RIGA GRADUATE SCHOOL OF LAW

"Right to Erasure" and Private Blockchain in the European Union: Legal Requirements and Technical Possibilites

BACHELOR THESIS

AUTHOR: Marina Valpītere

LL.B 2017/2018 year student

Student number B017017

SUPERVISOR: Dennis-Kenji Kipker

(PhD)

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, 2020

ABSTRACT

Blockchain, serving as one of the most complex networks used within an organization may be regarded as challenging for the applicability and realization of the General Data Protection Regulation Article 17, which gives the data subject right to erasure or a "right to be forgotten" to ones' personal data. The immutability and decentralized character of the system does not prescribe the erasure of personal data on the chain, as well as poses problems in determining the competent authority responsible for data protection compliance, when the data subject needs to exercise its rights under the GDPR. The thesis examines whether the compliance with the General Data Protection Regulation's Article 17 could be ensured while using private blockchain within an organization, by determining the authorities responsible for the compliance in decentralized system, and, examining the conditions when immutability may allow for data erasure. Thus, proposing possible solutions and developing the guidelines for businesses how to mitigate the enforcement of the Regulation regardless of technological pattern of private blockchain.

Keywords: data protection, compliance, immutability, erasure, blockchain, personal data, right to be forgotten, applicability, realization, permissioned, permissionless, nodes, decentralization, private blockchain, enforcement, encryption, pseudonymization, anonymization, consortium.

SUMMARY

First part of the thesis examines Article 17 of the General Data Protection Regulation. The examination includes the grounds for applicability of right to erasure and a "right to be forgotten", establishes the notion of "erasure" and right to be forgotten, the exceptions of the right based on its non-absolute nature and the result how data erasure under Article 17 has to be fulfilled. The comparative analysis between the repealed Directive 95/46 EC and GDPR provides clarification on how right to erasure and right to be forgotten had developed until codified in the Regulation. Mainly focusing on the differences between concepts provided in both legal frameworks, consequently establishing the broad scope of the erasure grounds that the data subject can exercise and the organization has to consider under the GDPR.

Second part of the thesis includes the intersection of GDPR Article 17 and private blockchain. The part focuses on technical analysis of the blockchain, in particular, the structure of the system and the potential causes of non-compatibility with the Regulation, which are two main aspects, decentralization and immutability. Subsequently, private blockchain is examined to understand its technological structure, determine the roles of the participants, consequently establish an entity regarded as the controller and processor in private blockchain, and whether there could be joint-controllership. Further, the part focuses on personal data in the blockchain, what are the parts of the system that may include personal data and whether that data may be regarded as personal, even though secured by means of cryptography. Establishing whether personal data appears on the chain would be followed by the examination of conditions when the data stored on the blockchain in encrypted form may be visible to third parties, although deprived of identifiers, thus not providing the necessary conditions for individuals' data protection to full extent.

Third part includes the interdisciplinary aspect, aimed at finding possible solutions for companies to ensure the compliance when using private blockchain with the Regulation without hampering the technological design of the chain, by looking at possibilities of mitigation of the enforcement of Article 17. The part provides possible solutions how to comply with the requirements of data erasure within the organization despite the resistance of private blockchain to erasure of the data. Solutions proposed by author clarify how to recognize the erasure request, where to store the data to minimize the impact of data protection requirements, and how to maintain the data inflows coming into the chain, and, how the erasure may be achieved on the blockchain using available technologies without physical reconstruction of the chain.

Further, the interdisciplinary part proposes governance steps to understand the allocation of responsibilities of participants and conduct correct risk assessment regarding erasure of the data via proposed solutions, to exclude possibility of restoring the data. The part further would be extended to development of internal guidelines for the organization based on Article 17, which can be used as a mechanism to reach the goal of prevention of the breach of right to erasure and the penalties arising from the general non-compliance of the blockchain with the GDPR.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS:

GDPR	General Data Protection Regulation
EU	European Union
CNIL	French Data Protection Authority
DPA	Data Protection Authorities
EC	European Commission
EDPB	European Data Protection Board
WP29	Article 29 Data Protection Working Party
MS	Member State of the Union
Directive	Directive 95/46 EC
DPA	Data protection authority
DLT	Distributed ledger technology
NODES	Network of distributed computers
B2B	Business to business transaction
ISS	Information society services

INTRODUCTION

The expansion of the blockchain technology has not only been a step towards the advanced use of technological facilities, but also has contributed to harder compliance with regulatory requirements of the General Data Protection Regulation, leading to an on-going discussion of privacy matters regarding personal data protection in the European Union. From the GDPR coming in force, companies using blockchain technology are required to achieve the compliance with the Regulation in a way that does not contradict the whole nature of the blockchain, which may not be achieved straight away and require detailed case-by-case analysis of the matter.

From the first introduction of the blockchain, it has become diversified in terms of broad range of its application, one could suppose that blockchain is widened to the concept of crypto currency, however, it has already expanded to other fields globally. [1] Blockchain has become one of the main systems used throughout different institutions in the European Union to facilitate both public and private services.[2] European countries have already established blockchain in public and private sector, for example, Malta adopted the platform of academic credentials based on the blockchain, which includes issuance and verification of certificates, and allows citizens to store their personal credentials in an app, giving citizens the control over their data and access of verified third parties to it.[3] The Netherlands use blockchain for pension administration system and asset redistribution system for citizens that have low-income, enabling to allocate costs more efficiently, govern payments and transactions, regulate the taxes and salaries, yet the part of personal data is available to the regulators. [4] Sweden uses blockchain for transactions concerning property, such as transfer of land tiles and the network is used for land registers to facilitate the security and transparency of the transactions. [5] Switzerland enables citizens of a municipality of Zug to participate in electronic voting, prove their residency digitally, and pay for parking places and bike rental services by creating a blockchain - based identity approved by the government, which allows

[1]Kulhari Shraddha. "The Midas touch of Blockchain: Leveraging It for Data Protection." in *Building-Blocks of a Data Protection Revolution: The Uneasy Case for Blockchain Technology to Secure Privacy and Identity*, (Baden-Baden, Germany: Nomos Verlagsgesellschaft MbH, 2018), pp. 15-16. Available on: www.jstor.org/stable/j.ctv941qz6.6. Accessed November 11, 2019.
[2]David Allessie, Maciej Sobolewski, Lorenzino Vaccari "Blockchain for digital government", *Publications Office of the European Union* (2019):1-88, p. 12, accessed November 12, 2019, doi:10.2760/942739.
[3]*Ibid*, p.22.
[4]*Ibid*, p.39.
[5]*Ibid*, p.26.

citizens to share their data with the government and third parties, disclosing a particular part of the information for regulatory purposes. [6]

In accordance with the GDPR, the Regulation does not specifically connect processing to the particular technological unit, but explains the processing as a set of actions performed on personal data, which include the processing itself, storing the data and any alterations made.[7] Thus, blockchain industry is affected by the GDPR, because some of its technological fundamentals may seem conflicting when it comes to application and realization of the provisions of the Regulation.

Encryption makes blockchain relatively safe data protection tool, as there is no particular visible personal data. Although, when blockchain is used within business organization, it may involve personal data to some extent. Nature of the data varies, it may be financial or private, as well as concerning the transfer of goods and services, generally depending on the business field that company operates in. Following that, organizations and their business partners would eventually have an access to information identifying the users, starting from e-mails, addresses, financial account details, IP addresses[8] and other similar information that pursuant to GDPR would qualify as personal data.[9] Potentially, if this information becomes available to non-trusted third parties or publicly available, data subject becomes at risk of exposure of current transactions including data subjects' personal data. [10]

Blockchain records the transactions in a permanent way among the parties and various computers, hence the first problematic aspect is that any record involved in the transaction cannot be modified without modification of all of the following blocks. [11] As a result, the immutability at the core of the system may pose problems in exercise of data subjects' rights under the GDPR, since technically the erasure or modification of personal data cannot be

[6]David Allessie, Maciej Sobolewski, Lorenzino Vaccari "Blockchain for digital government", *Publications Office of the European Union* (2019):1-88, p.31, accessed November 12, 2019, doi:10.2760/942739.

[7] 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, p. 1–88. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679. Accessed October 19, 2019. Article 4(2).

[8]Fergal Reid, Martin Harrigan "An Analysis of Anonymity in the Bitcoin System", *Clique Research Cluster, Complex & Adaptive Systems Laboratory University College Dublin, Ireland* (2012): 1-26, p.15. Available at: arXiv:1107.4524v2 [physics.soc-ph]. Download available at: https://arxiv.org/pdf/1107.4524.pdf.

[9]General Data Protection Regulation 2016/679, *supra* note 7, Article 4(1).

[10]Reid, *supra* note 8.

[11]Michèle Finck, "Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?", *European Parliamentary Research Service* (2019) :1-101, p.3, accessed November 1,2019, doi: 10.2861/535. Brussels, European Union, 2019.

performed, as data written on the blockchain is meant to be permanent, subsequently it cannot be modified or erased when appears *on* the chain.[12]

Blockchain is meant to provide integrity and safety of the data using peer-to-peer networks, creating complete distributed system with no central point of sharing the data between all peers.[13] Therefore, it implies that decentralized character of the chain does not give a clear understanding of the entity accountable for data processing and data protection principles in the organization, making it impossible to determine the controller, processor or joint-controllers at first glance.

