicability of the GDPR to wallet providers. The obligations under the Regulation attach to actors who determine purposes and means of processing, not to those who control the underlying infrastructure. As long as wallet providers process personal data in the context of their own operations, most notably through off-chain systems, they remain bound by the Regulation, notwithstanding their inability to alter the blockchain ledger.[689]

A further legal complexity arises from the way in which wallet interfaces render on-chain data intelligible. Although the provider cannot change the ledger, it does determine how information is retrieved, presented, aggregated, or linked within the interface. The creation of address books, the surfacing of historical transactions, the grouping of multiple addresses under a single identity, or the pre-population of user-specific histories all constitute processing operations within the meaning of Article 4 GDPR.[690] As a result, on-chain data, although immutable, is still processed by the provider at the interface level in a manner that is amenable to the obligations of erasure understood as suppression or delinking, rather than deletion.

5.2.2 Off-Chain Personal Data and the Architecture of Provider Responsibility

If on-chain data defines the immutable substrate of blockchain processing, off-chain data represents the domain in which wallet providers exercise genuine discretion and thus attract the core obligations of the GDPR. Off-chain data comprises all information generated, transmitted, or retained by the wallet software, its supporting infrastructure, and any ancillary

[689] Bayle, A., Koscina, M., Manset, D. and Perez-Kempner, O., (2018). *When blockchain meets the right to be forgotten: technology versus law in the healthcare industry*. In 2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI), pp. 788–792, IEEE. Available at: https://www.myhealthmydata.eu/wp-content/uploads/2019/10/When_Blockchain_Meets_the_Right_to_be_Forgotten.pdf, (Accessed: 10 December 2025).

[690] EDPB Guidelines 02/2025, paras 25–44.

services that form part of the operational environment.[691] Its scope is broader and more heterogeneous than that of on-chain identifiers, reflecting the fact that the wallet is not merely a cryptographic instrument but an application-layer ecosystem whose functioning depends on continuous interaction with networked resources.[692]

Off-chain personal data arises through multiple vectors.[693] The most fundamental is the act of connecting to the network. When a wallet broadcasts a transaction or queries account information, it generates network-level metadata such as IP addresses, device identifiers, session information, and routing logs. These data points, frequently overlooked in technical narratives celebrating decentralisation, constitute personal data under the GDPR because they relate to an identifiable natural person once combined with the user's device profile or behavioural patterns.[694] Even non-custodial wallets that do not store private keys frequently rely on remote procedure call nodes operated either by the provider itself or by third parties. The choice of RPC endpoint, whether default or user-configurable, is a processing decision within Article 4(2) GDPR, as it determines the destination and visibility of metadata flows.

A second layer of off-chain data arises from application telemetry and behavioural analytics. Many wallet providers, such as hot, hybrid, and even some hardware-linked systems, collect information relating to feature usage, error reporting, device configuration, and user interactions with the interface.[695] Whether this data is processed for security stability, performance optimisation, or commercial analytics, it constitutes personal data whenever it is linked, directly or indirectly, to a user or device.[696] The technical literature makes clear that even seemingly innocuous telemetry can create persistent identifiers sufficient for profiling. These datasets are fully within the provider's factual control: they are generated through

[691] EU Blockchain Observatory and Forum, (2018). *Blockchain and the GDPR*. An Initiative of the European Union, pp. 14–16. Available at: https://blockchain-observatory.ec.europa.eu/publications/blockchain-and-gdpr_en, (Accessed: 10 December 2025).
[692] EDPB Guidelines 02/2025, paras 11–14, 25–30, 90–97.
[693] For instance, when a user interacts with the blockchain through MetaMask, the wallet communicates with remote node infrastructure (such as Infura) to query balances or broadcast transactions, thereby generating off-chain metadata including IP addresses, timestamps, and device information, which may constitute personal data under the GDPR. Available at: https://ethereum.org/developers/docs/apis/json-rpc/, (Accessed: 10 December 2025).
[694] EDPB Guidelines 02/2025, paras 11–14, 25–30, 90–97.
[695] CNIL, (2025). *Mobile applications: CNIL publishes its recommendations for better privacy protection*. Deliberation No 2025-024, pp. 20, 33, 73–75. Available at: https://www.cnil.fr/en/mobile-applications-cnil-publishes-its-recommendations-better-privacy-protection, (Accessed: 10 December 2025).
[696] WP 136, Opinion 4/2007, pp. 9–14.

design choices, transmitted through provider-controlled infrastructure, and retained according to provider-determined policies.

A further and more intensive category of off-chain data arises in the custodial context. Here, the provider maintains internal account ledgers, authentication credentials, KYC/AML documentation, transaction histories, compliance notes, and risk classifications.[697] These categories of data are not incidental: they constitute the operational backbone of regulated financial intermediation. They are therefore collected and processed not only for the provision of services but also pursuant to legal obligations under the EU anti-money-laundering and counter-terrorist-financing regime.[698] Nevertheless, the coexistence of contractual and regulatory legal bases does not displace the controller's ongoing obligations under the GDPR. Retention periods, internal access, and secondary uses remain constrained by the principles of purpose limitation, data minimisation and storage limitation, and personal data must be erased once the purposes of processing cease or applicable retention periods expire.[699]

It is in the off-chain sphere that the contours of controllership become most visible. Unlike the immutable ledger, off-chain systems are designed, configured, and maintained by actors who determine the architecture of processing. Even apparently peripheral design decisions, for example, the choice to cache transaction histories locally, to maintain an address book, or to pre-populate user-specific recommendations, constitute processing operations attributable to the provider.[700] The fact that the technical function of the wallet requires certain forms of processing does not displace the application of data-protection law. Rather, it places heightened importance on ensuring that off-chain processing is proportionate, transparent, and amenable to erasure or suppression where Article 17 applies.

[697] EDPB Guidelines 02/2025, paras 3.2, 4.2, 4.3; GDPR Articles 4, 5, 6; Financial Action Task Force (FATF), (2025). *The FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation*. Recommendations 1, 10, 11, and 18. Available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF Recommendations 2012.pdf.coredownload.inline.pdf?nocache=true, (Accessed: 10 December 2025).
[698] Regulation (EU) 2023/1114, Articles 3(1)(15)(16), 59–68.
[699] See GDPR, Articles 5(1)(b), (c), (e) and 17(1); EDPB Guidelines 4/2019 on Article 25, paras 21–32; see also, EDPB Guidelines 02/2025, paras 4.3, 4.7 and 5.2;
[700] GDPR, Article 4(7); EDPB Guidelines 07/2020, paras 33–38, 47–49; EDPB Guidelines 02/2025, paras 6–8, 14–16.

The legal significance of this lies not merely in the volume of off-chain data processed, but in the provider's effective control over it. Unlike on-chain records, off-chain personal data can be amended, minimised, pseudonymised or erased without affecting the integrity of the distributed ledger. While the architecture of the blockchain imposes structural limits on deletion, the architecture of wallet software and supporting infrastructure does not, and therefore remains fully subject to the obligations of the GDPR.[701] The ability, and in some circumstances the duty, to remove or disconnect off-chain personal data establishes the domain in which Article 17 GDPR can operate meaningfully in blockchain systems. This divergence highlights the doctrinal significance of differentiating between data whose durability results from provider choice and data that is immutable by design.[702]

5.2.3 Functional and Joint Controllership in Wallet Infrastructures

The requirement for legal accountability is not eliminated by the distributed architecture of blockchain ecosystems; rather, it is distributed among the people who influence the data-processing environment. The GDPR embraces a functional understanding of controllership, based on factual influence over the purposes and methods of processing rather than formal designation. This principle, clarified in Wirtschaftsakademie, Fashion ID, Jehovan todistajat, and subsequent CJEU jurisprudence,[703] is central to analysing wallet infrastructures, where multiple actors participate in the processing chain and where the technical complexity of decentralised systems risks obscuring legally determinative relationships.

A functional analysis reveals that controllership is neither binary nor static. Rather, it is situational and distributed across the technical stack. Custodial wallet providers, as previously noted, determine both the purposes and the means of nearly all relevant processing activities: the generation and storage of private keys, account management, authentication, retention of transactional records, and transmission of off-chain data to third-party partners. Their position as infrastructure operators and financial intermediaries leaves little doubt that they qualify as controllers under Article 4(7) GDPR. The more contested questions arise in the non-custodial and hybrid contexts, where the involvement of multiple service layers fragments the processing operations and disperses influence across several actors.

[701] GDPR, Articles 4(7), 5(1)(c), 5(1)(e), 17 and 25; EDPB Guidelines 07/2020, paras 33–38, 47–49; EDPB Guidelines 02/2025, paras 14–18.
[702] GDPR, Articles 17 and 25.
[703] Wirtschaftsakademie Schleswig-Holstein, Case C-210/16, paras 28–29, 38; Jehovan todistajat, Case C-25/17, paras 68–69, 75; Fashion ID, Case C-40/17, paras 68–69, 74; and, EDPB Guidelines 07/2020, paras 7, 19, 33–38.

Non-custodial wallet providers frequently disclaim responsibility on the basis that they neither access nor store users' private keys.[704] However, EU data protection law does not treat key custody as determinative of controllership; rather, responsibility turns on factual influence over the purposes and essential means of processing.[705] What matters is the provider's influence over the purposes and means of off-chain processing: the selection of RPC endpoints, the routing of network traffic, the storage of device-specific information, the integration of third-party services, and the configuration of how on-chain data is presented or linked to user identities. Each of these design choices constitutes a processing decision within the meaning of the GDPR. The provider's factual ability to log, transmit, filter, or analyse metadata confers functional influence sufficient to trigger controllership obligations, irrespective of whether the underlying private key remains exclusively in the user's possession.

The analysis grows more complex when considering RPC node operators, indexers, and infrastructure partners. Where a wallet relies on an external provider, such as Infura, Alchemy, or a proprietary cluster, to broadcast transactions or query blockchain state, the infrastructure provider may qualify as a joint controller. Joint controllership in such cases does not depend on the existence of a shared or common intention, but on the factual convergence of decisions that jointly determine the purposes or essential means of processing.[706] The CJEU has made clear that even partial or indirect influence suffices: an actor need not determine all processing operations to be deemed a joint controller; contributing to the conditions under which processing takes place is enough. Accordingly, a wallet provider that preconfigures a default RPC endpoint and transmits user metadata to it participates jointly in determining the means of processing, and the RPC operator, by receiving and storing that metadata, equally participates in shaping the processing environment.[707]

Interface-level design choices provide a further illustration of functional controllership. Decisions to auto-populate transaction histories, aggregate multiple addresses under a single

[704] EDPB Guidelines 07/2020, para 19.
[705] EDPB Guidelines 07/2020, paras 7, 15, 21, 33, 36, 40.
[706] EDPB Guidelines 07/2020, paras 19, 33, 52; Fashion ID, Case C-40/17, paras 65, 69, 74.
[707] Wirtschaftsakademie Schleswig-Holstein, Case C-210/16, paras 38, 43; Fashion ID, Case C-40/17, paras 65, 69, 74; Jehovan todistajat, Case C-25/17, paras 68, 69.

interface identity, cache data locally, or generate user-specific analytics constitute determinations of the essential means, and, in some cases, the purposes, of processing.[708] That these operations draw upon on-chain information does not place them beyond the GDPR's scope; they constitute distinct processing activities carried out by the provider through the organisation, presentation, and contextualisation of data within the user interface. The decentralised storage of the underlying ledger data does not alter the legal character of these interface-level processing operations.[709]

This distributed model of influence has two implications for the right to erasure. First, wallet providers cannot avoid responsibility by appealing to the decentralised architecture of the underlying ledger; their off-chain and interface-level processing decisions constitute autonomous processing operations and are therefore independently actionable under the GDPR.[710] Second, the presence of multiple controllers or joint controllers requires a nuanced analysis of which actors are capable of implementing erasure measures and to what extent. While some might have complete control over their own databases, others would be constrained by the blockchain protocol's technological limitations or the durability of other records.[711] In the setting of distributed processing, Article 17 does not redece; rather, it necessitates a differentiated allocation of erasing obligations in accordance with the factual assessment of each actor's intents and means.

When combined, these findings show that controllership in wallet ecosystems is a functional framework for assigning data protection responsibilities in technically challenging and operationally interdependent situations rather than just an abstract legal designation. This analytical basis is necessary to comprehend why literal erasure is frequently impractical in decentralised systems and why data protection law must instead describe an effective forgetting model that can balance technological immutability with the GDPR's normative goals.

[708] EDPB Guidelines 07/2020, paras 33, 38, 58; Fashion ID, Case C-40/17, paras 69, 74; Wirtschaftsakademie Schleswig-Holstein, Case C-210/16, para 43.
[709] GDPR, Article 4(2); EDPB Guidelines 02/2025, paras 8, 10, 18; Google Spain, Case C-131/12, paras 28–30.
[710] GDPR, Article 17(1); EDPB Guidelines 07/2020, paras 32, 47; Google Spain, Case C-131/12, paras 28, 35;
[711] GDPR, Article 26(1); EDPB Guidelines 07/2020, paras 41–42, 57; Fashion ID, Case C-40/17, para 69; Wirtschaftsakademie Schleswig-Holstein, Case C-210/16, para 43.

5.3 Technical Limits of Literal Erasure in Blockchain Systems

The following sections complete the third analytical step of the chapter by translating Article 17 GDPR into a set of architecture-sensitive "effective forgetting" measures compatible with decentralised wallet systems.

The right to erasure requires a processing environment where a data controller can exert control over the removal, correction, or permanent inaccessibility of personal data.[712] However, the persistence, auditability, and redundancy of recorded data constitute a fundamentally new normative commitment that underpins blockchain technologies.[713] Once data has spread along the chain, this commitment, which is made possible by distributed consensus techniques and cryptographic linking, makes literal erasure technically impossible.[714] Therefore, any evaluation of the extent and limitations of Article 17 GDPR in decentralised systems must explicitly address the technical features that make deletion impossible as well as the legal ramifications of this structural limitation.

The cryptographic chaining of blocks, in which each block includes a hash of its predecessor, is the fundamental component of blockchain immutability. This creates a system where any modification of previous data would render all subsequent blocks invalid. Ledger integrity is enforced through consensus mechanisms that recognise as valid only those blocks whose histories remain cryptographically intact.[715] In Proof-of-Work systems, altering historical data would require recomputing the cumulative proof embedded in the chain, a task that is computationally infeasible for any actor lacking majority control of network hashing power.[716] Proof-of-Stake and Delegated Proof-of-Stake systems similarly bind the network to a single authoritative history through stake-weighted consensus, such that retroactive modification would require the coordinated participation of a supermajority of validators.[717] These constraints are not incidental but constitute the core trust model through which decentralised systems achieve coordination without reliance on a central authority.

The consequences for data protection law are stark. Once personal data is written to the ledger, it is replicated across thousands of nodes distributed globally. These nodes operate

[712] GDPR, Article 17(1) and Recital 66.
[713] EU Blockchain Observatory and Forum, 2018, pp. 16–18; EDPB Guidelines 07/2020, paras 72–75.
[714] EDPB Guidelines 02/2025, paras 15–44, 49–56.
[715] EDPB Guidelines 02/2025, paras 15–33; Nakamoto, 2008, pp. 2–3.
[716] Nakamoto, 2008, pp. 3, 6–8.
[717] *Ibid*, pp. 2–5.

autonomously and frequently fall outside both the territorial jurisdiction and the organisational control of any wallet provider or other identifiable controller.[718] No actor, whether private or regulatory, has the capacity to coordinate a revision of historical blocks, nor does the protocol provide a mechanism for the deletion of data embedded in canonical chain history. Even if a minority subset of nodes were to delete or modify entries, the network's consensus algorithm would treat the resulting chain as invalid.[719] In this way, blockchain immutability is a purposeful governance promise that replaces institutional authority with cryptographic assurance rather than just a technological inconvenience.

Literal erasure is also precluded by the economic model of decentralised networks. Nodes are incentivised to maintain complete records, both to verify new transactions and to ensure the validity of future operations.[720] Pruning mechanisms exist in some protocols, but they remove only locally cached data that can be reconstructed from the canonical chain and do not alter or delete historical records.[721] Even advanced privacy-enhancing technologies, such as zero-knowledge proofs, and commit-and-reveal schemes, do not retroactively erase data. They prevent leakage at the point of processing but do not modify the underlying chain, which continues to record commitments, state transitions, or encrypted artefacts that may be linkable through auxiliary analysis.

The legal significance of blockchain immutability has not yet been fully worked through by courts or regulators, and any assessment must therefore remain provisional. That said, the technical impossibility of deleting on-chain data does not appear to displace the applicability of the GDPR, which attaches obligations to controllers only within the limits of their factual influence.[722] At the same time, Article 17 cannot plausibly be interpreted in a manner that disregards technological constraints: the Regulation cannot require what is technically impossible,[723] nor can it sensibly impose responsibility for protocol-level design features that a controller does not operate or control. On this view, the right to erasure is most coherently understood as applying to those processing activities that do fall within the provider's remit,

[718] GDPR, Articles 3, 4(7) and Recital 26; Nakamoto, 2008, pp. 3–5; EDPB Guidelines 02/2025, paras 15–24.
[719] Ethereum yellow paper, 2014, paras 2.2, 4.4; EDPB Guidelines 02/2025, paras 49–56.
[720] Nakamoto, 2008, pp. 1–3; Antonopoulos, 2015, pp. 159–170, 231–236.
[721] Antonopoulos, 2015, pp. 159–170; Finck, 2019, pp. 3–9.
[722] EDPB Guidelines 02/2025, paras 6–9.
[723] Court of Justice of the European Union (2014) Banif Plus Bank Zrt. v Márton Lantos and Mártonné Lantos, Case C-312/14, ECLI:EU:C:2015:794, para 29. Available at: https://curia.europa.eu/juris/liste.jsf?num=C-312/14, (Accessed: 10 December 2025).

including off-chain storage, interface-level presentation of on-chain data, the maintenance of linkages between identifiers and individuals, and the contextual visibility of information.

This points towards a need to rethink how erasure operates, rather than to abandon the right itself. In blockchain environments, erasure cannot plausibly be understood as the literal removal of data from the ledger. Instead, it is more realistic to understand it as measures such as suppressing identifiers, breaking links between transactions, limiting onward disclosure, or reducing linkability through pseudonymisation or delinking. According to this interpretation, the technical criticism of literal erasure directs attention away from formal deletion and towards its practical consequences. When immutability is a feature of the technology, it is more likely that compliance will be attained by taking steps that render information practically unavailable, even if the underlying record still exists.

Accordingly, the technical impossibility of literal erasure does not, by itself, render Article 17 redundant. Rather, it suggests the need for a gradual adjustment of the doctrine so that it can operate within the practical constraints of decentralised systems. The next section explores this adjustment by developing the notion of "effective forgetting" as a way of aligning the objectives of the GDPR with the structural limits imposed by blockchain architecture.

5.4 From Erasure to Effective Forgetting

5.4.1 Conceptual Foundations of Effective Forgetting

The structural impossibility of literal erasure in blockchain systems does not exhaust the normative scope of Article 17 GDPR. While the Regulation frames erasure in terms that appear to assume the possibility of deleting data, the case law of the Court of Justice shows that the right to be forgotten has never depended exclusively on physical removal.

In decisions such as Google Spain, Google v CNIL, and GC and Others, the Court accepted that personal data could continue to exist, yet still required controllers to intervene in the way that data was made accessible.[724] In other words, the Court did not require content to be removed from the source websites on which it was published. Instead, obligations were imposed on intermediaries, particularly search engines, to limit access by measures such as delisting, reducing visibility, or applying territorial restrictions. On this reading, the interest

[724] Google Spain, Case C-131/12, paras 84, 88, and 94; Google v CNIL, Case C-507/17, paras 66, 68, 72; GC and Others, C-136/17, paras 53, 66 and 68.

protected by Article 17 is less about eliminating historical information and more about reducing its ongoing impact within the data subject's informational environment.

This line of case law supports an understanding of "effective forgetting" in the context of blockchain systems. On this view, compliance does not depend on the deletion of data from the ledger itself, which remains immutable, but on the way personal data is handled within the systems operated by the wallet provider. Effective forgetting refers to practices through which data is made difficult to access, disconnected from the individual, or deprived of practical significance within the provider's processing environment.[725] The right to erasure is therefore realised not by rewriting blockchain history, but by adjusting off-chain and interface-level processing in ways that limit visibility, sever associations, or otherwise neutralise the personal dimension of the data.[726]

The jurisprudence of the Court of Justice supports a functional understanding of erasure that does not depend exclusively on the physical deletion of data. In Google Spain, the Court required search engine operators to remove links to personal information from results lists even where the underlying content remained lawfully published on third-party websites.[727] Similarly, in GC and Others and Google v CNIL, the Court confirmed that the objective of Article 17 is not necessarily the destruction of information at source, but the reduction of its accessibility and practical relevance within the data subject's informational environment.[728] These decisions demonstrate that EU data protection law has already accepted that the effectiveness of erasure may depend on contextual factors such as visibility, retrievability, and the likelihood of continued dissemination. The legal interest protected by Article 17 therefore extends beyond literal deletion and encompasses measures capable of limiting the ongoing impact of personal data processing.

