RIGA GRADUATE SCHOOL OF LAW

Moving to Immutability: General Data Protection Regulation's Right to be Forgotten in Blockchain Transactions

BACHELOR THESIS

AUTHOR: Oona Elina Katariina Tuomi

LL.B 2021/2022 year student

student number B012005

PREFERRED SUPERVISOR: Ēriks Kristiāns Selga,

LL.M

DECLARATION OF HONOUR:

I declare that this thesis is my own work, and that all references to, or quotations from, the work of others are fully and correctly cited.

(Signed)……..

RIGA, 2024

ABSTRACT

Emerging technological advances are changing the world. Among the Internet of Things (IoT), blockchain is a revolutionary technology for data storage allowing the application of it in many different industries. The balance between innovation and regulatory aspects is increasingly burdensome to reach, especially with the new blockchain technology. Due to the architecture of blockchain, there is an undeniable clash between some of the GDPR's principles. In conjunction with storage and purpose restrictions, the right to be forgotten as stipulated in Article 17 of the GDPR is one of the most discussed blockchain-related topics. The lack of compliance stems from the immutable and decentralised nature of the blockchain, making it impossible to erase information from the chain itself, hence posing a threat to the right of privacy. This thesis aims to evaluate blockchain through the lens of the GDPR. More specifically the goal is to establish the connection between blockchain and the right to be forgotten established in Article 17 of the GDPR and understand the legal challenges arising from the technology itself.

Keywords: blockchain, right to be forgotten, immutability, data privacy, FinTech, personal data,

SUMMARY

This paper examines the extent to which blockchain technology and the General Data Protection Regulation (GDPR) intersect, with a particular emphasis on the fulfilment of the the right to be forgotten provided in Article 17. More specifically, the focus is on the conflict arising from the immutable nature of the blockchain when it comes to the requirements for data erasure set by Article 17.

This thesis is divided into three main chapters. The first chapter takes a look into the world of blockchain technology, providing a thorough explanation of its core concepts, technical underpinnings, and potential applications beyond the realm of finance. This comprehensive presentation provides a solid foundation for understanding how blockchain can be used in various industries. Problems stemming from the inability to erase personal information are outlined in this chapter from a technological viewpoint. Private and permissionless blockchains are discussed in contrast to public and permissionless blockchains, finding that permissionless blockchains may be a better solution for storing data due to the restriction methods available. The focus narrows to the most prominent solutions discussed by scholars: the possibilities of off-chain data storage, smart contracts, and hashing algorithms to support the "right to be forgotten" in blockchain ecosystems.

Furthermore, the second chapter explores the complexities of the General Data Protection Regulation (GDPR). It emphasizes the regulation's significance in our increasingly digital world and its reach, extending to various technologies. The chapter then focuses on a specific application: how the GDPR's principles are implemented with blockchain technology. Here, the focus narrows to how personal data is managed and categorized within blockchain networks. This covers the ramifications of the GDPR's jurisdictional and material scopes, as well as a thorough examination of how in the blockchain the data controllers and processors can be established. Perhaps most importantly, it explores the crucial link between other GDPR principles, particularly the "right to be forgotten" and how they function within the context of blockchain. In addition to the right to be forgotten, it is illustrated how the GDPR principles, such as data minimization, lawfulness and privacy by design intersect with the features of blockchain technology. Furthermore, MICA regulation and immutability in crypto asset transactions such as Bitcoin transactions are touched upon. Transfers of crypto assets have already faced some problems regarding data added to them, the aspiring problems recognized also by the INTERPOL.

The third part focuses on the intersection of legal, technological and economic challenges, providing insights into the opinions of the most prominent data protection authorities and academics. It is established whether or not there are effective solutions to the issues as of now. A variety of suggestions to mitigate the effect on privacy by the immutability of the blockchain are analysed. Technological advancements like smart contracts and off-chain data storage options are brought up in this context. The legal viewpoints of the European Union and other international studies as well as the opinions of the scholars are examined to demonstrate the continuous discussions and legislative endeavours aimed at harmonising data protection regulations with the rapidly developing blockchain technology.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

CETS 108	Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data, ETS 108.
Charter	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
CoE	Council of Europe
CNIL	French Data Protection Authority (National Commission on Informatics and Liberty)
DLT	Distributed Ledger Technology
DPA	Data Protection Authority
ECB	European Central Bank
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EEA	European Economic Area
EU	European Union
FinTech	Financial Technology
GDPR	Regulation (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), OJ L 119, 4.5.2016.
ICO	Information Commissioner's Office
INTERPOL	International Criminal Police Organization
IP	Intellectual Property

MICA	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 (Text with EEA relevance), 150 OJ L § (2023).
PII	Personally Identifiable Information
PPII	Potentially Personally Identifiable Information
TFR	Transfer of Funds Regulation
UNDP	The United Nations Development Programme
UNICEF	The United Nations Children's Fund
VASP	Virtual Asset Service Providers
WP29	Article 29 Working Party

INTRODUCTION

Data breaches are growing in number and personal data is becoming increasingly more difficult to protect. The protection of personal data is more frequently compromised even in the presence of centralised authority, as seen in the recent rise in data breaches.[1] There is no denying the importance of "starting over" or "forgetting the past", of erasing digital shadows in particular and leaving behind digital imprints in general.[2] Blockchain is offering a new decentralized and immutable platform, offering a modern solution for the security of the data. As these technologies gain popularity in the use of economic and social infrastructures, they also present significant legal issues, especially with regard to adhering to well-established data protection regulations such as GDPR. The General Data Protection Regulation (hereinafter - GDPR) was introduced by the European Union (hereinafter - EU) to harmonize data protection laws within the EU.[3] While the data is secure and protected through the means of integrity and accessibility, the decentralized and immutable nature of blockchain raises questions about compliance with some of the provisions of the Regulation.

When personal data is processed in the blockchain it becomes the subject of the GDPR. Companies may use blockchain in their business operations storing some of the personal information within the blockchain. Such data can be names, addresses, IP addresses, pictures or other data constituting personal data. A key feature of blockchain is that the data cannot be altered in any way. However, it is also one of the main shortcomings when it comes to GDPR compliance. More specifically, immutability is the term to describe this inability to be modified.[4] The architectural design of blockchains, in other words, the connections between blocks, makes it impossible to remove any block other than the final one without also erasing

---

[1] Stuart E Madnick, "The Continued Threat to Personal Data: Key Factors Behind the 2023 Increase," December 2023, accessed April 6, 2024, https://www.apple.com/newsroom/pdfs/The-Continued-Threat-to-Personal-Data-Key-Factors-Behind-the-2023-Increase.pdf.

[2] Lilian Mitrou and Maria Karyda, "EU's Data Protection Reform and the Right to Be Forgotten: A Legal Response to a Technological Challenge?," SSRN Scholarly Paper (Rochester, NY, February 5, 2012), accessed April 5, 2024, https://papers.ssrn.com/abstract=2165245.

[3] Regulation (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), OJ L 119, 4.5.2016. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC. Accessed January 4th, 2024.

[4] "Blockchain Facts: What Is It, How It Works, and How It Can Be Used," Investopedia, accessed January 26, 2024, https://www.investopedia.com/terms/b/blockchain.asp.

the blockchains' overall structure.[5] Immutability conflicts with one of the general principles of the GDPR - Article 17, which stipulates the right to erasure ('Right to be forgotten').[6] Still, one of the main reasons blockchain is becoming increasingly prevalent and seen as revolutionary stems from its immutability.

Decentralization is another characteristic of blockchain. In the financial markets, resolving the conflict between confidentiality and legal requirements is the responsibility of trusted intermediaries.[7] They uphold segregated data repositories that, when properly maintained, automatically safeguard members' privacy.[8] Blockchain, however, is a decentralized technology, meaning there is no central authority or entity to be determined as a data controller or a processor within the meaning of the GDPR definitions.[9] While such a feature presents many advantages, an underlying problem lies in determining the responsibility and therefore enforcing the data subjects' rights. Thus, a fundamental question is raised: To what extent do the unique technical blockchain characteristics, including its decentralized nature and immutability enable the fulfilment of the right to erasure (the right to be forgotten) stipulated in Article 17 of the GDPR? This thesis seeks to provide a comprehensive analysis of the legal ramifications of extending blockchain technology's right to be forgotten under the GDPR.

The primary concern is that immutability raises a contradiction with the GDPR's duties for individual rights. Personal data may never be erased from the blockchain, even in cases where it is harmful to the individual or inaccurate. It is nearly impossible to restrict what kind of data ends up in the blockchain. The International Criminal Police Organization (hereinafter – INTERPOL) has already raised concerns about the potential for blockchain to become a safe haven for illegal data hosting, such as including pictures of child sexual assault.[10] Decentralization and immutability make it impossible to remove such data or identify the parties in charge of it. In a way it can be compared to the dark web - the data in the blockchain is out of reach for any authorities.

---

[5] Inês Campos Ruas, Soumaya Ben Dhaou, and Zoran Jordanoski, "Blockchain and the GDPR – the Shift Needed to Move Forward," n.d., https://ceur-ws.org/Vol-3449/paper14.pdf.

[6] GDPR, *Supra* note 3, Article 17.

[7] Shlomit Azgad-Tromer, Joey Garcia, and Eran Tromer, "The Case for On Chain Privacy and Compliance," SSRN Scholarly Paper (Rochester, NY, June 27, 2023), https://papers.ssrn.com/abstract=4492919.

[8] *Ibid*.

[9] *Ibid*.

[10] INTERPOL, "INTERPOL Cyber Research Identifies Malware Threat to Virtual Currencies," accessed May 8, 2024, https://www.interpol.int/en/News-and-Events/News/2015/INTERPOL-cyber-research-identifies-malware-threat-to-virtual-currencies.

Due to the multi-layered application possibilities of blockchain technology, a case-by-case analysis is required. Different technologies are already being applied for higher GDPR compliance. These include off-chain data storing, data encryption methods and smart contracts giving individuals the possibility to take part in the use of their data. Some of these methods still fall short in protecting personal data, as blockchain may include encryption methods to hide visible personal information. It does not mean, however, that the data subject is completely unidentifiable due to such an encryption method, which places the personal data in danger. To examine the various aspects of these issues, three primary points of view are available: technical or architectural (immutability), economic (markets), and legal (laws).[11]

The objectives discussed concerning blockchain technology, include: i) whether or not the right to be forgotten truly has been infringed and what complications arise as a result; ii) determining possible technological and legal solutions for GDPR adherence; and iii) assessing these systems' viability for use in present and upcoming blockchain applications. The GDPR and its responsibilities in resolving these issues are examined using the doctrinal research technique. The study will utilise information from a wide range of official EU documents, research studies, scholarly publications, scholarly views, and case law from the European Court of Justice and other EU authorities. In addition to a legal approach, a technological approach is necessary to establish ways in which blockchain technology can be made more compliant with the GDPR. Some of the pertinent terminology is explained using a descriptive approach, particularly those that deal with blockchain technology and terms related to the legal framework that surrounds it. The GDPR's right to be forgotten principle is the primary lens through which blockchain is examined, but other considerations include the roles of controllers, processors, and/or joint controllers, data minimization and accuracy, data retention, and the rights of data subjects to rectification. Additionally, an analysis of the recently implemented Markets in Crypto-Assets Regulation (hereinafter - MICA) is conducted regarding personal data in Bitcoins. Since FinTech is centred on the financial sector and financial markets, following the data protection law presents an interdisciplinary challenge with implications for the economy and law.

This thesis is divided into three main parts. The first chapter discusses the definitions and technical part of blockchain to further understand the application of the GDPR. This part also highlights the different kinds of technologies used in blockchain and issues arising from

[11] Unal Tatar, Yasir Gokce, and Brian Nussbaum, "Law versus Technology: Blockchain, GDPR, and Tough Tradeoffs," *Computer Law & Security Review* 38 (September 1, 2020): 105454, https://doi.org/10.1016/j.clsr.2020.105454.

them. Technological solutions for the evident compliance issues are also discussed such as encryption methods by hashing, off-chain data storage and smart contracts. The following topics will be covered in detail in the second chapter of the paper: i) the context and history of the relevant framework such as the GDPR; ii) the notion of personal data in the scope of blockchain, including whether or not blockchain constitutes personal data for GDPR objectives and what kind of personal data can be stored in the blockchain; iii) The general principles of GDPR and the right to erasure is also further discussed in this part. In this context, also the determination of the controller or processor takes place; lastly iv) the MICA regulation and its implications on blockchain. The third chapter is devoted to the discussion of how the right to be forgotten and blockchain are connected, what the issues surrounding their interconnection are and whether there are any possible solutions. This chapter also discusses the opinions of the French Data Protection Authority (hereinafter - CNIL) and the European Blockchain Observatory Forum, as well as different aspects related to the legal challenges and the conflict between private and public interest.

There are certain restrictions on the scope of this research in this paper. This research is limited to the use of blockchain in financial transactions. Since the legislative framework under consideration - such as the GDPR and MICA - are implemented in the European Union, global aspects of the issue are not addressed in this research. In addition, blockchain technology is still relatively new and legislation pertaining to it is still in its infancy, there is also an inadequate amount of case law on the subject as of the time of writing this thesis. There have not been any cases within the European Union regarding the erasure of data from blockchain systems to offer any light on the issue. This restricts the scope of legal analysis and results in a more theoretical rather than practical approach. The continuous progress in digital technology and the requirement for legal frameworks to adapt to adequately safeguard individual rights highlights the importance of this research.