This gives a rise to legal complications of applicability and realization of Article 17 right to erasure and a "right to be forgotten".[14] The General Data Protection Regulation has introduced the fundamental right to erasure and a "right to be forgotten" in Article 17, which gives a right to the data subject to have their personal data erased upon request without undue delay, when the data is no longer needed for original purposes of collecting and processing, when the data subject withdraws the consent for the data processing, when the erasure is a fulfillment of the legal obligation under the law of the European Union and its Member States, if the data subject objects to the processing and there is no justified overriding legitimate ground for the processing, or if the data was in first place processed unlawfully. [15] However, the nature of this right is not absolute, meaning that this right applies only in particular circumstances determined on a case-by-case basis and has specific exclusions.[16]

As right to erasure, or as it is referred to "right to be forgotten" may be seen as one of the most complicated rights under the GDPR both in terms of applicability and realization, the thesis seeks to analyze the compliance relation between the private blockchain used within an organization and GDPR within the scope of the European Union. The thesis specifically focuses on substance of two main questions to be examined. Firstly, *whether* and *how* the compliance with GDPR's right to erasure or "right to be forgotten" can be ensured in a system that is technologically immutable. Secondly, how the companies that use private blockchain

[12]"GDPR, Blockchain and the French Data Protection Authority: Many Answers but Some Remaining Questions," *Stanford Journal of Blockchain Law & Policy* 2, no. 2 (2019): 1-14, p. 4. Available on: Hein Online database.
[13]Michèle Finck, "Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?", *European Parliamentary Research Service* (2019) :1-101, p.3, accessed November 1,2019, doi: 10.2861/535. Brussels, European Union, 2019.
[14]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, p. 1–88. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679. Accessed October 19, 2019. Article 17.
[15]*Ibid.*
[16]*Ibid.*

may mitigate the enforcement of the GDPR Article 17 in a system that undermines the applicability of the Regulation.

The methodology is comprised of doctrinal research, which includes the analysis of the legislation, in particular, the provisions of the General Data Protection Regulation, that are Article 17 and suitable recitals on the matter of data erasure and a right to be forgotten, and repealed Directive 95/46 EC for comparative analysis and case law under Directive that had established the right be forgotten in the first place. The doctrinal research would be supported by qualitative research of various scholarly articles concerning data protection and blockchain, its structure and governance, as well as technological fundamentals, literature and official reports and guidelines from the relevant authorities of the European Union. The following methods would be extended to interdisciplinary method, for the purposes of establishing the compliance with the GDPR from the perspective of the business organization, including aspects of internal governance and development of guidelines and documentation templates.

1. PART I: RIGHT TO ERASURE AND A "RIGHT TO BE FORGOTTEN"

1.1. Scope of personal data processed in the blockchain

The compatibility of the blockchain with the GDPR is determined by using specific elements part to the issue at individual approach to the case. The relationship between blockchain and GDPR has to be examined firstly by acknowledging the scope of the Regulation, therefore determining the circumstances in which personal data processed by the blockchain would be regarded as subject to applicability of GDPR.

The material and territorial scope of the GDPR covers any personal data processed and collected [17] and is applicable to anyone that controls the processing or processes personal data notwithstanding whether it is natural or legal person. [18]

[17] 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, p. 1–88. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679. Accessed January 22, 2020. Article 2(1).

[18] *Ibid.*

1.1.1. Territorial scope

Article 3 of the GDPR determines the territorial scope, where the territorial scope signifies the establishment of a controller or processor and its activities *within* the European Union for the purposes of the thesis. Consequently, if a legal or natural person deemed as data controller, data processor or joint-controller under the GDPR, having its establishment in the Union, and is involved in processing of personal data through any means, the GDPR applies. [19]

Therefore, if the processing of personal data within the blockchain takes place within the territorial scope of the Regulation, this distributed ledger processing becomes subject to EU data protection law. Following the market location principle, legal disputes arising under the GDPR will be under the law of the country where the data was collected. [20]

Public blockchain at most is not part to the specific location, since in the most cases it is permissionless, where any individual having necessary technological facilities in any part of the world can join the network and operate on it. [21] Thus, in determining the territorial scope, public blockchain may not be subject to single regulatory requirements. [22] In comparison, private blockchain usually is permissioned and located in a particular place, as within the organization or consortium, having a particular legal entity that identifies the participants and is a subject to particular regulatory requirements of the MS it operates in.[23]

1.1.2. Material scope

Pursuant to Article 2(1) GDPR, the Regulation applies when processing of personal data is utterly or partially conducted by automated means, as well as applicable to the processing that is carried out by other than automated means. Other categories of processing involve cases where personal data is intended for storing, or is stored by other than automated means, such as paper-based data storage and archiving purposes. [24] Accordingly, the GDPR applies to blockchain, since when blockchain does include personal data, this falls within "processing carried out by automated means" in accordance with Article 2(1).

---

[19]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, p. 1–88. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679. Accessed January 22, 2020. Article 3.

[20]*Ibid*.

[21]Tom Lyons, Ludovic Courcelas, Ken Timsit, "Legal and regulatory framework of blockchains and smart contracts", thematic report for *The European Union Blockchain Observatory and Forum*, p.13. Published September 27, 2019. Download available on: https://www.eublockchainforum.eu/reports. Accessed February 1, 2020.

[22]*Ibid.*

[23]*Ibid.*

[24]Cambridge Business English Dictionary. Definition of *filing system*, available on: https://dictionary.cambridge.org/dictionary/english/filing-system Accessed January 24, 2020.

1.2. Definition of right to erasure and a "right to be forgotten"

In accordance with Article 17 of the General Data Protection Regulation right to erasure gives a right of obtaining the erasure of individuals' personal data from the controller and the controller has the obligation of immediate action with regard to the data erasure in circumstances pursuant to Article 17(1) points a) to f). [25]

Giving data subjects' right to have their personal data erased contributes to constructive upholding to data protection principles, mainly limiting the amount of the data to that amount necessary for processing purposes and giving the data subject the control over their data.[26] In particular, the data subject has the right of removal of his or her personal data and a "right to be forgotten" in cases when withholding of that personal data breaches the General Data Protection Regulation, law of the European Union, or a law of the Member State the controller is a subject to. [27]

There is no particular criterion provided in GDPR how valid request of erasure has to be structured, thus it can take any form and may be referred to any part of an enterprise or an organization concerned.[28] The legal obligation under the GDPR creates the conditions that the erasure request has to be identified notwithstanding its form, so that the entity responsible may take all the necessary measures to comply with the obligation if the request is valid[29].[30] It is important to notice that the law itself still does not describe the procedure of data erasure in each individual case, or define the notion of "erasure". [31] Thus, the interpretation for "erasure" as provided in the Regulation may be up to the competent authority based on case-by-case analysis, taking into account the available technical and organizational measures available to

[25]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, p. 1–88. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679. Accessed October 31, 2019. Article 17(1).

[26]Handbook on European data protection law (Luxembourg: Publications Office of the European Union, 2018), p. 221. doi:10.2811/343461. Available on: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf. Published May 24, 2018. Accessed October 31, 2019.

[27]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, p. 1–88. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679. Accessed October 31, 2019. Recital 65.

[28]Information Commissioner's Office. Right to erasure, available on: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/. Accessed October 24, 2019.

[29]Valid request means that there are *no exceptions* under GDPR Article 17(3) points a)-e), since right to erasure or right to be forgotten *may be refused* in individual cases that fall under before mentioned points.

[30]Information Commissioner's Office, *supra* note 28.

[31]Paul Voigt, Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): a practical guide* (Hamburg, Berlin Germany: Springer Publishing 2017), p. 161, section 5.5.2.4.

the controller, nature of the processing, as well as referring to previous case law on the matter.[32]

Right to be forgotten is provided in complementing the right to erasure, after being recognized in CJEU judgment of *Google Spain* under the repealed Directive 95/46 EC[33], only later with adoption of the GDPR, right to be forgotten was finally codified as a fundamental right in Article 17 pursuant to right to erasure. [34] The notion of the right to be forgotten goes beyond a simple request of erasure of the data, it improves the overall protection of privacy online and includes the supervision of the obligations of immediate erasure of personal data. [35] The right to be forgotten requires that the request of erasure under Article 17(1) shall at least have an *implicit* wish of erasure of personal data, followed by the fact that each controller that is responsible for personal data in question has to be addressed by that request. [36] Article 17 "right to be forgotten" imposes a general obligation on the controller if the personal data is made public to inform other controllers and to track and remove any copies, replications and links connected to this data.[37] It also involves the principle of taking all reasonable steps to comply with the obligation that the controller shall uphold to, using all available organizational means and technological abilities. [38]

When receiving a well-founded request for erasure with no exceptions, there is an obligation to take vital steps in ensuring the erasure of the data from live systems and backup systems. [39] Data erasure from live systems may be simple to achieve, however the data may still remain in the backup system, where to achieve the erasure properly the system has to be permanently overwritten.[40] Permanent overwriting of the software can take particular time to achieve the result, this implies that the data has to be put "beyond use" until the erasure is

[32]Justin Kwik, "In Light of the Technical Impracticality of the Right to Erasure, What Answers Can Actor-Network Theories Provide," *Singapore Comparative Law Review 2019* (2019): 48-65, p.51.
[33]Judgement in *Google Spain*, C‑ 131/12, ECLI:EU:C:2014:317.
[34]Paul Voigt, Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): a practical guide* (Hamburg, Berlin Germany: Springer Publishing 2017), p.161.
[35]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, p. 1–88. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679. Accessed October 31, 2019. Recital 66.
[36]Voigt, *supra* note 34.
[37]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, p. 1–88. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679. Accessed October 31, 2019. Article 17.
[38]*Ibid*, Article 17(2).
[39]Information Commissioner's Office. Guide to the General Data Protection Regulation (GDPR) (2018):1-295. Available on: https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf. Published April 2, 2018. Accessed November 3, 2019.
[40]*Ibid*.

performed completely.[41] Hence, the obligation of the controller extends to implementing appropriate technical and organizational security measures to restrict access and put the data beyond use, or, if there is a possibility of immediate removal of the data, the removal must be done as the first consideration. [42]

The decisive element for erasure of the data has to be a *result*. Therefore, the means of erasure substantively do not play the major role in determining the result of the erasure where the data shall be no longer available to the controller, processor or any third party. [43] The result prescribes that the data is not accessible for the subjects mentioned and it does not make a difference if the data is physically destroyed, anonymized or permanently over-written in cases of use of the special software unless the result is satisfied. [44] However, one of the most important requirements is that the data shall not be restored with *marginal* effort. [45] Thus, the GDPR may be seen as providing a degree of flexibility with regard to erasure that in particular may be relevant to the blockchain system, where erasure via physical destruction of the data may not be performed, or if it may, in exclusive circumstances.