[725] Malgieri, G., (2016). Property and (Intellectual) Ownership of Consumers' Information: A New Taxonomy for Personal Data. Privacy in Germany - PinG, n. 4, 2016, 133 ff., pp. 6–13. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2916058, (Accessed: 10 December 2025).
[726] Jiménez-Gómez, B.S., (2020). *Risks of blockchain for data protection: a European approach*. Santa Clara High Tech. LJ 281, Volume 36, Issue 3, Article 2, pp. 321–334. Available at: https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1653&context=chtlj, (Accessed: 10 December 2025).
[727] Google Spain, Case C-131/12, paras 81–99.
[728] GC and Others, C-136/17, paras 53–57, 66–68, 77, 87–88; Google v CNIL, Case C-507/17, paras 41–44, 57–60, 64–66.

This functional logic becomes particularly significant in decentralised technological architectures, where the technical conditions of processing differ fundamentally from those assumed by traditional database models. Blockchain systems are designed to ensure persistence, redundancy, and auditability of recorded data.[729] As a result, the regulatory objective of erasure cannot be interpreted as requiring the modification of ledger entries that are structurally resistant to alteration. Instead, the right to erasure must be interpreted in light of the factual influence exercised by controllers over the surrounding data environment.[730] Where controllers retain the ability to influence the accessibility, contextualisation, or linkability of personal data, the protective function of Article 17 can be preserved even where the underlying record remains intact.[731] Effective forgetting therefore reflects not a departure from established doctrine, but a continuation of the Court's functional approach to ensuring that fundamental rights retain practical effectiveness in technologically evolving environments.

5.4.2 Off-Chain Erasure and Data Suppression

The most direct locus for implementing effective forgetting lies in off-chain data repositories. Wallet providers, particularly custodial actors, process extensive categories of personal data beyond the blockchain itself, including authentication records, device identifiers, customer support communications, behavioural analytics, and, in regulated contexts, KYC and AML documentation. Such practices are explicitly described in the privacy notices of major custodial wallet and exchange providers, including Coinbase and Binance, which list identity verification data, device information, and support interactions as off-chain personal data they control.[732] Article 17 GDPR applies fully to these datasets, subject only to statutory retention obligations.

---

[729] Swanson, T., (2015). *Consensus-as-a-Service: A Brief Report on the Emergence of Permissioned, Distributed Ledger Systems.* Available at: https://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf, (Accessed: 10 April 2026).

[730] Helberger, N., Karppinen, K. and D'acunto, L., (2018). *Exposure diversity as a design principle for recommender systems.* Information, communication & society, 21(2), pp. 191–207. Available at: https://www.tandfonline.com/doi/full/10.1080/1369118X.2016.1271900, (Accessed: 10 April 2026); see also, Kotsios, A., Magnani, M., Vega, D., Rossi, L. and Shklovski, I., (2019). *An analysis of the consequences of the general data protection regulation on social network research*. ACM Transactions on Social Computing, 2(3), pp. 1–22.

[731] Ohm, P., (2014). *Sensitive information*. S. Cal. L. Rev., 88, pp. 1135–1139. Available at: https://southerncalifornialawreview.com/wp-content/uploads/2018/01/88_1125.pdf, (Accessed: 10 April 2026).

[732] Coinbase, (2025). *Coinbase Global Privacy Policy*. Available at: https://www.coinbase.com/en-gb/legal/privacy, (Accessed: 10 December 2025); Binance, 2025. *Binance Privacy Portal*. Available at: https://www.binance.com/en/about-legal/privacy-portal, (Accessed: 10 December 2025).

Effective forgetting therefore requires the deletion or suppression of off-chain data once it is no longer necessary for the purposes for which it was collected. In custodial environments, this includes the erasure of internal account mappings linking user identities to blockchain addresses, the removal of historical activity logs, and the suppression of cached or duplicated data stored in backup systems, as reflected in account closure and data retention disclosures published by regulated exchanges such as Kraken.[733] Non-custodial wallet providers, while engaging in more limited processing, remain responsible for erasing application telemetry, RPC logs, and locally stored metadata within their control, including diagnostic and usage data described by browser-based wallets such as MetaMask when users interact with default RPC infrastructure.[734]

The accountability and audit language of wallet providers' GDPR-facing material increasingly emphasises the need for providers to implement retention schedules, secure deletion protocols, and internal documentation that can prove erasure has taken place.[735] Not only must data be removed, but it must be done in a way that is verifiable and compliant with the GDPR's accountability principle.

5.4.3 Delinking and the Neutralisation of Linkability

Where on-chain data cannot be erased, effective "forgetting" can instead be pursued through delinking: reducing the ability of observers to link persistent ledger entries to a data subject. This maps onto the privacy property of unlinkability, i.e., the inability of an attacker to infer whether two observed items or events are related.[736] It entails the dissociation of on-chain identifiers from off-chain profiles, device histories, or behavioural datasets that render those identifiers personally referable. This logic is reflected in certain wallet design practices. Privacy-oriented wallets, such as Wasabi, employ CoinJoin transactions to obscure

[733] Kraken, (2025). *Privacy Notice*. Available at: https://www.kraken.com/legal/privacy, (Accessed: 10 December 2025).
[734] MetaMask, (2025). Privacy preserving features in MetaMask. Available at: https://metamask.io/en-GB/news/product-spotlight-privacy-preserving-features-in-metamask, (Accessed: 10 December 2025).
[735] Coinbase, (2025). *Privacy Notice and Consent for New Applicants*. Available at: https://static-assets.coinbase.com/privacy_notice_and_consent_for_new_applicants_CB_payments.pdf, (Accessed: 10 December 2025).
[736] EDPB Guidelines 02/2025, paras 112–119; Google Spain, Case C-131/12, paras 36–38, 82–83, 94–96; Brusó, M., Chatzikokolakis, K., Etalle, S., Hartog., D., J., (2013). *Linking unlinkability*. In C. Palamidessi & M. Ryan (Eds.), Trustworthy Global Computing (TGC 2012), (Lecture Notes in Computer Science, Vol. 8191, pp. 129–144). Available at: https://www.researchgate.net/publication/279257580_Linking_Unlinkability, (Accessed: 12 December 2025).

transaction graphs and thereby reduce the persistence of linkages between blockchain addresses and user-associated profiles.[737]

In practice, delinking may be implemented through a range of technical and organisational measures, the specific configuration of which depends on the custodial model adopted by the service provider. Such measures may include (i) the removal of address books or identity mappings maintained within wallet software;[738] (ii) the disaggregation of multiple addresses that were previously consolidated under a single user profile; and (iii) the elimination of heuristics or interface features that surface inferred linkages between different addresses controlled by the same user.[739]

For custodial providers, which commonly maintain internal mappings between verified user identities and blockchain addresses, delinking may require the irreversible destruction of such mappings once applicable regulatory retention periods have elapsed.[740] By contrast, in non-custodial wallets, delinking is typically pursued by minimizing the collection, retention, and exposure of metadata that could enable inferences about relationships between public keys, since there is no centralized identity registry and privacy can be undermined by wallet-side metadata leakage.[741]

Neutralising linkability is consistent with the Court's dereferencing case-law in Google Spain and Google v CNIL, where the right to erasure is given effect by removing associations rather than deleting the underlying content.[742] Applied to wallets, the transaction record remains on-

[737] Wasabi, (2025). *Wasabi Documentation*. Available at: https://docs.wasabiwallet.io/, (Accessed: 12 December 2025).
[738] Stodt, F., Reich, C. and Stodt, F., (2024). *Digital Wallets and Identity Management: Pioneering Advances for Cloud Service Evolution*. International Journal on Advances in Software, 17(1 & 2), pp.13–22. Available at: https://www.researchgate.net/publication/382085119_Digital_Wallets_and_Identity_Management_Pioneering_Advances_for_Cloud_Service_Evolution, (Accessed: 12 December 2025).
[739] Meiklejohn et al., 2016, pp. 127–140.
[740] Erinle, Y., Kethepalli, Y., Feng, Y. and Xu, J., (2023). *Sok: Design, vulnerabilities, and security measures of cryptocurrency wallets. arXiv preprint arXiv: 2307.12874*, p. 6.
Available at: https://www.semanticscholar.org/reader/50b6223da198d5e18fd58e2798340dd9479f15a3, (Accessed: 12 December 2025).
[741] Gindre, F., Urbieta, M. and Rossi, G., (2022). *Patterns for Anonymity Enhancing Cryptocurrencies Non-Custodian Mobile Wallets*. In Proceedings of the 29th Conference on Pattern Languages of Programs, pp. 1–29. Available at: https://hillside.net/plop/2022/papers/G1_P3.pdf, (Accessed: 12 December 2025).
[742] Purtova, N., (2022). *From knowing by name to targeting: the meaning of identification under the GDPR*. International Data Privacy Law, Volume 12, No 3, pp. 163–183. Available at: https://www.researchgate.net/publication/361486992_From_knowing_by_name_to_targeting_the_meaning_of_identification_under_the_GDPR, (Accessed: 12 April 2026); see also, Tene, O. and Polonetsky, J., (2011).

chain, but the provider must ensure that its interface no longer presents that history in a way that identifies the requester or links it to them.

5.4.4 Interface-Level Mitigation and Contextual Decoupling

Wallet interfaces are key mediators of visibility. Even where providers cannot alter the underlying ledger, they control how on-chain data are retrieved, displayed, and contextualised. Effective forgetting therefore depends on intervention at the interface layer to reduce the informational salience of on-chain personal data.

Such measures may include: (i) removing historical transactions from default views;[743] (ii) clearing local caches that retain transaction histories or contract interactions;[744] (iii) disabling features that automatically cluster addresses;[745] (iv) refraining from generating user-specific analytics derived from past transactions;[746] and (v) ensuring that interfaces do not display deprecated or suppressed identifiers in a way that discloses their association with the data subject.[747] These measures reflect the GDPR's concern not only with the content of information, but with the conditions under which it is accessed, presented, and rendered intelligible.

In non-custodial and hybrid wallets, whose interfaces often aggregate data across numerous addresses or third-party services, contextual decoupling is especially important. In order to ensure that suppression requests are respected across all interface elements, including those that rely on external APIs or indexing services, providers must adapt these aggregation mechanisms.

Privacy in the age of big data: a time for big decisions. 64 STAN. L. REV. ONLINE 63, pp. 64–68. Available at: https://www.researchgate.net/publication/259892061_Privacy_in_the_Age_of_Big_Data_A_Time_for_Big_Decisions, (Accessed: 12 April 2026).

[743] GDPR, Article 4(2); WP216, Opinion 05/2014, 2014, pp. 7–12, 23–24; EDPB Guidelines 02/2025, paras 62–74.

[744] GDPR, Articles 4(2), 17(1), and 17(2); Article 29 Working Party, (2017). *Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation.* (2002/58/EC), pp. 12–13. Available at: https://ec.europa.eu/newsroom/article29/items/610140/en, (Accessed: 15 December 2025).

[745] GDPR, Recital 26; Meiklejohn et al., 2016, pp. 1–2, 7–8, 8–11; WP216, Opinion 05/2014, 2014, pp. 10–12, 22–23.

[746] GDPR, Articles 4(2), and 21; EDPB Guidelines 8/2020, paras 63–77; Jehovan todistajat, Case C-25/17, paras 52–62, 68–71.

[747] GDPR, Recital 39; WP216, Opinion 05/2014, 2014, pp. 20–21; European Data Protection Board, (2023). *Guidelines 01/2022 on data subject rights - Right of access*. Version 2.1, paras 10–11, 31–34, 41–44, 46–47. Available at: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012022-data-subject-rights-right-access_en, (Accessed: 12 December 2025).

5.4.5 Metadata Minimisation and Infrastructure Adjustments

Wallet providers exercise material influence over metadata flows, particularly where they operate or preconfigure RPC nodes, indexing services, or analytics endpoints. Effective forgetting requires that providers adjust these flows to minimise the continued generation or dissemination of personal data linked to the individual seeking erasure. This includes (i) ceasing to retain IP addresses, routing logs, or session identifiers associated with the user,[748] (ii) adjusting default RPC configurations to reduce unnecessary collection or retention,[749] (iii) implementing privacy-enhancing techniques such as proxying, traffic minimisation, or onion-routing,[750] and (iv) requiring infrastructure partners to comply with erasure requests where joint controllership applies.[751] Providers must also ensure that metadata suppression does not undermine the security or functionality of the wallet, consistent with the GDPR's principle of proportionality.

5.4.6 A Legal Test for Effective Forgetting under Article 17 GDPR

The preceding analysis suggests that the application of Article 17 GDPR in decentralised environments requires a structured method for determining when erasure obligations can be considered fulfilled despite the persistence of immutable ledger records.[752] Building on the functional approach to controllership and the proportionality principle embedded within EU data protection law, effective forgetting may be operationalised through a multi-step legal assessment capable of accommodating technological constraints while preserving the protective purpose of Article 17.[753]

First, controllers must identify the relevant layers of personal data processing within the system architecture. Blockchain-based services typically involve multiple categories of data, including on-chain identifiers, off-chain metadata, and interface-level representations of user activity.[754] Each layer involves distinct technical characteristics and varying degrees of

[748] GDPR, Articles 4(1), 4(2) and 5(1)(c)(e); Breyer v Bundesrepublik Deutschland, C-582/14, paras 3–8.
[749] GDPR, Article 4(2); EDPB Guidelines 07/2020, paras 1–4, 39–40; Wirtschaftsakademie Schleswig-Holstein, Case C-210/16, paras 31, 39–44, 45–48.
[750] GDPR, Article 25, and Recital 78; WP216, Opinion 05/2014, 2014, pp. 11–12; EDPB Guidelines 4/2019 on Article 25, pp. 21–22.
[751] GDPR, Article 26; Jehovan todistajat, Case C-25/17, paras 65–69; Fashion ID, Case C-40/17, paras 65–69, 75–79.
[752] Lenaerts, K. and Gutiérrez-Fons, J.A., (2013). T*o say what the law of the EU is: methods of interpretation and the European Court of Justice.* Colum. J. Eur. L., 20, pp. 10–16. Available at: https://lirias.kuleuven.be/1854710?limo=0, (Accessed: 12 April 2026).
[753] Grimmelmann, J., (2004). *Regulation by software*. Yale LJ, 114, pp. 1732–1736. Available at: https://james.grimmelmann.net/files/articles/regulation-by-software.pdf, (Accessed: 12 April 2026).
[754] EU Blockchain Observatory and Forum, 2018, Blockchain and the GDPR, pp. 14–19; see also, Atzei et al., 2017, pp. 1–22.

controllability.[755] On-chain data may include public keys, transaction hashes, timestamps, and smart contract interactions recorded permanently within the ledger. Off-chain data may include account credentials, device identifiers, IP addresses, telemetry logs, and behavioural analytics generated through the operation of wallet software and supporting infrastructure. Interface-level processing may involve the aggregation, visualisation, or contextual association of on-chain records within user-facing environments.[756] The legal assessment of erasure must therefore begin with a granular understanding of which categories of personal data are processed and where factual influence over those data can be exercised.

Second, controllers must determine the extent of their factual influence over the purposes and means of processing. In accordance with the functional interpretation of controllership developed in the jurisprudence of the Court of Justice, responsibility under the GDPR arises wherever an actor exerts influence over the conditions under which personal data are collected, structured, or made accessible.[757] The absence of direct control over blockchain infrastructure does not negate controllership where the actor determines how personal data are processed within the application layer.[758] Wallet providers, infrastructure intermediaries, analytics partners, and software developers may therefore each qualify as controllers or joint controllers in respect of specific processing operations.

Third, controllers must implement technically feasible measures capable of approximating the protective function of erasure.[759] Such measures may include deletion of off-chain personal data, suppression of cached records, removal of identity linkages, minimisation of metadata collection, or interface-level adjustments that reduce the accessibility of personal data.[760] Where deletion is not technically possible, controllers must consider whether

[755] Finck, 2019, pp. 11–18.
[756] EU Blockchain Observatory and Forum, 2018, Blockchain and the GDPR, pp. 24–30.
[757] Millard, C.J. ed., (2013). *Cloud computing law*. (Vol. 2). Oxford: Oxford University Press, pp. 3–16. Available at: https://www.researchgate.net/profile/Christopher-Millard-2/publication, (Accessed: 12 April 2026); see also, Klonick, K., (2017). *The new governors: The people, rules, and processes governing online speech*. Harv. L. Rev., 131, pp. 1625–1632. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2937985, (Accessed: 12 April 2026).
[758] Hartzog, W. and Selinger, E., (2013). *Big data in small hands*. Stan. L. Rev. Online, 66, pp. 81–88. Available at: https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=4027&context=faculty_scholarship, (Accessed: 12 April 2026).
[759] Gellert, R., (2018). *Understanding the notion of risk in the General Data Protection Regulation*. Computer Law & Security Review, Volume 34, Issue 2, Published by Elsevier Ltd, pp. 279–288. Available at: https://www.sciencedirect.com/science/article/pii/S0267364917302698, (Accessed: 12 April 2026).
[760] Rubinstein, I.S., (2013). *Big data: the end of privacy or a new beginning?*. International Data Privacy Law, NYU School of Law, Public Law Research Paper No. 12-56, pp. 1–14. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2157659, (Accessed: 12 April 2026).

alternative measures, such as delinking or contextual neutralisation, are capable of reducing the risk of identification to a degree consistent with the objectives of Article 17. The adequacy of such measures should be evaluated in light of their practical effect on the accessibility and interpretability of personal data.

Fourth, the implementation of effective forgetting must comply with the principle of proportionality. Controllers are required to adopt measures that are appropriate and reasonable in light of the available technological means, the risks posed to data subjects, and the legitimate interests pursued by the processing.[761] The GDPR does not require the adoption of measures that would undermine the security, integrity, or functionality of decentralised systems.[762] However, controllers must demonstrate that they have taken all reasonable steps to minimise the persistence of identifiable information within the scope of their factual influence.

The operationalisation of effective forgetting must also be situated within the limitations provided under Article 17(3) GDPR, which recognises that continued data availability may be justified where processing is necessary for compliance with legal obligations, the exercise of freedom of expression, or the establishment, exercise, or defence of legal claims. In blockchain ecosystems, transparency may contribute to objectives such as financial accountability, transaction verifiability, and market confidence. These considerations indicate that effective forgetting should not be interpreted as requiring the removal of data where continued accessibility serves legitimate regulatory or societal purposes, but rather as requiring proportionate technical and organisational measures capable of reducing unnecessary identifiability.

[761] De Vries, S.A., (2013). *Balancing fundamental rights with economic freedoms according to the European Court of Justice.* Volume 9, Issue 1, urn:nbn:nl:ui:10-1-112916, pp. 169–192. Available at: https://utrechtlawreview.org/articles/220/files/submission/proof/220-1-468-1-10-20130131.pdf, (Accessed: 12 April 2026).

[762] Koops, B.J. and Leenes, R., (2014). *Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law*. International Review of Law, Computers & Technology, 28(2), pp. 1–13. Available at: https://www.researchgate.net/publication/259289517_Privacy_regulation_cannot_be_hardcoded_A_critical_comment_on_the_'privacy_by_design'_provision_in_data-protection_law, (Accessed: 12 April 2026).

Finally, the accountability principle requires that controllers document the measures adopted in order to demonstrate compliance with Article 17.[763] Records of data-retention schedules, technical suppression mechanisms, and organisational procedures provide evidence that erasure obligations have been implemented in a manner consistent with the requirements of EU data protection law. The effective application of Article 17 in decentralised environments therefore depends not on the elimination of data persistence altogether, but on the demonstrable reduction of identifiability and accessibility within the scope of controllable processing activities.

5.4.7 Proportionality in Architecture-Sensitive Compliance

The scope for implementing these measures depends on the wallet's architectural model. Custodial wallets retain substantial capacity for off-chain deletion and delinking, but remain unable to alter on-chain records. Non-custodial wallets are subject to more limited erasure obligations, yet must still suppress or delink off-chain metadata under their control. Hybrid wallets combine elements of both models, inheriting their respective constraints while also permitting intervention at both hardware and software layers. By contrast, smart-contract and organisational wallets offer the narrowest scope for effective forgetting, as core governance and transaction logic is encoded on-chain and cannot be modified. In such cases, compliance is necessarily confined to off-chain suppression and the reduction of interface-level visibility.

The GDPR's proportionality principle is central to managing these constraints. should implement appropriate technical and organisational measures that are feasible in light of the state of the art, effective at reducing risks to data subjects, and designed so they don't undermine the system's security and integrity.[764] "Effective forgetting" therefore entails differentiated obligations, calibrated to each actor's factual influence over the processing and the technical architecture in which the processing occurs.[765] This approach reflects recent scholarship emphasising that GDPR compliance in blockchain systems must be assessed through a proportionality-based, case-specific analysis, taking into account technical

[763] Alhadeff, J., Van Alsenoy, B. and Dumortier, J. (2012). '*The accountability principle in data protection regulation: Origin, development and future directions'*, in Guagnin, D., Hempel, L., Ilten, C., Kroener, I., Neyland, D. and Postigo, H. (eds.) *Managing privacy through accountability.* Basingstoke: Palgrave Macmillan, pp. 61–84. https://doi.org/10.1057/9781137032225.
[764] EDPB Guidelines 07/2020, para 80, 83–84.
[765] CNIL, 2018, pp. 1–3, 4–7, 7–9.

feasibility, governance structures, and each actor's factual influence over the processing rather than formal designations alone.[766]

This compliance framework gives operational content to the concept of effective forgetting by identifying concrete measures that wallet providers can implement at the off-chain, interface, and metadata layers.[767] It shows that, although literal erasure is unattainable in decentralised systems, Article 17 GDPR retains normative force when understood as requiring the suppression of linkability, accessibility, and contextual salience. The framework also underscores the need for an architecture-sensitive approach: compliance does not follow from a uniform prescription, but from a calibrated allocation of obligations that reflects the technical and organisational characteristics of each wallet model.