1. BLOCKCHAIN

The Fourth Industrial Revolution has arrived with recent technological advances such as blockchain, according to some experts.[12] Problems in the use of blockchain stem not only from the gaps in legislation due to adapting to the technological changes brought by it, but also from the architectural limitations with technology when it comes to adhering to the requirements set by law. Legal challenges include but are not limited to the privacy concerns arising from the clash of immutability and requirements for personal data to be erased in certain conditions. Additionally, regulatory compliance is difficult to reach because of its decentralised nature. In a public blockchain especially, erasing data without leaving traces or increasing the likelihood of recovery efforts is nearly impossible due to the ledger's openness to all members and possibly the general public.

Blockchain is one of the technologies aiming to enhance and automate the provision of financial services that have increased in the last decade and are referred to as 'Financial Technology' (hereinafter - FinTech).[13] Blockchain, which is the core technology or infrastructure used when using cryptocurrency, was first introduced in 2009.[14] In 2021, the market for blockchain technology was estimated to be worth 5.85 billion US dollars worldwide, expected to grow to 1,235.71 billion US dollars by 2030, or 82.8 per cent annually compounded.[15]

The key to understanding GDPR compliance of blockchain is to have some kind of comprehension of the technology itself before diving into the above-mentioned dilemmas. In simple terms, blockchain technology is a new worldwide resource that allows for information storage and communication without the need for a centralised authority.[16] Blockchain is not synonymous with Bitcoin or cryptocurrency, despite the common misconception among the society. While the most common use of blockchain is in cryptocurrency applications, it is used

---

[12] Shuo-Yan Chou, "The Fourth Industrial Revolution: Digital Fusion with Internet of Things," *Journal of International Affairs* 72, no. 1 (2018): 107–20.
[13] "Financial Technology (Fintech): Its Uses and Impact on Our Lives," Investopedia, accessed January 26, 2024, https://www.investopedia.com/terms/f/fintech.asp.
[14] Tatar et al., *supra* note 11.
[15] Statista, "Blockchain Technology Market Size Worldwide 2030," Statista, accessed January 30, 2024, https://www.statista.com/statistics/1319369/global-blockchain-technology-market-size/.
[16] Jiménez-Gómez, Briseida Sofia, "RISKS OF BLOCKCHAIN FOR DATA PROTECTION: A EUROPEAN APPROACH," *Santa Clara High Technology Law Journal* 36, no. 3 (April 2, 2020): 281.

for much more, with applications in the financial, insurance, communications, and healthcare industries.[17] More specifically, by effectively guaranteeing the transparency and integrity of the data, it may be used for uses in corporate, identity management, data management in social organisations, and democratic participation, including election voting systems.[18] As a result of growing popularity, blockchain technology has the potential to significantly alter society while also providing substantial financial advantages.

The European Commission has made evident efforts to promote the use of blockchain and its application in the future. In addition to investing EUR 200 million in research and development programmes that assist the use of blockchain in technological and social domains, the European Commission established the EU Blockchain Observatory and Forum in February 2018.[19] The European Blockchain Partnership (EBP) was signed by more than 21 EU member states on April 10, 2018, and they committed to working together to build a European Blockchain Services Infrastructure (EBSI) that will facilitate the provision of digital public services across borders while maintaining the highest security and privacy standards.[20] As of right now, there are 30 signatory nations. This demonstrates the enormous influence that blockchain technology will have in the future across multiple countries and different industries. Mariya Gabriel, Commissioner for Digital Economy and Society, stated that blockchain technology will be used in all public services in the future.[21] Taking the lead, 10 international United Nations institutions including The World Food Programme (WFP), UN Women, UNICEF, UNOPS, and UNDP are experimenting with blockchain applications, particularly for operational activities and more are considering possible blockchain applications.[22]

The characteristics of blockchain, according to the French Data Protection Agency (National Commission on Informatics and Liberty, or CNIL), include transparency, sharing and decentralisation, irreversibility, and disintermediation.[23] Although blockchain is included in the

---

[17] Tatar et al., *supra* note 11, p. 2.
[18] Shraddha Kulhari, "The Midas Touch of Blockchain: Leveraging It for Data Protection," in *Building-Blocks of a Data Protection Revolution*, 1st ed., *The Uneasy Case for Blockchain Technology to Secure Privacy and Identity*, (Nomos Verlagsgesellschaft mbH, 2018), pp. 15-22, accessed May 5, https://www.jstor.org/stable/j.ctv941qz6.6.
[19] European Commission, "European Countries Join Blockchain Partnership | Shaping Europe's Digital Future," April 10, 2018, accessed May 8, 2024, https://digital-strategy.ec.europa.eu/en/news/european-countries-join-blockchain-partnership.
[20] *Ibid*.
[21] *Ibid*.
[22] Petru Dumitriu and Joint Inspection Unit, "Blockchain Applications in the United Nations System: Towards a State of Readiness: Report of the Joint Inspection Unit," 2020, accessed May 1, 2024, https://digitallibrary.un.org/record/3906141.
[23] CNIL, "Blockchain and the GDPR: Solutions for a Responsible Use of the Blockchain in the Context of Personal Data," accessed November 28, 2023, https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data.

larger category of Financial Technology (FinTech), it is important to recognise the different functions that each has in the financial industry. Blockchain is the underlying technology behind cryptocurrencies and many other technologies, whereas FinTech primarily focuses on technology for enhancing and automating the supply of financial services.[24] Furthermore, the term "blockchain" is frequently used interchangeably with "Distributed Ledger Technology," or DLTs, to refer to a broader family of technologies. Blockchain's core technology, distributed ledger technology (DLT), is a decentralised system free from monetary authority.[25] Put another way, blockchain may be thought of as a distributed database that emphasises peer-to-peer transmission for communication.[26] In essence, it is an immutable, free method to record or register transactions because it is meant to be shared among users.[27] However, it's crucial to remember that there isn't just one blockchain technology; rather, blockchain exists in a variety of forms and capacities.

1.2. Technical design of Blockchain

The way that data is kept on a ledger is referred to as "Blockchain".[28] Blockchain may be thought of as the transaction history stored chronologically on a computer network.[29] The network of computers is essentially created by the users in the blockchain. The computers that make up the network are called "nodes" and a blockchain is created when smaller information called "blocks" are arranged in chronological order using encryption.[30] According to its definition, blockchain is a "type of database: a structured collection of information" where data integrity and data identification are achieved via the critical application of cryptographic functions.[31] The fundamental method of blockchain, distributed ledger technology, only permits the addition of new data, which grows exponentially when replicated across several computers.[32]

---

[24] Saule T. Omarova, "Technology v Technocracy: Fintech as a Regulatory Challenge," *Journal of Financial Regulation* 6, no. 1 (June 25, 2020): pp. 75-124, accessed March 4, 2024, https://doi.org/10.1093/jfr/fjaa004.
[25] Mani Karthik Suhas Suripeddi and Pradnya Purandare, "Blockchain and GDPR – A Study on Compatibility Issues of the Distributed Ledger Technology with GDPR Data Processing," *Journal of Physics: Conference Series* 1964, no. 4 (July 1, 2021): 042005, accessed April 17, 2024, https://doi.org/10.1088/1742-6596/1964/4/042005.
[26] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," n.d., accessed May 4, 2024, https://www.researchgate.net/publication/228640975_Bitcoin_A_Peer-to-Peer_Electronic_Cash_System.
[27] Suripeddi and Purandare, *supra* note 25.
[28] Jiménez-Gómez, *supra* note 16.
[29] Kulhari, *supra* note 18, p.16.
[30] *Ibid*.
[31] Jean Bacon, Johan David Michels, Christopher Millard, and Jatinder Singh, "Blockchain Demystified," SSRN Scholarly Paper, Rochester, NY, December 20, 2017, accessed April 5, 2024, https://papers.ssrn.com/abstract=3091218.
[32] European Parliament, Directorate General for Parliamentary Research Services, *Blockchain and the General Data Protection Regulation: Can Distributed Ledgers Be Squared with European Data Protection Law?* LU: Publications Office, 2019, accessed May 8, 2024, https://data.europa.eu/doi/10.2861/535.

As the network is built by the users, blockchain is decentralized, which means that every node in the network exchanges data directly with other nodes, without the need for intermediaries or trusted third parties.[33] The data is stored on the blockchain and on each individual's computer and it is possible for every node linked to the blockchain network to send and receive transactions.[34] Moreover, every node connected to the network is equipped with a copy of the whole blockchain identical to others and undergoes frequent synchronisation with other nodes to guarantee that all nodes are using the same shared database.[35] Transparency is ensured since each user has access to their own copy of the blockchain and its contents.

The accuracy of the data is ensured through validation, as all of the blocks added to the network need confirmation from each node in the blockchain, which is called consensus within the blockchain.[36] As the block is stored on every user's computer separately, it makes the modification or erasure of the data practically impossible and less prone to errors. The block, however, could contain information such as personal data where storing it in multiple computers seems like an ominous option. This storing of data and access to it in the public blockchain is one of the most problematic features.

1.2.1. Immutability

Imagine a situation where some data such as falsifying information, some other misinformation, or inappropriate pictures such as pictures of a naked person is added to the blockchain. The main problems raised in this study are related to immutability or the impossibility of deleting or changing data after it is placed on the blockchain. This is a result of the public blockchain's architectural design, as discussed above. From the perspective of this research, the public and immutable character of DLT or blockchain is a major concern and will be discussed throughout this paper. In cases such as the above, if the individual would want the information removed, it is practically impossible to correct the situation due to multiple participants. Herein also lies the tension between an infringement on personal freedoms and the right to be forgotten to be discussed in a later chapter.

---

[33] Aafaf Ouaddah, Anas Elkalam, and Abdellah Ouahman, "FairAccess: A New Blockchain-Based Access Control Framework for the Internet of Things," *Security and Communication Networks* 9 (February 1, 2017), accessed March 4, 2024, https://doi.org/10.1002/sec.1748.
[34] Kulhari, *supra* note 18, pp.15-22.
[35] Nakamoto, *supra* note 26.
[36] Kulhari, *supra* note 18. pp.15-22.

1.2.2. Private and/or permissioned blockchains and public and permissionless blockchains

To understand the immutability perspective in public blockchains and in general, as well as other GDPR-related issues, it is important to differentiate between private and/or permissioned blockchains as well as public and permissionless blockchains. Although sounding very similar, each term has its own meaning within the blockchain. The accessibility to the blockchain poses difficulties to privacy, as there is a higher potential that privacy may be infringed when the data is available to a larger base.

The difference between a public and private blockchain is that in a public blockchain, the information is shared between particular users in a transaction.[37] Initially, a public blockchain allows for network accessibility for all users, whereas a private blockchain restricts network access to a certain group of authorized people.[38] Although both public and private blockchain have their own strengths, a public blockchain is considered more secure than a private blockchain, since a private blockchain primarily relies on access restrictions to limit who can join the network.[39] Because every node validates the transaction, tampering with the data is extremely difficult in a public blockchain. Therefore, a widespread user base increases validation and improves security. All the data is accessible to everyone in the network, constituting a problem regarding data minimization since no data besides the strictly necessary should be stored.[40] In a private blockchain, the restriction on the network makes it easier to practice control by the established authority, making the data more prone to security threats such as data tampering, internal fraud, and single points of failure as data is easier to modify.[41]

The division in the latter group of permissioned and permissionless blockchain relates to who may contribute information to the blockchain, determining whether it is a permissioned or permissionless blockchain. A blockchain is referred to as permissionless when anybody can share to the network, while a permissioned blockchain only permits a specific person to add to the network under authorization.[42] Also, users' actions on permissioned blockchains are restricted by their network permissions. The terms private and permissioned blockchains are often used interchangeably with each other as well as public and permissionless blockchains.

---

[37] Jiménez-Gómez, *supra* note 16.
[38] *Ibid*.
[39] Ouaddah et al., supra note 33.
[40] Ruas et al, *supra* note 5.
[41] Gousia Habib, Sparsh Sharma, Sara Ibrahim, Imtiaz Ahmad, Shaima Qureshi, and Malik Ishfaq, "Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing," *Future Internet* 14, no. 11 (November 2022): 341, https://doi.org/10.3390/fi14110341.
[42] Jiménez-Gómez, *supra* note 16.

Related to the access to the blockchain, the users have public keys and private keys. The public key, which is a string of characters and numbers that represents the user, and the private key, which is a password that should never be shared with anybody else, are related to the verification process.[43] The biggest issues again arise from public blockchains as public keys contain personal data and act as blockchain identities.[44] Such data may be viewed by everyone on a permissionless blockchain, which is undoubtedly very undesirable from a privacy standpoint.[45] The data encrypted with the public key may be decrypted with the private key.[46] Therefore a sensible course of action for the privacy of the data is to employ appropriate encryption methods, in which the data entering the chain is encrypted and the key is external. The way to exercise the right to be forgotten would then be by destroying the key.