1.3. Right to be forgotten and right to erasure in GDPR compared to repealed Directive 95/46 EC

Under Directive 95/46 EC, right to erasure was provided in Article 12 "right to access". [46] Article 12(b) guaranteed that the data subject has a right of obtaining the erasure, rectification or blocking the data from the controller if the processing does not comply with the provisions of the Directive or the data is stored in an incompatible way.[47] The Directive mentions that in particular, this article shall be applied in cases where non-compliance exists because of inaccurate or incomplete data. [48]

The decision of *Google Spain* referred to legal right to be forgotten, extended the notion of right to erasure in Article 12(b) of the Directive 95/46 EC, and connected it to right

[41]Information Commissioner's Office. Guide to the General Data Protection Regulation (GDPR) (2018):1-295. Available on: https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf. Published April 2, 2018. Accessed November 3, 2019.
[42]Justin Kwik, "In Light of the Technical Impracticality of the Right to Erasure, What Answers Can Actor-Network Theories Provide," *Singapore Comparative Law Review* 2019 (2019): 48-65, p.51.
[43]Paul Voigt, Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): a practical guide* (Hamburg, Berlin Germany: Springer Publishing 2017), p. 161, section 5.5.2.4.
[44]*Ibid.*
[45]*Ibid.*
[46]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, *OJ L* 281, 23.11.1995, p. 31–50. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046. Accessed November 1, 2019. Article 12.
[47]*Ibid*, Article 12(b).
[48]*Ibid.*

to object Article 14(a) of the Directive. [49] Hence, the request contained two rights of the data subject that may be considered as relevant ground for right to be forgotten. Therefore, allowing individuals to ask for the removal of the links, copies and references that contain personal data online, on the basis of being prejudicial to the data subjects' fundamental rights as protection of the data and privacy of the data subject concerned and if the data is incompatible with Article 6(1) (e) - (f) of the Directive. [50] Therefore, Article 12(b) in conjunction with Article 14 subparagraph (a) of the first paragraph have to be interpreted accordingly, even if the publication of the data was at first place lawful.[51]

Although the court did not specifically *grant* the right to be forgotten, it explained the balance between accessibility of the data and public interest, meaning if the data appears to be irrelevant, inadequate or the time for the relevance of this data has already passed, or it is incompatible with the provisions, an individual has a right to request the erasure and the entity to whom the request was made is obliged to remove the data if there is no overriding ground for non-removal. [52] As the court noted, the right shall be granted in certain conditions when the fundamental data protection rights are of a higher importance that public interest in accessibility of the information, thus, the conditions for this right shall be individually examined.[53]

Under the GDPR the right to erasure, known also as "right to be forgotten" is a codified fundamental right, applicable in particular circumstances provided in Article 17 of the GDPR. [54] Right to erasure, right to be forgotten applies if personal data does not anymore serve the necessary purpose for processing or collecting and the original means of processing and collecting of the data have already been fulfilled. [55] The absence of overriding legitimate interest serves as a basis for applicability of right to erasure and right to be forgotten. Legitimate interest of the processing by the controller or a third party shall not override the

[49]Judgement in *Google Spain*, C‑ 131/12, ECLI:EU:C:2014:317, para. 98-99.
[50]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, *OJ L* 281, 23.11.1995, p. 31–50. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046. Accessed November 2, 2019. Article 6(1).
[51]Judgement in *Google Spain*, C‑ 131/12, ECLI:EU:C:2014:317, para. 88-99.
[52]Judgement in *Google Spain*, C‑ 131/12, ECLI:EU:C:2014:317, para. 100 (4.).
[53]Handbook on European data protection law (Luxembourg: Publications Office of the European Union, 2018), p.225, available on: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf, doi:10.2811/343461. Published May 24, 2018. Accessed November 5, 2019.
[54]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, p. 1–88. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679. Accessed November 4, 2019. Article 17.
[55]*Ibid*, Article 17.1. (a).

fundamental rights of an individual whose data is in the concern. [56] Therefore, right to erasure, right to be forgotten applies when individual objects to the processing of personal data relying on Article 21(1) of the GDPR and the controller or a third party has no justification of legitimate means of the processing laid out in Article 21(2). [57] If individuals' personal data had been unlawfully processed, it becomes a ground for invoking the right to erasure or right to be forgotten, this provision includes general non-compliance with the Regulation and lack of a legal permission.[58] When controller is subject to law of the Member State or the Union, right to be forgotten and right to erasure applies in cases where personal data has to be erased to ensure compliance with the statutory obligation. [59] Right to erasure "right to be forgotten" also applies if personal data has been collected for purposes of ISS offerings to the child (pursuant to Article 8 GDPR), however it may require broad interpretation of the notion of the ISS.[60] Non-absolute nature of the right limits the applicability of right to be forgotten to the extent where data processing deems necessary, such as the exercise of right to freedom of expression and information, when law of the Union or Member State which the controller is subject to requires the processing as a legal obligation, if the processing is necessary to be carried out for public interest, health, exercise of the rights of official authorities, research purposes of public interest, as well as in situations concerning legal claims, their establishment, defence and exercise. [61]

As follows, right to erasure and a right to be forgotten may be seen as two distinct parts of the right having a common intention, merged into one Article 17 of the GDPR. As provided in Article 12 of the Directive, where right to erasure mostly focused on limitation or stopping the unlawful use of the data subject's personal data[62], right to be forgotten pursuant to right to erasure laid out in Article 17 has extended the rights of the data subject by giving rise to more grounds such as withdrawal of the consent and objection to the processing.[63] By virtue of extension of the notion and the right to erasure itself, General Data Protection

[56] *Ibid.*, Article 17.1.(c), p.9.
[57] *Ibid.*, Article 17.1.(c).
[58] Paul Voigt, Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): a practical guide* (Hamburg, Berlin Germany: Springer Publishing 2017), p.158, para. 1.
[59] 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, p. 1–88. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679. Accessed November 4, 2019. Article 17.1.(e).
[60] *Ibid*, Article 17.1.(f).
[61] *Ibid*, Article 17.3.(a-e).
[62] 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, *OJ L* 281, 23.11.1995, p. 31–50. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046. Accessed November 5, 2019. Article 12.
[63] *See* Judgement in *Google Spain*, C‑ 131/12, ECLI:EU:C:2014:317.

Regulation had created a broader scope of right to erasure, including right to be forgotten, giving data subjects more grounds to base their objection to the processing or storing of their personal data.[64] Consequently, the GDPR has broadened the scope that organizations need to take into account when reviewing erasure requests and harmonized the compliance requirements across the union by being automatically binding on all MS.[65]

2. PART Ⅱ: APPLICATION OF ARTICLE 17 TO BLOCKCHAIN

2.1. Blockchain systems

2.1.1. General structure

Technical structure of the blockchain creates difficulties while ensuring the compliance with the Regulation, therefore the main concepts of decentralization and immutability of the blockchain that can be a potential obstacle to realization of rights of the data subject conferred by Article 17 must be examined.

As most companies operate on a system that prescribes centralized ledger, it usually does not pose obstacles to realization of the data subject's rights under the GDPR. Centralized ledger system implies that the data is stored in that ledger, having a centralized intermediary, which is the controller that verifies, maintains, and manipulates the data, can modify, record or erase the transactions. [66] Thus, centralized ledger allows the data subject to enforce its rights by having a clear understanding of an entity who has the control over the data concerned and overall data protection requirements of the company.

However, decentralized ledger as blockchain allows different parties to engage in the transactions, without centralized intermediary having control over the transaction, hence the transaction is under joint supervision by the distributed set of participants. [67] In general, blockchain is a decentralized digital database, which also is referred to as distributed ledger

[64]Francoise Gilbert, "European Data Protection 2.0: New Compliance Requirements in Sight - What the Proposed EU Data Protection Regulation Means for U.S. Companies," *Santa Clara Computer & High Technology Law Journal* 28, no. 4 (2011-2012): 815-864, p. 829.
[65]White & Case LLP. Dr. Detlev Gabel, Tim Hickman, "Chapter 9: Rights of data subjects – Unlocking the EU General Data Protection Regulation", available on: https://www.whitecase.com/publications/article/chapter-9-rights-data-subjects-unlocking-eu-general-data-protection-regulation. Accessed November 5, 2019. Published April 5, 2019.
[66]Dirk A. Zetzsche, Ross P. Buckley, Douglas W. Arner, "The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain," *University of Illinois Law Review* 2018, no. 4 (2018): 1361-1406, p.1370.
[67]Patrick Van Eecke, Anne-Gabrielle Haie, "Blockchain and the GDPR: The EU Blockchain Observatory Report," *European Data Protection Law Review* (EDPL) 4, no. 4 (2018): p. 531-534, p.531.

technology. [68] The problematic aspect of the system of distributed ledger is that the data is spread among all participants, which in case of the blockchain are nodes, which combine all of the data input to form a "block", linking it to the next block by reaching an agreement of its compatibility with the system, therefore creating a "chain" of these blocks.[69] Taking into consideration the technical structure of the chain, blockchain is not a single system, but rather a class of systems merging multiple transactions in one block, that later is added to existent blocks, and some of the data contained in each of the blocks can be deemed personal.[70] The block contains particular elements that may have personal data in them, which are size header, reference to the hash from the previous block, time stamp of the transaction performed and list of different transactions part to this block, as well as the data about the data subject in an encrypted form. [71]