Taken together, this chapter demonstrates that while blockchain protocols resist erasure by design, wallet providers occupy a legally decisive position at which Article 17 GDPR can be operationalised. By distinguishing wallet architectures, allocating functional controllership, and developing an architecture-sensitive model of effective forgetting, the chapter provides a concrete answer to the dissertation's first research question and establishes the foundation for the normative and policy analysis that follows.

5.5 Regulatory Implications of Effective Forgetting

The concept of effective forgetting also reflects the broader structure of the GDPR's data-processing principles under Article 5.[768] The principles of data minimisation, storage limitation, integrity and confidentiality, and accountability collectively require controllers to design processing operations in a manner that reduces unnecessary exposure of personal data and limits the duration of identifiability. In decentralised environments, these principles operate as interpretative tools guiding the implementation of Article 17. Data minimisation supports architectural decisions that avoid recording personal data directly on-chain wherever alternative technical solutions are available.[769] Storage limitation reinforces obligations to remove or suppress off-chain metadata once the purposes of processing have expired.[770] The integrity and confidentiality principle supports the use of cryptographic and organisational

[766] Zafar, 2025, pp. 2–3, 6–9.
[767] CNIL, 2018, pp. 4–9.
[768] GDPR, Article 5.
[769] GDPR, Article 5(1)(c).
[770] GDPR, Article 5(1)(e).

safeguards designed to reduce the accessibility of personal data to unauthorised actors.[771] Accountability requires controllers to demonstrate that such measures have been implemented in a structured and verifiable manner.[772] Effective forgetting therefore represents a systemic interpretation of GDPR principles applied to technologically persistent environments.

This chapter extends the analysis by examining how the concept of effective forgetting may inform regulatory interpretation and supervisory practice. It explores potential pathways through which regulators, industry stakeholders, and protocol developers may integrate effective forgetting into shared governance systems by building on the analytical framework developed in the preceding sections. The discussion also addresses the practical limitations of this approach and identifies areas in which unresolved tensions and open questions remain.

The preceding analysis demonstrates that immutability offers no exemption from the GDPR;[773] despite the persistence of blockchain records, wallet providers remain bound by their Article 17 obligations. What this demands, however, is a recalibration of regulatory application: one grounded in technological neutrality and consistent with the Court of Justice's practical interpretation of controller obligations. This chapter examines the implications of effective forgetting for European data protection authorities, the European Data Protection Board, and other supervisory bodies. It argues that regulatory practice must move beyond enforcement models premised on data alterability and instead engage with the layered, multi-actor forms of processing that characterise blockchain ecosystems.

A first regulatory implication concerns the interpretation of controllership. As shown above, wallet providers often shape the presentation, association, and retention of personal data in ways that go beyond the mere transmission of user-initiated transactions.[774] Under the functional approach to controllership developed by the Court of Justice in Wirtschaftsakademie, Fashion ID, and Jehovan todistajat, such influence may suffice to establish controllership even where the provider has no control over the underlying ledger. Data protection authorities should therefore recognise that blockchain-specific actors, such as wallet developers, RPC node operators, indexing services, and hardware manufacturers, may

[771] GDPR, Articles 5(1)(f), 32.
[772] GDPR, Articles 5(2), 24.
[773] GDPR, Article 1(2); Recital 15.
[774] Kuner et al., 2020, pp. 37–40.

each qualify as controllers or joint controllers in respect of distinct stages of the processing chain.[775] A governance framework based on rigid actor classifications is poorly adapted to decentralised systems; regulatory analysis should instead proceed on the basis of a layered allocation of responsibility reflecting the varying degrees of factual influence exercised across the ecosystem.

A second implication concerns the articulation of erasure obligations. Current regulatory guidance, including the Article 29 Working Party's Opinion on Anonymisation, the EDPB's Guidelines on the interplay between the GDPR and blockchain, and case-specific analyses by data protection authorities, remains grounded in assumptions derived from mutable database systems.[776] These instruments often restate the statutory language of "erasure" without clarifying whether functional equivalents can satisfy the substantive objectives of Article 17 in immutable environments. Therefore, where it is physically impossible to remove the underlying data, regulators should specifically acknowledge effective forgetting as a legitimate interpretation of erasure. This recognition must be followed by precise standards that indicate whether contextual neutralisation, delinking, or suppression will be adequate. Doing so would give providers greater legal certainty and promote more consistent implementation across different Member States.[777]

A third implication for regulation concerns mechanisms for supervision and enforcement. Traditional compliance audits assume that controllers maintain centralised databases from which data can be removed on request.[778] In blockchain-based environments, processing may be distributed across client software, remote nodes, analytics partners, and cloud-based telemetry services.[779] Supervisory authorities will need to adapt their investigative and forensic methods to these environments, including auditing interface behaviour, reviewing API communication patterns, and assessing metadata retention by infrastructure partners.[780] Enforcement strategies should also be tailored to wallet architecture: custodial actors may be

[775] GDPR Article 4(7) and Recital 79; see also, Wirtschaftsakademie Schleswig-Holstein, Case C-210/16; Fashion ID, Case C-40/17; Jehovan todistajat, Case C-25/17.
[776] WP216, Opinion 05/2014, 2014, paras 10–12, 26–28; EDPB Guidelines 2/2019, pp. 24–25, 43–45, and 52–56.
[777] GDPR, Article 5; EU Charter, Article 52(1).
[778] Kuner et al., 2020, pp. 92–95.
[779] Quintais, J.P., Bodo, B., Giannopoulou, A. and Ferrari, V., (2019). *Blockchain and the law: A critical evaluation*. Stanford Journal of Blockchain Law & Policy, 2 (1), pp. 86–88, 175–184. Available at: https://pure.uva.nl/ws/files/42676576/Blockchain_and_the_Law.pdf, (Accessed: 12 December 2025).
[780] GDPR, Articles 58(1)(a)–(e); Kuner et al., 2020, pp. 92–95.

subject to stricter erasure expectations, while non-custodial or hardware-based providers may have narrower but still meaningful duties to suppress off-chain data and avoid unnecessary linkage.

A fourth implication concerns the interaction between data protection law and sector-specific financial regulation.[781] Custodial wallet providers are now progressively falling under the EU's AML/CFT travel rule, which requires them to gather, share, and store information about the originator and recipient of crypto-asset transfers.[782] In addition, the EBA's Travel Rule Guidelines set out more detailed supervisory requirements and operational compliance measures, including protocols for instances of absent information, technical barriers, and transfers to or from self-hosted wallets.[783] Accordingly, Article 17 GDPR duties need to be understood in the context of these legally mandated retention obligations.[784] Where erasure rights intersect with mandatory AML retention obligations, the law permits postponement of deletion for the duration of the statutory period, but no longer.[785] Effective cooperation between data protection supervisors, financial regulators, and cybersecurity authorities is necessary to balance these competing demands and protecting individual rights, while maintaining crucial oversight functions and avoiding retention beyond what is absolutely necessary.

Supervisory authorities might also develop blockchain-specific codes of conduct or certification schemes aimed at wallet providers. These could set basic expectations around metadata minimisation, default RPC configurations, interface-based suppression, and how long off-chain data should be retained. Given how varied wallet infrastructures are, any standards need to be flexible enough to accommodate custodial, non-custodial, smart-contract, and hybrid wallet models; each with its own compliance requirements.

[781] Lynskey, 2015, pp. 14, 35–39, 41–43.
[782] Regulation (EU) 2023/1113, Articles 3, 14–17, 26.
[783] European Banking Authority, (2024). Guidelines on information requirements in relation to transfers of funds and certain crypto-assets transfers under Regulation (EU) 2023/1113. ('Travel Rule Guidelines'), Final Report, EBA/GL/2024/11, paras 5–6, 12–14, 21–26, and 34–41.
Available at: https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/anti-money-laundering-and-countering-financing-terrorism/guidelines-information-requirements-relation-transfers-funds-and-certain-crypto-assets-transfers, (Accessed: 19 December 2025).
[784] GDPR, Article 17(3)(b), Article 6(1)(c); see also, GC and Others, C-136/17, paras 66–68.
[785] GDPR, Article 5(1)(e), Article 17(3)(b); see also Tele2 Sverige C-203/15, paras 96–99, 101–103; and, Court of Justice of the European Union, (2008). Case C-524/06, Heinz Huber v Bundesrepublik Deutschland, ECLI:EU:C:2008:724, paras 58–63, 66–68. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62006CJ0524, (Accessed: 19 December 2025).

Certification schemes, whether through Article 42 GDPR or industry-led accreditation programmes, could help achieve more consistent implementation of effective forgetting across jurisdictions. They would also reduce regulatory fragmentation and provide stronger assurances to both users and regulators.

Taken together, these implications indicate that effective forgetting concerns not only the interpretation of erasure but also the orientation of supervisory practice. In permissionless or genuinely decentralised environments, supervision cannot assume a readily identifiable controller with unilateral power to alter data stores or reverse transactions.[786] Regulatory frameworks must therefore be applied in a manner that preserves the effectiveness of fundamental rights within architectures in which modification may be technically or governance-constrained by distribution and relative immutability. On this understanding, effective forgetting operates as a governance approach that maintains the practical applicability of the GDPR where data alteration is structurally limited, requiring functional equivalents, for example, access restriction, key destruction, or rendering data practically inaccessible, rather than literal deletion.

5.6 Technical and Industry Governance Mechanisms

While regulatory authorities play an important role in interpreting the scope and limits of erasure obligations, the realisation of effective forgetting in practice depends primarily on the technical and organisational choices made by industry actors. Blockchain ecosystems are not shaped by statutory compliance alone. They are constituted through a network of standards bodies, open-source developers, infrastructure providers, and wallet developers whose design decisions determine how personal data is collected, transmitted, and retained. This section therefore examines how effective forgetting can be integrated into the design and governance of wallet infrastructures, on the premise that technical standards and industry practices often have a more immediate impact on user experience than formal regulatory requirements.

A first dimension of industry governance relates to standards-setting and protocol design.[787] Wallet software, RPC endpoints, key-management architectures, and user-interface conventions are often shaped by open-source standards developed within technical

[786] Wright, Filippi, 2018, pp. 131–133,134–136.
[787] GDPR, Article 25; see also, Bygrave, L.A., 2002. *Data Protection Law: Approaching Its Rationale. Logic and Limits.* (The Hague: Kluwer Law International, 2002), at, 316, pp. 165–172.

communities such as the Ethereum Foundation,[788] the WalletConnect consortium,[789] and the W3C Decentralized Identifier Working Groups.[790] These standards determine default practices in areas including address derivation, transaction propagation, data caching, and node communication. Incorporating principles of effective forgetting at this level could produce effects across the ecosystem.[791] By way of illustration, protocol specifications could discourage the retention of IP addresses in RPC interactions, promote standardised address-rotation practices in wallet design, or establish metadata-minimising APIs as default implementations. Because these standards bodies operate through consensus-based and technically driven governance processes, they are well placed to disseminate privacy-protective design choices at scale.

A second dimension concerns the role of infrastructure intermediaries, including RPC node operators, indexing services, and blockchain explorers. Although these actors are often peripheral to direct regulatory oversight, they shape the collection, organisation, and exposure of personal data.[792] In the ordinary course of operation, their systems generate and retain network-level metadata such as IP addresses, transaction-relay information, and access logs, and they determine how on-chain data is indexed and made searchable.[793] Addressing effective forgetting therefore requires that such intermediaries apply defined retention limits, metadata-reduction measures, and suppression techniques consistent with the obligations identified above. Wallet providers should also structure their relationships with these intermediaries through appropriate data-processing or joint controllership arrangements, so that responsibility for metadata processing is clearly allocated.

A third dimension concerns wallet-level design governance, which determines how users encounter and interpret on-chain data. Interface choices made by wallet providers, such as whether to display historical transactions, link multiple addresses, or present analytics derived from prior activity, significantly influence the contextual visibility of personal

[788] Ethereum Foundation, (2025). *JSON-RPC API*. Available at: https://ethereum.org/developers/docs/apis/json-rpc/, (Accessed: 19 December 2025).
[789] WalletConnect, (2025). *Relay Protocol (Specification/Documentation).* Available at: https://specs.walletconnect.com/2.0/, (Accessed: 19 December 2025).
[790] W3C, (2015). *World Wide Web Consortium Process Document.* Available at: https://www.w3.org/2015/Process-20150901/, (Accessed: 19 December 2025); see also, W3C, (2022). Decentralized Identifiers (DIDs) v1.0: Core Architecture, Data Model, and Representations. Available at: https://www.w3.org/TR/did-1.0/, (Accessed: 19 December 2025).
[791] Finck, 2018, pp. 133–137.
[792] EDPB Guidelines 07/2020, paras 54–68.
[793] GDPR, Article 4(1); Finck, 2018, pp. 119–120, 134–136, 140–141.

data.[794] Supporting effective forgetting therefore requires interface designs that enable suppression, delinking, or contextual neutralisation of such information. These design approaches could be harmonised across providers through shared technical guidelines or industry codes of conduct developed in line with Article 40 GDPR.[795] Such coordination would promote consistent compliance expectations and reduce the risk that divergent interface practices undermine user privacy.

A fourth dimension concerns open-source governance and community accountability. Many popular wallet clients are released under open-source licences, allowing external code review and community-submitted modifications.[796] This governance model creates opportunities to incorporate effective-forgetting techniques into released software through community review, auditing, or structured improvement proposals.[797] However, decentralised decision-making can slow the adoption of privacy-focused changes, and without formal institutional structures, implementation varies considerably across projects.[798] Still, open-source governance provides an important mechanism for building privacy-supportive design choices into wallet architecture, particularly when supported by foundations or dedicated working groups.[799]

A fifth dimension concerns industry certification and audit mechanisms. Technical compliance requires verifiable evidence of implementation.[800] Certification schemes under Article 42 GDPR, alongside sector-specific initiatives developed by industry bodies, can translate abstract data-protection principles into concrete and verifiable benchmarks for metadata suppression, secure deletion, address delinking, and interface-level controls. This responds to long-standing critiques that rights such as the right to be forgotten risk remaining ineffective unless supported by enforceable technical and organisational measures capable of operationalising "forgetting" in practice.[801]

[794] EDPB Guidelines 4/2019, paras 40–43, 54–55.
[795] Kamara, I. (2020). *Article 40: Codes of Conduct*. in Kuner, C., Bygrave, L.A. and Docksey, C. (eds) The EU General Data Protection Regulation (GDPR): A Commentary. Oxford: Oxford University Press, section 5.
[796] For instance, MetaMask, LedgerLive, and TrustWallet.
[797] Benkler, Y., (2006). *The Wealth of Networks. How Social Production Transforms Markets and Freedom*. Yale University Press, ISBN-13: 978-0-300-11056-2 (alk. paper), pp. 60–63. Available at: https://www.benkler.org/Benkler_Wealth_Of_Networks.pdf, (Accessed: 22 December 2025).
[798] Werbach, 2018, pp. 97–109.
[799] GDPR, Article 40(1)(2); Kamara, 2020, pp. 717–723; Bygrave, 2002, pp. 165–169.
[800] GDPR, Articles 5(2), 42–43, and Recital 39; see also, Kuner et al., 2020, pp. 309–320.
[801] GDPR, Articles 25, 42; Koops, 2011, pp. 249–255

Independent audits can assess whether wallet providers comply with retention schedules, apply data minimisation principles, and configure their systems in line with those standards. Such mechanisms also introduce incentive effects, as certification allows providers to demonstrate adherence to recognised privacy safeguards and distinguish themselves within competitive markets.[802]

The implementation of effective forgetting must be considered within the broader governance dynamics of decentralised networks. Although wallet providers operate primarily at the application layer, protocol-level developments such as account abstraction, zero-knowledge proof integration, and privacy-preserving transaction mechanisms increasingly influence the extent to which data is exposed or retained on-chain. Governance arrangements should therefore enable coordination between protocol developers and wallet providers so that new technical features are consistent with the principles developed in this dissertation.[803] In the absence of such coordination, privacy-enhancing protocol innovations may remain underused, while wallet-level privacy measures may be constrained by protocol designs that continue to generate or reveal metadata and transaction linkages.[804]

Taking everything into account, these governance mechanisms illustrate that effective forgetting extends beyond doctrinal interpretation and regulatory enforcement. It necessitates adjustments to the technical and organisational norms and standards, that influence and shape wallet design and blockchain infrastructure. Industry participants have a direct impact on implementation of Article 17 of the GDPR safeguards through standards, interface design, infrastructure governance, and certification schemes. The feasibility of effective forgetting therefore turns on whether decentralised governance models embed privacy considerations within system design and day-to-day operations, rather than approaching them merely as externally imposed legal duties.

5.7 Multi-Stakeholder Allocation of Responsibility

Effective forgetting cannot be implemented by wallet providers acting alone. In blockchain ecosystems and technologies, personal data is generated, communicated, processed,

[802] GDPR, Articles 5(1)(c)(e), 24; Kuner et al., 2020, pp. 25–32.
[803] Gregorio, G., D., (2022). *Digital Constitutionalism in Europe*. Reframing Rights and Powers in the Algorithmic Society. Cambridge University Press, 3, The Law of the Platforms, pp. 80–122. Available at: https://www.cambridge.org/core/books/digital-constitutionalism-in-europe/law-of-the-platforms/DA41AF99D14B885E60EC0CFC7E4F6106, (Accessed: 22 December 2025).
[804] Bygrave, 2002, pp. 165–169.

transformed and presented by a number of players whose actions are only partially coordinated through multi-layered processing chains.[805] Unlike centralised platforms, where data flows are largely determined and mostly controlled by a single entity, decentralised systems distribute responsibility and accountability across technical, organisational, and infrastructural components.[806] This distribution does not diminish the applicability of the GDPR.[807] Instead, it calls for a differentiated allocation of obligations based on factual influence over processing, in line with the functional approach to controllership developed in EU jurisprudence.[808] This section examines how responsibility should be allocated in order to enable the operationalisation of effective forgetting across the ecosystem.

The allocation of responsibility within decentralised ecosystems may therefore be conceptualised as a layered structure reflecting differentiated degrees of factual influence over personal data processing. Wallet providers typically determine the interface-level presentation and off-chain storage of personal data, thereby exercising primary responsibility for implementing delinking and suppression measures. Infrastructure intermediaries, including RPC providers and indexing services, influence the generation and retention of network-level metadata and may therefore qualify as joint controllers in relation to metadata processing activities. Analytics providers shape the persistence of identity linkages through clustering and attribution techniques, thereby affecting the durability of personal-data associations that data subjects may seek to neutralise. Protocol developers and governance bodies determine architectural conditions that influence the long-term persistence and exposure of personal data. This layered allocation of responsibility reflects the functional logic of the GDPR and ensures that accountability is distributed in accordance with actual influence over the processing environment.

As established in this chapter, a first locus of responsibility lies with wallet providers, who constitute the primary interface through which individuals access and interact with blockchain networks. Through their design and architectural choices, wallet providers shape not only the presentation of on-chain information but also the generation, retention, and

[805] EDPB Guidelines 07/2020, paras 1–4, 6–10, 42–43, 45.
[806] Gregorio, 2022, pp. 83–90.
[807] EDPB Guidelines 07/2020, paras 10–14, 42–45.
[808] GDPR, Article 4(7); Wirtschaftsakademie Schleswig-Holstein, Case C-210/16, paras 27–30, 35–39, 42–44.

dissemination of off-chain metadata.[809] Where they determine the purposes and means of these processing activities, they qualify as controllers, or in some cases joint controllers, and therefore bear primary responsibility for implementing measures such as suppression, delinking, retention limits, and interface-level contextual neutralisation.[810] Wallet providers also occupy a coordinating position within the broader processing ecosystem.[811] By choosing and configuring the technical infrastructure their applications rely on, including RPC nodes, indexing tools, and analytics endpoints, industry actors effectively shape and control subsequent data flows.[812] Their responsibility is thus twofold: it is direct, insofar as it concerns personal data processed within their own systems, and relational, insofar as it extends to shaping the processing practices of interconnected actors.