1.2.3. Hash function

Another dilemma comes up regarding data availability, particularly with public permissionless blockchains: How can our data remain private if it is stored everywhere on multiple devices? There are several approaches to guaranteeing sufficient data privacy, but it all may come down to finding an encryption methodology that avoids the identification of an individual. A term often used in blockchain is “hashing” or “hash” in short. Adding a block to the chain of blocks can be done through this hashing process.[47] A digital fingerprint generated by a particular hash function, commonly known as a "hash," is used to authenticate data in the blockchain and protect its privacy.[48] Essentially, it is a mathematical or cryptographic function where if inputting a certain value, it consistently comes up with the same output value as a result, which is unpredictable, unique, totally randomized and irreversible.[49]

This is one solution offered to encrypt the data by anonymization and therefore not falling within the category of personal data nor the scope of the GDPR. Concealing data by substituting fake identifiers for personally identifiable information is known as pseudonymization, whereas the identifiability of the data subject is irreversibly obscured by anonymization.[50] The data that is personal will not instantly become anonymous only by using a hash algorithm, as a computer

---

[43] European Parliament, *supra* note 32.
[44] *Ibid*.
[45] Michèle Finck, "Blockchains and Data Protection in the European Union," *European Data Protection Law Review* 4, no. 1 (2018): pp. 17-35, accessed April 7, 2024, https://doi.org/10.21552/edpl/2018/1/6.
[46] *Ibid*.
[47] European Parliament, *supra* note 32.
[48] Kulhari, *supra* note 18, p.16.
[49] Felten, "Does Hashing Make Data ‘Anonymous’?" Federal Trade Commission, April 22, 2012, accessed May 6, 2024, https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2012/04/does-hashing-make-data-anonymous.
[50] Tsegaye Ture, "GDPR, Blockchain and the Right to Be Forgotten" (University of Helsinki, 2021), accessed May 9, 2024, http://hdl.handle.net/10138/335279.

can still calculate a hash derived from a social security number and connect it to the social security number of a person.[51] Hashing does not render the data anonymous but rather pseudonymous.[52] Therefore this might not be an efficient or compliant solution for declaring personal data anonymous as hashed data can still qualify as personal data under GDPR.[53]

1.2.4. Off-chain storing

Once data is inserted in the ledger it cannot be changed. Recent technology advancements have led to an architectural solution to the immutability challenge. One possible solution that is suggested is off-chain storage also referred to as 'hashing out', in which the data is externally kept apart from the blockchain. Users' data is kept to a minimum on the blockchain network since only the hash data is kept and available to the owner of the private key, who also controls, processes, and may alter this data.[54] The person or organisation holding the key makes decisions on the management, processing, and alteration of the data.[55] This would ensure not only the data minimization but also the ability to modify and erase the data through an established data controller. Needless to say, it is still impossible to erase the data from the blockchain, but storing personal data on the off-chain would serve as a possible way to achieve compatibility. According to several research, if a deletion request is received, all off-chain data could be deleted, enabling the right to practice the right to erasure.[56] Separating payment information containing personal data and blockchain would therefore serve as a way to mitigate risks regarding privacy concerns. This would also limit the exposure of sensitive information to other participants in the blockchain. Additionally, it would minimize the personal data processed and give control over the personal data as in this way there may be a possibility to alter the data or erase it.

1.2.5. Smart contracts

Any application of blockchain technology may give rise to concerns around consent gathering. Another way to address privacy concerns is smart contracts. Smart contracts are digital agreements that automatically trigger the fulfilment of a contractual obligation, such as payment

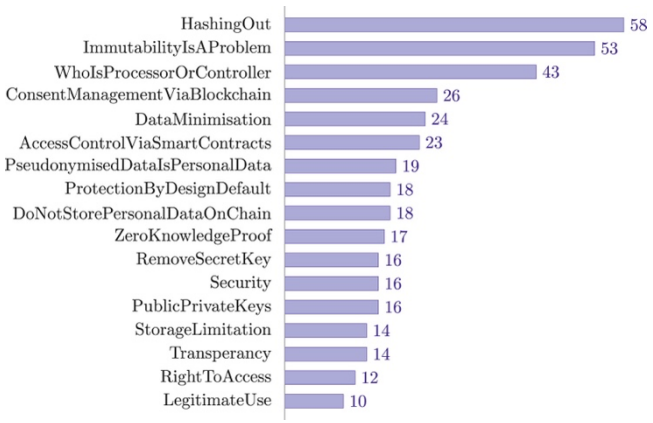
[51] Felten, *supra* note 49.
[52] *Ibid*.
[53] European Parliament, *supra* note 32.
[54] Ruas et al, *supra* note 5.
[55] *Ibid*.
[56] Rahime Belen-Saglam, Enes Altuncu, Yang Lu, and Shujun Li, "A Systematic Literature Review of the Tension between the GDPR and Public Blockchain Systems," *Blockchain: Research and Applications* 4, no. 2 (June 1, 2023): 100129, accessed April 1, 2024, https://doi.org/10.1016/j.bcra.2023.100129.

when a buyer gets the product from a seller.[57] These are software applications used when data is stored in an unchangeable public ledger, often referred to as a secure public ledger with a single source of truth that is not accessible to the public.[58] This would not only enable data protection by design but also would help in determining data controllers. Smart contracts provide a dynamic consent management solution and a way to include people in the use of their personal information.[59] They can be used to get around Article 24 concerning the definition of data dontroller, as a comprehensive contract outlining the respective roles and obligations of users, nodes, and miners must be carried out in drafting the contract.[60] In this way, well drafted smart contracts indeed can guarantee privacy by design, also when consent is incorporated in these contracts. Here a common thread among researchers searching for technical solutions emerges - access control.[61] This need for controlling deletion or alteration requests hints at the potential of smart contracts to navigate this complex issue.[62]

Although understanding the technology and the issues arising from it when it comes to GDPR compliance is overall crucial, each application of the technology has to be evaluated separately when determining compliance. The article "A Systematic Literature Review" provides general statistics on articles discussing GDPR compliance issues and public blockchain in 2023.[63] This offers insight to the main issues under evaluation. The codes that received the most attention (the ones that were used in more than 10 articles) were as follows;

Figure 1.

[57] Kati Suominen, Andrew Chatzky, William Reinsch, and Jonathan Robison, "10 Big Questions (and Myths) Surrounding Blockchain," in *Harnessing Blockchain for American Business and Prosperity*, (Center for Strategic and International Studies (CSIS), 2018), accessed April 6, 2024, https://www.jstor.org/stable/resrep22491.6.
[58] T. J. de Graaf, "From Old to New: From Internet to Smart Contracts and from People to Smart Contracts," *Computer Law & Security Review* 35, no. 5 (October 1, 2019): 105322, accessed February 28, 2024, https://doi.org/10.1016/j.clsr.2019.04.005.
[59] Ruas et al, *supra* note 5.
[60] *Ibid*.
[61] Mateusz Godyn, Michal Kedziora, Yingying Ren, Yongxin Liu, and Houbing Herbert Song, "Analysis of Solutions for a Blockchain Compliance with GDPR," *Scientific Reports* 12, no. 1 (September 2, 2022): 15021, accessed March 5, 2024, https://doi.org/10.1038/s41598-022-19341-y.
[62] *Ibid*.
[63] Belen-Saglam et al., *supra* note 56.



Source; https://www.sciencedirect.com/science/article/pii/S2096720923000040

The research of the article “A Systematic Literature Review” addresses only public blockchain, highlighting the most often discussed subjects in literal evaluations. These categories identify the main issues arising from blockchain technology in contrast to GDPR compliance as a whole and can be used as a guidance.

2. GENERAL DATA PROTECTION REGULATION

In 2017, the Economist reported that data surpassed oil in its value.[64] Data is now the most valuable asset on earth. Most of our data has been moved online and data flows have significantly grown in volume, leading to a growing need for regulation in the area.[65] This is particularly true regarding the power dynamics between large corporations and individuals. BigTech names such as Facebook, Amazon and Google are getting bigger and large volumes of personal data of individuals are exchanged and moved today between different parties on a global scale. These are now the largest companies in the world.[66] Personal data has been commercialized and it has become a valuable resource that is traded between different companies. More and more parties want to access valuable personal data, and personal data in the blockchain is no exception.

2.1. History of data protection and GDPR

The right to privacy and family life is a fundamental freedom embedded in Article 8 of the European Convention on Human Rights (hereinafter - ECHR)[67]. It is protected also by the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereinafter - CETS 108)[68]. In addition, "[e]veryone has the right to the protection of personal data concerning him or her," according to Article 8 of the European Charter of

---

[64] The Economist, "The World's Most Valuable Resource Is No Longer Oil, but Data," *The Economist*, accessed February 4, 2024, https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

[65] The volume of data being produced worldwide is growing rapidly. It is expected to grow from 33 zettabytes, i.e. 10^{21} bytes or one thousand billion gigabytes, in 2018, to 175 zettabytes in 2025. Sofija Voronova, "Understanding EU Data Protection Policy," European Parliament, n.d., accessed May 5, 2024, https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/698898/EPRS_BRI(2022)698898_EN.pdf.

[66] TradingView, "Biggest Companies in the World by Market Cap," accessed April 11, 2024, https://www.tradingview.com/markets/world-stocks/worlds-largest-companies/.

[67] Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14*, 4 November 1950, ETS 5, art. 8, para. 1, accessed January 4, 2024, https://www.echr.coe.int/documents/convention_eng.pdf.

[68] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, opened for signature January 28, 1981, E.T.S. No. 108, 18 I.L.M. 677.

Fundamental Rights (EUCFR).[69] This highlights the importance of safeguarding both the right to privacy and as a separate group - the right to data protection.

Legislation has been in turmoil over the past ten years as new laws have been introduced to address the new problems that technological development has brought forth while struggling to keep up with technological development. The European Union and the Council of Europe (hereinafter - CoE) have been active participants in creating an adequate data protection framework and legal standards in the EU area, starting from the proposal for a comprehensive reform of data protection rules by the European Commission in 2012.[70] In the proposal, the European Commission presented a complete reform of the EU's 1995 data protection rules, more specifically the Data Protection Directive.[71] As a result of this reform and based on the 1995 Data Protection Directive, the General Data Protection Regulation was formed and entered into force in May 2018.[72]

2.2. Application of the GDPR to blockchain

GDPR is a technology-neutral regulation, which means it does not favour any technology in particular and allows rather broad application to many technologies. This leaves room for interpretation of its application regarding blockchain. It is noteworthy that due to the variable technologies used in blockchain as seen above, the analysis of its application and compliance with the GDPR cannot be carried out in a generalized manner.

2.2.1. Scope of the GDPR

GDPR was implemented with the intention of giving people more control over their data and addressing challenges and obstacles brought to the protection of data by new technologies.[73] The GDPR binds all 27 EU Member states, impacting both businesses and individuals as data controllers or data processors handling the data of EU citizens.[74] Article 3 of the GDPR defines the territorial scope to encompass activities of an establishment of a data controller or processor,

---

[69] Charter of Fundamental Rights of the European Union, art. 8, Dec. 18, 2000, 2000 O.J. (C 364) 10 [hereinafter EUCFR]. *See generally* Consolidated Version of The Treaty on European Union art. 6(1), Oct. 26, 2012, 2012 O.J. (C 326) 13 [hereinafter TFEU].
[70] European Commission, "Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses," an official website of the European Union, January 25, 2012, https://ec.europa.eu/commission/presscorner/detail/en/IP_12_46.
[71] "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 Free Movement of Such Data," 281 OJ L § (1995), http://data.europa.eu/eli/dir/1995/46/oj/eng.
[72] GDPR, *Supra* note 3.
[73] Orla Lynskey, "Control over Personal Data in a Digital Age: Google Spain v AEPD and Mario Costeja Gonzalez," *The Modern Law Review* 78, no. 3 (2015): 522-34, accessed February 6, 2024, https://doi.org/10.1111/1468-2230.12126.
[74] Article 3(1), GDPR.

no matter whether the processing of personal data takes place in the EU or not.[75] Therefore, the GDPR also applies to businesses located outside of the EU and processing the personal data of EU citizens thereof. Blockchain is subject to the GDPR to the extent where personal data of EU citizens are processed within the blockchain and legal disputes can be brought up to the Data Protection Authority (DPA) established in each Member State pursuant to Article 51 of the GDPR.[76]

Any action taken on personal data, including collecting, storing, preserving, altering, retrieving, publishing, making accessible, deleting, or destroying, is referred to as data processing.[77] Organisations must take measures to limit the collection and processing of such data as well as shield such information from wrongful use.[78] The processing of personal data can be either manual or automatic.[79] Article 2(1) of GDPR holds that it applies:

> to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.[80]

Blockchain falls within the data processed through automated means, containing personal data in the scope of GDPR.[81] However, the GDPR will not apply to the processing of personal data if the blockchain platform offers end users in the EU a "publicly available electronic communications service".[82] Instead, the e-Privacy Directive's special regime will apply.[83]

According to some, the GDPR is a risk-based law that aims to assess risks and implement mitigating measures through the processor and controller of data.[84] The Safe Harbour Decision and the Data Privacy Shield were both independently overturned by the European Court of Justice (ECJ) in the *Schrems* cases.[85] The conclusion was that they did not

---

[75] *Ibid*.
[76] GDPR, Article 51.
[77] GDPR, Article 4(2).
[78] According to a number of GDPR article 4 principles, including data minimization, purpose limitation, storage limitation, and integrity and confidentiality principles.
[79] GDPR, Article 4(2).
[80] GDPR, Article 2(1).
[81] European Parliament, *supra* note 32.
[82] Bacon et al., *supra* note 31.
[83] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector ('ePrivacy Directive').
[84] Giovanni De Gregorio and Pietro Dunn, "The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age," SSRN Scholarly Paper, Rochester, NY, March 31, 2022, p. 4, accessed May 1, 2024, https://doi.org/10.2139/ssrn.4071437.
[85] Case C-362/14, Maximillian Schrems v. Data Protection Commissioner (Schrems I), ECLI:EU:C:2015:650; and Case C-311/18, Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II), ECLI:EU:C:2020:559.

fully adhere to the GDPR's principles and provide enough protection for European citizens against the risks associated with having their data transferred to the United States.[86]

The two most evident risks that must be assessed from the perspective of the GDPR and immutability are the reversibility risk and the linkability risk. The term "reversibility risk" refers to the requirement that the method used should so effective that it is not only impossible to identify a specific person, but also that the procedure cannot be undone.[87] The inability to link encrypted data to that particular person or to other pieces of information is known as the linkability risk.[88] The risk does not disappear even when financial services are provided through distributed ledgers such as in blockchain.[89] Assessing these risks are in the centre of determining blockchain compliance with the GDPR.