The data on the distributed ledger is shared between multiple nodes, where each node as well stores synchronized copy of that data. [72] Blockchain is a peer-to-peer network, therefore it prescribes a network of computers where the tasks and their contribution to the system is distributed equally among all of the peers.[73] In blockchain, each node serves as a different peer, consequently representing certain devices or particular data points[74], whenever new data is entered, the common network of the nodes is created, so that they take part in verification of the transaction before adding it to the following ledger. [75] Node ensures that the availability of the data processed, stored and collected by means of decentralized network is strengthened through duplication of the data in each of the following blocks. [76] Node can be natural or legal person that means that nodes can range from being under control of private individual, any company, particular organization, or even a machine. [77] All nodes are equally

[68]Michèle Finck, "Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?", *European Parliamentary Research Service* (2019) :1-101, p.3, accessed November 1,2019, doi: 10.2861/535. Brussels, European Union, 2019.
[69]Dirk A. Zetzsche, Ross P. Buckley, Douglas W. Arner, "The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain," *University of Illinois Law Review* 2018, no. 4 (2018): 1361-1406, p.1371.
[70]Finck, *supra* note 68.
[71]Petri Helo, Yuqiuge Hao, "Blockchains in operations and supply chains: A model and reference implementation", *Computers & Industrial Engineering*, Vol. 136 (2019): 242-251, p.248, accessed December 19, 2019, https://doi.org/10.1016/j.cie.2019.07.023. Available on: Science Direct database.
[72]Finck, *supra* note 70.
[73]Amelia Wallace, "Protection of Personal Data in Blockchain Technology - An investigation on the compatibility of the General Data Protection Regulation and the public blockchain", *Master's Thesis*, Stockholm University, p. 10. Download available at: http://www.diva-portal.org/smash/get/diva2:1298747/FULLTEXT01.pdf.
[74]*Ibid*.
[75]Michèle Finck, "Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?", *European Parliamentary Research Service* (2019) : 1-101, p.4, accessed December 21, 2019, doi: 10.2861/535. Brussels, European Union, 2019.
[76]*Ibid*.
[77]Michèle Finck, "Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?", *European Parliamentary Research Service* (2019) : 1-101, p.5, accessed December 21, 2019, doi: 10.2861/535. Brussels, European Union, 2019.

involved in the process whenever new data comes into the chain, nevertheless their roles are different in terms of functioning and potential applicability of the GDPR. Validating nodes have a permission to add the data to the blockchain by using the consensus mechanism[78], which prescribes the expression of the acceptance of all of the nodes involved to regard block as valid and proceed with its extension, or reject the invalid block.[79] Validating nodes are the part of decentralized system that is involved in decision-making, data storage, transaction verification and maintenance of consensus mechanism to ensure proper functioning of the blockchain.[80] These nodes store full copy of the chain, thus ensuring immutability, security and decentralized nature of the ledger.[81] Mining nodes are also involved in validating new transactions using consensus mechanism, thus generate new blocks with particular hash in conformity with that block. [82] Participating nodes are the computers storing synchronized data replications, and if blockchain user is connected to participating node, data may be then added to the ledger, but it has to go through validation process first.[83] Participating nodes are considered to receive the data to spread it between the participants, keep copies of certain parts of the chain and verify the transaction that is included in that part. [84]

To participate in the blockchain, generally, it requires installation of software, which is accessible to anyone with the connection to internet, thus this individual becomes a separate node with the right to add and store the data on the blockchain.[85] Since the network is available to everyone, the data is consequently visible to every user, but it is encrypted and hidden. [86] The network itself is transparent, thus information about blockchain transaction included in the block becomes available to every participant, and the hash, address of the parties, transaction value and block number, as well as location in particular cases may be seen. [87] The fundamental aspect is that although blockchain is supposed to facilitate privacy

[78]Tom Lyons, Ludovic Courcelas, Ken Timsit, "Blockchain and the GDPR", thematic Report for *The European Union Blockchain Observatory and Forum*, p.14. Published 16 October 2018. Available on: https://www.eublockchainforum.eu/reports. Accessed December 29, 2019.
[79]Christian Cachin, Marko Vukolic, "Blockchain Consensus Protocols in the Wild", IBM *Research* (2017): 1-24, p. 5 (Section 3.1. para. 4.). Download available at: https://arxiv.org/pdf/1707.01873. Accessed December 30, 2019.
[80]Nodes.com. Blockchain Nodes: An In-Depth Guide. Available on: https://nodes.com/. Accessed December 30, 2019.
[81]Ceyhun Necati Pehlivan, Inés Isidro Read, "Blockchain and Data Protection: A Compatible Couple?" (The Netherlands: Kluwer Law International BV, 2020), *Global Privacy Law Review*, Vol. 1, Issue 1 (2020): 39-48, pp.40-41. Available at: Kluwer Law.
[82]*Ibid*, p.41.
[83]Lyons, *supra* note 78.
[84]Ceyhun, *supra* note 82.
[85]*Ibid*.
[86]Tom Lyons, Ludovic Courcelas, Ken Timsit, "Blockchain and the GDPR", thematic Report for *The European Union Blockchain Observatory and Forum*, p.15. Published 16 October 2018. Download available on: https://www.eublockchainforum.eu/reports. Accessed November 14, 2019.
[87]Aleksei Gudkov, "Control on Blockchain Network," *Nova Law Review* 42, no. 3 (Spring 2018): 353-374, p.357.

and anonymity of the users, the data on the blockchain may not be anonymous to fall out of scope of the GDPR[88], rather pseudonymous, such as giving a pseudonym for individual user or organization in the transaction, or using hash to hide the information identifying the natural person. [89]

One of the crucial aspects of technological structure of the blockchain that complicates the exercise of right to erasure or right to be forgotten is immutability. Since the system entails that the previous blocks are added to the next but are not removed, blockchain is qualified as an append-only ledger. [90] DLT in its essence prescribes that the system shall preclude or complicate the task for individual to solely perform any modifications on previous transactions and their history.[91] This is realized by the fact that all participants of the blockchain have a shared supervision of access to the data and its transformation, making modification or erasure of the data almost impossible unless reaching an agreement of all nodes. [92] Immutability in blockchain is ensured through tamper-proof mechanism that presupposes that the data in the system cannot be changed or deleted when it is already added to the block.[93] Moreover, one of the most important considerations about blockchain's immutability in general is that the chain, which is already built, cannot be destroyed, thus any mistakes and uncertainties on the chain are irreversible. [94] It complicates the use of blockchain from users' perspective, because not only the user cannot modify or remove the data which may be inaccurate or wrong, but also at the same time user cannot exercise the right to erasure (right to be forgotten), due to immutability of all information that blockchain transaction

[88]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, p. 1–88. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679. Accessed February 7, 2020. Recital 26.

[89]Aleksei Gudkov, "Control on Blockchain Network," *Nova Law Review* 42, no. 3 (Spring 2018): 353-374, p.358.

[90]Chunpeng Ge, Siwei Sun, Pawel Szalachowski, "Permissionless Blockchains and Secure Logging", *ST Electronics - SUTD Cyber Security Laboratory, Singapore University of Technology and Design* (2019):1-5, p.1. Available at: arXiv:1903.03954 [cs.CR]. Download available at: https://arxiv.org/pdf/1903.03954v1.pdf.

[91]Michel Rauchs, Apolline Blandin, Keith Bear, Stephen McKeon, "2nd Global Enterprise Blockchain Benchmarking Study", *Cambridge Centre for Alternative Finance, University of Cambridge: Judge Business school* (2019): 1-72, p.13. Available on: https://www.crowdfundinsider.com/wp-content/uploads/2019/09/2019-ccaf-second-global-enterprise-blockchain-report.pdf . Accessed February 8, 2020.

[92]Dr Garrick Hileman & Michel Rauchs, "Global Blockchain Benchmarking Study", *Cambridge Centre for Alternative Finance, University of Cambridge: Judge Business school*, (2017):1-121, p.14. Available on: https://www.crowdfundinsider.com/wp-content/uploads/2017/09/2017-Global-Blockchain-Benchmarking-Study_Hileman.pdf . Accessed February 8, 2020.

[93]Fran Casino, Eugenia Politou, Efthymios Alepis, Constantinos Patsakis, "Immutability and Decentralized Storage: An Analysis of Emerging Threats" (2019): 4737-4744, p.4739, accessed February 3, 2020, doi: 10.1109/ACCESS.2019.2962017.