A second category of relevant actors consists of RPC node operators and other blockchain infrastructure providers. Although frequently marginalised in regulatory discussions, these entities process significant volumes of metadata, including IP addresses, timestamps, and request patterns, whenever a wallet queries blockchain state or submits transactions.[813] Where a wallet provider selects a default infrastructure service and routes user activity through it by design, as illustrated by the commonly cited MetaMask and Infura configuration, the infrastructure provider may participate in determining both the purposes and the means of processing, and at least in part, the purposes for which associated metadata are processed.[814] In such circumstances, the conditions for joint controllership under the GDPR may be satisfied. The operationalisation of effective forgetting therefore depends on the alignment of erasure and suppression practices across both wallet providers and infrastructure intermediaries.[815] This requires that metadata retention, deletion, and suppression measures be implemented consistently, and that the allocation of responsibilities be formalised through contractual arrangements specifying retention periods, technical safeguards, and compliance obligations.[816] Absent such coordination, an erasure request addressed solely to the wallet

[809] Finck, M., (2019). *Blockchain Regulation and Governance in Europe*. Cambridge University Press. ISBN 9781108609708, pp. 143–145.
[810] GDPR, 4(7); see also, GDPR Commentary 2020, pp. 145–156.
[811] Finck, M., (2019). Blockchain Regulation and Governance in Europe, pp. 45–56.
[812] EDPB Guidelines 07/2020, paras 12, 20–21, 25–26.
[813] Getblock, (2025). *Eth_call – Ethereum, API Reference*. Available at: https://docs.getblock.io/api-reference/ethereum-eth/eth_call-ethereum, (Accessed: 22 December 2025).
[814] Getblock, (2025). *How to Add GetBlock RPC Endpoints to MetaMask*. Available at: https://getblock.medium.com/how-to-add-getblock-rpc-endpoints-to-metamask-3a964abdec2a, (Accessed: 22 December 2025); see also, WP169, Opinion 1/2010, 2010, pp. 4, 14–15, 20–21.
[815] EDPB Guidelines 07/2020, paras 48, 57–58.
[816] GDPR, Articles 26 and 28; GDPR Commentary 2020, pp. 582–588, 599–611.

provider would leave intact parallel metadata stores maintained by infrastructure actors, thereby undermining the practical effectiveness of Article 17 GDPR.

A third set of actors includes blockchain analytics firms, whose business models depend on aggregating, clustering, and attributing on-chain activity. These firms play a crucial role in deanonymisation: by linking addresses, heuristically identifying behavioural patterns, and correlating on-chain and off-chain signals, they transform pseudonymous data into identifiable profiles.[817] Although analytics firms often claim that their activities involve only publicly available data, the layering and inference processes they employ generate assessments and profiles that relate to identifiable individuals and therefore constitute personal-data processing under EU law.[818] Their operations therefore directly influence whether effective forgetting can be achieved, as they determine the durability of linkages the user seeks to suppress.[819] For effective forgetting to function, wallet providers and analytics firms must recalibrate their relationships: either by limiting data sharing, by preventing interface calls that route user queries to analytics providers, or by requiring that analytics partners honour suppression requests within the scope of their operations.

A fourth locus of responsibility concerns blockchain foundations and protocol governance bodies. Although these actors do not typically engage in user-level personal data processing, they define the architectural conditions under which personal data is produced, exposed, and rendered persistent.[820] Protocol design decisions relating to transaction formats, mempool visibility, fee mechanisms, and account abstraction directly shape the degree to which user activity can be linked, traced, or retained over time.[821] While such entities will rarely qualify as controllers for the purposes of the GDPR, their influence over protocol evolution positions them to enable or restrict technical pathways for effective forgetting. Their governance responsibility therefore lies in ensuring that protocol-level design choices support, rather than

[817] Meiklejohn et al., 2016, pp. 86–93; European Data Protection Board, (2025). *Guidelines 01/2025 on Pseudonymisation*. (version for public consultation), paras 21–22, 42.
[818] GDPR, Article 4(1); Peter Nowak v Data Protection Commissioner, C-434/16, paras 34–35, 36–39, 42–43; EDPB Guidelines 07/2020, paras 161–170.
[819] CNIL, 2018, pp. 1–10.
[820] Gregorio, 2022, pp. 83–90.
[821] Meiklejohn et al., 2016, pp. 86–93; Decker, C., Wattenhofer, R., (2013). *Information propagation in the Bitcoin network*. Conference: Peer-to-Peer Computing (P2P), 2013 IEEE Thirteenth International Conference, pp. 1–10.
Available at:
https://www.researchgate.net/publication/261434466_Information_propagation_in_the_Bitcoin_network, (Accessed: 22 December 2025).

undermine, interface-level suppression and delinking measures, including through privacy-preserving defaults, metadata-minimising standards, and optional account architectures that reduce long-term linkability.[822]

A fifth category consists of decentralised application developers and smart contract deployers, whose code frequently mediates user interaction with on-chain systems. Where smart contracts embed persistent identifiers or record user-related information on-chain, developers may generate immutable traces that cannot be meaningfully suppressed at the interface level.[823] Although the applicability of the GDPR to smart contract deployers is context-dependent, developers who determine the purposes for which personal data is recorded on-chain may qualify as controllers or joint controllers.[824] Effective forgetting therefore requires the adoption of privacy-by-design practices at the development stage, including the avoidance of on-chain storage of personal data where feasible, the use of off-chain architectures for sensitive elements, and the incorporation of upgrade, revocation, or migration mechanisms compatible with decentralised governance structures.[825]

Finally, users themselves influence the practical feasibility of effective forgetting. Although the GDPR does not impose obligations on natural persons acting in a purely personal or household capacity,[826] users retain significant control over key management practices, address reuse, and the selection of privacy-enhancing tools. Weak operational practices, such as reusing addresses across distinct contexts, can generate durable linkability that no provider can fully neutralise ex post.[827] While such behaviour does not attract legal liability, governance frameworks may incorporate educational measures, interface-level prompts, and privacy-protective default configurations aimed at promoting usage patterns that reduce long-term identifiability.

---

[822] Hildebrandt, M., (2018). *Algorithmic regulation and the rule of law*. Phil. Trans. R. Soc. A 376:20170355. Research Article, Volume 376, Issue 2128.
Available at: https://royalsocietypublishing.org/rsta/article/376/2128/20170355/115625/Algorithmic-regulation-and-the-rule-of, (Accessed: 22 December 2025); see also, EDPB Guidelines 07/2020, paras 18–21.
[823] Wright, Filippi, 2018, pp. 2, 13, 35–37.
[824] GDPR, Article 4(7); EDPB Guidelines 07/2020, paras 46–68.
[825] GDPR, Article 25; EDPB Guidelines 4/2019, paras 44–50, 60, 73–76; CNIL, 2018, pp. 1–10.
[826] GDPR, Article 2(2)(c) and Recital 18; see also, Court of Justice of the European Union, (2014). *Ryneš v Úřad pro ochranu osobních údajů (C-212/13)*. EU:C:2014:2428, paras 30–33. Available at: https://curia.europa.eu/juris/document/document.jsf?docid=160561&doclang=EN, (Accessed: 22 December 2025).
[827] Meiklejohn et al., 2016, pp. 86–93; see also, Narayanan et al., 2016, pp. 165–175.

5.8 Practical Implementation Scenarios for Effective Forgetting

The practical operation of effective forgetting becomes clearer when applied to specific wallet architectures. In custodial wallet environments, providers maintain extensive off-chain records linking verified user identities to blockchain addresses and transaction histories. Where erasure conditions under Article 17 are satisfied, effective forgetting may involve deletion of identity verification records once legally mandated retention periods have expired, removal of internal mappings connecting individuals to specific blockchain addresses, and suppression of behavioural analytics derived from prior transaction activity. Although the underlying ledger entries remain intact, the dissociation of identity attributes from persistent transaction records substantially reduces the identifiability of the data subject within the provider's processing environment.

In non-custodial wallet environments, providers exercise more limited influence over personal data processing, but nevertheless generate metadata through application telemetry, device identifiers, and interactions with remote infrastructure services. Effective forgetting may therefore involve deletion of diagnostic logs, minimisation of telemetry collection, removal of cached transaction histories stored within the application environment, and adjustments to default network configurations that reduce the continued generation of identifiable metadata.

Smart-contract and organisational wallets present more constrained opportunities for implementing effective forgetting, as governance logic and transactional data are frequently embedded directly within immutable smart-contract code. In such contexts, effective forgetting may be limited to the removal of off-chain identity mappings, the suppression of interface-level associations between addresses and individuals, and the reduction of metadata flows generated through interaction with supporting infrastructure. Although these measures cannot eliminate historical on-chain traces, they reduce the degree to which such traces remain practically attributable to identifiable individuals.

These scenarios illustrate that the feasibility of effective forgetting depends on the interaction between legal obligations and technical architecture. The scope of erasure obligations is therefore not uniform across blockchain environments, but varies according to the degree of influence exercised by each actor over personal data processing operations.

5.9 Embedding Effective Forgetting in Protocol Design

The feasibility of effective forgetting is constrained by the architectural commitments of contemporary blockchain systems. Core design elements and features include public verifiability, permanent record-keeping, and transparent state transitions, nevertheless they significantly limit the ability to alter or suppress personal data once it has been recorded on-chain.[828] On the other hand, blockchain protocols are far from static. Through technical iteration and governance mechanisms that determine how data is created, revealed, and connected across time, they undergo continuous evolution. Emerging innovations at the protocol layer now offer ways to diminish identifiability and constrain data persistence, even where outright deletion remains technically unfeasible. What follows explores how these technical shifts relate to the GDPR's normative architecture and what they might mean for governance design going forward. This section addresses the broader normative and policy dimension of the dissertation by examining how privacy-preserving architectural developments may influence the future interpretation of controllership, accountability, and data-protection compliance within decentralised digital infrastructures.

One potential route for embedding effective forgetting involves account abstraction and programmable key-management architectures. Frameworks such as Ethereum's ERC-4337 decouple user accounts from fixed cryptographic primitives and permit changes to key material, authorisation rules, and account logic over time.[829] Although these mechanisms were not developed for data-protection purposes, they enable forms of key rotation and account reconfiguration that reduce linkability between past and future transactions.[830] Account abstraction cannot eliminate historical on-chain data, but it can disrupt the continuity of identifiers and thereby limit the enduring relevance of immutable traces.[831] From a data-protection perspective, this architectural shift is consistent with the objective of minimising linkability and illustrates how effective forgetting may be supported at the structural level rather than confined to interface-level measures.

A second pathway concerns the use of zero-knowledge proof systems, including zk-SNARKs, zk-STARKs, and related constructions. These techniques allow participants to

[828] EDPB Guidelines 01/2025, paras 14–21.
[829] Buterin, V., Weiss, Y., Tirosh, D., Nacson, S., Forshtat, A., Gazso, K., Hess, D., (2021). *ERC-4337: Account Abstraction Using Alt Mempool' (Ethereum Improvement Proposals*). Available at: https://eips.ethereum.org/EIPS/eip-4337, (Accessed: 22 December 2025).
[830] *Ibid*. see also, Meiklejohn et al., 2016, pp. 86–93.
[831] EDPB Guidelines 01/2025, paras 18–23.

prove compliance with transaction rules without revealing the underlying data, which reduces public exposure of personal information.[832] When built directly into the protocol, zero-knowledge proofs can reduce transaction linkability and decrease the amount of sensitive metadata that appears publicly on-chain.[833] Rather than enabling erasure, these architectures minimize disclosure from the outset, effectively reframing the challenge that effective forgetting attempts to solve.[834] At the same time, zero-knowledge systems raise governance and accountability concerns. Their technical complexity may concentrate control in a limited set of trusted-setup participants, verification services, or specialised operators, creating uncertainty as to how responsibility for data-processing decisions should be allocated.[835] From a data-protection perspective, however, the privacy-by-design properties of zero-knowledge protocols offer a structural context in which effective forgetting is more plausibly supported than in fully transparent ledger models.

A third pathway concerns ephemeral account architectures, which have been examined in both academic and industry research. These approaches rely on temporary identifiers that rotate or expire automatically according to predefined intervals or triggering conditions.[836] By limiting the duration for which an identifier remains valid or linkable to a single user, such architectures reduce longitudinal linkability.[837] Although historical ledger entries remain immutable, their analytical value is diminished by the absence of continuity between past and subsequent interactions.[838] When implemented at the protocol level rather than solely at the

[832] Ben-Sasson, E., Chiesa, A., Green, M., Tromer, E., Virza, M., (2015). *Secure Sampling of Public Parameters for Succinct Zero Knowledge Proofs*. IEEE Symposium on Security and Privacy (SP), 287–302; Groth, J., (2016). *On the Size of Pairing-based Non-interactive Arguments*. IACR Cryptology ePrint Archive/EUROCRYPT, pp. 305–326. Available at: https://eprint.iacr.org/2016/260.pdf, (Accessed: 22 December 2025).
[833] Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., (2014). *Zerocash: Decentralized Anonymous Payments from Bitcoin*. Conference: 2014 IEEE Symposium on Security and Privacy (SP). Available at: https://www.researchgate.net/publication/286668243_Zerocash_Decentralized_Anonymous_Payments_from_Bitcoin, (Accessed: 22 December 2025).
[834] EDPB Guidelines 01/2025, paras 130–135.
[835] Park, C., Chung, M., Ryu, D., (2023*). A Blockchain-based Protocol of Trusted Setup Ceremony for Zero-knowledge Proof*. Proceedings of the 2023 5th Blockchain and Internet of Things Conference, ISBN 9798400708213, pp. 35–40. Available at: https://dl.acm.org/doi/10.1145/3625078.3625083, (Accessed: 22 December 2025).
[836] Troncoso et al., 2017, pp. 318–323.
[837] WP216, Opinion 05/2014, pp. 11–13; see also, El Emam, K., Alvarez, C., (2015). *A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques*. International Data Privacy Law, 5(1), Volume 5, Issue 1, pp.73–87.
Available at: https://academic.oup.com/idpl/article/5/1/73/2863828?login=true, (Accessed: 22 December 2025).
[838] Narayanan et al., 2016, pp. 165–168.

wallet layer, ephemeral identifiers may therefore constitute a structural form of privacy by design consistent with Article 25 GDPR.[839]

A fourth domain concerns privacy-preserving transaction-routing protocols, including decentralised relayers, mix-net architectures, and transaction-batching schemes. These approaches obscure network-level metadata such as IP addresses, timing information, and node interaction patterns, which in line with WP29 guidance that identifiability includes singling out, linkability, and inference may constitute personal data under the GDPR.[840] By altering the paths through which transactions are propagated, they limit the creation and retention of metadata that would otherwise fall beyond the scope of wallet-level erasure mechanisms.[841] From a data-protection perspective, such architectures reduce reliance on ex post erasure by constraining the collection of personal data at the point of transmission. Their integration at the protocol or client level therefore provides stronger structural support for effective forgetting.

A fifth and emerging area concerns the integration of on-chain and off-chain hybrid storage frameworks capable of supporting limited forms of revocability or updateability. In such systems, certain data are stored off-chain and referenced on-chain through commitment schemes, hash pointers, or state channels, allowing the off-chain component to be modified or suppressed at a later stage.[842] While these architectures cannot eliminate on-chain references entirely, they relocate the substantive content of personal data outside the immutable ledger and into an environment where erasure is technically feasible.[843] Protocol-level support for hybrid storage models could therefore offer a more systematic compliance pathway, particularly for applications that currently record unnecessarily granular personal data directly on-chain.

[839] EDPB Guidelines 4/2019, paras 7–16, 33–39; see also, The Royal Society, (2015). *Protecting Privacy in Practice*. The current use, development and limits of Privacy Enhancing Technologies in data analysis. ISBN: 978-1-78252-390-1, pp. 22–26. Available at: https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/protecting-privacy-in-practice.pdf, (Accessed: 22 December 2025).
[840] GDPR, Recital 30; WP216, Opinion 05/2014, 2014, pp. 10–11.
[841] Decker, C., Wattenhofer, R., 2013, pp. 1–10; see also, Meiklejohn et al., 2016, pp. 86–93.
[842] CNIL, 2018, pp. 1–10; Finck, 2019, pp. 37–44.
[843] WP216, Opinion 05/2014, pp. 7–9; CNIL, 2018, pp. 1–10.

Embedding effective forgetting within future blockchain architectures ultimately depends on the governance mechanisms through which protocol changes are adopted.[844] Protocol design is shaped not only by technical feasibility but also by the political and economic incentives that structure decision-making within decentralised communities.[845] Features that enhance privacy may encounter resistance resulting from concerns about regulatory scrutiny, law-enforcement access, or network externalities. On the other hand, users may strongly support proposals that are privacy-focused, whereas core developers and engineers who oversee protocol maintenance may sideline them.

For effective forgetting to work, there need to be governance systems that can regularly assess privacy risks, think through data-protection impacts, and incorporate those issues directly into protocol planning.[846] This could involve establishing formal privacy reviews within protocol foundations,[847] mandating data-protection assessments for improvement proposals,[848] or forming multi-stakeholder groups to evaluate whether proposed protocol changes align with GDPR principles.

These advancements indicate that protecting data in decentralised systems can't depend solely on application-layer measures. Although wallet providers currently play a major role in facilitating effective forgetting, ensuring the GDPR remains coherent within blockchain ecosystems over the long term will require embedding privacy-by-design principles directly into protocol architecture. As a result, this would shift data protection from a reactive approach centered on managing immutability's consequences toward a proactive model built around structural minimisation, limited linkability, and selective visibility. Therefore, protocol evolution encompasses more than just technical advancement; it offers a governance mechanism through which blockchain infrastructures can be redesigned to meet the normative expectations of European data-protection law.

Protocol-level privacy architectures also carry implications for the broader development of EU digital governance. The concept of effective forgetting suggests that compliance in

[844] De Filippi, P. and Loveluck, B., (2016). *The invisible politics of bitcoin: governance crisis of a decentralized infrastructure.* Internet policy review, 5(4), pp. 10–12; 17–18. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2852691, (Accessed: 24 December 2025).
[845] Werbach, 2018, pp. 95–111.
[846] GDPR, Articles 25, 35, 36.
[847] Walch, 2019, pp. 40–42.
[848] De Filippi, Loveluck, 2016, pp. 58–60, 61–63.

decentralised environments depends not only on remedial measures applied after data disclosure, but also on structural design choices capable of reducing linkability and limiting unnecessary persistence of personal data. This perspective aligns with the logic of Articles 17 and 25 GDPR, which together encourage technical and organisational configurations that minimise risks to data subjects throughout the lifecycle of processing.[849] The emphasis on structural risk reduction is also reflected in academic discussions of privacy by design as an architectural principle capable of shaping the informational environment in which personal data are generated and processed.[850] In decentralised systems, where technical persistence limits the feasibility of traditional deletion-based remedies, such design-oriented safeguards may play an increasingly important role in ensuring that data protection obligations retain practical effectiveness.

From a governance perspective, the emergence of privacy-enhancing blockchain architectures highlights the distributed allocation of responsibility across actors who shape how personal data becomes accessible and interpretable.[851] Protocol developers, wallet providers, and infrastructure intermediaries may each influence the conditions under which personal data can be linked, aggregated, or contextualised.[852] This distribution of influence is consistent with the functional interpretation of controllership in EU data protection law, according to which responsibility arises wherever actors participate in determining relevant elements of the processing environment.[853] Effective forgetting therefore reinforces the relevance of coordinated governance approaches capable of integrating data protection considerations into technical development processes, rather than treating compliance solely as an ex post obligation imposed on individual service providers.[854]

[849] GDPR, Articles 17 and 25.
[850] Finck, 2019, pp. 75–82; see also, Cavoukian, A., (2009). *Privacy by design: The 7 foundational principles*. Information and privacy commissioner of Ontario, Canada, 5(2009), p.12. Available at: https://student.cs.uwaterloo.ca/~cs492/papers/7foundationalprinciples_longer.pdf, (Accessed: 05 April 2026).
[851] Yeung, K., (2018). *Algorithmic regulation: A critical interrogation*. Regulation & governance, 12(4), pp. 505–523. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972505, (Accessed: 05 April 2026).
[852] Reidenberg, J.R., (1997). *Lex informatica: The formulation of information policy rules through technology*. 76 Tex. L. Rev. 553 (1997-1998), pp. 553–558. Available at: https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1041&context=faculty_scholarship, (Accessed: 05 April 2026).
[853] GDPR, Article 4(7); EDPB Guidelines 07/2020, paras 20–27.
[854] Brownsword, R., (2019). *Law, technology and society: reimagining the regulatory environment*. Routledge, ISBN: 978-1-351-12818-6 (ebk), pp. 63–69.

In this sense, the gradual incorporation of privacy-preserving design features into distributed ledger infrastructures illustrates the capacity of EU data protection law to remain operational within technologically evolving environments.[855] The development of structurally privacy-compatible architectures may reduce the tension between immutability and erasure by ensuring that identifiability is limited at the point of system design, thereby supporting the continued effectiveness of fundamental rights protection in decentralised processing contexts.[856]

These developments suggest that future regulatory guidance, including EDPB interpretative frameworks and EU digital governance initiatives, may increasingly need to address how privacy-by-design principles can be operationalised within decentralised infrastructures. In this respect, effective forgetting functions not only as a compliance mechanism, but as a governance-oriented interpretative principle capable of supporting the continued applicability of EU data protection law within evolving technological environments.

5.10 Limits, Risks, and Open Questions

The preceding analysis shows that effective forgetting provides a legally and technically plausible bridge between decentralised architectures and the GDPR. Nevertheless, the solution remains partial. By rendering data functionally inaccessible rather than removing it, this approach manages the tension between immutability and erasure without fully resolving it. The following section therefore examines the remaining points of misalignment between legal requirements, industry practice, and protocol design, highlighting unresolved risks that require further consideration.