2.2.2. Personal data within the blockchain

Personal data in the blockchain may be identified in variable different forms, which might make it difficult to determine whether the GDPR applies. Firstly, all personal data of individuals is subject to the GDPR, as any information of an identified or identifiable natural person, or "data subject," is considered personal data under the GDPR.[90] The “data subjects”, in this context, are the participants in the blockchain transaction. Shared data can be not only text but also files such as pictures, documents and music as an example.[91] All information where the data subject is directly identifiable is considered personally identifiable information (hereinafter - PII), which is often used by companies to identify the customer.[92] PII can be described as “any subset of attribute values of an individual person which sufficiently identifies this individual person within any set of persons”.[93] Article 4 defines personal data as any information relating to an identified or identifiable natural person, such as name, identification number, geographical information that leads to an address, a photo, or any other online identifier unique to that natural person's physical, physiological, genetic, mental, economic, cultural, or social attributes, qualifying as PII.[94] The CJEU confirmed in the *Breyer* case that

---

[86] Gregorio and Dunn, *supra* note 84, p.19.
[87] European Data Protection Board, "Secure Personal Data | European Data Protection Board," accessed April 30, 2024, https://www.edpb.europa.eu/sme-data-protection-guide/secure-personal-data_en.
[88] *Ibid.*
[89] Zetzsche, Dirk A., Ross P. Buckley, and Douglas W. Arner, "The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain," SSRN Scholarly Paper, Rochester, NY, August 13, 2017, accessed May 3, 2024, https://doi.org/10.2139/ssrn.3018214.
[90] GDPR Art. 4.1.
[91] Finck, *supra* note 45.
[92] Md Mehedi Hassan Onik, Chul-Soo Kim, Nam-Yong Lee, and Jinhong Yang, "Privacy-Aware Blockchain for Personal Data Sharing and Tracking," *Open Computer Science* 9 (April 15, 2019): pp. 80-91, accessed March 6, 2024, https://doi.org/10.1515/comp-2019-0005.
[93] *Ibid*.
[94] European Parliament, *supra* note 32.

even an IP address can qualify as PII.[95] Mishandling personal data may lead to a breach of the right to privacy, as a person can be identified from a transaction.

2.2.3. Pseudonymized and anonymized data

Potentially personally identifiable information (PPII) or indirect identifiers (quasi-identifiers) can be used to generate PII.[96] According to Article 4(5), pseudonymization makes it impossible to link a specific piece of personal information with a specific data subject unless it is linked to certain additional information that may be used to identify that data subject.[97] Previously mentioned hashing methodology in blockchain usually constitutes as such. The CJEU held in Case C-582/14 – *Patrick Breyer v Bundesrepublik Deutschland*, that the possibility of identifying seemed insignificant if the data subject's identity was legally forbidden or nearly difficult to establish in cases where it requires a disproportionate amount of resources (time, money, and labour).[98]

It is possible that personal information is not necessarily directly connected to a certain person. GDPR does not apply to anonymous data, but pseudonymised data still falls within the scope of the GDPR.[99] Therefore this is one of the complex issues regarding GDPR compliance, as anonymisation or pseudonymisation is largely a technical question as discussed in the earlier chapter. Pseudonymization replaces the identity of the data subject in a way that necessitates additional information to be able to identify them again, whereas anonymization permanently removes any means of identifying the data subject.[100] The definitions in the categories are not clear - The Working Party 29's Opinion 2014/05 (WP216) previously defined pseudonymization under GDPR, but the EDPB has not formally adopted this, making it unclear whether hashed information is considered pseudonymous or anonymous.[101] The consensus however seems to be that such information would be pseudonymous.

2.2.4. Specific types of personal data in the blockchain

When it comes to blockchain, two types of personal data can be established – miners' and participants' identifiers, and additional data in the blockchain, also referred to as

---

[95] Case C-582/14, Patrick Breyer v. Bundesrepublik Deutschland, 2016 EUR-Lex CELEX 62014CJ0582, ¶ 16 (Oct. 19, 2016)
[96] Finck, *supra* note 45.
[97] GDPR, Article 4(5).
[98] Jiménez-Gómez, *supra* note 16.
[99] GDPR Recital 26.
[100] Ture, *supra* note 50.
[101] Silvan Jongerius, "Right to Be Forgotten under GDPR in Blockchain - Blog," TechGDPR (blog), August 13, 2019, accessed May 5, 2024, https://techgdpr.com/blog/gdpr-right-to-be-forgotten-blockchain/.

'payload'.[102] Identifiers for each participant are needed for the blockchain to function correctly and they essentially comprise a string of seemingly random alphanumeric characters that serve as the participant's account public key, which is connected to a private key only known to the participant.[103] Public keys are connected to private individuals, which might lead to possible identification, especially when combined with other data. Recital 30 GDPR defines public keys as a kind of identifiers.[104] The issue with public keys is that, if they are related to an individual, it may be possible to identify a natural person through the public key. Data in the public key may not count as personal data by itself, but combined with other information it comprises as such, hence being pseudonymous data according to Article 3(5) GDPR.[105] Additionally, according to the study carried out by the European Parliament, some of the hash data qualifies as personal data under the GDPR, as a person may be identified or identifiable in the same way when combining information. [106]

In transactions, any additional information contained in a transaction, or "payload" in the blockchain, that can be related to natural persons also other than the participants and where they may be directly or indirectly identifiable, is referred to as personal data.[107] This is additional data that can be stored in the blockchain during the transaction, depending on the technology. Names, addresses, and dates of birth are examples of this type of data.[108] Transactional data can be identified as additional data - the term "transactional data" is used to describe additional types of data that are not public keys but may be utilised on blockchains.[109] However, here it an be established that it is not always the case that transactional data amounts to personal data, as it depends on whether or not it can be used alone or combined with other data to identify a person.[110] Here it can be seen that proper data accounting, hence minimization of personal data is essential to protect the data even within the blockchain. Especially in the context of financial transactions based on cryptocurrencies where the other party to the transaction is often a natural person.

2.2.5. Data controller and processor

[102] CNIL, *supra* note 23.
[103] *Ibid*.
[104] European Parliament, *supra* note 32.
[105] *Ibid*.
[106] *Ibid*.
[107] CNIL, *supra* note 23.
[108] *Ibid*.
[109] European Parliament, *supra* note 32.
[110] Article 4(5), GDPR.

One may wonder if the lack of central authority on the blockchain diminishes the value of the right to be forgotten because no single large corporation is in possession of this personal data. As seen in the Cambridge Analytica case, the importance of the right to be forgotten is indeed highlighted when large corporations collect significant amounts of data and use it unethically.[111] Despite that, there can be cases where the information within the blockchain might be harmful to an individual such as in the example in the previous situation where someone shares inappropriate photos of another person to a blockchain. In such cases, the importance of the right remains and even enhances the importance. After the Cambridge Analytica scandal, it can be seen that storing vast amounts of personal data can be dangerous from a privacy perspective when data is handled by some companies in a centralized manner.[112] By piecing together small data fragments, centralized systems can create a detailed profile of an individual. The decentralized characteristic of blockchain allows the safety of the data by storing it in multiple locations, making it more difficult or impossible for entities to gather information in a way that would give them a comprehensive representation of a person. However, this very advantage presents a challenge for the "right to be forgotten" within blockchain ecosystems.

Given that the GDPR is based on a centralised data management system, it does not address the decentralisation and immutability that are unique to blockchain technology. GDPR establishes the roles of “data controller” and “data processor”.[113] This is important from the immutability perspective, as determining the controller or processor essentially determines who can erase the data. Perhaps the most important consequence of defining a data controller is that it allows one to determine accountability responsibility for taking possible action regarding the data, such as modifying or erasing it. As for the erasure of the data, it would need to be established where the data is stored in order to determine who would have access as well as the right and responsibility to perform any action on the data. As was stated in the previous chapter of this paper, the data is stored on several devices, or "nodes," that are linked to the blockchain network.

In the absence of central authority, it raises the question of who owns and has the ability to control the data. The “data controller” is defined in Article 4(7):

---

[111] Supra note 95.

[112] The New York Times, "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far - The New York Times," accessed April 22, 2024, https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

[113] GDPR, Article 4.

> "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 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".[114]

When centralised authority is lacking, this becomes troublesome. A similar issue can arises from the definition of "data processor": "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".[115]

Who controls or processes the data and falls under the term "data processor" if any, and who is the owner of the data and who bears responsibility for the data are the main questions in this case. A data controller is necessary for a data processor to exist, as it is the data processor that handles data for the controller.[116] Both definitions in the GDPR specify that in addition to legal entities or other parties, an individual as a natural person may also bear the responsibility of being a controller, but at the same time does not address situations in the absence of such.[117] Taking this into account, it holds that the participant, and therefore the data controller, can be either a natural person in cases where the data processing is not strictly personal, or a legal entity that registers personal data in a blockchain. This is relevant in determining the party responsible for the data for erasure purposes.

Guidance on this matter was released in 2018 by the French Data Protection Authority (CNIL) in a report about the blockchain in relation to personal data.[118] The report aims to offer solutions for processing personal data within the blockchain, addressing its compatibility with the GDPR. In its analysis, CNIL points out that the GDPR was created during a period when certain entities had centralised control over data.[119] Participants who choose to transmit data for validation by the miners and who have the authority to write on the chain are defined as data controllers by CNIL, as blockchain participants provide the means (data format, blockchain technology utilisation, etc.) and purposes (objectives sought by the processing) of the processing.[120] As an example, a bank is a data controller if, as part of its client management procedures, it uploads the data of its clients onto a blockchain.[121] Developers of smart contracts

[114] Article 4(7), GDPR.
[115] Article 4(8), GDPR.
[116] *Ibid*.
[117] GDPR, Article 4.
[118] CNIL, *supra* note 23.
[119] *Ibid*.
[120] *Ibid*.
[121] *Ibid*.

handling personal data on behalf of data controllers, and in some cases, miners validating the transaction, may function as data processors.[122]

According to certain publications, every node functions as a joint controller, which implies that they all can be held accountable.[123] Joint responsibility can be distributed differently according to the situation in question, either to one individual legal person, to groups or all legal persons, or collective group as one legal entity.[124] More specifically this would fall under the joint controllership under Article 26 of GDPR. However, academics agree that determining the responsible persons as well as clear responsibilities is not all that simple, leading to a failure in this mechanism.[125] Additionally holding large groups accountable may complicate the matter and create another issue.

When it comes to decentralized, open and permissionless cryptocurrency platforms, distinguishing data controllers is a complex matter. At the macro level, the platform's overarching goal is to enable a peer-to-peer electronic currency system.[126] Platform developers do not fit the criteria of a data controller, as they often are not handling any personal data themselves; instead, they just grant others access to the system.[127] Yet, especially when talking about public blockchain where information is accessible to everyone it could be argued that the individual was aware of the risks when agreeing to use such a technology to begin with. On a micro-level, by choosing to do their transaction using cryptocurrency for example, the individuals arguably choose the means of processing.[128] Nevertheless, the Bitcoin user who initiated the transaction cannot be deemed the controller, as this would lead to an insufficient fulfilment of the execution of their rights.[129]

2.3. Principles of GDPR

Within the material scope, the problem is that the definition of personal data may not be completely clear. The data subject needs to be identifiable from the data stored in the blockchain for the data to be qualified as personal data as seen above.[130] In cases where personal data is involved in the blockchain transaction, the GDPR general principles apply, which brings us to

---

[122] *Ibid*.
[123] Belen-Saglam et al., *supra* note 56, p. 9.
[124] Thomas Buocz, Tina Ehrke-Rabel, Elisabeth Hödl, and Iris Eisenberger, "Bitcoin and the GDPR: Allocating Responsibility in Distributed Networks," *Computer Law & Security Review* 35, no. 2 (April 1, 2019): 182-198, accessed April 7, 2024, https://doi.org/10.1016/j.clsr.2018.12.003.
[125] *Ibid*, p. 44.
[126] Bacon et al., *supra* note 31.
[127] *Ibid.*
[128] *Ibid*
[129] Buocz et al., *supra* note 124.
[130] Supra note 74.

the application of these principles concerning blockchain in connection with the principle of the right to be forgotten.

Multiple principles can be distinguished relating to blockchain and the GDPR – The implementation of Data Protection by Design and by Default principles (Article 25), the principles for Lawfulness of Processing (Article 6), data storage and minimization (Article 5(1)(c)), and the rights of data subjects (such as the Right to Access (Article 15), the Right to Rectification (Article 16), the Right to Erasure ('Right to be Forgotten') (Article 17), the Right to File a Complaint with a Supervisory Authority (Article 77), the Right to Compensation and Liability (Article 82), and the Transfers of Personal Data to Third Countries (Article 44-50) are among the challenges identified by the GDPR.[131]

However, this is not to say that blockchain would be totally at odds with the regulations; rather, one benefit of adopting blockchain is the data's availability (Article 32) and integrity (Article 5). Because blockchains are used in a decentralized manner, they are not only secure against failure but also ensure that neither party has exclusive control over the managed data, thus guaranteeing availability.[132] Blockchains are immutable and protected data storage, in which case data integrity is guaranteed.