[94]Gudkov, ,*supra* note 89.

covers.[95] Yet, erasure or modification on the chain is not completely impossible, it could be done by rewriting the chain, but it does require technological resources that are expensive and may not be available to anyone.[96]

Theoretically, right to erasure and right to be forgotten cannot be realized on the blockchain, since the ledger is resistant to any modification or erasure of the data, or, that means that the implementation of the right cannot be achieved straightforwardly. The erasure process undermines technical structure of the blockchain, either erasure would require deconstruction of the blockchain backwards to the point where the data intended for erasure is located, including the piece of that data, but then reconstructing it again starting from the deleted concept to the end.[97] Since these measures are hard to implement every time the data subject makes a request for erasure and various technical resources are required to support them, instead of focusing on complete technical immutability of the blockchain, the conditions if certain blockchain can be modified need to be examined, taking into account whether all of the available resources allow any modification.[98]

2.1.2. Private blockchain

Among different types of blockchain, private blockchain is widely used by enterprises and governmental organizations, where the choice of private blockchain as an operating network is guided by the degree of control that organization exercises, because of established trust and transparency between the participants. Private blockchain is widely used among different businesses, it contributes to fast transactions, due to limited participation, which is especially relevant in financial sector, as well it reduces some costs associated with functioning and allows to perform work more efficiently.[99] Moreover, the use of private blockchain is expanding in commerce, also guided by the fact that the chain may facilitate not only the movement of assets, but also movement of goods and services, logistic services, replace notaries and use of supply-chains.[100] The main factor making private blockchain distinct from

[95]Aleksei Gudkov, "Control on Blockchain Network," *Nova Law Review* 42, no. 3 (Spring 2018): 353-374, p.372.
[96]Verypossible.com. Brian Zambrano, "Blockchain Explained: How Does Immutability Work?", available on: https://www.verypossible.com/blog/blockchain-explained-how-does-immutability-work. Published February 27, 2018. Accessed February 5, 2020.
[97]Pritesh Shah, Daniel Forester, Davis Polk Wardwell Llp, Matthias Berberich, Carolin Raspé, Hengeler Mueller, "Blockchain Technology: Data Privacy Issues and Potential Mitigation Strategies" , *Practical Law Data Privacy Advisor* (2019): p.6. Thomson Reuters, 2019.
[98]COINDESK. Gideon Greenspan, "The Blockchain Immutability Myth", available on: https://www.coindesk.com/blockchain-immutability-myth. Published May 9, 2017. Accessed February 10, 2020.
[99]Julie Frizzo-Barker, Peter A.Chow-White, Philippa R.Adams, Jennifer Mentanko, Dung Ha, Sandy Green, "Blockchain as a disruptive technology for business: A systematic review", *International Journal of Information Management* 51 (2020): 1-14, p.8. https://doi.org/10.1016/j.ijinfomgt.2019.10.014.
[100]*Ibid*.

other types is that the participants to the network are known and the permissions of who has an access and right to modify the data is limited, the transactions usually are processed by selected nodes in private blockchain, which could be verified by certain central authority or a database that approved and selected them.[101]

Private blockchain could be divided in two main groups currently used for different business purposes, being private permissioned and private permisionless. Private permissioned blockchain limits the information accessible to only participating nodes, thus *only optional* participating nodes can transact and view transaction log. [102] Permissioned network prescribes that the owner or an architect of this network determines the participation of nodes and confers responsibilities, which nodes are participating and which nodes are validating. [103] Private permissionless blockchain, similarly to permissioned also limits the access of who can transact and see the transaction log, however verification process is accessible to anyone. [104] Consortium blockchain also is widely used among groups of enterprises and may be put into the same category as private, however it may be looked upon as a combination of private and public blockchain. [105] In case of consortium, a group of organizations or individuals using the chain decides on rules, which nodes can participate in the chain, take part in validation process and consensus mechanism.[106]

Despite its decentralized nature, private blockchain may be regarded as creating similar structure to centralized system, thus conflicting with the essence of the blockchain *per se.*[107] Private blockchain in most of the cases would be owned by particular enterprise, consortium or an individual, to participate and access the network, the invitation from the creator, owner or administrator of private blockchain is required.[108] Private blockchain has a

---

[101]Petri Helo, Yuqiuge Hao, "Blockchains in operations and supply chains: A model and reference implementation", *Computers & Industrial Engineering* Vol. 136 (2019): 242-251, p.246. https://doi.org/10.1016/j.cie.2019.07.023. Available on: Science Direct database.

[102]Alexandre Anderberg, Amanda Andonova, Elena Bellia Mario, Calès Ludovic, Inamorato Dos Santos Andreia, Kounelis Ioannis, Nai Fovino Igor, Petracco Giudici Marco, Papanagiotou Evangelia,Sobolewski Maciej,Rossetti Fiammetta, Spirito Laura, ed. By Figueiredo Do Nascimento and Susana Roque Mendes Polvora, "Blockchain Now and Tomorrow" (Publications Office of the European Union, Luxembourg, 2019). Table 1: Examples of blockchain types, p.15. doi:10.2760/901029. Download available on: https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/blockchain-now-and-tomorrow. Accessed November 3,2019

[103]*Ibid.*

[104]*Ibid.*

[105]Muneeb Ul Hassan, Mubashir Husain Rehmani, Dr. Jinjun Chen, "Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions", *Future Generation Computer Systems* 97 (2019): 512-529, p.516, accessed December 5, 2019, https://doi.org/10.1016/j.future.2019.02.060.

[106]*Ibid.*

[107]Ceyhun Necati Pehlivan, Inés Isidro Read "Blockchain and Data Protection: A Compatible Couple?" (The Netherlands: Kluwer Law International BV, 2020), *Global Privacy Law Review*, Vol. 1, Issue 1 (2020): 39-48, p.41. Available at: Kluwer law.

[108]*Ibid.*

centralized entity supervising the system, which is an owner, creator or administrator that determines the participants to the network and decides on who can be involved in a mining process by having a degree of control over the system.[109] The fact that private blockchain has *dominant authority* brings it closer to centralized structure, although participants are distributed in accordance with their functions, that dominant authority could be regarded as giving permission to perform these functions and create rules applying to each of the participants engaged in the private chain.[110]

On the one hand, private blockchain also is considered an immutable network, but on the other hand it may not be completely accurate, since the immutability is satisfied only before an individual or an enterprise using it intervenes. Data on the blockchain may be altered in particular circumstances when all the participants involved in consensus mechanism agree upon that data modification. [111] On that account, assuming that the participants are limited and known within the organization using private blockchain, they may agree on consensus to modify and erase the data if necessary, since the dominant authority usually determines the consensus rules.[112] Thus, if that dominant authority has created the rules, the same authority can theoretically modify them in accordance to achieve the necessary means of erasure or data modification. Because all nodes part to the chain are completely under scrutiny of a particular organization or entity, on that account actions as restoring the process of the transaction may be allowed in accordance with the rules governing private blockchain, whether by modification of the rules or creating particular erasure governing rules at the beginning. [113] For example in case of consortium, it may provide for data modification or revoking the transaction, if all nodes controlling the chain agree, same applies for single organization, thus going contrary to chain's technical immutability and irreversibility, at the same time giving a chance for compatibility with the GDPR.[114]

---

[109]Ceyhun Necati Pehlivan, Inés Isidro Read "Blockchain and Data Protection: A Compatible Couple?" (The Netherlands: Kluwer Law International BV, 2020), *Global Privacy Law Review*, Vol. 1, Issue 1 (2020): 39-48, p.41. Available at: Kluwer law.

[110]Anisha Mirchandani, "The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR," Fordham Intellectual Property, *Media & Entertainment Law Journal* 29, no. 4 (Summer 2019): 1201-1242, p.1212.

[111]Cindy Compert, Maurizio Luinetti, Bertrand Portier, "Blockchain and GDPR: How blockchain could address five areas associated with GDPR compliance", *IBM Corporation (IBM Security) white paper* (2018): 1-8, p.6. Download available on: https://www.ibm.com/downloads/cas/2EXR2XYP. Accessed February 9, 2020.

[112]Mirchandani, *supra* note 110, p.1213.

[113]Rongyue Zheng, Jianlin Jiang, Xiaohan Hao ,Wei Ren , Feng Xiong, Yi Ren, "bcBIM: A Blockchain-Based Big Data Model for BIM Modification Audit and Provenance in Mobile Cloud", *Hindawi Mathematical Problems in Engineering* (2019) : 1-14, p.3, accessed March 2 ,2020, https://doi.org/10.1155/2019/5349538.

[114]Muneeb Ul Hassan, Mubashir Husain Rehmani, Dr. Jinjun Chen, "Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions", *Future Generation Computer Systems* 97 (2019): 512-529, p.516, accessed March 2, 2020, https://doi.org/10.1016/j.future.2019.02.060.

Private blockchain may allow the organization or the consortium to comply with the GDPR to particular extent, but it will depend on what are the organization's compliance requirements and obligations conferred upon entities in the chain, and, knowing the identity of the participants and their responsibilities, due to transparency of the chain.[115] As well as its structure similar to centralized computing may allow for intervention in functioning of the chain by modification of the rules or creating particular data erasure clause in protocol rules at the beginning, which would simplify the erasure process and applicability of the Regulation.[116]

3. CONTROLLER, JOINT-CONTROLLERS AND PROCESSOR IN BLOCKCHAIN

3.1. Controller

Although private blockchain does not clearly imply the controller and processor, determining the "controller" and "processor" clarifies the entities held responsible for the processing of personal data for the purposes of applicability of the Regulation. [117] Controller under the GDPR serves as a key element of data processing that has overall control and decision-making power over the data. [118] Article 4(7) of the GDPR defines the controller as an entity that solely or jointly determines the manner and purpose of how personal data is processed or collected, where this entity may be natural or legal person, agency and public authority. [119] The entity or criteria for the controller may also be determined by the law of the Union or its Member State, where the means and purposes of processing of personal data are laid down in the law of the Union or its Member State. [120]

Since GDPR is focused on centralized responsibility, meaning that the controller has to be at the core of the processing activities, the blockchain undermines this assumption, because its decentralized system has no specified entity to be regarded as a controller.[121]

---

[115]Ceyhun Necati Pehlivan, Inés Isidro Read "Blockchain and Data Protection: A Compatible Couple?" (The Netherlands: Kluwer Law International BV, 2020), *Global Privacy Law Review* 1, no. 1 (2020): 39-48, p.41. Available at: Kluwer law.

[116]*Ibid.*

[117]Tom Lyons, Ludovic Courcelas, Ken Timsit, "Blockchain and the GDPR", thematic Report for *The European Union Blockchain Observatory and Forum*, p.11. Published 16 October 2018. Download available on: https://www.eublockchainforum.eu/reports. Accessed February 5, 2020.

[118]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, p. 1–88. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679. Accessed November 4, 2019. Article 4(7).