The persistence of personal data on public blockchains is the most substantial limitation. Despite the fact how sophisticated suppression or delinking mechanisms and tec become, the underlying ledger entries remain publicly accessible to any party capable of querying the blockchain directly.[857] Effective forgetting implemented through regulated intermediaries controls what users encounter through specific interfaces, wallet applications, block explorers operated by compliant entities, but it cannot prevent access by actors who interact with the

[855] Ranchordas, S., 2021. Experimental regulations for AI: sandboxes for morals and mores. Morals & Machines, 1(1), pp. 86–100. Available at: https://pure.rug.nl/ws/portalfiles/portal/173181551/2747_5182_2021_1_88.pdf, (Accessed: 05 April 2026).
[856] Sater, S., (2017). *Blockchain and the European Union's General Data Protection Regulation: A chance to harmonize international data flows*., pp. 1–38. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3080987, (Accessed: 05 April 2026).
[857] CNIL, 2018, pp. 1–10.

blockchain through other means. Analytics firms continue to collect and process transaction data for attribution and risk assessment purposes. Academic scholars and researchers download complete blockchain histories for empirical study. State authorities access public ledgers for investigative purposes.[858] This enduring accessibility exposes the limitations of any erasure-based strategy and indicates that effective forgetting represents, at best, a workable but incomplete solution. The continued openness of blockchain data to third-party scrutiny stands as an inevitable source of friction between the GDPR's protective aims and the architectural realities of distributed ledgers.

A second limitation stems from the diversity of industry practices. Because wallet providers, node operators, analytics companies, and protocol developers all operate under different business models and governance structures, it is practically impossible to adopt privacy protections. This fragmentation is highlighted by the MetaMask–Infura incident in 2022: mainstream wallets may collect IP and address metadata by default,[859] while privacy-focused applications like Wasabi build coinjoin-based unlinkability directly into their protocols,[860] reflecting fundamentally different baseline privacy approaches. At the infrastructure level, majority of Ethereum nodes are operated by volunteers or transient entities,[861] that lack the organisational stability needed to maintain long-term suppression or delinking mechanisms. The GDPR's accountability framework, which presumes stable, clearly identifiable entities capable of long-term compliance, is at tension with this fragmented landscape, undermining the consistency that effective forgetting depends on.[862]

A third constraint stems from the danger that interface-based suppression might create a false sense of erasure. Although wallet interfaces merely filter what appears on screen without interacting with the blockchain itself, users may come to believe that concealed data has been permanently erased. This chapter establishes this distinction clearly: what gets displayed can be controlled, but the ledger remains unchanged. Where this misunderstanding takes hold, the protective function of effective forgetting weakens; users operate under mistaken beliefs about the actual accessibility of their information. The resulting knowledge gap raises serious

[858] Belen-Saglam et al., 2023, pp. 25–32.
[859] Consensys, MetaMask and Infura Privacy Policy Update (2025).
[860] Wasabi, (2025). Wasabi Documentation.
[861] Gencer, A.E., Basu, S., Eyal, I., Van Renesse, R. and Sirer, E.G., (2018). *Decentralization in bitcoin and ethereum networks*. In International conference on financial cryptography and data security, pp. 439-457. Available at: https://arxiv.org/abs/1801.03998, (Accessed: 24 December 2025).
[862] GDPR, Recital 74; see also, EDPB Guidelines 07/2020, paras 10–14.

normative questions: data protection law is meant to empower individuals over their own data, yet the very obscurity of suppression mechanisms risks doing the opposite, masking the ongoing existence of indelible records and thereby eroding informed agency.[863]

A fourth remaining friction stems from the interface between data-protection requirements and other regulatory frameworks, most notably AML/CFT duties under the Transfer of Funds and Markets in Crypto-Assets Regulation. Custodial providers are legally required to collect, retain, and transmit identifiable data for law enforcement purposes, which directly constrains the temporal scope of erasure because data cannot be deleted before mandatory retention periods expire.[864] Moreover, the existence of parallel regulatory logics, namely privacy versus financial surveillance, raises questions about how proportionality[865] should be applied when fundamental rights collide with security mandates. The jurisprudence of the CJEU on data retention offers some guidance, but it has not yet been fully extended to decentralised contexts.

A fifth limit concerns protocol-level inertia and governance divergence. Although innovations such as account abstraction and zero-knowledge systems offer pathways to reduce the exposure of personal data, their adoption is contingent on collective governance decisions within protocol communities. These communities frequently prioritise goals that diverge from regulatory expectations: public transparency and auditability may be treated as core economic or ideological values, while privacy-enhancing upgrades can be resisted where they are seen to increase centralisation risks, add complexity, or threaten miner/validator incentives.[866] The governance structures of decentralised networks, characterised by informal coordination, political contention, and economic incentives misaligned with privacy, may impede the adoption of features that would structurally support effective forgetting. This tension reflects a broader unresolved question: can decentralised governance processes internalise the normative requirements of data protection without external legal compulsion?

[863] GDPR Recital 7; Recital 39.
[864] Regulation (EU) 2023/1113, Articles 4–6; Regulation (EU) 2023/1114, Articles 63–65.
[865] Directive 2002/58/EC, Article 15(1); GDPR, Art 23(1)(a)–(e); Digital Rights Ireland, C-293/12, paras 41–42, 51–52, 69; see also Court of Justice of the European Union, (2020). *La Quadrature du Net and Others, Joined Cases C-511/18, C-512/18, C-520/18*. ECLI:EU:C:2020:791, paras 137–139, 166–168, 171–181. Available at: https://curia.europa.eu/juris/liste.jsf?language=en&num=C-511/18, (Accessed: 24 December 2025).
[866] Quintais et al., 2019, pp. 83–88, 86–92; see also, Kiayias, A., Lazos, P., (2022). *SoK: blockchain governance*. In Proceedings of the 4th ACM Conference on Advances in Financial Technologies, pp. 61-73. Available at: https://arxiv.org/abs/2201.07188, (Accessed: 24 December 2025).

A sixth limit concerns the residual risk of re-identification. Even where providers implement delinking, address rotation, and metadata minimisation, third-party analytical capabilities continue to advance, enabling the reconstruction of identity linkages ex post. Blockchain analytics firms increasingly use behavioural heuristics, clustering algorithms, and machine-learning–based attribution to re-associate pseudonymous identifiers with natural persons.[867] Empirical work demonstrates that as few as two or three quasi-identifiers may suffice to re-identify individuals in large-scale datasets,[868] suggesting that effective forgetting is vulnerable to future analytical improvements. This adversarial dynamic raises the question of whether effective forgetting can remain sufficiently robust in the face of technological advances that reinforce linkability. It also introduces a normative concern regarding whether regulators should impose obligations on analytics firms and whether such obligations would be technically enforceable.[869]

Finally, the concept of effective forgetting itself raises doctrinal questions that remain unresolved in European data protection law. While the CJEU's jurisprudence supports functional interpretations of erasure, it has never directly addressed immutable ledgers. It remains unclear whether effective forgetting must be recognised as a formal category under Article 17, whether DPAs should articulate specific criteria for assessing sufficiency, or whether courts will accept the proposition that interface-level suppression satisfies a right framed in the language of deletion. The adoption of effective forgetting may be hindered by the doctrinal ambiguity surrounding its status, which would also weaken legal certainty for users and suppliers.

When taken as a whole, these limitations reveal forgetting for what it is: a practical legal accommodation that enables data-protection entitlements to operate in a setting inherently hostile to deletion. Although it eases the friction between blockchain's permanence and the GDPR's rights architecture, it does not eliminate that friction entirely. Far from undermining the significance of effective forgetting, however, these shortcomings underscore the

[867] Goldfeder, S., Kalodner, H., Reisman, D. and Narayanan, A., (2017). *When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies*. arXiv preprint arXiv:1708.04748, pp. 1–2. Available at: https://arxiv.org/abs/1708.04748, (Accessed: 24 December 2025).

[868] Sweeney, L., (2002*). k-Anonymity: A Model for Protecting Privacy*. International Journal on Uncertainty, Fuzziness and Knowledge-Based Systems, 10 (5), 2002; 557-570. (esp showing 87% identifiability using three quasi-identifiers).
Available at: https://epic.org/wp-content/uploads/privacy/reidentification/Sweeney_Article.pdf, (Accessed: 24 December 2025).

[869] GDPR, Articles 5(1)(c), 25; EDPB, Guidelines 07/2020, paras 15–17.

importance of sustained progress across legal interpretation, technical innovation, and governance experimentation in decentralised contexts. They further suggest that continued empirical observation and doctrinal analysis will prove critical in determining whether effective forgetting can endure as blockchain infrastructure and regulatory regimes mature.

The concept of effective forgetting therefore represents a doctrinal adaptation aimed at preserving the effectiveness of fundamental rights within technologically evolving environments. Rather than treating blockchain architectures as inherently incompatible with the GDPR, the analysis demonstrates that data protection law retains the capacity to regulate decentralised systems through functional interpretation of controllership and erasure obligations. By distinguishing between immutable ledger persistence and controllable layers of data processing, effective forgetting provides a structured method for reconciling technological innovation with the normative commitments of EU data protection law. The continued development of this concept will depend on the evolution of regulatory guidance, judicial interpretation, and technical design practices capable of supporting privacy-preserving architectures within decentralised ecosystems.

Chapter 6. Conclusion

The regulation of data protection within decentralised technological environments presents a structural tension. The GDPR presupposes reversibility and alteration; blockchain systems prioritise permanent record-keeping, decentralised control, and transparent state transitions.

Against this background, this dissertation has examined *whether custodial and non-custodial wallet providers comply with Article 17 GDPR's right to erasure, and if so, does compliance require reconceptualising erasure as effective forgetting?*

At general level, this dissertation has found that while the GDPR and blockchain are not naturally compatible legal-technological models, they are not mutually exclusive. State and private actors remain bound to ensure the continued effectiveness of rights-protection even when operating or regulating within decentralised infrastructures. Accordingly, the GDPR can still operate within blockchain environments provided that its doctrinal concepts are adapted in a manner that reflects the technological and institutional context of processing.

The analysis confirms that while blockchain architectures challenge traditional assumptions underlying data erasure, the GDPR remains capable of operating within decentralised environments where its doctrinal concepts are interpreted in light of technological constraints affecting the persistence and accessibility of personal data.

At a more specific level, the analysis demonstrates that compliance with Article 17 GDPR is possible, but only if erasure is understood functionally rather than literally. Blockchain's technical immutability makes absolute deletion impossible once data reaches the ledger. However, this does not foreclose compliance. CJEU jurisprudence, particularly in search engine cases, treats erasure as achieved when data becomes functionally inaccessible: when linkability breaks down, when context no longer supports identification, when interfaces no longer surface the information. Wallet providers control substantial off-chain processing: user interfaces, metadata flows, key management systems, transaction indexing. Their influence over these layers gives them the means to operationalise effective forgetting even where on-chain deletion remains technically infeasible.

DOCTRINAL FOUNDATIONS

What constitutes effective forgetting in blockchain systems, and can functional inaccessibility satisfy Article 17's purposes?

Chapter 2 demonstrated that the GDPR is not technologically rigid. Rather, it contains built-in principles of proportionality, contextual interpretation, and technological neutrality. Chapter 3 further examined the Right to be Forgotten by analysing the CJEU's jurisprudence in Google Spain, Google v CNIL, GC and Others, and related case law. This research found that Article 17 does not rely solely on physical erasure, but instead is fundamentally oriented toward the restoration of informational autonomy by limiting accessibility, linkability, and contextual exposure of personal data. This doctrinal development forms the basis upon which "effective forgetting" may be established as a functional equivalent to erasure in decentralised systems.

Whether this interpretation proves sustainable depends on how courts balance competing interests. Erasure can be satisifed by interface management and access controls, according to the CJEU's functional approach in search engine instances, which calls for delinking from results rather than deletion from source websites. However, the analogy has its limitations. Search engines operate within identifiable jurisdictions; blockchain networks span borders in ways that complicate enforcement. The Court's delinking orders work because search engines have operators subject to EU jurisdiction; blockchain protocols may lack comparable enforcement targets.

To what extent can principles from CJEU jurisprudence, particularly Google Spain and Google v CNIL, be adapted to the unique architecture of blockchain networks?

There are significant differences in the technology. Search engines aggregate and index information stored elsewhere; blockchain systems replicate identical data across distributed nodes. Blockchain nodes cannot remove on-chain data without consensus-breaking forks; search engines can delist without impacting source material. Nevertheless, the Court's analytical framework, focusing on controllership based on factual influence, evaluating proportionality between competing rights, and acknowledging delinking as satisfying erasure obligations, offers adaptable principles.

Chapter 3 demonstrates that the Court's emphasis on who structures access to data, rather than who originates it, maps onto wallet providers' role in blockchain ecosystems. These intermediaries do not control ledger contents but decisively shape which data users encounter, how transaction histories surface, and whether pseudonymous identifiers link to off-chain identity information. This allocation of power is accommodated by the jurisprudence's functional approach to controllership. Similar to this, the Court's proportionality analysis when balancing erasure rights against other interests applies to blockchain situations where algorithmic trust, network security, transaction finality, and immutability serve legitimate purposes and must be weighed against individual rights.

The right to erasure does not operate in isolation but forms part of a broader framework of competing fundamental rights and legitimate interests recognised under Article 17(3) GDPR. In blockchain environments, transparency and persistence may contribute to objectives such as financial integrity, fraud prevention, and legal accountability. The concept of effective forgetting therefore operates within this balancing structure, ensuring that data protection obligations are implemented proportionately without undermining functions that rely on verifiable and auditable transaction records.

However, the analogy has limits. Search engines operate within a single jurisdiction's legal framework; blockchain networks span borders in ways that complicate enforcement. Considering that search engines have identifiable operators subject to EU jurisdiction, the Court's delinking orders are effective; blockchain protocols might not have comparable enforcement targets. These structural differences mean the jurisprudence provides guidance but not complete answers.

GOVERNANCE AND CONTROLLERSHIP

How should controllership be allocated in decentralised ecosystems?

Chapter 4 turned to the technical structure of blockchain systems and examined the position of wallet providers within that architecture. It shown that wallet providers function as environments where a variety of personal data is processed and handled, rather than just as cryptographic tools, regardless of whether they are custodial, non-custodial, hybrid, or smart-contract based. Their systems link on-chain identifiers with substantial volumes of off-chain metadata, and their design choices shape how information is generated, stored, transmitted,

and presented to users. Because wallet providers exercise this factual influence over the conditions under which data is processed, they fall within the GDPR's functional conception of a controller.

Against this background, custodial wallet providers plainly qualify as controllers given their discretion over user data. Non-custodial providers present closer questions: their reduced control over private keys and transaction initiation suggests more limited responsibility, but their influence over metadata, interface presentation, and off-chain indexes still implies controllership in respect of those specific processing activities. Accountability under the GDPR should attach accordingly, requiring wallet providers to implement and demonstrate compliance only in relation to processing operations over which they exercise such factual influence. Whether this allocation proves workable depends on enforcement. Declaring distributed networks collectively responsible may appear conceptually satisfying, but it provides limited practical guidance when violations occur and concrete remedies must be identified.

OPERATIONAL MECHANISMS

What mechanisms can operationalise effective forgetting without compromising blockchain integrity?

Chapter 5 set out the dissertation's central theoretical contribution: effective forgetting as the only model through which Article 17's aims can be realised in decentralised environments. The chapter constructed a typology of wallet-provider models, analysed how controllership is distributed, and demonstrated that literal erasure is technically impossible once data is embedded on-chain. It then proposed a structured compliance framework operating across four domains:

Off-chain deletion and suppression: Wallet providers can delete account credentials, KYC documents, communication logs, and metadata from their own systems. This mirrors conventional data controller obligations and raises no special technical challenges.

Delinking of identifiers: Where wallet services maintain transaction explorers, account histories, or address books linking blockchain identifiers to real-world identities, these

linkages can be severed. Users retain on-chain data but lose the contextual information enabling identification.

Interface-level neutralisation: Wallet applications can suppress display of specific transactions, addresses, or interaction histories in user-facing interfaces. The data persists on-chain but becomes invisible to ordinary users of that wallet service.

Metadata governance: Since much personal data in blockchain contexts derives from metadata, timestamps, IP addresses, device identifiers collected during wallet interactions, strict metadata minimisation and deletion policies can prevent identification even where transaction data remains public.

These mechanisms preserve blockchain integrity, the distributed ledger continues operating, consensus rules remain intact, no historical revision occurs, while enabling compliance with erasure requests. Their effectiveness depends on comprehensive implementation. Deleting data from one wallet provider's servers accomplishes little if analytics firms and block explorers maintain copies linked to the same identifiers. Effective forgetting requires coordinated action across the ecosystem or acceptance that partial compliance, delinking within a specific service, satisfies Article 17 where fuller deletion is infeasible.

This framework constitutes the dissertation's main original contribution. It offers a legally defensible and technologically grounded method for interpreting and enforcing erasure rights within blockchain wallet ecosystems. However, some scenarios resist accommodation: where pseudonymous addresses become publicly linked to real identities through media coverage or legal proceedings, no wallet provider action can restore anonymity. Where on-chain transaction patterns themselves reveal identity through behavioural analysis, interface suppression provides limited protection. These edge cases indicate that effective forgetting has boundaries; contexts where neither literal deletion nor functional inaccessibility can satisfy data subjects' interests.

REGULATORY AND GOVERNANCE IMPLICATIONS

What are the normative and policy implications of embedding effective forgetting in blockchain governance frameworks?

Section 5.9 examined the regulatory, governance, and policy implications of making effective forgetting operational in practice. The chapter moved from the question of whether compliance is technically possible to how it would be supervised, allocated among actors, and embedded into future system design. It showed that feasibility does not rest on wallet providers alone. Other actors, such as RPC operators, analytics firms, protocol foundations, and dApp developers, shape the persistence and linkability of personal data and therefore play a role in determining whether erasure rights can have practical effect. The chapter argued that effective forgetting requires a model of distributed governance in which responsibilities are allocated according to factual influence over data flows. It also assessed possible architectural developments, including account abstraction, zero-knowledge proofs, ephemeral addresses, and privacy-preserving routing, as mechanisms that could support privacy at the protocol level. At the same time, it identified limits that currently constrain full realisation of the model, including the continued public accessibility of on-chain data, divergent industry practices, mandatory retention under AML/CFT rules, resistance within protocol-governance processes, and the increasing sophistication of deanonymisation techniques.

THREE OVERARCHING CONCLUSIONS

First, the GDPR is not inherently incompatible with blockchain technology. Although immutability prevents literal erasure, the GDPR's emphasis on user autonomy, proportionality, and contextual interpretation allows for a functional approach to the right to erasure. Regulatory incompatibility is not structurally predetermined; it depends on how the GDPR is interpreted and applied. CJEU jurisprudence supports this functional reading, though whether regulators will accept it for blockchain contexts remains to be tested through enforcement and litigation.

Second, blockchain wallet providers are central to operationalising Article 17. They are the points at which personal data becomes organised, structured, and mediated. They determine how much off-chain data is collected, how information is displayed to users, and how transactions are transmitted. Their proximity to users, their institutional identifiability, and their influence over data flows make them the most viable governance actors within otherwise decentralised ecosystems. This positioning gives them both the capacity and the responsibility to implement effective forgetting mechanisms.

Third, effective forgetting should be recognised as the appropriate compliance standard for Article 17 in decentralised environments. This dissertation has formulated effective forgetting as a standard sensitive to system architecture and operationalised it through a concrete framework for wallet providers. This constitutes an original contribution to data-protection scholarship and blockchain governance debates. It offers a principled means of reconciling legal expectations with technical constraints. It restores user autonomy not by altering the ledger itself, but by reshaping the informational conditions through which the ledger is experienced and interpreted. It is consistent with CJEU jurisprudence on functional erasure, respects the technological logic of distributed systems, and provides a practical model that regulators and industry actors can adopt.

This dissertation does not conclude that the concept of effective forgetting resolves all tensions between privacy and decentralisation. Rather, this research finds that the right to erasure can remain workable and normatively meaningful when interpreted through a model that prioritises functional outcomes, namely, the practical inaccessibility of personal data, instead of literal deletion. The broader implication is that data-protection law must continue to develop through sustained dialogue between legal doctrine and technical design. Technical architectures influence the extent to which legal rights can be realised in practice, just as legal norms and regulatory expectations shape the trajectory of technological development.

The demand for legal and technological communication is growing as blockchain systems spread and take on more intricate social and economic roles. The practical impacts that suppression mechanisms are supposed to give should be evaluated empirically in future research. It should also investigate whether decentralised governance mechanisms may internalise fundamental rights without outside legal pressure, as well as how courts handle effective forgetfulness within judicial reasoning. In addition to demonstrating that privacy protection in decentralised contexts is not only feasible but also essential if technological progress is to continue to be compatible with individual autonomy and constitutional rights, this dissertation offers the conceptual and analytical framework for that investigation.

The conceptual and analytical framework for that work is provided by this dissertation, which shows that privacy protection in decentralised systems is not only feasible but also necessary to guarantee that technological innovation does not compromise individual autonomy and constitutional rights under EU data protection law.

References

1. Legislation

Council of Europe (1950) European Convention for the Protection of Human Rights and Fundamental Freedoms. ETS No. 5, Article 8.

Council of Europe (1981) Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. ETS No. 108.

Conference of the Representatives of the Governments of the Member States (2007) Consolidated version of the Treaty on the Functioning of the European Union. OJ C 115/1.

Data Protection Commission. (2022). Decision in the matter of LB v. Meta Platforms Ireland Limited (Facebook Service), IN-18-5-5.

Data Protection Commission (DPC), (2022). Decision in the matter of TSA v. Meta Platforms Ireland Limited (Instagram Service).

European Data Protection Board, (2019). Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR. Version, 2.0.

European Commission, (2017). Building a European Data Economy (Communication) COM (2017) 9 final.