2.3.1. Lawful basis for data collection

It is unclear at first glance who could collect consent in blockchain. A legitimate legal basis must exist in order to process personal data, as per the principle of lawfulness of processing defined in Article 6 of the GDPR.[133] More often than not, consent is needed to collect personal data on the data subjects.[134] It is difficult to identify the person or people acting as the data controller (or processors) in charge of getting consent due to the decentralized nature of blockchain. There are two aspects of blockchain to be differentiated in considering the legal basis - whereas permissioned blockchains could depend on the fulfilment of a contract, permissionless blockchains may depend on user agreement.[135]

The right to withdraw consent is granted to the data subject under Article 7, and if the processing is based on consent, this right would oblige the controller to take reasonable steps

---

[131] Ruas et al. *supra* note 5.
[132] Christoph Stach, Clémentine Gritti, Dennis Przytarski, and Bernhard Mitschang, "Assessment and Treatment of Privacy Issues in Blockchain Systems," *ACM SIGAPP Applied Computing Review* 22, no. 3 (November 3, 2022): 5-24, accessed April 3, 2024, https://doi.org/10.1145/3570733.3570734.
[133] GDPR, Article 6.
[134] Belen-Saglam et al., *supra* note 56, p. 4.
[135] International Association of Privacy Professionals, "Blockchain and the GDPR: Addressing the Compliance Challenge," December 14, 2018, https://iapp.org/news/a/blockchain-and-the-gdpr-addressing-the-compliance-challenge/.

to erase the data in the absence of another lawful basis.[136] To comply with the GDPR, controllers and processors are required to fulfil specific responsibilities and obligations pertaining to the rights of these data subjects. Consent, however, is only one of the legal basis. In this context, the controller's or a third party's legitimate interest could constitute a legal basis for processing personal data, according to Article 6(1)(f).[137] Insights provided to the interpretation of legitimate interest from the service provider perspective can be established from the *Bryer* case.[138] As per the ruling, it is permissible for a service provider to gather and handle personal data without the consent of the data subject provided that data collection and processing is required to enable the data subject to utilise those services.[139] Yet, the interests of the fundamental rights and freedoms of the data subject prevail, such as held by the CJEU in the *Google Spain* case, where the rights arising from Article 7 and Article 8 of the Charter were emphasized.[140] Additionally, it was declared by the court that the mere economic interest of the operator does not constitute a proper legitimate interest alone. If the removal of the information affects the legitimate interests of other users such as the interests of having access to that information, the balance between those interests of data subjects should be evaluated depending on the case.[141] When thinking from the perspective of blockchain, a data subject may wish to have their personal information deleted from the blockchain. Such removal means that the whole chain and the information within get removed along with it, which might impact the rights of other data subjects as participants in the blockchain.

Using blockchain itself serves as a platform for different kinds of data transfers, such as transactions of crypto assets. It could be argued that it counts as a legitimate interest as without the underlying consent of the data subject to set up a crypto wallet, they agree to the use of blockchain. In this sense, even without the consent of the data subject, it could be established that essentially the data subject understands that by establishing a crypto wallet they agree to use blockchain technology, as blockchain is the most used technology behind cryptocurrencies and one can not buy or sell cryptocurrencies without using the technology. This aligns with the requirement to enable the utilisation of the services to the data subject.

---

[136] GDPR, Article 7.
[137] GDPR, Article 6(1).

[138] *Bryer*, supra note
[139] Shraddha Kulhari, "Fitting the Blockchain Solution into the GDPR Puzzle," in *Building-Blocks of a Data Protection Revolution*, 1st ed., *The Uneasy Case for Blockchain Technology to Secure Privacy and Identity* (Nomos Verlagsgesellschaft mbH, 2018), 38-52, accessed May 8, 2024, https://www.jstor.org/stable/j.ctv941qz6.8.
[140] Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González Grand Chamber [2014] C- 131/12.
[141] *Ibid*, para 81.

2.3.2. Right to be forgotten

Perhaps the most controversial principle of GDPR when it comes to blockchain is 'the right to erasure' or 'the right to be forgotten'. The data cannot be removed. To understand and evaluate the right to be forgotten, the aforementioned terms such as personal data, legitimate basis and establishing the data controller and processor are relevant. First, let us consider a situation where an individual would want Facebook to delete all their data. All they would have to do is submit an implicit request for them to remove their data and Facebook would have to do so within 30 days. Very broadly said, the right to be forgotten is the right of an individual to have all their data erased, with some limitations and exceptions. In this case, their personal data, hence all the data they can be identified from should be erased as there might not be a legitimate basis any longer and the data controller, Facebook, would have to oblige.

Article 17 of the GDPR gives data subjects the right, under certain conditions, to have their personal data erased.[142] The Court of Justice of The European Union (hereinafter - CJEU) first defined the right to be forgotten as a fundamental right in the 2014 case of *Google Spain v AEPD and Mario Costeja González*.[143] This right was later implemented in Article 17 of the General Data Protection Regulation, which holds that;

> "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay…".[144]

The right to be erased only applies to data that is already in existence at the time the request is submitted; it does not extend to data that could be produced in the future.[145] The word "erasure" is not further defined under the GDPR. Nonetheless, the Court of Justice of the European Union (CJEU) has held in the *Nowak* case that the destruction of personal data is equivalent to erasure.[146] The French Data Protection Authority defines potential applications, such as offering the ability to remove all information about an individual; including a mechanism for processors to be automatically notified when data pertaining to that individual is deleted; and making sure backups have data erasure enabled, or offer a different option that does not recover deleted information about that individual.[147]

---

[142] GDPR, Article 17.
[143] Google Spain, *supra* note 140.
[144] GDPR, Article 17.
[145] Information Commissioner's Office (ICO), "Right to Erasure," ICO, August 4, 2023, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-erasure/.
[146] Case C-434/16 *Peter Nowak v Data Protection Commissioner* [2017] EU:C:2017:994, para 55.
[147] The French Data Protection Authority (CNIL), "Sheet N°13: Prepare for the Exercise of People's Rights," accessed May 2, 2024, https://www.cnil.fr/en/sheet-ndeg13-prepare-exercise-peoples-rights.

In practice, an individual would be entitled to request the company that is processing their data to delete their data from their databases completely without undue delay, which is considered to be one month.[148] The previous applies where one of the following grounds is fulfilled as per Article 17 of GDPR:

> "a) the personal data ara no longer necessary in relation to the purposes for which it was collected or otherwise processed;
> b) the data subject withdraws her consent or objects to the processing of personal data; or
> c) the processing does not comply with the data protection framework."[149]

It can be established that the right to erasure is encompassed within the right to be forgotten. The right to bring any concerns resulting from the violation of data protection duties before the supervisory body set up in each Member State is another aspect of the right to be forgotten.[150] Consequently, the right to be forgotten encompasses various rights for the individual regarding the complete protection of their data online as well as obligations for data controllers, such as the duty to notify controllers handling the personal data that the data subject has asked for the erasure by such controllers of any links to, copies of, or replications of those personal data following their public disclosure.[151]

The data controllers have other principles to comply with and erase the data even when not requested by the data subject. Article 6(1) of the GDPR states that information shall be deleted when it is no longer needed for the reasons for which it was collected.[152] It could be argued however, that the data in the blockchain, serves as a record of the transactions done in the past, and it might be relevant to identify the parties involved in the transactions even after the transaction has served its purpose. According to the storage limitation principle, personal data cannot be held for an indefinite period of time as time limits should be established either for erasure or review of the data.[153] It is established that the data is necessary for the blockchain to function successfully and that it has to exist permanently as there is no blockchain without the data.[154] This is problematic when it comes to blockchain, as there might be no authority making a systematic review to determine whether the data is still needed after it has been stored

---

[148] GDPR.eu, "Everything You Need to Know about the 'Right to Be Forgotten,'" November 5, 2018, https://gdpr.eu/right-to-be-forgotten/.
[149] Kulhari, *Supra* note 139.
[150] GDPR, Article 77.
[151] GDPR, Article 77(2).
[152] GDPR, Article 6(1).
[153] European Commission, "For How Long Can Data Be Kept and Is It Necessary to Update It? - European Commission," accessed April 15, 2024, https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/how-long-can-data-be-kept-and-it-necessary-update-it_en.
[154] Godyn et al., *supra* note 61.

in the blockchain, and even if there is, the information cannot be erased. As a result, the CNIL believes that this data cannot be further minimized and that its retention lengths are essentially equal to the lifespan of the blockchain.[155]

Within the right to be forgotten, what it means to be forgotten in connection to blockchain is that the data that can lead to an identification of a person is erased. However, without erasing the entire chain, this is technically either extremely difficult or impossible, endangering the integrity of the data. Consequently, due to the immutable nature of blockchain, the right to be forgotten poses a unique challenge. When it comes to public blockchain, the right to be forgotten in cross-border transfers of personal data is especially problematic since the data is saved on every node that contains the entire dataset, regardless of where the node is physically situated or even unknown.[156] It is challenging for the person to find out who to contact in the first place and where the data is specifically kept. From a GDPR standpoint, there is always a data controller who undertakes the obligations under the regulation, to whom the data subject can turn to enforce their right. However, this does not apply to the blockchain as it is decentralized and lacks an administrator or authority undertaking these obligations, meaning in most cases it is extremely difficult to identify the controller or where the data is being processed. The problem lies in the fact that in the unlikely event of being able to locate the potential controller, the controller won't be able to erase the data without wiping the blockchain as a whole.[157] This would be rather impractical and unreliable, hence unsafe, as there are multiple users involved in the chain. Wiping one person's data would remove all of the other data even if those participants wanted to keep their data in the blockchain.[158]

As seen by the limitations embodied in paragraph 3 of Article 17 of the GDPR (the right to erasure), the right to privacy is not absolute.[159] There are exceptions, and the right to be forgotten may not be applied in situations where data can be processed based on other grounds, hence there is a legitimate purpose for data processing. A corporation may have a commercial objective for data processing. There are other grounds as well, including preferences, on which processing of the data can be continued in the event of a need for the data to file a lawsuit or defend against one or other public interests or legal obligations placed on the controller.[160]

---

[155] CNIL, *supra* note 23.
[156] Belen-Saglam et al., *supra* note 56.
[157] Godyn et al., *supra* note 61.
[158] *Ibid*.
[159] GDPR Article 17, para. 3.
[160] GDPR Article 17, para. 3(e).

Hence, in the case such as above where an individual would like their personal data erased, it is not guaranteed that all of their data is removed as these kinds of exceptions may apply.

2.3.3. Data Protection by Design

If something goes on the blockchain such as an inappropriate picture of a person – the data, such as a picture on the blockchain cannot be taken out of the blockchain. How can the data be prevented from going on the blockchain in the first place? One preventative aspect of the data protection regime is the 'data protection by design' or 'Privacy by Design'. It is embedded in Article 25 of the GDPR on Data Protection by Design and by Default.[161] It obliges the data controller and processor to implement appropriate technical and organisational measures such as pseudonymisation to safeguard the data and evaluate the necessity of processing personal data for each purpose, ensuring data minimisation. In such a case of an inappropriate picture, it would then be evaluated if such information is needed for the data processing.

Two opposing arguments can be made when considering this principle - Blockchain technology is in its nature protecting the personal data of the users. However, the design or technology is also what makes the blockchain incompliant with the GDPR as it does not provide the possibility for data modification, rectification, or erasure. The CNIL addresses this concept by recommending that the data controller consider whether selecting this technology to carry out its processing is appropriate in the first place before moving further.[162] This means that the data controller should seek other ways to reach the desired outcome without involving blockchain and the processing of personal data therein. This would mean a data controller would need to be established prior to the processing of data, which might compose another issue.