[119]*Ibid.*

[120]*Ibid.*

[121]*Ibid.*

Commission Nationale de l'Informatique et des Libertés (CNIL) in its report suggests that any participant, which has the right to write and add data on the chain or send the data to nodes, can be classified as data controller in blockchain. [122] Firstly, to be the controller, the participant can be a natural person, when the data processing concerns commercial and professional activities that do not involve strict personal data to particular extent.[123] Secondly, the participant can be a legal person registering personal data in the blockchain, this action involves the recording of personal data of the client in the system and where such actions take place, a legal person that is responsible for this recording of personal data is a data controller. [124]

Following that, to determine the controller under the GDPR, the relevant analysis of Article 4(7) shall be applied to the blockchain users by understanding the roles of participants and interpretation of the article itself. Purposes of the processing in Article 4(7) determine the motivation why the data should be processed in the first place and role of the participants in data processing.[125] When entity determines purposes of the processing, it is regarded as *primary* indicator of who is the controller, because means of the processing may not be determined by the controller, but left to processors who follow the guidance of purposes provided by the controller. [126] By virtue of looking at the concept of "means of the processing", the technical and organizational questions are meant by this concept, including not only technical details, such as the choice of system that shall be used (for example private permissioned/permissionless blockchain), but assessment of what data should be collected, who is allowed to access the data and time limitation of processing activities. [127]

Thus, in blockchain, the controller may be the participant of the chain that uploads the data on the blockchain, which is logical, since in this case that participant uploads the data for specific purpose and decides on the way of the data processing – via blockchain. [128] Referring to permissioned or permisionless private blockchain, usually there is a legal entity as central operator of company or consortium, determining the means and purposes of processing

[122]The CNIL (Commission nationale de l'informatique et des libertés). *Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data*. Published November 6, 2018. Download available on: https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf. Accessed December 15, 2019.
[123]*Ibid.*
[124]*Ibid.*
[125]Article 29 Working Party. *Opinion 1/2010 on the concepts of "controller" and "processor" (WP 169)*, p. 13, available on: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf. Adopted February 16, 2010. Accessed March 2, 2020.
[126]*Ibid*.
[127]*Ibid*, p.14.
[128]International Finance Corporation. John Salmon, Gordon Myers, "Blockchain and Associated Legal Issues for Emerging Markets", p.3, available on: https://www.ifc.org/wps/wcm/connect/da7da0dd-2068-4728-b846-7cffcd1fd24a/EMCompass-Note-63-Blockchain-and-Legal-Issues-in-Emerging-Markets.pdf?MOD=AJPERES&CVID=mxocw9F. Accessed March 19, 2020.

personal data and exercising a particular degree of control over the blockchain by establishing governance rules determining the functions of participants, thus it may simplify the task of finding the controller. [129] By restricting some participants to upload the data on the chain, private blockchain may eliminate the variety of possible controllers, and minimize them to one particular entity, or number of entities, that may be regarded as the controller under the GDPR, depending on their functions on the chain.[130]

3.2. Processor

Pursuant to Article 4(8), a processor can be a legal or natural person, agency and public authority, or any other body that does process personal data on behalf of the controller. [131] Similar as the controller, the processor can take any legal form with an identifier to the data processing activities. [132]

Given regard to the blockchain and entity considered a processor in the system, it assumes the decision of the controller to assign all processing activities, or part of them to independent assignee, therefore it can be interpreted that nodes as a part of P2P network act as external data processors. [133]

In private blockchain apart from central operator, there are other participants involved in operating activities of the blockchain that could be regarded as processors, if they operate the system on behalf of that central operator, these participants may be nodes or entities engaged in blockchain mining (miners). [134] One of the particular points to be taken into account about the processors, the central operator of private blockchain or the consortium has to ensure the compliance of these entities with legal requirements and their accountability by

[129]Pritesh Shah, Daniel Forester, Davis Polk & Wardwell Llp, Matthias Berberich, Carolin Raspé, Hengeler Mueller, with Practical Law Data Privacy Advisor, "Blockchain Technology: Data Privacy Issues and Potential Mitigation Strategies", *Thomson Reuters* (2019): 1-8, pp. 4-5. Available on : https://www.davispolk.com/files/blockchain_technology_data_privacy_issues_and_potential_mitigation_strategies_w-021-8235.pdf. Accessed March 27, 2020.

[130]International Finance Corporation. John Salmon, Gordon Myers, "Blockchain and Associated Legal Issues for Emerging Markets", p.4, available on: https://www.ifc.org/wps/wcm/connect/da7da0dd-2068-4728-b846-7cffcd1fd24a/EMCompass-Note-63-Blockchain-and-Legal-Issues-in-Emerging-Markets.pdf?MOD=AJPERES&CVID=mxocw9F. Accessed March 19, 2020.

[131]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, p. 1–88. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679. Accessed November 15, 2019. Article 4(8).

[132]*Ibid.*

[133]Pritesh Shah, Daniel Forester, Davis Polk & Wardwell Llp, Matthias Berberich, Carolin Raspé, Hengeler Mueller, with Practical Law Data Privacy Advisor, "Blockchain Technology: Data Privacy Issues and Potential Mitigation Strategies", *Thomson Reuters* (2019): 1-8, p.5. Available on : https://www.davispolk.com/files/blockchain_technology_data_privacy_issues_and_potential_mitigation_strategies_w-021-8235.pdf. Accessed March 27, 2020.

[134]*Ibid*.

creating contractual relationship or agreements with them.[135] If central operator of private blockchain solely performs all activities in respect of that network, there may be no processors at all.[136]

3.3. Joint controllers

Pursuant to Article 26(1) of the GDPR, if two or more controllers determine the means and purposes of the data processing, these controllers shall be regarded as joint controllers. [137] The responsibilities shall be determined in a transparent manner for compliance with the GDPR. [138]

The transparent manner of allocating the responsibilities between each of the controller working jointly helps to ensure that freedoms and rights of the data subject in question are protected, so the controllership is not located in different organizations or spread between various natural persons. [139] Notwithstanding of what responsibilities are conferred to each of the joint controllers, data subjects have to be notified about the responsibilities, which are to be determined by the arrangement between the controllers, unless the responsibilities are provided by national law of the Member State to which the controllers are subject. [140] WP29 clarifies that the contractual arrangement between joint controllers has to determine the responsibilities of the lead controller - controller that is responsible for overall compliance with the Regulation, including the notification of the competent authorities when the breach occurs. [141]

---

[135]Pritesh Shah, Daniel Forester, Davis Polk & Wardwell Llp, Matthias Berberich, Carolin Raspé, Hengeler Mueller, with Practical Law Data Privacy Advisor, "Blockchain Technology: Data Privacy Issues and Potential Mitigation Strategies", *Thomson Reuters* (2019): 1-8, p.5. Available on : https://www.davispolk.com/files/blockchain_technology_data_privacy_issues_and_potential_mitigation_strategies_w-021-8235.pdf. Accessed March 27, 2020.

[136]*Ibid*.

[137]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, p. 1–88. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679. Accessed November 22, 2019. Article 26(1).

[138]*Ibid.*

[139]David Allessie, Maciej Sobolewski, Lorenzino Vaccari "Blockchain for digital government", *Publications Office of the European Union* (2019):1-88, p. 12. Accessed November 12, 2019. doi:10.2760/942739.

[140]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, p. 1–88. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679. Accessed November 22, 2019. Article 26.

[141]Article 29 Data Protection Working Party. *Guidelines on Personal data breach notification under Regulation 2016/679*, p.13. Available on: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052. Last adopted on February 6, 2018. Accessed February 18, 2020.

Since blockchain has a number of participants that may be dealing with personal data, joint-controllership may be assumed. [142] However, generally there is no arrangement between participants that is required under GDPR to qualify as joint-controllers and the contribution may be different, thus only in individual cases joint-controllership could be justified, due to the fact that although participants are considered equal in the network, their functions and influence on other participants still have to be accessed individually.[143] As an example, in a case of the consortium, when blockchain is joined and used by number of companies for their own purposes, including new entries of personal data, these companies may qualify as joint-controllers, however it is still a subject to individual assessment and the arrangement.[144] Otherwise, the consortium would have a main controller as a particular organization where other organizations would be controlled by that organization.[145] Main controller would be then determined by contribution, ownership, and the governing rules, so it is assumed that data protection rules would be a duty of the dominant controller organization. [146]

4. PERSONAL DATA IN BLOCKCHAIN

According to Article 4(1), personal data is any information, which is directly or indirectly identified and identifiable, including information on the data subject like genetic, physical, economic, social and cultural, physiological, and mental that in particular has to be linked to the data subject. [147] Article 4(1) in the GDPR also provides the possibility of having data that in itself is not considered personal, but in conjunction with additional information becomes personal data.[148]

For the Regulation to apply, the data in blockchain has to qualify as personal data conforming to Article 4(1). For the purposes of determining which data falls within the notion