European Parliament and Council (1995) Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive). OJ L 281.

European Parliament and Council (2006) Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services and amending Directive 2002/58/EC (Data Retention Directive). OJ L 105, pp. 54–63.

European Parliament and of the Council (2014) Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014, on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (recast) Text with EEA relevance, L 173/349.

European Parliament and Council (2016) Regulation (EU) 2016/679 (General Data Protection Regulation). OJ L 119.

European Parliament and Council (2016) Directive (EU) 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. OJ L 119/132.

European Parliament and Council (2023) Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets. OJ L 150, pp. 1–39.

European Parliament and Council (2023) Regulation (EU) 2023/1114 on markets in crypto assets (MiCA). OJ L 150/40.

European Parliament, (2014). Protection of individuals with regard to the processing of personal data (European Parliament legislative resolution of 12 March 2014 on COM(2012)0011 — 2012/0011(COD).

European Data Protection Board, (2023). Binding Decision 1/2023 on the dispute submitted by the Irish SA on data transfers by Meta Platforms Ireland Limited for its Facebook service (Art. 65 GDPR).

European Union (2007) Charter of Fundamental Rights of the European Union. OJ C 303/1.

European Union, (2022), Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology, Official Journal of the European Union, L 151.

OECD (1980, amended 2013) Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. OECD Legal Instruments, OECD/LEGAL/0188.
Valukas, R., A., (2010). Lehman Brothers Holding Inc. Chapter 11 Proceedings Examiner's Lehman Brothers Holding Inc. Chapter 11 Proceedings Examiner's Report. Volume 1, YPFS Resource Library.
Valukas, R., A., (2010). Lehman Brothers Holding Inc. Chapter 11 Proceedings Examiner's Lehman Brothers Holding Inc. Chapter 11 Proceedings Examiner's Report. Vol. 3, Section III.A.4 'Repo 105'. United States Bankruptcy Court, Southern District of New York. Chicago & New York: Jenner & Block LLP.

2. Case Law

Court of Justice of the European Union, (1976). Rewe-Zentralfinanz eG and Rewe-Zentral AG v Landwirtschaftskammer für das Saarland (Case 33/76), EU:C:1976:188, European Court Reports 1976.
Court of Justice of the European Union, (1976). Comet BV v Produktschap voor Siergewassen (Case 45/76), EU:C:1976:191, European Court Reports 1976.
Court of Justice of the European Union, (2003). Case C-101/01, Bodil Lindqvist, EU:C:2003:596.
Court of Justice of the European Union, (2008). Case C-524/06, Heinz Huber v Bundesrepublik Deutschland, ECLI:EU:C:2008:724.
Court of Justice of the European Union, (2009). College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer. Case C-553/07, EU:C:2009:293.
Court of Justice of the European Union, (2011). Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL, (SABAM) (C-70/10) ECLI:EU:C:2011:771.
Court of Justice of the European Union (2014) Banif Plus Bank Zrt. v Márton Lantos and Mártonné Lantos, Case C-312/14, ECLI:EU:C:2015:794
Court of Justice of the European Union (2014) Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12, ECLI:EU:C:2014:317.
Court of Justice of the European Union (2014) Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others (Joined Cases C-293/12 and C-594/12), ECLI:EU:C:2014:238.
Court of Justice of the European Union (2014) Ryneš v Úřad pro ochranu osobních údajů (C 212/13). EU:C:2014:2428
Court of Justice of the European Union (2015) Maximillian Schrems v Data Protection Commissioner, Case C-362/14 (Schrems I), ECLI:EU:C:2015:650.
Court of Justice of the European Union, (2016). Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Watson, ECLI:EU:C:2016:970.
Court of Justice of the European Union, (2016). Patrick Breyer v Bundesrepublik Deutschland (Case C-582/14, ECLI:EU:C:2016:779.
Court of Justice of the European Union, (2017), Peter Nowak v Data Protection Commissioner. ECLI:EU:C:2017:994.
European Court of Justice, (2017), Case C-398/15 Camera di Commercio, Industria,

Artigianato e Agricoltura di Lecce v Salvatore Manni. ECLI:EU:C:2017:197.
Court of Justice of the European Union (2018) Unabhängiges Landeszentrum für Datenschutz
Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, Case C-210/16, ECLI:EU:C:2018:388.
Court of Justice of the European Union (2018) Tietosuojavaltuutettu v Jehovan todistajat, Case
C-25/17, ECLI:EU:C:2018:551.
Court of Justice of the European Union (2019) Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV, Case C-40/17, ECLI:EU:C:2019:629.
Court of Justice of the European Union (2019) Google LLC v CNIL, Case C-507/17, ECLI:EU:C:2019:772.
Court of Justice of the European Union, (2019). Case C-673/17, Planet49 GmbH v. Verbraucherzentrale Bundesverband eV. ECLI:EU:C:2019:801.
Court of Justice of the European Union (2020). Orange Romania SA v Autoritatea Naţională de Supraveghere a Prelucrării, Case C-61/19, ECLI:EU:C:2020:901.
Datelor cu Caracter Personal (ANSPDCP). C-61/19 - Orange Romania.
Court of Justice of the European Union (2020) Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (Schrems II), Case C-311/18, ECLI:EU:C:2020:559.
Court of Justice of the European Union, (2020). La Quadrature du Net and Others, Joined Cases
C-511/18, C-512/18, C-520/18. ECLI:EU:C:2020:791.
Court of Justice of the European Union (2022) TU and RE v Google LLC, Case C-460/20, ECLI:EU:C:2022:962.
Court of Justice of the European Union (2022) Ligue des droits humains v Conseil des ministres, Case C-817/19, ECLI:EU:C:2022:63.
Court of Justice of the European Union, (2024), Case C-46/23 Budapest Főváros IV. Kerület Újpest Önkormányzat Polgármesteri Hivatala v Nemzeti Adatvédelmi és Információszabadság Hatóság., ECLI:EU:C:2024:239.
European Court of Justice, (2025), Case C-655/23 Quirin Privatbank, ECLI:EU:C:2025:655.
Court of Justice of the European Union (2025), EDPS v SRB (Notion de données à caractère personnel), Case C-413/23 P, ECLI:EU:C:2025:645
European Court of Human Rights (2003) Peck v United Kingdom, Application no. 44647/98.
European Court of Human Rights (2004) Von Hannover v Germany (No. 1), Application no. 59320/00.
European Court of Human Rights (2012) Axel Springer AG v Germany, Application no. 39954/08.
European Court of Human Rights, (2013). Case of Węgrzynowski and Smolczewski v. Poland.
Application no. 33846/07.
European Court of Human Rights (2014) Lillo-Stenberg and Sæther v Norway, Application no.
13258/09.
European Court of Human Rights, (2018). M.L. and W.W. v. Germany. Applications nos. 60798/10 and 65599/10.
Bundesverfassungsgericht (BVerfG) (1983) Volkszählungsurteil (Census decision), Judgment of 15 December 1983, 1 BvR 209/83.
High Court of Justice of England and Wales (2018) NT1 and NT2 v Google LLC [2018] EWHC

799 (QB).

3. EU Institutional Documents and Soft Law

Article 29 Working Party, (2007). Opinion 4/2007 on the concept of personal data. 01248/07/EN, WP136.

Article 29 Data Protection Working Party (2010) Opinion 1/2010 on the concepts of "controller" and "processor", WP 169.

Article 29 Data Protection Working Party (2014) Opinion 05/2014 on Anonymisation Techniques, WP 216.

Article 29 Working Party, (2017). Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation. (2002/58/EC)

Article 29 Data Protection Working Party (2017) Guidelines on Data Protection Impact Assessment (DPIA), WP 248 rev.01.

Boucher, P., Nascimento, S., Kritikos, M., (2017). How blockchain technology could change our lives. STOA (European Parliament).

Commission Nationale de l'Informatique et des Libertés (CNIL) (2018) Solutions for a Responsible Use of the Blockchain in the Context of Personal Data.

CNIL (2019) Deliberation SAN-2019-001 of 21 January 2019 against Google LLC.

CNIL (2021) Deliberation No. SAN-2021-023 of 31 December 2021 concerning Google LLC and Google Ireland Ltd.

CNIL, (2025). Mobile applications: CNIL publishes its recommendations for better privacy protection. Deliberation No 2025-024.

DLT and Blockchain Working Group, The GDPR and the blockchain technology.

European Banking Authority, (2019). Report with Advice for the European Commission on Crypto-assets. EBA Report.

European Banking Authority, (2020). Annual Report 2019. ISSN 1977-9046, ISBN 978-92 9245-659-7, Luxembourg: Publications Office of the European Union, 2020.

European Banking Authority, (2024). Guidelines on information requirements in relation to transfers of funds and certain crypto-assets transfers under Regulation (EU) 2023/1113. ('Travel Rule Guidelines'), Final Report, EBA/GL/2024/11.

European Commission, (2025). Blockchain and web3 strategy. Shaping Europe's digital future,

Blockchain Strategy.

European Commission, (2026). The European Blockchain Sandbox Report. Final Best Practices Report (3rd cohort).

European Data Protection Board (2019) Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of online services.

European Data Protection Board (2020) Guidelines 4/2019 on data protection by design and by default.

European Data Protection Board, (2019). Opinion 5/2019 on the interplay between the ePrivacy

Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities.

European Data Protection Board, (2020). Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications. Version 2.

European Data Protection Board (2020) Guidelines 05/2020 on consent under Regulation 2016/679.

European Data Protection Board (2020) Guidelines 07/2020 on the concepts of controller and processor in the GDPR.

European Data Protection Board (2021) Guidelines 8/2020 on the targeting of social media

users.
European Data Protection Board, (2023). Guidelines 01/2022 on data subject rights - Right of
access. Version 2.1.
European Data Protection Board, (2023). Report of the Work Undertaken by the Supervisory Authorities within the 101 Task Force.
European Data Protection Board, (2025). Guidelines 01/2025 on Pseudonymisation. (version for public consultation).
European Data Protection Board, (2025). Guidelines 02/2025 on processing of personal data through blockchain technologies. Version 1.1.
EU Blockchain Observatory and Forum, (2018). Blockchain and the GDPR. An Initiative of the European Union.
EU Blockchain Observatory and Forum, (2019). Blockchain and digital identity. Luxembourg:
Publications Office of the European Union.
Financial Action Task Force (FATF), (2025). The FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation.
Ministry of Digital Affairs, DLT and Blockchain Working Group, (2019). The GDPR and the blockchain technology. Warsaw: Ministry of Digital Affairs.
Opinion of Advocate General Szpunar (2019) in Case C- 507/ 17, Google Inc. v Commission nationale de l'informatique et des libertés (CNIL), (ECLI:EU:C:2019:15).
Seira, A., Allen, J., Watsky, C. and Alley, R., (2024). Governance of permissionless blockchain
networks. FEDS Notes. Washington: Board of Governors of the Federal Reserve System.

4. Literature

Alhadeff, J., Van Alsenoy, B. and Dumortier, J. (2012). 'The accountability principle in data protection regulation: Origin, development and future directions', in Guagnin, D., Hempel, L., Ilten, C., Kroener, I., Neyland, D. and Postigo, H. (eds.) Managing privacy through accountability. Basingstoke: Palgrave Macmillan.
Alharby, M., Aldweesh, A., Van Moorsel, A., (2018). Blockchain-based smart contracts: A systematic mapping study of academic research. In 2018 International Conference on Cloud Computing, Big Data and Blockchain.
Andrejevic, M. (2011) 'Surveillance and alienation in the online economy', Surveillance & Society, 8(3).
Antonopoulos, A.M. (2015) Mastering Bitcoin: Unlocking Digital Cryptocurrencies. 1st edn. Sebastopol, CA: O'Reilly Media.
Atzei, N., Bartoletti, M. and Cimoli, T. (2017) 'A survey of attacks on Ethereum smart contracts
(SoK)', in International Conference on Principles of Security and Trust.
Atzori, M., (2017). Blockchain Technology and Decentralized Governance: Is the State Still Necessary? Journal of Governance and Regulation, Volume 6, Issue 1.
Augusto, A., Belchior, R., Correia, M., Vasconcelos, A., Zhang, L. and Hardjono, T., (2024). SoK: security and privacy of blockchain interoperability [extended version]. Authorea Preprints.
Ayed, A.B. (2017) 'A conceptual secure blockchain-based electronic voting system', International Journal of Network Security & Its Applications, 9(3).
Azadinamin, A., (2013). The Bankruptcy of Lehman Brothers: Causes of Failure &

Recommendations Going Forward. Article in Social Science Research.
Badr, B., Horrocks, R. and Wu, X.B., (2018). Blockchain By Example: A developer's guide to creating decentralized applications using Bitcoin, Ethereum, and Hyperledger. Packt Publishing Ltd.
Baker, H.K. and Kim, H.J. (2021). A glossary of blockchain terms. in Baker, H.K., Kiymaz, E. and Smith, G. (eds.) Blockchain Applications in Finance. Bingley: Emerald Publishing.
Bakos, Y., Halaburda, H., (2021). Tradeoffs in Permissioned vs Permissionless Blockchains: Trust and Performance.
Balkin, J.M., (2015). Information fiduciaries and the first amendment. UCDL Vol., 49, No 4:1183.
Bandara, T., (2024). Blockchain Technology in International Trade: Legal and Regulatory Implications. ResearchGate.
Barocas, S. and Selbst, A.D., (2016). Big data's disparate impact. Calif. L. Rev., 104.
Bashir, I., (2017). Mastering blockchain. Distributed ledger technology, decentralization, and smart contracts explained, Second Edition, Packt Publishing Ltd.
Bayle, A., Koscina, M., Manset, D. and Perez-Kempner, O., (2018). When blockchain meets the right to be forgotten: technology versus law in the healthcare industry. IEEE/WIC/ACM International Conference on Web Intelligence (WI), IEEE.
BBC (2019) 'Data on 540 million Facebook users exposed', BBC News, 3 April.
Beck, R., Mueller-Bloch, C., (2018). Governance in the Blockchain Economy: A Framework and Research Agenda. Journal of the Association for Information Systems, 19(10):1020-1034.
Beer, D. (2016) Metric Power. Basingstoke: Palgrave Macmillan.
Belen-Saglam, R., Altuncu, E., Lu, Y. and Li, S. (2023) 'A systematic literature review of the tension between the GDPR and public blockchain systems', Blockchain: Research and Applications, 4(2), p. 100129.
Benkler, Y., (2006). The Wealth of Networks. How Social Production Transforms Markets and
Freedom. Yale University Press, ISBN-13: 978-0-300-11056-2 (alk. paper).
Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., (2014). Zerocash: Decentralized Anonymous Payments from Bitcoin. Conference: 2014 IEEE Symposium on Security and Privacy (SP).
Ben-Sasson, E., Chiesa, A., Green, M., Tromer, E., Virza, M., (2015). Secure Sampling of Public Parameters for Succinct Zero Knowledge Proofs. IEEE Symposium on Security and Privacy (SP).
Binns, R., (2018). Fairness in machine learning: Lessons from political philosophy. Proceedings of the 1st Conference on Fairness, Accountability and Transparency, PMLR 81.
Bitcoin Wiki. Genesis block.
Boldyreva, E.L., Grishina, N.Y. and Duisembina, Y., (2018). Cambridge Analytica: Ethics and
online manipulation with decision-making process. In: The European Proceedings of Social and Behavioural Sciences, 18th PCSF Conference, Future Academy.
Bolfing, A., (2021). Cryptographic Primitives in Blockchain Technology: A mathematical introduction. Oxford University Publishing.
Boyd, d. and Crawford, K. (2012) 'Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon', Information, Communication & Society, 15(5).
Bradford, A., (2020). The Brussels effect: How the European Union rules the world. Oxford

University Press. 107 NW. U. L. REV. 1.
Brands, S., (1995). Restrictive Binding of Secret-Key Certificates. In: L.C. Guillou and J.-J. Quisquater, eds. Advances in Cryptology – EUROCRYPT ’95: International Conference on the Theory and Application of Cryptographic Techniques. Saint-Malo, France, May 21–25, 1995. Proceedings. Lecture Notes in Computer Science, vol. 921. Berlin, Heidelberg: Springer.
Brin, D. (1998) The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom? New York: Basic Books.
Broussard, M. (2018) Artificial Unintelligence: How Computers Misunderstand the World. Cambridge, MA: MIT Press.
Brownsword, R., (2016). Technological management and the rule of law. Law, Innovation and Technology, 8(1).
Brownsword, R., (2019). Law, technology and society: reimagining the regulatory environment. Routledge, ISBN: 978-1-351-12818-6 (ebk).
Brusó, M., Chatzikokolakis, K., Etalle, S., Hartog., D., J., (2013). Linking unlinkability. In C. Palamidessi & M. Ryan (Eds.), Trustworthy Global Computing (TGC 2012) (Lecture Notes in Computer Science, Vol. 8191).
Burniske, C., Tatar, J., (2017). Cryptoassets: The Innovative Investor’s Guide to Bitcoin and Beyond. McGraw-Hill Education.
Buterin, V., (2015). On Public and Private Blockchains. Ethereum Blog.
Bygrave, L.A., 2002. Data Protection Law: Approaching Its Rationale. Logic and Limits (The Hague: Kluwer Law International, 2002), at, 316.
Bygrave, L.A., (2014). Data privacy law: an international perspective. Oxford University Press, ISBN 978–0–19–967555–5.
Calo, R., (2013). Digital market manipulation. Geo. Wash. L. Rev., 82.
Carnegy-Arbuthnott, H.M., (2023). Privacy, publicity, and the right to be forgotten. Journal of Political Philosophy, Volume 31, Issue 4.
Carrie, J. (2019) ‘Hundreds of millions of Facebook records exposed on public servers – report’, The Guardian.
Casey, M. & Vigna, P. (2018). The Truth Machine: The Blockchain and the Future of Everything. New York: St. Martin’s Press.
Castells, M. (2001) The Internet Galaxy: Reflections on the Internet, Business, and Society. Oxford: Oxford University Press.
Cavoukian, A., (2009). Privacy by design: The 7 foundational principles. Information and privacy commissioner of Ontario, Canada, 5(2009).
CBS, (2019). Facebook reportedly received users' sensitive health data from apps: "It’s incredibly dishonest."
Celeste, E., (2022). Digital constitutionalism: The role of internet bills of rights. Routledge.
Chaum, D. (1983). Blind signatures for untraceable payments. in Chaum, D., Rivest, R.L. and Sherman, A.T. (eds.) Advances in Cryptology: Proceedings of CRYPTO 82. New York: Springer.
Chen, T. et al., (2017). Under-optimized Smart Contracts Devour Your Money. Conference: SANER(IEEE International Conferece on Software Analysis, Evolution, and Reengineering).
Childers, T.L. and Houston, M.J., (1984). Conditions for a picture-superiority effect on consumer memory. Journal of consumer research.
Chohan, W., U., (2021). The Double Spending Problem and Cryptocurrencies.
Choo, M. and Findlay, M., 2021. Data Reuse and Its Impacts on Digital Labour Platforms.

SMU Centre for AI & Data Governance Research Paper.
Cirone, E., (2021). Blockchain and the General Data Protection Regulation: an irreconcilable regulatory approach? Queen Mary Law Journal, Collections 38 and 51.
Cohen, Julie E., (2019). Between Truth and Power: The Legal Constructions of Informational Capitalism. Oxford University Press, ISBN 9780190246693.
Cohen, J.E. (2019). Turning Privacy Inside Out. Theoretical Inquiries in Law, 20(1).
Coinbase (2025) Crypto Glossary.
Coinbase (2025) What Is a Non-Fungible Token (NFT)?
Coinmetro, (2025). Regulatory Sandboxes: Fostering Crypto Innovation Within Legal Frameworks.
Conte de Leon, D., Stalick, A.Q., Jillepalli, A.A., Haney, M.A., Sheldon, F.T., (2017). Blockchain: properties and misconceptions. Asia Pacific Journal of Innovation and Entrepreneurship, 11(3).
Craig, P. and de Búrca, G., (2020). EU Law: Text, Cases, and Materials. 7th edn. Oxford: Oxford University Press, ch 3 ('The Development of European Integration'.
Cryptopedia Staff, 2025. Custodial vs. Non-Custodial Wallets. Cryptocurrency Wallets.
De Caria, R., (2020). Blockchain and smart contracts: Legal issues and regulatory responses between public and private economic law. Italian LJ, 6.
Decker, C., Wattenhofer, R., (2013). Information propagation in the Bitcoin network. Conference: Peer-to-Peer Computing (P2P), 2013 IEEE Thirteenth International Conference.
De Filippi, P. and Loveluck, B., (2016). The invisible politics of bitcoin: governance crisis of a decentralized infrastructure. Internet policy review, 5(4).
De Hert, P. and Papakonstantinou, V. (2012) 'The proposed data protection regulation replacing
Directive 95/46/EC: A sound system for the protection of individuals', Computer Law & Security Review, 28(2).
De Vries, S.A., (2013). Balancing fundamental rights with economic freedoms according to the
European Court of Justice. Volume 9, Issue 1, urn:nbn:nl:ui:10-1-112916.
Delmolino, K., Arnett, M., Kosba, A., Miller, A., Shi, E., (2016). Step by step towards creating
a safe smart contract: Lessons and insights from a cryptocurrency lab. In International conference on financial cryptography and data security.
Deloitte Insights, (2021). Deloitte's 2021 Global Blockchain Survey: A new age of digital assets.
Deloitte Touche Tohmatsu Limited, (2022). Blockchain: Legal implications, questions, opportunities and risks. CoRe Creative Services. RITM1153882.
De Vries A., (2018). Bitcoin's Growing Energy Problem. Joule, 2(5).
Dewey, J., N., (2018). Global legal insights: Blockchain & cryptocurrency regulation 2019 (1st
ed.). Global Legal Group Ltd.
Diffie, W. and Hellman, M., (1976). New Directions in Cryptography. Vol. IT-22, N6 IEEE Transactions on Information Theory.
Dowsley, R.B., Farias, M.C., Larangeira, M., Nascimento, A.C. and Virdee, J., (2022). A spendable cold wallet from QR video. In International Conference on Security and Cryptography.
Drescher, D., (2017). Blockchain Basics: A Non-Technical Introduction in 25 steps. Apress.
Driscoll, K.R., (2010). Murphy Was an Optimist. In: E. Schoitsch, ed. Computer Safety,

Reliability, and Security. SAFECOMP 2010: 29th International Conference, Vienna, Austria, September 14–17, 2010. Proceedings. Lecture Notes in Computer Science, vol. 6351. Berlin, Heidelberg: Springer.