One suggested approach to provide privacy features in the blockchain is to use smart contracts to ensure that privacy is reached starting from the beginning. Instead of the actual data, a smart contract would just contain the hash to that data, or ask consent from the user to make them more involved in the storing of their data.[163]

2.3.4. Data transfers outside the EU

The data in the blockchain is stored in multiple nodes, spreading the data globally across computers all around the world. However, not every country has the appropriate safety measures in place for safeguarding data. Thus a question relates to the application of European

[161] Article 25, GDPR.
[162] CNIL, *supra* note 23.
[163] Finck, *supra* note 45.

data protection requirements to the transfer of data to third countries.[164] As seen in the *Schrems* case, without any objective justification to access the data based on specific considerations of national security or crime prevention, the privacy of the individual may not be guaranteed in the third country.[165] Without those surveillance practices being accompanied by appropriate safeguards against abuse of power, the right to privacy would be rendered meaningless.[166] It is quite likely that there will be cross-border transactions outside of the EU, particularly on public blockchain where anyone can join the network. Public blockchains operate globally, with data scattered across numerous computers worldwide, where enforcing GDPR's data protection requirements within such a decentralized system proves highly challenging.[167] The authors concur that questions about jurisdiction and enforcement in such cases will inevitably come up and that it may be appropriate to handle each case individually.[168]

2.4. Markets in Crypto-Assets Regulation (MICA) and GDPR

In financial markets, law enforcement's interest is to be informed of crimes and acts of terrorism before they happen, clashing with the right to privacy.[169] Authorities may need to enquire for information about financial transactions to battle illegal activity, including money laundering. Normally, the balancing of these rights is done through a financial intermediary.[170] Law enforcement depends on the blockchain's traceability and transparency in decentralised financial and cryptocurrency marketplaces to ensure legality.[171]

A brief discussion on blockchain technology-based cryptocurrency is essential after the introduction of the new regulation in the area considering blockchain transactions. The unified EU-level regulatory framework for the financial industry of crypto-assets was established by the introduction of the Regulation on Crypto-assets Markets (MICA), which was accepted by the Council of the European Union (EU) and entered into force in June 2023.[172] The Markets

---

[164] *Ibid*.
[165] Council of Europe, European Court of Human Rights, European Data Protection Supervisor, and European Union Agency for Fundamental Rights (EU body or agency), *Handbook on European Data Protection Law: 2018 Edition* (Luxembourg:Publications Office of the European Union, 2018), accessed May 8, 2024, https://data.europa.eu/doi/10.2811/343461.
[166] *Ibid.*
[167] Jean-Pie Gauci-Maistre, Despoina Xynou, and Daniela Gaffarena, "Blockchain Technology vs. GDPR: Conflict Resolution Required," Lexology, January 29, 2019, accessed March 5, 2024,https://www.lexology.com/library/detail.aspx?g=3b1e8b19-61bd-4e7c-a22a-314e11b1a769.
[168] *Ibid.*
[169] Azgad-Tromer et al., *supra* note 7.
[170] *Ibid*.
[171] *Ibid*.
[172] European Securities and Markets Authority, “Markets in Crypto-Assets Regulation (MiCA),” accessed April 16, 2024, https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica.

in Crypto-Assets regulation mostly oversees the regulation of blockchain, particularly concerning crypto-assets.[173] MICA intervenes to govern those sectors that are not covered by current financial legislation, as there was a lack of sufficient regulation in the area after the introduction of cryptocurrencies.[174] That said, there is a good likelihood that when MICA is implemented, any cryptocurrency or cryptocurrency player that is currently unregulated will become such under MICA.[175] After the implementation phase, organisations that are currently offering crypto-asset services are scheduled to begin the MICA application in December 2024, and the transitional phase will come to an end in July 2026.[176]

Financial markets are subject to regulatory oversight, and this principle now extends to the realm of Financial Technology such as blockchain as well. MICA provides a unified set of rules applicable to blockchain and crypto-assets, providing certainty, especially to the financial application of blockchain as MICA intends to reduce the risks involved in digital finance development while promoting its growth.[177] Before MICA, the blockchain and crypto-asset market regulations were mainly based on the national legislation of each EU Member State, only partially regulated by the broader scope of the EU rules applicable to digital and financial services, such as the GDPR, Anti-money laundering framework and others.

MICA directly addresses the importance of enabling the use of innovative technologies and directly addresses Distributed Ledger Technology (DLT) that is centralized, including blockchain in its wording.[178] This indicates that the rule covers both blockchain and DLT-based cryptocurrencies in their application since it acknowledges that crypto-asset technology is derived from both of those technologies. MICA defines crypto assets as "a digital representation of a value or of a right that is able to be transferred and stored electronically using distributed ledger technology or similar technology".[179] It applies to crypto asset service providers offering and marketing crypto assets to the public in the EU but leaves out person-to-person transfers.[180] It also excludes financial instruments and decentralized DLTs from its scope and, to some

---

[173] "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 (Text with EEA Relevance)," 150 OJ L § (2023), http://data.europa.eu/eli/reg/2023/1114/oj/eng.
[174] European Securities and Markets Authority, *supra* note 172.
[175] Tomasz Tomczak, "Crypto-Assets and Crypto-Assets' Subcategories under MiCA Regulation," *Capital Markets Law Journal* 17, no. 3 (July 1, 2022): 365–82, accessed May 5, 2024, https://doi.org/10.1093/cmlj/kmac008.
[176] European Securities and Markets Authority, *supra* note 172.
[177] Latvijas Banka, "MiCA Regulation - Fintech Latvia," March 31, 2022, accessed May 5, 2024, https://fintechlatvia.eu/crypto-asset/mica-regulation/.
[178] MICA, *supra* note 173.
[179] MICA, Article 3(1)(5).
[180] MICA, *supra* note 173.

extent, electronic money, as decentralised finance (DeFi) and non-fungible tokens (NFT) are out of its scope.[181]

MICA regulation also interacts with the GDPR. It does not address the compatibility issues with GDPR, but it is stated that all crypto-asset services processing personal data shall do it in accordance with the GDPR.[182] Accordingly, all entities covered by MICA are required to make sure that their operations are carried out in a way that complies with GDPR, protecting personal information while undergoing regulatory reviews. Consequently, as MICA requires entities to comply with the GDPR, it encompasses the right to be forgotten and all the obligations set upon to data controllers in crypto-asset transactions. MICA also sets the same requirements for the competent authorities, in its Article 101 MICA holds that:

> With regard to the processing of personal data within the scope of this Regulation, competent authorities shall carry out their tasks for the purposes of this Regulation in accordance with Regulation (EU) 2016/679.[183]

Additionally, it holds that no personal data should be disclosed when publishing information.[184] In addition, MICA mandates that service providers guarantee that third parties engaged in outsourcing adhere to the requirements specified in the applicable data protection legislation, which would be the case if the third parties were based in the Union.[185] Falling under MICA, cross-border data transfers involving crypto assets within the EU must also adhere to the GDPR.

Alongside voting for the MICA Regulation, the EU Parliament approved the Travel Rule for crypto assets for Virtual Asset Service Providers (VASPs).[186] The new Regulation on the Traceability of Transfers of Funds (TFR) ensures the traceability of crypto-assets transfers and the authentication of users, aligning with FATF standards.[187] It will apply as of December 2024.[188] The Travel Rule requires service providers in the EU to always know who the crypto asset wallets belong to, enhancing the traceability of transfers and helping to tackle money laundering.[189] Similarly to MICA, the travel rule also obliges the entities handling personal data

---

[181] Clifford Chance, "Crypto Regulation: The Introduction of Mica into the Eu Regulatory Landscape," available on: https://www.cliffordchance.com/briefings/2022/12/crypto-regulation--an-introduction-of-mica-into-the-eu-regulator.html.
[182] MICA, Recital 117.
[183] MICA, Article 101.
[184] MICA, Article 95.
[185] MICA, Article 66(1)(g).
[186] European Parliament, "Crypto-Assets: Green Light to New Rules for Tracing Transfers in the EU," April 20, 2023, accessed May 10, 2024, https://www.europarl.europa.eu/news/en/press-room/20230414IPR80133/crypto-assets-green-light-to-new-rules-for-tracing-transfers-in-the-eu.
[187] "Regulation (EU) 2023/ 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," n.d.
[188] CNIL, *supra* note 23.
[189] European Parliament, *supra* note 186.

to comply with the GDPR.[190] Since personal information is stored under the travel rule, this is noteworthy from the perspective of the right to be forgotten.

The Travel Rule is a non-technological solution to the issue, as there is no need to care about the ability to get rid of the chain when knowing who is responsible. To guarantee that personal data involved in crypto-asset transactions is sufficiently secured, MICA interacts with GDPR, while MICA primarily oversees the financial elements of blockchain and distributed ledger technology. This creates certainty in the market and encourages innovation in the financial sector in this way.[191]

While MICA interacts with the GDPR, the immutability is not considered. Essentially defining a controller might be easier in crypto asset transactions, but while technology develops, there should be a legitimate solution for this in the next MICA Regulation to address situations where the central authority is absent. Additionally, as considered in the TFR regulation, guidelines for transfers of personal data to third countries should be drafted by the EDPB together with EBA to address situations where personal data obligations set by GDPR are not met, hence determining whether the transfer of crypto assets should be executed, rejected or suspended in such cases.[192]

The preamble of MICA can show the legislative intent of the legislation. MICA should not apply to situations in which crypto-asset services are offered in a fully decentralised manner, without any intermediary.[193] This provides clarity from the perspective of the right to be forgotten. In cases where there is a centralised authority or at least an intermediary, responsibility can be distributed and it is more likely that the services are provided in a more GDPR-compliant manner. ESMA register covers crypto-asset white papers for crypto-assets other than asset-referenced tokens and e-money tokens; issuers of asset-referenced tokens; issuers of e-money tokens; and crypto-asset service providers.[194] It is considerably simpler to hold such entities accountable in situations of fraud and deception. A single centralized institution providing the previously mentioned services can be held responsible for any shortcomings and it serves as an incentive for them to comply with regulations. However, this

---

[190] The Financial Action Task Force (FATF), "Targeted Update on Implementation of FATF's Standards on VAs and VASPs," accessed May 2, 2024, https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023.html.
[191] Evren Hakim, "The Legal Status of Cryptocurrency within the European Union: An Analysis of the MICA Regulation" (2024), available on: https://doi.org/10.13140/RG.2.2.23260.36482.
[192] "Regulation (EU) 2023/ 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," n.d.
[193] MICA, Para 22.
[194] MICA, Article 109.

leaves a gap in the legislation regarding fully decentralized platforms. Particularly in terms of data security, these appear to be mostly unregulated.

A discussion can be had about comparing blockchain to the dark web. The dark web contains all sorts of information and is harnessed for criminal and malicious activities.[195] Such information in the dark web cannot be controlled and includes drug trafficking, distribution of illegal weapons, child pornography and stolen goods.[196] All of this information is hidden and accessible for individuals only through anonymised Tor software. Similarly to the blockchain network, Tor relies upon a network of volunteer computers to route users' web traffic through a series of other users' computers, which prevents the traffic from being linked back to the original user.[197] No national authority has the power to access the servers where the information is embedded.

In a similar way, the content added to the blockchain can be out of the reach of any authorities. There is a lot of pornography on the dark web – in blockchain, the situation can be similar. Researchers have discovered images of child abuse on bitcoin's blockchain.[198] In relation to this the INTERPOL has recognized the harnessing of blockchain for storing child abuse images.[199] In their warning, they noted that because of how the blockchain is designed, malware can be inserted and permanently hosted without the means to wipe this kind of material as of now.[200] The issue lies in the inability to take any action on this kind of data, leading to more serious breaches than infringement of personal data privacy.

A thought could be given to publicly accessible wallets – if a wallet is big enough, it could be determined who the wallet belongs to, based on traceable transactions (PPII). When setting up a wallet a person essentially agrees to all of the wallet transactions be publicly accessible. At the same time, it is worth of evaluation– if a wallet is publicly available – the user would not choose or use the wallet for transactions unless wanting to use blockchain and for it to be publicly accessible as it is embedded in the technology. Another perspective on immutability is that practice blockchain is immutable. However, in a scenario where one person has all the coins, technically they can erase the data. Therefore blockchain is not completely immutable if a person owns all the coins. In practice, this would be an unlikely scenario to happen.

---

[195] Kristin Finklea, Specialist in Domestic Security, "Dark Web," no. Congressional Research Service, March 10, 2017, accessed April 15, 2024.
[196] *Ibid*.
[197] *Ibid*.
[198] Samuel Gibbs, "Child Abuse Imagery Found within Bitcoin's Blockchain," *The Guardian*, March 20, 2018, sec. Technology, https://www.theguardian.com/technology/2018/mar/20/child-abuse-imagery-bitcoin-blockchain-illegal-content.
[199] INTERPOL, *supra* note 10.
[200] *Ibid*.

It can be concluded that everything falling outside the regulated system of MICA can be considered a dark web - described as the unknown, unknown in terms of users, substance, depth, and breadth.[201] There is little capacity for any authority to deal with any of it. This leaves a gap for more research on crimes other than financial crimes relating to blockchain and the data stored within it. It does not look like there are clear answers provided by MICA regarding the right to be forgotten. However, it does show legislative awareness that data protection and privacy is indeed an issue also in crypto-asset markets using blockchain. It also demonstrated that there is a heightened risk when it comes to privacy in crypto-asset transactions.

3. INTERACTION BETWEEN BLOCKCHAIN AND DATA PROTECTION REGIME

3.1. Solutions for GDPR Compliance

Law should be adequate enough to protect the rights of its subjects while enabling and encouraging economic growth, development and innovation in the society. Blockchain has the potential to make databases work in a new, more efficient way. However, in case of conflict, it is often the subject of the law that has to make changes in its way of acting, rather than changing the law itself. When it comes to technological advancements, more often cases are seen where new rules need to be created to address the gaps. However, the judgements on potential changes should be based on how the rules function after being observed in action.

According to the study by the European Parliament, the conflict between blockchain technology and the General Data Protection Regulation has been extensively discussed in policy circles, academia, and the business sector due to the two underlying principles of data controller and modification or erasure of the data.[202] The topic of how to strike a balance between innovation and regulation and between public and private interests complicates the dispute. It can be questioned whether the benefits in this case outweigh the harm caused to individual privacy. Surely, there are justifications for each side and these two need to be in balance in any democracy.[203] Because innovators must be allowed to innovate to ensure economic prosperity, legislators must be flexible in their approach to decentralisation, enable flexibility, and give

[201] Finklea, *supra* note 195.
[202] European Parliament, *supra* note 32.
[203] Mitrou and Karyda, *Supra* note 2.

legal clarity in their interpretations and guidance to the industry about how to implement the law.[204]

The solutions CNIL has offered to address the incompatibility is firstly to consider whether using blockchain is needed to begin with, per Article 25 of the GDPR of privacy by design.[205] However, this limits the use of blockchain technology, and it does not seem effective to address the issues long term. It may serve as a temporary solution until other, more effective, and technology-friendly solutions are developed. Ultimately, this approach does not solve the underlying issue as it is now. While the privacy by design principle is addressed in parts of the literature, further in-depth discussion among academics is necessary.[206] The CNIL also assesses the technological options for Privacy by Design, as selecting the right kind of blockchain may safeguard data in methods like encryption, commitment, fingerprints created by a hash function and a key, and so on. The architecture of the data should be considered to contain 2 layers where one layer consists of the personal data and the other layer has the blockchain data, where this information is then possible to erase as required.