[142]Dr. Dennis-Kenji Kipker, Hauke Bruns, "Blockchains für Versorgungsketten im Lebensmittelsektor und der Datenschutz", *Computer und Recht* 3 (2020):210-216, pp.214-215.
[143]*Ibid.*
[144]Pritesh Shah, Daniel Forester, Davis Polk & Wardwell Llp, Matthias Berberich, Carolin Raspé, Hengeler Mueller, with Practical Law Data Privacy Advisor, "Blockchain Technology: Data Privacy Issues and Potential Mitigation Strategies", *Thomson Reuters* (2019): 1-8, p.5.. Available on : https://www.davispolk.com/files/blockchain_technology_data_privacy_issues_and_potential_mitigation_strategies_w-021-8235.pdf. Accessed March 27, 2020.
[145]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, p. 1–88. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679. Accessed November 22, 2019. Recital 37.
[146]*Ibid.*
[147]*Ibid,* Article 4(1).
[148]*Ibid.*

of personal data, the data can be divided in two categories, such as personal identifiable information, and information being potentially identifiable. [149]

a.) Personal identifiable information shall undeniably fall under Article 4(1) as being a data having direct link to the data subject, that is a possibility for the data subject to be exactly identifiable in a sample of other data subjects. [150] Personal identifiable information can contain the name and surname of the data subject, which has to be linked with one of the identifiers mentioned further, since a name itself cannot point at a particular person.[151] As well as identification, which contains passport, social security codes, ID number or other similar documentation, habitual or workplace address, biometrics and biological information, credit card information, as well as phone number or data related to online environment such as login to the website, password and email, or digital identity. [152]

b.) Potentially identifiable information is a more complicated notion, since for identification of the particular person data shall be combined with personal identifiable information to create a full profile of an individual. [153] One of the particular types that the GDPR provides is that the data subject can be associated with an online identifier, which relates to the device used by the individual, to be precise, applications, different tools and internet protocols (IP), cookies, radio frequency, personalized advertising, fingerprints and face recognizing tools. [154] For such identifiers to be associated with the data subject the online identifier has to leave a *trace* that combined with other distinct identifiers, in particular, those included in personal identifiable information, and as well, additional information, together may denote to a particular data subject.[155]

[149]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 (2019): 80-91, p.83, accessed January 20,2020, https://doi.org/10.1515/comp-2019-0005.
[150]*Ibid.*
[151]Information Commissioner's Office. What are identifiers and related factors, available on: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-are-identifiers-and-related-factors/. Accessed January 5, 2020.
[152]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 (2019): 80-91, p.83, accessed January 20,2020, https://doi.org/10.1515/comp-2019-0005.Table 1.
[153]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 (2019): 80-91, pp.82-83, accessed January 20,2020, https://doi.org/10.1515/comp-2019-0005.
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, p. 1–88. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679. Accessed January 9, 2020. Recital 30.
[155]*Ibid.*

4.1.Personal data in private blockchain

When reviewing the personal data on the blockchain, to safeguard personal data, blockchain uses cryptography, which does not disclose any visible personal data at first glance. However, some of the data in encrypted form could still lead to personal data pursuant to GDPR, thus the examination of each component under the GDPR is mandatory. To determine whether private blockchain does include personal data, the crucial factor is to understand whether data, which by its technological functions is encrypted or converted into hash, could still be regarded as personal data in conformity with the GDPR.

4.1.1. Encrypted data

Blockchain uses various ways how to ensure safety of the data, so the information about the parties and inside of the transaction would not be disclosed to any third party and ensuring that information disclosed may not be undoubtedly regarded as personal data. Encryption is a data protection in digital era, where the data subject is provided confidentiality and integrity with respect to personal data. [156]

According to WP29, encryption could be a way of ensuring confidentiality of ones' personal data only with the correct implementation, thus covering all the transactions and natural person's data so the result is guaranteed and secure confidentiality of the parties.[157] Although encryption could serve as a contribution to safeguarding personal data, encrypted data does not become automatically anonymous to *fall out* of the scope of GDPR, via encryption, the data becomes pseudonymous, as personal data takes another form that reduces the linkability to data subject, however it does not prevent the occurrence of re-identification of the data subject with particular identifiers.[158]

4.1.2. Public and private keys

Each user of the blockchain is given a code of letters or numbers that represent the particular data subject, which is being shared with others to initiate and participate in the transaction,

[156]Article 29 Data Protection Working Party. *Statement of the WP29 on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU*, p. 1, available on: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622229. Published April 11 2018. Accessed February 16, 2020.
[157]*Ibid*.
[158]GDPR Report. Data masking: anonymization or pseudonymization?, available on: https://gdpr.report/news/2017/09/28/data-masking-anonymization-pseudonymization/ . Published September 28, 2017. Accessed February 15, 2020.

this code of letters is called public key. [159] Public key is regarded as publicly available information that is essential for identification of the person.[160]

Public key is a mathematical algorithm that includes linking the public key, with specific private key granted to each of the participants of the transaction, so later the data encrypted through the public key can be decrypted with the private. [161] The keys have to match with the piece of the data, so that the transaction is being broadcasted to other participants to be verified and written on the chain.[162] For simple transaction to occur, the blockchain user with the given public key encrypts a plain text message to a particular recipient, that recipient has to have user's private key to see the data, so by virtue of private key the message may be decrypted.[163] All the users that have corresponding private key have an access to the data encrypted and can check whether public key belongs to the person who initiates the transaction via certificate.[164] Public/private key is reversible encryption, or, asymmetric encryption, given that the plain text encrypted in/by public key (which could be an identity of the person or financial account) is easily reversed by using corresponding private key.[165] Hence, it is paramount for any blockchain user to secure its private key, when disclosing to other users or preserve it, so it would not be available to non-trusted third parties, giving access to user's data.[166]

In practice, there have been cases where the identification of the data subject occurred through use of public key, if identity of the data subject behind the encrypted data is revealed that could also lead to disclosure of all the transactions of the public key owner. The data could be disclosed voluntarily for different purposes, where in some cases through means of particular technology or service provider, one public key could be decrypted with the other public key of the same person, if person did disclose multiple public keys. [167] Data may be

---

[159] Tom Lyons, Ludovic Courcelas, Ken Timsit, "Blockchain and the GDPR", thematic report for *The European Union Blockchain Observatory and Forum*, p.19. Published 16 October 2018. Download available on: https://www.eublockchainforum.eu/reports. Accessed February 18, 2020.

[160] Blockchain.com. Public and private keys, available on: https://support.blockchain.com/hc/en-us/articles/360000951966-Public-and-private-keys. Accessed February 19, 2020.

[161] Tom Lyons, Ludovic Courcelas, Ken Timsit, "Blockchain and the GDPR", thematic report for *The European Union Blockchain Observatory and Forum*, p.19. Published 16 October 2018. Download available on: https://www.eublockchainforum.eu/reports. Accessed February 18, 2020.

[162] Reggie O'Shields, "Smart Contracts: Legal Agreements for the Blockchain," *North Carolina Banking Institute* 21 (2017): 177-194, p.180.

[163] Jessica Schroers, "Are public keys personal data?", available on: https://www.law.kuleuven.be/citip/blog/are-public-keys-personal-data/. Accessed January 29, 2020. Published May 8, 2018.

[164] *Ibid*.

[165] Tom Lyons, Ludovic Courcelas, Ken Timsit, "Blockchain and the GDPR", thematic report for *The European Union Blockchain Observatory and Forum*, p.20. Published 16 October 2018. Download available on: https://www.eublockchainforum.eu/reports. Accessed February 18, 2020.

[166] O'Shields, *supra* note 162.

[167] Fergal Reid, Martin Harrigan "An Analysis of Anonymity in the Bitcoin System", *Clique Research Cluster, Complex & Adaptive Systems Laboratory University College Dublin, Ireland* (2012): 1-26, p.16. Available at: arXiv:1107.4524v2 [physics.soc-ph]. Download available at: https://arxiv.org/pdf/1107.4524.pdf.

disclosed through illegal means, such as data leaks from the company, or through additional information that could lead to connection of public key to particular individual, or when it is needed in conformity with regulatory requirements such as anti - money laundering provisions, as well as commercial purposes, and other such as know your customer policy. [168] Public keys also could be connected and traced back to IP address of the data subject, unless the user uses anonymizing browser.[169]

Thus, personal data in public key only would exist straightforwardly if the public key denotes to specific *natural* person, but, by means of cryptography, public key is deprived of any identifiers that can point to the specific data subject. [170] As data is encrypted, public key has to be matched with additional personal identifiable information to qualify as personal data, where Recital 30 of the GDPR mentions particular identifiers leaving traces, so the identifier can be connected to specific data subject. [171] Provided that, public key may be traced back to IP address of the data subject, which is regarded as one of the potential online traces to identify certain individual. [172] If, after examination of IP address and additional information, having multiple public keys that may denote to particular data subject, as well as actions performed with public/private keys related to regulatory requirements and commercial policies allow building a profile of the data subject that would mean that public key in this case *cannot* completely secure personal data to the extent needed. [173]

Following that, public keys may be regarded as pseudonymous data under the GDPR, which still falls under the scope of protection of the Regulation. [174] Thus, public key may include personal data that could be accessed by either having private key for decryption or combining public key with any additional identifiers pointing to specific natural person, consequently, is a subject to data protection under the GDPR. Nevertheless, when determining whether the data can be attributed to a specific individual, the content, such as what is included in the public key and whether that information contains personal data, as

[168]Muneeb Ul Hassan, Mubashir Husain Rehmani, Dr. Jinjun Chen, "Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions", *Future Generation Computer Systems* 97 (2019): 512-529, p.518. https://doi.org/10.1016/j.future.2019.02.060.
[169]Fergal Reid, Martin Harrigan "An Analysis of Anonymity in the Bitcoin System", *Clique Research Cluster, Complex & Adaptive Systems Laboratory University College Dublin, Ireland* (2012): 1-26, p.17. Available at: arXiv:1107.4524v2 [physics.soc-ph]. Download available at: https://arxiv.org/pdf/1107.4524.pdf.
[170]*Ibid*.
[171]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, p. 1–88. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679. Accessed January 28, 2020. Recital 30.
[172]*Ibid*.
[173]*Ibid*.
[174]*Ibid*, Recital 26.

well as purposes for processing and consequences of processing activities shall be subject to proper examination. [175]

4.1.3. Hash functions

Although hashing may be considered as one of the most secure mechanisms of data protection in the blockchain, there is still an on-going debate about does the hash data in fact then constitute anonymous data.[176] If examining it under the GDPR in strict sense, hashing does not necessarily turn the data concerned into anonymous data, consequently in most cases hash would constitute pseudonymous data. [177]