Ducato, R., (2020). Data protection, scientific research, and the role of information. Computer Law & Security Review, 37.

Ducrée, J., (2022). Satoshi Nakamoto and the Origins of Bitcoin -- Narratio in Nomine, Datis et Numeris. School of Physics Sciences, Dublin City University.

Edwards, L. and Veale, M. (2017) 'Slave to the algorithm? Why a "right to an explanation" is probably not the remedy you are looking for', Duke Law & Technology Review, 16(1).

El Emam, K., Alvarez, C., (2015). A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques. International Data Privacy Law, 5(1), Volume 5, Issue 1.

Erinle, Y., Kethepalli, Y., Feng, Y. and Xu, J., (2023). Sok: Design, vulnerabilities, and security measures of cryptocurrency wallets. *arXiv preprint arXiv: 2307.12874.*

Eubanks, V. (2018). Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor. New York: St. Martin's Press.

Fenwick, M., Vermeulen, E.P.M. (2019). A primer on blockchain, smart contracts & crypto assets. Lex Research Topics in Corporate Law & Economics Working Paper No. 2019-3.

Finck, M. (2018) 'Blockchains and data protection in the European Union', European Data Protection Law Review, 4(1).

Finck, M., (2019). Smart contracts as a form of solely automated processing under the GDPR. International Data Privacy Law, 9(2).

Finck, M., Moscon, V., (2019). Copyright Law on Blockchains: Between New Forms of Rights Administration and Digital Rights Management 2.0. IIC - International Review of Intellectual Property and Competition Law, Vol 50.

Finck, M., (2019). Blockchain Regulation and Governance in Europe. Cambridge University Press, ISBN: 9781108465458.

Finck, M., (2019). Blockchain and the General Data Protection Regulation, Can distributed ledgers be squared with European data protection law? European Parliamentary Research Service.

Finck, M. Pallas, F. (2020). They Who Must Not Be Identified — Distinguishing Personal from Non-Personal Data under the GDPR. International Data Privacy Law, Volume 10, Issue 1.

Fischer, M.J., Lynch, N.A., Paterson, M.S., (1985). Impossibility of distributed consensus with one faulty process. Journal of the ACM (JACM), 32(2).

Floridi, L., (2005). The ontological interpretation of informational privacy. Ethics and information technology, 7(4).

Floridi, L. (2014) The Fourth Revolution: How the Infosphere is Reshaping Human Reality. Oxford: Oxford University Press.

Floridi, L., (2015). The Right to be Forgotten: A Philosophical View. Section III, Availability vs. Accessibility of Information.

Frantziou, E., (2014). Further Developments in the Right to be Forgotten: The European Court
of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos. Human Rights Law Review, 14(4).
Frosio, G.F. (2017) 'Right to be forgotten: Much ado about nothing', Colorado Technology Law Journal, 15(2).
Fuster, G.G., (2014). The emergence of personal data protection as a fundamental right of the EU. Vol. 16. Springer Science & Business.
G. Nick. (2022). How Many IoT Devices are there in 2025? Techjury Blog.
Ganne, E., (2018). Can Blockchain revolutionize international trade? World Trade Organization.
Gellert, R., (2018). Understanding the notion of risk in the General Data Protection Regulation.
Computer Law & Security Review, Volume 34, Issue 2, Published by Elsevier Ltd.
Gellman, B. and Poitras, L. (2013) 'U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program', The Washington Post, 6 June.
Gencer, A.E., Basu, S., Eyal, I., Van Renesse, R. and Sirer, E.G., (2018). Decentralization in bitcoin and ethereum networks. In International conference on financial cryptography and data security.
Gervais, A., Karame, G.O., Wüst, K., Glykantzis, V., Ritzdorf, H. and Capkun, S., (2016). On the security and performance of proof of work blockchains. In Proceedings of the 2016 ACM SIGSAC conference on computer and communications security.
Ghosh, A. (2022). RegTech: From KYC to KYD to … KYDL. MEDIUM.
Gilbert, D., (2019). Facebook Just Paid a $5 Billion Fine for Privacy Breaches. Now it Wants Access to Your Brain.
Gindre, F., Urbieta, M. and Rossi, G., (2022). Patterns for Anonymity Enhancing Cryptocurrencies Non-Custodian Mobile Wallets. In Proceedings of the 29th Conference on Pattern Languages of Programs.
Glaser, F., (2017). Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain enabled System and Use Case Analysis. Proceedings of the 50th Hawaii International Conference on System Sciences.
Goldfeder, S., Kalodner, H., Reisman, D. and Narayanan, A., (2017). When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies. arXiv preprint arXiv:1708.04748.
Goldsmith, J., (2007). Who controls the Internet? Illusions of a borderless world. Strategic Direction, 23(11).
Greenberg, A. (2022) Tracers in the Dark: The Global Hunt for the Crime Lords of Cryptocurrency. 1st edn. New York: Knopf Doubleday Publishing Group.
Greenfield, A. (2013) Against the Smart City. New York: Do Projects.
Greenfield, A. (2017) Radical Technologies: The Design of Everyday Life. London: Verso Books.
Gregorio, G., D., (2022). Digital Constitutionalism in Europe. Reframing Rights and Powers in the Algorithmic Society. Cambridge University Press.
Grimmelmann, J., (2004). Regulation by software. Yale LJ, 114.
Groth, J., (2016). On the Size of Pairing-based Non-interactive Arguments. IACR Cryptology ePrint Archive/EUROCRYPT.
Ghanbari, H. and Koskinen, K. (2024) 'When data breach hits a psychotherapy clinic: The Vastaamo case', Journal of Information Technology Teaching Cases, 0(0).
Godfrey-Welch, D., Lagrois, R., Law, J., Anderwald, R.S. and Engels, D.W., (2018). Blockchain in payment card systems. SMU Data Science Review, 1(1).

Goodchild, M.F. (2007) 'Citizens as sensors: The world of volunteered geography', GeoJournal, 69(4).
Gstrein, O.J. and Kochenov, D., (2020). Digital identity and distributed ledger technology: Paving the way to a neo-feudal brave new world?. Frontiers in Blockchain, Blockchain for Good, Volume 3.
Guri, M. 2018. BeatCoin: Leaking private keys from air-gapped cryptocurrency wallets. arXiv:1804.08714 arXiv.
Gyntelberg, J., Fender, G., (2008). Overview: global financial crisis spurs unprecedented policy actions. BIS Quarterly Review.
Hacker, P., Thomale, C., (2018). Crypto-securities regulation: ICOs, token sales and cryptocurrencies under EU financial law. European Company and Financial Law Review, 15(4).
Hartzog, W. and Selinger, E., (2013). Big data in small hands. Stan. L. Rev. Online, 66.
Hassan, F.U., Ali, A., Latif, S., Qadir, J., Kanhere, S., Singh, J. and Crowcroft, J. (2019). Blockchain and the future of the internet: A comprehensive review.
Hayes, A., Rasure, E., Perez, Y., (2023). Who is Satoshi Nakamoto? Investopedia.
Helberger, N., Karppinen, K. and D'acunto, L., (2018). Exposure diversity as a design principle for recommender systems. Information, communication & society, 21(2).
Helberger, N., Pierson, J. and Poell, T., (2018). Governing online platforms: From contested to cooperative responsibility. The information society, 34(1).
Herath, H.M.A.D., M.J. Sabani, A., Shafana, M.S., (2021). Identifying Suite Type of Blockchain for Application: Public and Private. Department of Information and Communication Technology.
Herian R, (2018). Legal Recognition of Blockchain Registries and Smart Contracts. Research Handbook on the Law of Emerging Technologies (EE Elgar, forthcoming).
Herian, R., (2019). Regulating blockchain: Critical perspectives in law and technology. Routledge.
Herrmann, D., & Lindemann, J. (2016). Obtaining personal data and asking for erasure: Do app vendors and website owners honour your privacy rights? arXiv preprint.
Hijmans, H., (2016). The European Union as Guardian of Internet Privacy. The Story of Art 16 TFEU. Law, Governance and Technology Series 31, Volume 31, ISBN 978-3-319-34090-6.
Hildebrandt, M., (2018). Algorithmic regulation and the rule of law. Phil. Trans. R. Soc. A 376:20170355. Research Article, Volume 376, Issue 2128.
Hoffman, D., Bruening, P., Carter, S., (2016). The Right to Obscurity: How We Can Implement the Google Spain Decision. 17 N.C. J.L. & Tech.
Homoliak, I. and Perešíni, M. (2024) 'SoK: Cryptocurrency wallets – A security review and classification based on authentication factors', in 2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC).
Hoofnagle, C.J., Van Der Sloot, B. and Borgesius, F.Z., (2019). The European Union general data protection regulation: what it is and what it means. Information & communications technology law, 28(1).
Hoven, M., (2012). Balancing privacy and speech in the right to be forgotten. Harvard Journal of Law & Technology.

Hornung, G., Schnabel, C., (2009). Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination. Computer Law & Security Review, 25(1).
House, L., C., Masatlioglu, Y., (2015). Managing markets for toxic assets. Journal of Monetary Economics.
Huang, K., Budorin, D., Tan, L. JY., Ma, W. & Zhang, Z. W. (eds.) 2023. A Comprehensive Guide for Web3 Security. From Technology, Economic and Legal Aspects.
Huang, H., Yin, Z., Yang, Q., Li, T., Luo, X., Zhou, L. and Zheng, Z., (2024). Scalability and Security of Blockchain-empowered Metaverse: A Survey. IEEE Open Journal of the Computer Society.
Hutchinson, T., (2006). Researching and writing in law. Thomas Lawbook Co., ABN 64 058 914 668.
Irion, K. and Luchetta, G., (2013). Online personal data processing and EU data protection reform. In CEPS Task Force Report of the CEPS Digital Forum, ISBN 978-94-6138-302-0.
IT Governance Privacy Team, (2020). EU General Data Protection Regulation: An Implementation and Compliance Guide. Fourth Edition, IT Governance Publishing.
Jasanoff, S. (2004) 'The idiom of co-production', in Jasanoff, S. (ed.) States of Knowledge: The Co-Production of Science and Social Order. London: Routledge.
Jasanoff, S. (2005) Designs on Nature: Science and Democracy in Europe and the United States. Princeton, NJ: Princeton University Press.
Jeffers, A., (2011). How Lehman Brothers Used Repo 105 to Manipulate Their Financial Statements. Article, Department of Accounting and Finance Faculty Scholarship and Creative Works.
Jiménez-Gómez, B.S., (2020). *Risks of blockchain for data protection: a European approach*. Santa Clara High Tech. LJ 281, Volume 36, Issue 3, Article 2.
Jimenez-Gomez, B.S. (2023). Distributed Ledger Technology in Financial Markets: The European Union Experiment. Cuadernos de Derecho Transnacional, vol. 15, no. 2.
Jokić, S., Cvetković, A., S., Adamović, S., Ristić, N., Spalević, P., (2019). Comparative Analysis of Cryptocurrency Wallets vs Traditional Wallets. ISSN 0350-137X, EISSN 2334-9190.
Joseph, S. (2024) 'Balancing data privacy and compliance in blockchain-based financial systems', Journal of Engineering Research and Reports, 26(9).
Kamarinou, D., Millard, C., Singh, J. and Leenes, R., (2017). Machine learning with personal data. Queen Mary School of Law Legal Studies Research Paper No. 247/2016, Oxford: Hart Publishing.
Kamara, I. (2020). Article 40: Codes of Conduct. In The EU General Data Protection Regulation (GDPR): A Commentary, edited by Christopher Kuner, Lee A. Bygrave, and Christopher Docksey. Oxford: Oxford University Press.
Kaminski, M., E., (2019). Binary Governance: Lessons from the GDPR's Approach to Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability. 92 S. CAL. L. REV. 1529.
Kang, C. (2019) 'F.T.C. approves Facebook fine of about $5 billion', The New York Times, 12 July.
Karjian, R., (2024). A timeline and history of blockchain technology. TechTarget.
Kennedy, J. F. (1963). Man is still the most extraordinary computer of all. In John F. Kennedy Quotes. Today in Science.
Kenyon, M. (2017). Jon Penney on the Chilling Effects of Online Surveillance.

Kerikmäe, T. and Särav, S., (2017). Paradigms for automatization of logic and legal reasoning.
Law and Logic: Contemporary Issues. Duncker & Humblot.
Kersic, V., Vidovic, U., Vrecko, A., Domajnko, M. and Turkanovic, M., (2023). Orchestrating digital wallets for on-and off-chain decentralized identity management.
Kiayias, A., Lazos, P., (2022). SoK: blockchain governance. In Proceedings of the 4th ACM Conference on Advances in Financial Technologies.
King, M. (2016). The End of Alchemy: Money, Banking, and the Future of the Global Economy. New York: W. W. Norton.
Kirkpatrick, D. (2010) The Facebook Effect: The Inside Story of the Company That Is Connecting the World. New York: Simon & Schuster.
Kitchin, R. (2014) The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences. London: SAGE.
Kitchin, R. (2016) 'Thinking critically about and researching algorithms', Information, Communication & Society, 20(1).
Klonick, K., (2017). The new governors: The people, rules, and processes governing online speech. Harv. L. Rev., 131.
Koch, R., (2024). Cryptocurrency Basics for Litigators. TECHNOLOGY IN THE LAW PRACTICE.
Kolber, A.J., (2018). Not-so-smart blockchain contracts and artificial responsibility. Stan. Tech.
L. Rev., 21.
Koops, B.J. (2011) 'Forgetting footprints, shunning shadows: A critical analysis of the right to
be forgotten in big data practice', SCRIPTed, 8(3).
Koops, B.J. and Leenes, R., (2014). Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design'provision in data-protection law. International Review of Law, Computers & Technology, 28(2).
Kosba, A. et al., (2016). IEEE Symposium on Security and Privacy (SP), ISSN: 2375-1207.
Koshy, P., Koshy, D., McDaniel, P., (2014). An analysis of anonymity in bitcoin using p2p network traffic. In International conference on financial cryptography and data security.
Kotsios, A., Magnani, M., Vega, D., Rossi, L. and Shklovski, I., (2019). An analysis of the consequences of the general data protection regulation on social network research. ACM Transactions on Social Computing, 2(3).
Koulu, R., (2016). Blockchains and online dispute resolution: smart contracts as an alternative
to enforcement. SCRIPTed, Vol. 13 No. 1.
Krückeberg, S., Scholz, P. (2019). Cryptocurrencies as an Asset Class. In Goutte, S., Guesmi, K., Saadi, S. (eds) Cryptofinance and Mechanisms of Exchange: The Making of Virtual Currency. Cham: Springer Nature Switzerland AG.
Kulk, S. and Zuiderveen Borgesius, F., (2019). Privacy, freedom of expression, and the right to
be forgotten in Europe. In: R. Leenes, R. van Brakel, S. Gutwirth and P. De Hert, eds. Data Protection and Privacy: The Internet of Bodies. Oxford: Hart Publishing.
Kuner, C. (2007) European Data Protection Law: Corporate Compliance and Regulation. Oxford: Oxford University Press.
Kuner, C., (2011). Regulation of Transborder Data Flows Under Data Protection and Privacy Law: Past, Present, and Future. OECD Digital Economy Papers No. 187.
Kuner, C., Bygrave, L.A. and Docksey, C. (eds.) (2020). The GDPR: General Data Protection

Regulation (EU) 2016/679: Commentary. Oxford: Oxford University Press.
Langer, A.M. (2020). Analysis and Design of Next-Generation Software Architectures: 5G, IoT, Blockchain, and Quantum Computing. 1st ed. Cham: Springer International Publishing.
Lamport, L., Shostak, R. and Pease, M., (1982). The Byzantine generals problem. ACM Transactions on Programming Languages and Systems (TOPLAS), 4(3).
Larangeira, M., (2025). Secure and Practical Cold (and Hot) Staking. In Proceedings of the 22nd International Conference on Security and Cryptography (SECRYPT).
Law Insider (n.d.) 'Communication data'. Law Insider.
Ledger Academy (2020) Not Your Keys, Not Your Coins: Explained.
Le Maux, J. and Morin, D., (2011). Black and white and red all over: Lehman Brothers' inevitable bankruptcy splashed across its financial statements. International Journal of Business & Social Science, 2(20).
Lenaerts, K. and Gutiérrez-Fons, J.A., (2013). To say what the law of the EU is: methods of interpretation and the European Court of Justice. Colum. J. Eur. L., 20.
Lenzner, R., (2010). Lehman Lies But Nobody's In Jail. Forbes.
Li, T., Villaronga, E.F. and Kieseberg, P., (2018). Humans forget, machines remember: Artificial intelligence and the right to be forgotten. Boston University School of Law Faculty Scholarship.
Lovelock, D., Reynolds, M., Granetto, B., Kandaswamy, R., (2017). Forecast: Blockchain Business Value, Worldwide, 2017-2030. GARTNER.
Lynskey, O., (2015). Control over Personal Data in a Digital Age: Google Spain v AEPD and Mano Costeja Gonzalez. The Modern Law Review, Vol. 78, No. 3.
Lynskey, O., (2015). The Foundations of EU Data Protection Law. Oxford Studies in European Law.
Lyon, D. (2018) The Culture of Surveillance: Watching as a Way of Life. Cambridge: Polity Press.
Lyons, T., Courcelas, L. and Timsit, K., 2019, September. Legal and regulatory framework of blockchains and smart contracts. In The European Union Blockchain Observatory and Forum.
Lupton, D. (2016) The Quantified Self. Cambridge: Polity Press.
Luu, L., Chu, D., Olickel, H., Saxena, P. and Hobor, A. (2016) 'Making smart contracts smarter', in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16).
MacAskill, E. and Dance, G. (2013) 'NSA files: Decoded – What the revelations mean for you', The Guardian, 1 November.
Mahmoud, Q.H., Lescisin, M. and AlTaei, M., (2019). Research challenges and opportunities in blockchain and cryptocurrencies. Internet Technology Letters 2(2):e93, John Wiley & Sons, Ltd.
Malgieri, G., (2016). Property and (Intellectual) Ownership of Consumers' Information: A New Taxonomy for Personal Data. Privacy in Germany - PinG, n. 4, 2016, 133 ff.
Mangipudi, E. V., Desai, U., Mondal, M., Minaei, M., and Kate, A. 2023. Uncovering Impact of Mental Models towards Adoption of Multi-device Threshold Crypto-Wallets. CCS '23: Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security.
Manovich, L. (2001) The Language of New Media. Cambridge, MA: MIT Press.
Mantelero, A., (2014). The future of consumer data protection in the EU Re-thinking the