One solution outside technological means could simply be not using chains that don't have a control mechanism. Choosing a blockchain that requires authorization for accessing it or controls the ability to modify or erase it, would be a way towards legal compliance. The CNIL contends that private, permissioned blockchains need to be encouraged as they provide for greater control over the governance of personal data, particularly concerning transfers made outside of the European Union.[207] From a legal perspective, this ensures that the data is not accessible to everyone as the data is stored within a specific network, possibly constituting joint controllers and making it easier for erasure. Within a small network, agreeing on the responsibilities and remaining control of the data is more likely guaranteed, and it is possible to limit the accessibility of participants within and outside of the network. The CNIL specifies the problem of data transits beyond the European Union, stating that also permissioned blockchains are fully subject to the need for suitable protections for transfers outside of the EU, such as legally enforceable business policies or standard clauses in contracts.[208] The solution in question of encouraging the use of permissioned blockchain tackles the basic concerns around

---

[204] Lyytinen Lescrauwaet et al., "Adaptive Legal Frameworks and Economic Dynamics in Emerging Tech-Nologies: Navigating the Intersection for Responsible Innovation," *Law and Economics* 16 (October 30, 2022): 202–20, https://doi.org/10.35335/laweco.v16i3.61.
[205] CNIL, *supra* note 23.
[206] AKM Bahalul Haque et al., "GDPR Compliant Blockchains-A Systematic Literature Review," *IEEE Access* 9 (2021): 50593–606, https://doi.org/10.1109/ACCESS.2021.3069877.
[207] CNIL, *supra* note 23.
[208] *Ibid*.

the right to be forgotten and data deletion by instituting a central authority that possesses the capacity to regulate data and authorise new members to the network, also in data transfers. This leads to the conclusion that private and permissioned blockchains are easier to create than public and permissionless networks in a way that complies with EU data protection rules.[209] However, private blockchains can limit the territorial scope or the application of blockchain technology and therefore more exploration is needed for solutions for public blockchains.[210]

From an immutability standpoint, blockchain might not be legally compliant, but in situations where there is a control mechanism, such as a data controller, it helps identify the accountable party. It also grants the individual the right to request to be forgotten and exercise their rights. Having a control mechanism that ensures that blockchain is legally compliant would mitigate the risks to an individual and ensure greater regulatory compliance. Even in cases where it is not possible to get rid of the chain, companies can be required to limit access to the chain and ultimately there is someone from whom to claim damages.

Returning to the situation discussed above, where personal information is in blockchain and a person wants it removed, how does one enforce the right to be forgotten? The answer depends on the technology used, as it may be much easier to enforce the right when using a private blockchain than when using a public one. In private permissioned blockchains there may be an opportunity to erase or modify the data, and even in public permissionless blockchains access to the data can be restricted by proper encryption methods. However, due to the immutable properties of blockchain, especially public blockchain, the data remains in the blockchain due to its immutability. Essentially there are some distinguishable technological solutions – data encryption, off-chain storage and advanced cryptographic techniques as discussed. Some argue for these solutions, holding that data on the blockchain should be kept immutable rather than seeking alternative ways to modify the underlying technology, as it falls under the "umbrella" of Article 17(2) of the GDPR and is thus not a no-law zone.[211] A potential course of action would be to file a lawsuit or claim with a data privacy agency (DPA), demanding damages and a court order requiring the removal of data or the shutdown of any nodes that violate this right. From an enforcement standpoint, this would be extremely difficult as in practice there is uncertainty of the controller and where to submit the complaint. The

[209] European Parliament, *supra* note 32.
[210] Haque et al., *supra* note 206.
[211] Moreno José Miguel Moreira, "Blockchain and The Right to Be Forgotten: A Happy 'Marriage'?," *Tilburg University Law School*, n.d., http://arno.uvt.nl/show.cgi?fid=149423.

underlying issue is from whom to claim damages. Bringing the claim to the DPA of a Member State may be in vain if it is impossible to determine the data controller.

In the future, blockchain can be seen even as a possibility for storing personally identifiable information such as names, passport numbers and birthdates under globally unique decentralized identifiers (DIDs).[212] This of course would be done with the proper encryption methods and the possibility to modify the data. Nonetheless, in search of solutions other scholars argue that to maintain data integrity and trust, it is not advised to modify or remove data from the blockchain.[213]

CONCLUSION

The right to be forgotten presents itself as a societal dilemma of the modern digitalised world. The clash of privacy regulations and technology is a broader challenge highlighted by the struggle between blockchain and GDPR compliance. Questions raised in this research evaluate the extent to which the right to be forgotten is enabled. Additionally, it is discussed whether the current legal framework should be restructured to answer the challenges of modern technology, or whether the technology itself should be built and modified to comply with data protection requirements. These questions are rather complex, as no simple answer can be given.

While blockchain enhances many areas to be reached by the current privacy regulations such as the data availability as it is almost impossible to modify or erase, data accuracy due to multiple participants validating the data, and data transparency and integrity, the very technology that makes these qualities possible also inevitably leads to issues in other domains. Problems with GDPR compliance arise mainly from the immutable and decentralized nature of blockchain, leading to possible breaches, especially in the right to be forgotten (right to erasure) embedded in Article 17 and problems in determining the relevant participants such as data controller or processor. Determining the appropriate authorities in a dispute also becomes problematic when a data controller cannot be identified. The question of whether or not there is a breach of Article 17 of the right to be forgotten is dependent on the technology used and naturally, the type of data that is processed in the blockchain. Therefore, a definite answer

[212] Suominen et al., *supra* note 57.
[213] Haque et al., *supra* note 206.

cannot be given about the extent of the incompliance. Nevertheless, if personal data is indeed processed, there is likely a violation of this right.

Whether blockchain processes personal data depends on the technological design as well as whether or not personal data is used in its operation. In cases where personal data is not processed or it is processed in a way that an individual is not identifiable, or where the data is made anonymous, the GDPR does not apply. However, it is more often that personal data is processed in some way within the blockchain, making the GDPR and its principles applicable. In addition to the GDPR, MICA regulation directly addresses DLTs, blockchain and its application on crypto assets deriving from those technologies. While MICA or the Travel Rule do not directly address GDPR compliance regarding the right to be forgotten, they require the subjects of the regulation to comply with it. This would be applicable in cases where personal data is handled in crypto-asset transactions.

As of now, the general consensus among those discussing the use of blockchain seems to be that the technology needs to be adapted to the GDPR. By design and default, blockchain technology is not GDPR compliant. Stated differently, the current drafting of the GDPR makes it incompatible with blockchain technology and creates obstacles for the introduction of new technologies such as blockchain. However, based on this research scholars agree that the evaluation should be done on a case-by-case basis.

As said in the beginning, blockchain technology can vary and have different functions. The compliance largely depends on what kind of technology is used and what kind of information the blockchain contains. A study carried out by the European Parliament about blockchain compliance with GDPR essentially mirrors the conclusions of this paper, holding that it cannot be concluded in a generalised fashion whether blockchains are either compatible or incompatible with European data protection law.[214] It is not always that blockchain is uncompliant with the GDPR, as there might be ways to make some parts of the data, mainly the personal data erasable. Other ways exist too, such as utilizing smart contracts to obtain consent. Hence, solutions in the future might entail finding a way to separate personal data from the blockchain itself or make sure it is not processed in the first place. Nonetheless, the balance between individual rights and innovation requires an open dialogue between legislators and innovators in a constant manner, keeping up with the technological changes in the industry.

Academics have suggested multiple technological as well as legal ways to get around this issue. Research and development on possible solutions have proposed hashing out as a way

[214] European Parliament, *supra* note 32.

to reach compatibility through off-chain data storing, meaning storing the personal data outside of the blockchain itself and therefore enabling the possibility to modify and erase the data through the data controller storing the off-chain data. The pursuit of such solutions indicates that there is a movement towards finding more technological solutions for aligning blockchain with legal requirements in the future. Although somewhat promising solutions have been provided, the problem lies in the fact that these procedures might still limit the full utilization of blockchain, consequently discouraging the use of blockchain. A more legal solution offered by the French Data Protection Authority in its approach to Privacy by Design to abstain from using blockchain unless utmost necessary, is not a seemingly innovation-friendly solution, but rather a temporary fix. They also emphasized questioning which type of blockchain should be used, such as differentiating between the permissionless and permissioned blockchain. Promoting permissioned blockchain still limits the full potential of the blockchain.

More research needs to be done on GDPR-friendly solutions for blockchain without compromising the use of the whole technology. Currently, the majority of authorities and experts concur that storing personal data on the blockchain is not advised.[215] Nonetheless, in order to guarantee adherence to data privacy regulations and preserve individual rights and basic freedoms, collaboration between the government and the tech industry is required. As of now, the application and advancement of blockchain technology are threatened by the conflicts between the technology and the right to be forgotten among others.

[215] Ruas et al, *supra* note 5.

BIBLIOGRAPHY

1. Primary sources

1.1. Legislation

1. Charter of Fundamental Rights of the European Union (Charter), OJ C 326, 26.10.2012. Available on: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:12012P/TXT. Accessed January 4th, 2024.

2. Consolidated text: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02002L0058-20091219.

3. Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5, available on: https://www.echr.coe.int/documents/convention_eng.pdf. Accessed January 4th, 2024.

4. 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 free movement of such data (Data Protection Directive) OJ L 281, 23.11.1995. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046. Accessed January 4th, 2024.

5. Regulation (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), OJ L 119, 4.5.2016. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC. Accessed January 4th, 2024.

6. 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 (Text with EEA relevance), 150

OJ L § (2023). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1114. Accessed January 4th, 2024.

7. United Nations. Universal Declaration of Human Rights, 217 A (III), 10.12.1948. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52011DC0886. Accessed January 4th, 2024.

1.2. Cases

1. *Judgement in Google Spain SL and Google Inc. v Agencia Española de Protección de Datos* (AEPD), C-131/12, ECLI:EU:C:2014:317.

2. *Judgement in Maximilian Schrems v. Data Protection Commissioner,* Case C-362/14, EU:C:2015:650.

3. *Judgement in Maximilian Schrems v Data Protection Commissioner (Ireland) and Facebook Ireland Ltd*., Case C-311/18 (Court of Justice of the European Union, July 16, 2020).

4. *Judgement in Nowak, Peter v Data Protection Commissioner*. Case C-434/16. EU:C:2017:994. (Court of Justice of the European Union, December 20, 2017).

5. *Judgement in Patrick Breyer v Bundesrepublik Deutschland*, No. Case C-582/14 (ECJ October 19, 2016). ECLI:EU:C:2016:339.

2. Secondary sources

2.1. Books

1. Chance, Clifford. "Crypto Regulation: The Introduction of Mica into the EU Regulatory Landscape," December 2022. https://www.cliffordchance.com/briefings/2022/12/crypto-regulation--an-introduction-of-mica-into-the-eu-regulator.html. Accessed May 7, 2024.

2. nCouncil of Europe, European Court of Human Rights, European Data Protection Supervisor, and European Union Agency for Fundamental Rights (EU body or agency). *Handbook on European Data Protection Law: 2018 Edition*. LU: Publications Office of the European Union, 2018. https://data.europa.eu/doi/10.2811/343461. Accessed May 8, 2024.

3. European Parliament. Directorate General for Parliamentary Research Services. *Blockchain and the General Data Protection Regulation: Can Distributed Ledgers Be Squared with European Data Protection Law?* LU: Publications Office, 2019. https://data.europa.eu/doi/10.2861/535. Accessed May 8, 2024.

4. Kulhari, Shraddha. “Fitting the Blockchain Solution into the GDPR Puzzle.” In *Building-Blocks of a Data Protection Revolution*, 1st ed., 38–52. The Uneasy Case for Blockchain Technology to Secure Privacy and Identity. Nomos Verlagsgesellschaft mbH, 2018. https://www.jstor.org/stable/j.ctv941qz6.8. Accessed May 8, 2024.

5. Kulhari, Shraddha. “The Midas Touch of Blockchain: Leveraging It for Data Protection.” In *Building-Blocks of a Data Protection Revolution*, 1st ed., 15–22. The Uneasy Case for Blockchain Technology to Secure Privacy and Identity. Nomos Verlagsgesellschaft mbH, 2018. https://www.jstor.org/stable/j.ctv941qz6.6. Accessed May 8, 2024.

2.2. Articles

1. Azgad-Tromer, Shlomit, Joey Garcia, and Eran Tromer. "The Case for On-Chain Privacy and Compliance." SSRN Scholarly Paper. Rochester, NY, June 27, 2023. Accessed April 1, 2024. https://papers.ssrn.com/abstract=4492919.

2. Bacon, Jean, Johan David Michels, Christopher Millard, and Jatinder Singh. "Blockchain Demystified." SSRN Scholarly Paper. Rochester, NY, December 20, 2017. Accessed April 5, 2024. https://papers.ssrn.com/abstract=3091218.

3. Belen-Saglam, Rahime, Enes Altuncu, Yang Lu, and Shujun Li. "A Systematic Literature Review of the Tension between the GDPR and Public Blockchain Systems." *Blockchain: Research and Applications* 4, no. 2 (June 1, 2023): 100129. Accessed April 1, 2024. https://doi.org/10.1016/j.bcra.2023.100129.

2. Buocz, Thomas, Tina Ehrke-Rabel, Elisabeth Hödl, and Iris Eisenberger. "Bitcoin and the GDPR: Allocating Responsibility in Distributed Networks." *Computer Law & Security Review* 35, no. 2 (April 1, 2019): 182-98. Accessed April 7, 2024. https://doi.org/10.1016/j.clsr.2018.12.003.

3. Chou, Shuo-Yan. "The Fourth Industrial Revolution: Digital Fusion with Internet of Things." *Journal of International Affairs* 72, no. 1 (2018): 107-20.

4. De Gregorio, Giovanni, and Pietro Dunn. "The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age." SSRN Scholarly Paper. Rochester, NY, March 31, 2022. Accessed May 1, 2024. https://doi.org/10.2139/ssrn.4071437.

5. Dumitriu, Petru, and Joint Inspection Unit. "Blockchain Applications in the United Nations System: Towards a State of Readiness: Report of the Joint Inspection Unit." 2020. Accessed May 1, 2024. https://digitallibrary.un.org/record/3906141.

6. Finck, Michèle. "Blockchains and Data Protection in the European Union." *European Data Protection Law Review* 4, no. 1 (2018): 17-35. Accessed April 7, 2024. https://doi.org/10.21552/edpl/2018/1/6.

7. Finklea, Kristin. "Specialist in Domestic Security March 10, 2017." Dark Web, no. Congressional Research Service (March 10, 2017). Accessed April 15, 2024. https://crsreports.congress.gov/product/pdf/IF/IF12172.

8. Gauci-Maistre Xynou, Jean-Pie, Despoina Xynou, and Daniela Gaffarena. "Blockchain Technology vs. GDPR: Conflict Resolution Required." Lexology, January 29, 2019. Accessed March 5, 2024. https://www.lexology.com/library/detail.aspx?g=b76fd3f5-ac2f-40dc-9284-ccbba6983009.

9. Godyn, Mateusz, Michal Kedziora, Yingying Ren, Yongxin Liu, and Houbing Herbert Song. "Analysis of Solutions for a Blockchain Compliance with GDPR." *Scientific Reports* 12, no. 1 (September 2, 2022): 15021. Accessed March 5, 2024. https://doi.org/10.1038/s41598-022-19341-y.

10. Graaf, T. J. de. "From Old to New: From Internet to Smart Contracts and from People to Smart Contracts." *Computer Law & Security Review* 35, no. 5 (October 1, 2019): 105322. Accessed February 28, 2024. https://doi.org/10.1016/j.clsr.2019.04.005.

11. Habib, Gousia, Sparsh Sharma, Sara Ibrahim, Imtiaz Ahmad, Shaima Qureshi, and Malik Ishfaq. "Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing." *Future Internet* 14, no. 11 (November 2022): 341. https://doi.org/10.3390/fi14110341.

12. Hakim, Evren. "The Legal Status of Cryptocurrency within the European Union: An Analysis of the MICA Regulation," 2024. Accessed April 15, 2024. https://doi.org/10.13140/RG.2.2.23260.36482.

13. Haque, AKM Bahalul, AKM Najmul Islam, Sami Hyrynsalmi, Bilal Naqvi, and Kari Smolander. "GDPR Compliant Blockchains-A Systematic Literature Review." *IEEE Access* 9 (2021): 50593-606. Accessed May 5, 2024. https://doi.org/10.1109/ACCESS.2021.3069877.

14. Jiménez-Gómez, Briseida Sofia. "RISKS OF BLOCKCHAIN FOR DATA PROTECTION: A EUROPEAN APPROACH." *Santa Clara High Technology Law Journal* 36, no. 3 (April 2, 2020): 281.

15. Jongerius, Silvan. "Right to Be Forgotten under GDPR in Blockchain - Blog." TechGDPR (blog), August 13, 2019. Accessed May 5, 2024. https://techgdpr.com/blog/gdpr-right-to-be-forgotten-blockchain/.

16. José Miguel Moreira, Moreno. "Blockchain and The Right to Be Forgotten: A Happy 'Marriage'?" Tilburg University Law School, n.d. Accessed May 5, 2024. http://arno.uvt.nl/show.cgi?fid=149423.

17. Lescrauwaet, Lyytinen, Hekkert Wagner, Cheng Yoon, and Sovacool Shukla. "Adaptive Legal Frameworks and Economic Dynamics in Emerging Technologies: Navigating the Intersection for Responsible Innovation." *Law and Economics* 16 (October 30, 2022): 202–20. Accessed May 5, 2024. https://doi.org/10.35335/laweco.v16i3.61.

18. Lynskey, Orla. "Control over Personal Data in a Digital Age: Google Spain v AEPD and Mario Costeja Gonzalez." *The Modern Law Review* 78, no. 3 (2015): 522–34. Accessed February 6, 2024. https://doi.org/10.1111/1468-2230.12126.

19. Madnick, Professor Stuart E. "The Continued Threat to Personal Data: Key Factors Behind the 2023 Increase," December 2023. Accessed May 4, 2024. https://www.apple.com/newsroom/pdfs/The-Continued-Threat-to-Personal-Data-Key-Factors-Behind-the-2023-Increase.pdf.

20. Mitrou, Lilian, and Maria Karyda. "EU's Data Protection Reform and the Right to Be Forgotten: A Legal Response to a Technological Challenge?" SSRN Scholarly Paper. Rochester, NY, February 5, 2012. Accessed May 2, 2024. https://papers.ssrn.com/abstract=2165245.

21. Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System," n.d. Accessed May 4, 2024. https://www.researchgate.net/publication/228640975_Bitcoin_A_Peer-to-Peer_Electronic_Cash_System.

22. Omarova, Saule T. "Technology v Technocracy: Fintech as a Regulatory Challenge." *Journal of Financial Regulation* 6, no. 1 (June 25, 2020): 75–124. Accessed March 4, 2024. https://doi.org/10.1093/jfr/fjaa004.

23. Onik, Md Mehedi Hassan, Chul-Soo Kim, Nam-Yong Lee, and Jinhong Yang. "Privacy-Aware Blockchain for Personal Data Sharing and Tracking." *Open Computer Science* 9 (April 15, 2019): 80–91. Accessed March 6, 2024. https://doi.org/10.1515/comp-2019-0005.

24. Ouaddah, Aafaf, Anas Elkalam, and Abdellah Ouahman. "FairAccess: A New Blockchain-Based Access Control Framework for the Internet of Things." *Security and Communication Networks* 9 (February 1, 2017). Accessed March 4, 2024. https://doi.org/10.1002/sec.1748.

25. Ruas, Inês Campos, Soumaya Ben Dhaou, and Zoran Jordanoski. "Blockchain and the GDPR – the Shift Needed to Move Forward," n.d. Accessed May 3, 2024. https://ceur-ws.org/Vol-3449/paper14.pdf.

26. Sofija, VORONOVA. "Understanding EU Data Protection Policy." European Parliament, n.d. Accessed May 5, 2024. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/698898/EPRS_BRI(2022)698898_EN.pdf.

29. Stach, Christoph, Clémentine Gritti, Dennis Przytarski, and Bernhard Mitschang. "Assessment and Treatment of Privacy Issues in Blockchain Systems." *ACM SIGAPP Applied Computing Review* 22, no. 3 (November 3, 2022): 5–24. Accessed April 3, 2024. https://doi.org/10.1145/3570733.3570734.

30. Suominen, Kati, Andrew Chatzky, William Reinsch, and Jonathan Robison. "10 Big Questions (and Myths) Surrounding Blockchain." Harnessing Blockchain for American Business and Prosperity. Center for Strategic and International Studies (CSIS), 2018. Accessed April 6, 2024. https://www.jstor.org/stable/resrep22491.6.

31. Suripeddi, Mani Karthik Suhas, and Pradnya Purandare. "Blockchain and GDPR – A Study on Compatibility Issues of the Distributed Ledger Technology with GDPR Data Processing." *Journal of Physics: Conference Series* 1964, no. 4 (July 1, 2021): 042005. Accessed April 17, 2024. https://doi.org/10.1088/1742-6596/1964/4/042005.

32. Tatar, Unal, Yasir Gokce, and Brian Nussbaum. "Law versus Technology: Blockchain, GDPR, and Tough Tradeoffs." *Computer Law & Security Review* 38 (September 1, 2020): 105454. Accessed April 18, 2024. https://doi.org/10.1016/j.clsr.2020.105454.

33. The French Data Protection Authority (CNIL). "Sheet N°13: Prepare for the Exercise of People's Rights." Accessed May 2, 2024. https://www.cnil.fr/en/sheet-ndeg13-prepare-exercise-peoples-rights.

34. Tomczak, Tomasz. "Crypto-Assets and Crypto-Assets' Subcategories under MiCA Regulation." *Capital Markets Law Journal* 17, no. 3 (July 1, 2022): 365–82. Accessed May 3, 2024. https://doi.org/10.1093/cmlj/kmac008.

35. Ture, Tsegaye. "GDPR, Blockchain and the Right to Be Forgotten." University of Helsinki, 2021. Accessed May 9, 2024. http://hdl.handle.net/10138/335279.

36. Zetzsche, Dirk A., Ross P. Buckley, and Douglas W. Arner. "The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain." SSRN Scholarly Paper. Rochester, NY, August 13, 2017. Accessed May 3, 2024. https://doi.org/10.2139/ssrn.3018214.

2.3. Official Websites

1. CNIL. "Blockchain and the GDPR: Solutions for a Responsible Use of the Blockchain in the Context of Personal Data." Accessed November 28, 2023. https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data.

2. European Commission. "Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses." An official website of the European Union, January 25, 2012. https://ec.europa.eu/commission/presscorner/detail/en/IP_12_46.

3. European Commission. "For How Long Can Data Be Kept and Is It Necessary to Update It? - European Commission." Accessed April 15, 2024. https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/how-long-can-data-be-kept-and-it-necessary-update-it_en.

4. European Commission. "European Countries Join Blockchain Partnership | Shaping Europe's Digital Future," April 10, 2018. Accessed May 6, 2024. https://digital-strategy.ec.europa.eu/en/news/european-countries-join-blockchain-partnership.

5. European Data Protection Board. "Secure Personal Data | European Data Protection Board." Accessed April 30, 2024. https://www.edpb.europa.eu/sme-data-protection-guide/secure-personal-data_en.

6. European Parliament. "Crypto-Assets: Green Light to New Rules for Tracing Transfers in the EU | News | European Parliament," April 20, 2023. https://www.europarl.europa.eu/news/en/press-room/20230414IPR80133/crypto-assets-green-light-to-new-rules-for-tracing-transfers-in-the-eu.

7. European Securities and Markets Authority. "Markets in Crypto-Assets Regulation (MiCA)." Accessed April 16, 2024. https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica.

8. Felten. "Does Hashing Make Data 'Anonymous'?" Federal Trade Commission, April 22, 2012. https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2012/04/does-hashing-make-data-anonymous.

9. International Association of Privacy Professionals. "Blockchain and the GDPR: Addressing the Compliance Challenge," December 14, 2018. https://iapp.org/news/a/blockchain-and-the-gdpr-addressing-the-compliance-challenge/.

10. INTERPOL. "INTERPOL Cyber Research Identifies Malware Threat to Virtual Currencies." Accessed May 8, 2024. https://www.interpol.int/en/News-and-Events/News/2015/INTERPOL-cyber-research-identifies-malware-threat-to-virtual-currencies.

11. Latvijas Banka. "MiCA Regulation - Fintech Latvia," March 31, 2022. https://fintechlatvia.eu/crypto-asset/mica-regulation/.

12. The Financial Action Task Force (FATF). "Targeted Update on Implementation of FATF's Standards on VAs and VASPs." Accessed May 2, 2024. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Targeted-update-virtual-assets-vasps.html.

2.4. Internet resources

1. Euronews. "EU Countries Approve Technical Details of AI Act | Euronews." Accessed February 5, 2024. https://www.euronews.com/my-europe/2024/02/02/eu-countries-approve-technical-details-of-ai-act.

3. GDPR.eu. "Everything You Need to Know about the 'Right to Be Forgotten,'" November 5, 2018. https://gdpr.eu/right-to-be-forgotten/.

4. Gibbs, Samuel. "Child Abuse Imagery Found within Bitcoin's Blockchain." *The Guardian*, March 20, 2018, sec. Technology. https://www.theguardian.com/technology/2018/mar/20/child-abuse-imagery-bitcoin-blockchain-illegal-content.

5. Information Commissioner's Office (ICO). "Right to Erasure." ICO, August 4, 2023. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-erasure/.

6. INTERPOL. "INTERPOL Cyber Research Identifies Malware Threat to Virtual Currencies." Accessed May 8, 2024. https://www.interpol.int/en/News-and-Events/News/2015/INTERPOL-cyber-research-identifies-malware-threat-to-virtual-currencies.

7. Investopedia. "Blockchain Facts: What Is It, How It Works, and How It Can Be Used." Investopedia. Accessed January 26, 2024. https://www.investopedia.com/terms/b/blockchain.asp.

8. Investopedia. "Financial Technology (Fintech): Its Uses and Impact on Our Lives." Investopedia. Accessed January 26, 2024. https://www.investopedia.com/terms/f/fintech.asp.

9. Statista. "Blockchain Technology Market Size Worldwide 2030." Statista. Accessed January 30, 2024. https://www.statista.com/statistics/1319369/global-blockchain-technology-market-size/.

10. The Economist. "The World's Most Valuable Resource Is No Longer Oil, but Data." *The Economist.* Accessed February 4, 2024. https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

11. The New York Times. "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far - The New York Times." Accessed April 22, 2024. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

12. TradingView. "Biggest Companies in the World by Market Cap." Accessed April 11, 2024. https://www.tradingview.com/markets/world-stocks/worlds-largest-companies/.