"notice and consent" paradigm in the new era of predictive analytics. Computer Law & Security Review, 30(6).
Mayer-Schönberger, V., (2009). Delete: The Virtue of Forgetting in the Digital Age. Princeton University Press.
Mayer-Schönberger, V. and Cukier, K. (2013). Big data: A revolution that will transform how we live, work, and think.
McConville, M. Chui, W., H., ed., (2017). Research methods for law. Edinburgh University Press. Second Edition.
McDonald, O., (2021). Cryptocurrencies: MONEY , TRUST AND REGULATION. ISBN 978
1-78821-420-9, Agenda Publishing.
McLuhan, M. (1994) Understanding Media: The Extensions of Man. Cambridge, MA: MIT Press.
Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G.M. and Savage, S., (2013). A fistful of bitcoins: characterizing payments among men with no names. In Proceedings of the 2013 conference on Internet measurement conference.
Mercurio, B. and Yu, L. (2023) Regulating Cross-Border Data Flows. Cambridge: Cambridge University Press.
Meyer, D., (2018). Blockchain technology is on a collision course with EU privacy law. International Association of Privacy Professionals Article, The Privacy Advisors.
Michalski, R., Dziubałtowska, D., Macek, P., (2020). Revealing the character of nodes in a blockchain with supervised learning. Ieee Access.
Millard, C.J. ed., (2013). Cloud computing law. (Vol. 2). Oxford: Oxford University Press.
Mittelstadt, B.D., Allo, P., Taddeo, M., Wachter, S. and Floridi, L., (2016). The ethics of algorithms: Mapping the debate. Big data & society, 3(2), p.2053951716679679.
Moerel, L., (2019). Blockchain & Data Protection… and Why They Are Not on a Collision Course. European Review of Private Law 6-2019, 825–852, Kluwer Law International BV, The Netherlands.
Moerel, L. (2020). Blockchain and data protection. in DiMatteo, L.A., Cannarsa, M. And Poncibò, C. (eds.) The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms. Cambridge: Cambridge University Press.
Moerel, L. and Prins, C., (2016). Privacy for the homo digitalis: Proposal for a new regulatory
framework for data protection in the light of Big Data and the internet of things. International Data Privacy Law.
Mokyr, J. (2014). The next age of invention: Technology's future is brighter than pessimists allow. City Journal, Preface.
Mosleh, M., Dalili, K. and Heydari, B., (2016). Distributed or monolithic? A computational architecture decision framework. IEEE Systems journal, 12(1).
Mougayar, W. (2016). The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. Hoboken, NJ: John Wiley & Sons.
Mulligan, C., Scott, J.Z., Warren, S. and Rangaswami, J.P., (2018). Blockchain beyond the hype: A practical framework for business leaders. In white paper of the World Economic Forum.
Napieralska, A., Kępczyński , P., (2024). Redefining accountability: navigating legal challenges of participant liability in decentralized autonomous organizations. Networking and Internet Architecture (cs.NI).
Narayanan, A., Clark, J., (2017). Bitcoin's Academic Pedigree. Communications of the ACM, Volume 60, Issue 12.
Narayanan A., Bonneau J., Felten E., Miller A., Goldfeder S., (2016). Bitcoin and

cryptocurrency technologies. Princeton University Press.
Neisse, R., Steri, G. and Nai-Fovino, I., (2017). A blockchain-based approach for data accountability and provenance tracking. In Proceedings of the 12th international conference on availability, reliability and security.
Nissenbaum, H. (2010) Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford, CA: Stanford University Press.
Nyrén, O., Stenbeck, M. and Grönberg, H., (2014). The European Parliament proposal for the new EU General Data Protection Regulation may severely restrict European epidemiological research. European journal of epidemiology, 29(4).
O'Connell, A. and Frick, W. (2014). You've Got the Information, But What Does it Mean? Welcome to "From Data to Action." Harvard Business Review.
Ohm, P., (2010). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. UCLA Law Review, Vol. 57, p. 1701, U of Colorado Law Legal Studies Research Paper No. 9-12.
Pace, R.M. and Coelho, E.R. (2022) 'Information as a weapon of mass disruption: From information disorder to cognitive warfare', Revista da Escola de Guerra Naval, 28(3).
Paivio, A., (1990). Mental representations: A dual coding approach. Oxford Psychology Series, N9, Oxford university press, ISBN 0-19-503936-X.
Papadogiannakis, E., Kourtellis, N., Papadopoulos, P., & Markatos, E. P. (2021). User tracking in the post-cookie era: How websites bypass GDPR consent to track users. In Proceedings of the Web Conference 2021.
Park, C., Chung, M., Ryu, D., (2023). A Blockchain-based Protocol of Trusted Setup Ceremony for Zero-knowledge Proof. Proceedings of the 2023 5th Blockchain and Internet of Things Conference.
Pasquale, F., (2015). The Black Box Society: The Secret Algorithms That Control Money and Information. Cambridge, MA: Harvard University Press.
Phan, P.H., Mian, S.A. and Lamine, W. eds., (2016). Technology entrepreneurship and business incubation: Theory, practice, lessons learned. World Scientific.
Pierce, B. (2023) Tweet: 'The blockchain is going to change everything more than the Internet has'. X (formerly Twitter).
Pilkington, M., (2016). Blockchain Technology: Principles and Applications. Research Handbook on Digital Transformations, edited by F. Xavier Olleros and Majlinda Zhegu. Edward Elgar.
Pisa, M. and Juden, M., (2017). Blockchain and economic development: Hype vs. reality. Center for global development policy paper, 107(150).
Pistor, K. (2019) The Code of Capital: How the Law Creates Wealth and Inequality. Princeton, NJ: Princeton University Press.
Politou, E., Alepis, E., Virvou, M., Patsakis, C., (2022). Privacy and Data Protection Challenges in the Distributed Era. Learning and Analytics in Intelligent Systems, Vol 26, ISBN 978-3-030-85442-3, Springer.
Pollicino, O., De Gregorio, G. & Bassini, M. (2021). Blockchain and Public Law: Global Challenges in the Era of Decentralisation. Edward Elgar.
Popper, N., (2015). Digital gold : Bitcoin and the inside story of the misfits and millionaires

trying to reinvent money. New York, NY : Harper, an Imprint of HarperCollins Publishers.
Porter, J., (2019). Google fined €50 million for GDPR violation in France. The Verge.
Pouwelse, J., Garbacki, P., Epema, D. and Sips, H., (2005). The bittorrent p2p file-sharing system: Measurements and analysis. In International workshop on peer-to-peer systems. Berlin, Heidelberg: Springer Berlin Heidelberg.
Purtova, N., (2018). The law of everything. Broad concept of personal data and future of EU data protection law. Law, Innovation and Technology, 10(1).
Purtova, N., (2022). From knowing by name to targeting: the meaning of identification under the GDPR. International Data Privacy Law, Volume 12, No 3.
Quintais, J.P., Bodo, B., Giannopoulou, A. and Ferrari, V., (2019). Blockchain and the law: A critical evaluation. Stanford Journal of Blockchain Law & Policy, 2 (1).
Ranchordas, S., 2021. Experimental regulations for AI: sandboxes for morals and mores. Morals & Machines, 1(1).
Raskin, M. and Yermack, D. (2016) 'Digital currencies, decentralized ledgers, and the future of financial services', in Conti-Brown, P. and Lastra, R.M. (eds.) Research Handbook on Central Banking. Cheltenham: Edward Elgar Publishing.
Rauchs, M., Blandin, A., Klein, K., Pieters, G.C., Recanatini, M. and Zhang, B.Z. (2018) 2nd Global Cryptoasset Benchmarking Study. Cambridge: Cambridge Centre for Alternative Finance, University of Cambridge.
Reidenberg, J.R., (1997). Lex informatica: The formulation of information policy rules through
technology. 76 Tex. L. Rev. 553 (1997-1998).
Reijers, W., Wuisman, I., Mannan, M., Orgad, L., et al., (2021). Now the Code Runs Itself: On
Chain and Off-Chain Governance of Blockchain Technologies. Topoi.
Riahi, A., Challal, Y., Natalizio, E., Chtourou, Z. and Bouabdallah, A., (2013). A systemic approach for IoT security. In 2013 IEEE international conference on distributed computing in sensor systems.
Rosenfeld, M., (2012). Analysis of hashrate-based double-spending. arXiv.
Rotolo, D., Hicks, D. and Martin, B.R. (2015) 'What is an emerging technology?', Research Policy, 44(10).
Rouvroy, A. and Berns, T. (2013). Algorithmic Governmentality and Prospects of Emancipation. Révues Multitudes.
Royakkers, L. and Sjoerd D.. Zwart, (2015). Moral responsibility and the problem of many hands. Routledge.
Rubinstein, I.S., (2013). Big data: the end of privacy or a new beginning?. International Data Privacy Law, NYU School of Law, Public Law Research Paper No. 12-56.
Saberi, S., Kouhizadeh, M., Sarkis, J. and Shen, L. (2019) 'Blockchain technology and its relationships to sustainable supply chain management', International Journal of Production Research, 57(7).
Sadowski, J. (2020) Too Smart: How Digital Capitalism is Extracting Data, Controlling Our Lives, and Taking Over the World. Cambridge, MA: MIT Press.
Sahu, N., Gajera, M., Chaudhary, A. and Ivey-Law, H., (2023). SeDe: Balancing Blockchain Privacy and Regulatory Compliance by Selective De-Anonymization. arXiv preprint arXiv:2311.08167.
Salazar, J. and Silvestre, S., (2017) Internet of things. PROJECT.
Sartor, G., (2015). The Right to Be Forgotten in the Draft Data Protection Regulation. International Data Privacy Law, vol. 5, no. 1.
Satariano, A. (2022) 'Meta fined $1.3 billion for violating E.U. data privacy rules', The New

York Times, 22 May.
Sater, S., (2017). Blockchain and the European Union's General Data Protection Regulation: A Chance to Harmonize International Data Flows. SSRN Electronic Journal.
Savirimuthu, J., (2019). Review of Blockchain Regulation and Governance in Europe by Michèle Finck and The Blockchain and the New Architecture of Trust by Kevin Werbach, University of Liverpool Repository.
Scaling Parrots (2025) 'Blockchain hash: What is it and what is it for?', Scaling Parrots Blog.
Schär, F. (2021) 'Decentralized finance: On blockchain- and smart contract-based financial markets', Federal Reserve Bank of St. Louis Review / SSRN preprint.
Schiff, D.N., 1976. Socio-legal theory: Social structure and law. The Modern Law Review, 39(3).
Schmidt, E. and Cohen, J. (2013) The New Digital Age: Reshaping the Future of People, Nations and Business. New York: Knopf.
Schollmeier, R., (2001). A definition of peer-to-peer networking for the classification of peer to-peer architectures and applications. In Proceedings first international conference on peer-to-peer computing, IEEE.
Sevin, A., Osman Mohammed, A.A., (2024). Comparative Study of Blockchain Hashing Algorithms with a Proposal for HashLEA. Applied Sciences, 14(24), p.11967.
Seymour, T., Goodell, G., (2024). Custodial and Non-Custodial Wallets. Manuscript. arXiv.
Shubber, K. (2013) 'A simple guide to GCHQ's internet surveillance programme Tempora', Wired UK, 21 June.
Solanki, A., Singh, A.K. and Tanwar, S. eds., (2023). Blockchain Technology for IoE: Security
and Privacy Perspectives. CRC Press.
Solove, D., J., (2023). The Limitations of Privacy Rights. 98(3) Notre Dame Law Review 977.
Stodt, F., Reich, C. and Stodt, F., (2024). Digital Wallets and Identity Management: Pioneering
Advances for Cloud Service Evolution. International Journal on Advances in Software, 17(1 & 2).
Staton, W. (2015). Information as a Weapon: The Real Threat of Privacy & Data in 2015. Medium.
Strehle, E., (2020). Public Versus Private Blockchains. Blockchain Research Lab, BRL Working Paper Series No. 14.
Suzor, N.P., (2019). Lawless: The secret rules that govern our digital lives. Cambridge University Press.
Svantesson, D.J.B., (2017). Solving the Internet Jurisdiction Puzzle. IRL Press Oxford University Press, Oxford Scholarship Online, ISBN: 9780198795674.
Swan, M. (2015). Blockchain: Blueprint for a New Economy. Sebastopol: O'Reilly Media, sections d. What Is the Blockchain? and e. The Connected World and Blockchain: The Fifth Disruptive Computing Paradigm.
Swanson, T., (2015). Consensus-as-a-Service: A Brief Report on the Emergence of Permissioned, Distributed Ledger Systems.
Sweeney, L., (2002). k-Anonymity: A Model for Protecting Privacy. International Journal on Uncertainty, Fuzziness and Knowledge-Based Systems, 10 (5), 2002; 557-570.
Szabo, N. (1996) 'Smart contracts: Building blocks for digital markets', unpublished manuscript.
Tanenbaum, A.S. and Van Steen, M. (2006) Distributed Systems: Principles and Paradigms. Upper Saddle River, NJ: Pearson Prentice Hall.
Tapscott, D. and Tapscott, A. (2016) Blockchain Revolution: How the Technology Behind

Bitcoin and Other Cryptocurrencies is Changing the World. New York: Penguin.
Taylor, L., Floridi, L. and van der Sloot, B. (eds.) (2016). Group Privacy: New Challenges of Data Technologies. Dordrecht: Springer.
Tene, O. and Polonetsky, J., (2011). Privacy in the age of big data: a time for big decisions. 64
STAN. L. REV. ONLINE 63.
Tews, S., (2024). Beyond Bitcoin: Unlocking Blockchain's Potential. AEIdeas.
The Economist (2017) 'The world's most valuable resource is no longer oil, but data', The Economist, 6 May.
The Editors of Encyclopaedia Britannica, (2014). "Fiat money," Encyclopaedia Britannica.
The European Business Review, (2021). Future of Blockchain: How will it revolutionize the world in 2022 and Beyond.
The Royal Society, (2015). Protecting Privacy in Practice. The current use, development and limits of Privacy Enhancing Technologies in data analysis. ISBN: 978-1-78252-390-1.
Thierer, A, (2012). Europe's 'Right to Be Forgotten': Privacy as Internet Censorship. The Technology Liberation Front.
Torreblanca, J.I. (2015). Digital weapons, Digital vulnerability is a great concern for governments and companies. European Council on Foreign Relations.
Torres, C.F., Willi, F. and Shinde, S.,(2023). Is your wallet snitching on you? an analysis on the privacy implications of web3. In 32nd USENIX Security Symposium (USENIX Security 23).
Townsend, A. (2013) Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia. New York: W.W. Norton & Company.
Troncoso, C., Isaakidis, M., Danezis, G. and Halpin, H., (2017). Systematizing decentralization
and privacy: Lessons from 15 years of research and deployments. Proceedings on Privacy Enhancing Technologies.
Tschorsch, F., Scheuermann, B., (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Communications Surveys & Tutorials, 18(3).
Tsesis, A. (2014) 'The right to erasure: Privacy, data brokers, and the indefinite retention of data', Wake Forest Law Review, 49.
Turégano-Fuentes, F., Caba-Doussoux, P., Jover-Navalón, J.M., Martín-Pérez, E., Fernández Luengas, D., Díez-Valladares, L., Pérez-Díaz, D., Yuste-García, P., Guadalajara Labajo, H., Ríos-Blanco, R. and Hernando-Trancho, F., (2008). Injury patterns from major urban terrorist bombings in trains: the Madrid experience. World journal of surgery, 32(6).
Uncular, S., (2019). The right to removal in the time of post-Google Spain: myth or reality under general data protection regulation?. International Review of Law, Computers & Technology, 33(3).
UpGuard Team. (2019). Losing Face: Two More Cases of Third-Party Facebook App Data Exposure.
Van Hoecke, M. (ed.) (2011). Methodologies of legal research: Which kind of method for what
kind of discipline? Oxford: Hart Publishing.
Velleman, J., D., (2001). The Genesis of Shame. Philosophy & Public Affairs, Vol. 30, No. 1.
Vladkov-Mirazchiyski, P. (2025). Contemporary gaps in research on digital divide in education: A literature review. Universal Access in the Information Society, 24, pp. 991–1008.
Voigt, P. and Von dem Bussche, A., (2017). The EU General Data Protection Regulation

(GDPR). A practical guide, 1st ed., Cham: Springer International Publishing, 10(3152676.
Von Hafe, F., Wagle, Y., Guede-Fernández, F., Giordano, A.P., Silva, L. and Azevedo, S., (2025). Legal frameworks for blockchain applications: a comparative study with implications for innovation in Europe. Frontiers in Blockchain, 8.
Voss, W.G. (2021) 'Airline commercial use of EU personal data in the context of the GDPR, British Airways and Schrems II', Colorado Technology Law Journal, 19(2).
Vrabec, H., U., (2021). Data Subject Rights Under the GDPR. With a Commentary through the Lens of the Data- driven Economy. Oxford University Press.
Vukolić, M. (2017) 'Rethinking permissioned blockchains', in Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts.
Wachter, S. and Mittelstadt, B. (2019) 'A right to reasonable inferences: Re-thinking data protection law in the age of big data and AI', Columbia Business Law Review, 2019(2).
Walch, A., (2016). The path of the blockchain lexicon (and the law). Review of Banking & Financial Law, 36.
Walch, A., (2019). Deconstructing'decentralization': Exploring the core claim of crypto systems. in Brummer (ed), Cryptoassets Cryptoassets: Legal, Regulatory, and Monetary Perspectives, Oxford University Press.
Walch, A., 2019. „In Code (rs) we trust: Software developers as fiduciaries in public blockchains ". U: Regulating Blockchain: Techno-Social and Legal Challenges, Philipp Hacker, Ioannis Lianos, Georgios Dimitropoulos i Stefan Eich.
Walters, R., Trakman, L., & Zeller, B. (2019). Data protection law: A comparative analysis of Asia-Pacific and European approaches.
Wang, K., (2025). Regulating Cryptocurrency Non-Custodial Service Providers Through the Bank Secrecy Act. The University of Chicago Business Law Review. Rev., 4:2.
Wardaningsih, A.D., (2025). PERSONAL DATA AS A COMMODITY IN THE DIGITAL ECONOMY. Berumpun: International Journal of Social, Politics, and Humanities, 8(1).
Water, R., (2018). Facebook sued by US regulator over Cambridge Analytica scandal. Financial Times.
Weingärtner, T., (2024). Blockchain for Digital Identity. In: Jaafar, F., Pierre, S., (eds), Blockchain and Artificial Intelligence-Based Solution to Enhance the Privacy in Digital Identity and IoT, CRC Press.
Werbach, K., (2018). The Blockchain and the New Architecture of Trust. The MIT Press. ISBN 9780262038935.
Werbach, K. and Cornell, N., (2017). Contracts ex machina. Duke Law Journal, Vol: 67:313, p.327.
Whittaker, Z., (2019). Researchers find 540 million Facebook user records on exposed servers.
Winklevoss, T. (2013) Tweet. X (formerly Twitter).
Werro, F. (2009) 'The right to inform v the right to be forgotten: a transatlantic clash', in Colombi Ciacchi, A. et al. (eds.) Liability in the Third Millennium. Baden-Baden: Nomos.
Winner, L., (2020). The Whale and the Reactor: A Search for Limits in an Age of High Technology. 2nd ed. Chicago: University of Chicago Press.
Wright, A., Filippi, P., D., (2018). Blockchain and the Law. The Rule of Code. Harvard

Universtity Press.
Wörner, D., Von Bomhard, T., Schreier, Y.P. and Bilgeri, D., (2016). The bitcoin ecosystem: Disruption beyond financial services? Twenty-Fourth European Conference on Information Systems (ECIS), İstanbul,Turkey.
YCHARTS, (2025). Bitcoin Blockchain Size (I:BBS).
Yeung, K., (2018). Algorithmic regulation: A critical interrogation. Regulation & governance, 12(4).
Yeung, K. and Bygrave, L.A., (2022). Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship. Regulation & Governance, 16(1).
Yli-Huumo, J., Ko, D., Choi, S., Park, S. and Smolander, K., (2016). Where is current research on blockchain technology?—a systematic review. PloS one, 11(10), p.e0163477.
Zafar, A., (2025). Reconciling blockchain technology and data protection laws: regulatory challenges, technical solutions, and practical pathways. Journal of Cybersecurity, 11(1), p.tyaf002.
Zetzsche, D., A., Buckley, R., P., Arner, D., W., (2019). The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators. Volume, 60. Number 2. Harvard International Law Journal.
Zetzsche, D.A., Arner, D.W. and Buckley, R.P., (2020). Decentralized finance. Journal of Financial Regulation, 6(2).
Zetzsche, D.A., Nikolakopoulou, A. (2024). Crypto Custody and Crypto Wallets – An Empirical Assessment. FutureFinTech Working Paper Series, SSRN.
Zhou, R., (2023). Research on the Development of the Digital Economy based on Blockchain Technology. Iris Online Journal of Arts and Social Sciences, Volume 1, Issue 2, ISSN: 2837-4509.
Zook, M. and Graham, M. (2007). The creative reconstruction of the internet: Google and the privatization of cyberspace and DigiPlace.
Zuboff, S. (2019) The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs.
Zyskind, G., Nathan, O., (2015). Decentralizing privacy: Using blockchain to protect personal data. In 2015 IEEE security and privacy workshops.

5. Technical Standards and White Papers

Buterin, V., Weiss, Y., Tirosh, D., Nacson, S., Forshtat, A., Gazso, K., Hess, D., (2021). ERC 4337: Account Abstraction Using Alt Mempool' (Ethereum Improvement Proposals).
BitcoinCore (2025) Running a Full Node: Support the Bitcoin Network by Running Your Own Full Node.
Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper, 151(2014).
Ethereum Foundation, (2025). JSON-RPC API.
International Organization for Standardization, (2015). ISO/IEC 2382:2015 Information technology—Vocabulary. Geneva: ISO.
Getblock, (2025). Eth_call – Ethereum, API Reference.
Getblock, (2025). How to Add GetBlock RPC Endpoints to MetaMask.
King, S., Nadal, S., (2012). PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. Semantic Scholar.

Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. Working paper.
Newman, D., (2025). Light vs Full vs Archive Ethereum Nodes. GETBLOCK.
WalletConnect, (2025). Relay Protocol (Specification/Documentation).
Werkheiser, B., (2024). How do ERC-4337 smart contract wallets work? Alchemy.
Wood, G., (2014). Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper, 151(2014).
W3C, (2022). Decentralized Identifiers (DIDs) v1.0: Core Architecture, Data Model, and Representations.
W3C, (2015). World Wide Web Consortium Process Document.

6. Corporate Policies and Privacy Notices

Binance, 2025. Binance Privacy Portal.
Coinbase, (2025). Coinbase Global Privacy Policy.
Coinbase, (2025). Privacy Notice and Consent for New Applicants.
Consensys (2022) MetaMask: Privacy Policy and Technical Architecture.
Kraken, (2025). Privacy Notice.
MetaMask, (2025). Privacy preserving features in MetaMask.
Wasabi, (2025). Wasabi Documentation.