To give a brief overview, in the first place, the transaction, which is a new data entry, is converted into a hash transaction[178], which mathematically secures the transmission of the transaction for a particular recipient, so it later can be added to the ledger.[179] Hash is of a limited length that does not change depending on the amount of the data input. Therefore when the data exceeds the fixed amount of how much the hash can remember, the system does not remember the data itself, but it keeps the track of the hash, which is an output result of the data and is resistant to any modification. [180] Hash transaction usually involves basic information on the parties, such as who is a sender/receiver, contains data and time of performance of the transaction itself, type of the transaction and quantity, if it concerns assets.[181] When the data is hashed, it is merged with other hashes that were coded approximately at the same time of the hash concerned, to form a block that is later added to the ledger. [182]

Hash is an encryption that replaces identifiers of the data subject with a particular pseudonym that can be reversed only in individual cases and at the first sight does not

[175]Information Commissioner's Office. What is personal data?, available on: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/. Accessed March 3, 2020.
[176]Anisha Mirchandani, "The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR," *Fordham Intellectual Property, Media & Entertainment Law Journal* 29, no. 4 (Summer 2019): 1201-1242, p.1224.
[177]*Ibid*.
[178]Vida J. Morkunas, Jeannette Paschen, Edward Boon, "How Blockchain Technologies Impact Your Business Model", *Kelley School of Business, Indiana University* (2019):1-12, p.2, accessed February 10, 2020, https://doi.org/10.1016/j.bushor.2019.01.009. Published by Elsevier Inc. Available on: https://fardapaper.ir/mohavaha/uploads/2019/08/Fardapaper-How-blockchain-technologies-impact-your-business-model.pdf Available at: Science Direct database.
[179]Blockgeeks. Ameer Rosic, "What Is Hashing? [Step-by-Step Guide-Under Hood of Blockchain]", available on: https://blockgeeks.com/guides/what-is-hashing/. Accessed: March 2, 2020.
[180]*Ibid.*
[181]*Ibid.*
[182]Jake Goldenfein, Dan Hunter, "Blockchains, Orphan Works, and the Public Domain," *Columbia Journal of Law & the Arts* 41, no. 1 (2017): 1-44, p. 8.

disclose anything about party to the transaction.[183] By means of cryptography, hash is only one-way algorithm, that means that by having the hash it is mostly unlikely that someone can obtain the data which is hashed, although it determinate hash relates to particular piece of data. [184] However, it also explains why obtaining the data included in hash is referred to as *infeasible*, rather than completely impossible, since each hash output corresponds to a particular data input, data input may be derived if the quantity of data is relatively small.[185] Although hash is supposed to be irrevocable, if hash is used as a single identifier, it significantly increases the risk of re-identification of the original data input by using statistical and computation methods.[186] If the identifiers and personal data of the data subject is linked to the hash, that makes it more vulnerable and open to linkability risks, consequently the amount of personal data contained in the hash increases the risk of it identification, since identifying at least one of the data pieces contained in it may lead to identification of another. [187] Thus, hashing may not be regarded as anonymous, to fall out of the GDPR.

This applies to additional identifiers that may intersect with personal data, which are called pseudo identifiers (or indirect identifiers), as a result of a) hash is supposed to connect these indirect identifiers with one another in accordance with the purposes of the processing carried out, b) hash is linked to any indirect identifier apart from purposes of the processing carried out. [188] There could be cases when additional information which was not firstly included in original processing may allow for identification of the contents of the hash, such as the date of hashing, that in some circumstances may be connected to other figures completed at that time, as well as the position of the hash can lead to particular information stored at the same date or before, as well as details related to computing services, access to these services and other similar information pieces may serve as identifiers. [189]

---

[183]Anisha Mirchandani, "The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR," *Fordham Intellectual Property, Media & Entertainment Law Journal* 29, no. 4 (Summer 2019): 1201-1242, p.1224.

[184]Cindy Compert, Maurizio Luinetti, Bertrand Portier, "Blockchain and GDPR: How blockchain could address five areas associated with GDPR compliance", *IBM Corporation (IBM Security) white paper* (2018): 1-8, p.7. Download available on: https://www.ibm.com/downloads/cas/2EXR2XYP. Accessed February 9, 2020.

[185]Blockgeeks. Ameer Rosic, "What Is Hashing? [Step-by-Step Guide-Under Hood of Blockchain]", available on: https://blockgeeks.com/guides/what-is-hashing/. Accessed: March 2, 2020.

[186]European Data Protection Supervisor, Agencia Española de Protección de Datos | AEPD. *Introduction to the Hash Function as a Personal Data Pseudonymisation Technique*, p.12. Available on: https://edps.europa.eu/sites/edp/files/publication/19-10-30_aepd-edps_paper_hash_final_en.pdf, Accessed March 11, 2020.

[187]*Ibid*, p.13

[188]European Data Protection Supervisor, Agencia Española de Protección de Datos | AEPD. *Introduction to the Hash Function as a Personal Data Pseudonymisation Technique*, p.14. Available on: https://edps.europa.eu/sites/edp/files/publication/19-10-30_aepd-edps_paper_hash_final_en.pdf, Accessed March 11, 2020.

[189]*Ibid.*

What is more, deriving the data may be available through use of "bruce-force method", which involves having a data input from the sample of the data, then hashing it and trying to find the matching hash, thus determining where is the data concerned, however the process would be lengthy and hard to achieve, since it requires vast technological resources for computation. [190]

4.1.4. Transactional data

Transactional data is usually referred to the data used in blockchain, mainly the data purely about the transaction. [191] The list of personal data included in transactional data is non-exclusive and varies on a case-by-case basis, depending on the purpose of organization using private blockchain.

Usually, transaction data includes information about blockchain users, details about the transaction, time of performance, as well as other relevant information, such as location of the user, information concerning financial services, contracts. [192] For example, transactional data may contain personal data such as name, address, birth date, academic information, financial information, personal identification numbers, wallet and other, which would qualify as personal data pursuant to GDPR.[193]

There is a possibility when transactional data would not be considered personal data, if it concerns transfer of the particular information that cannot be linked to the data subject. As an example, an asset transferred from one party to another without any additional information and specification of the asset, which may be information that is not related to *natural person*, but is used for any scientific purposes.[194] As well, that information is consequently deprived of any identifiers.[195] However, thinking logically, most of the time transactional data would deal with personal data that falls under the GDPR, especially in cases where the data concerns natural person. If organization is established for financial or commercial purposes, it is likely that there would be personal data of the natural person circulating in the transactions between natural person and organization, B2B transactions, and their business partners as well serving

[190]Blockgeeks. Ameer Rosic, "What Is Hashing? [Step-by-Step Guide-Under Hood of Blockchain]", available on: https://blockgeeks.com/guides/what-is-hashing/. Accessed: March 2, 2020.
[191]Debra Zahay, James Peltier, Don Schultz, Abbie Griffin, "The Role of Transactional versus Relational Data in IMC Programs: Bringing Customer Data Together", *Journal of Advertising Research* 44 no.1 (2004): 3-18, p.6, accessed February 27, 2020, https://doi.org/10.1017/S0021849904040188.
[192]GoCoding. Barry Allen, "Transaction Data in Blockchain". Available on: https://gocoding.org/transaction-data-in-blockchain/. Published June 30, 2019. Accessed March 12, 2020.
[193]Michèle Finck, "Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?", *European Parliamentary Research Service* (2019): 1-101, p. 28, accessed March 13, 2020, doi: 10.2861/535. Brussels, European Union, 2019.
[194]*Ibid.*
[195]*Ibid.*

as third parties. Hence, if the data contained in the transaction in direct or indirect way can lead to specific natural person, taking into account that encrypting, pseudonymizing or hashing data neither completely protect personal data, nor turn it into anonymous data, therefore transactional data may be considered as personal.

5. PART Ⅲ: POSSIBLE APPROACHES TO MITIGATION OF GDPR ENFORCEMENT ON THE COMPANIES USING PRIVATE BLOCKCHAIN

Some data that may be subject to GDPR is ultimately stored in the blockchain, starting from financial data if blockchain is being used by financial institution, followed by names of participants, timestamps and pseudonymous data, as well as non-equivocation or security logging, moreover the list is non-exhaustive. [196] In spite of the fact that immutability of the blockchain makes the erasure of the data stored in the network almost impossible, private blockchain may allow for some modifications.

As for organization using private blockchain, considering both legal and moral reasoning, this organization sooner or later would be bound by the obligation to erase data subject's personal data upon request, either it is stored on the blockchain or not. [197] The erasure of data subjects' personal data may be a complicated task for organization, therefore before the request for the data erasure appears, it is of the utmost importance for organization to follow the compliance of the processing activities carried out.[198]

5.1. Regulating "unwanted" data

It may be assumed if the organization choses to use private blockchain as an operating network, taking into account that it is an append-only ledger, it is likely that the organization may not want to store personal data on the chain or minimize the inflows of personal data, to avoid complete immutability. Minimization principle is also enshrined in the GDPR as principle of lawful data processing under Article 5(1) c, thus the organization must find the balance between that data that is necessary for blockchain transaction, and the data that may be excluded or separated.[199] Regulating the data that an organization should avoid storing on

[196]Martin Florian, Sophie Beaucamp, Sebastian Henningsen, Björn Scheuermann, "Erasing Data from Blockchain Nodes": 1-10, p.1. Available at: arXiv:1904.08901v1 [cs.CR]. Download available at: https://arxiv.org/pdf/1904.08901.pdf.
[197]*Ibid*.
[198]IT Governance Privacy Team, *EU General Data Protection Regulation (GDPR): an implementation and compliance guide* (Ely, Cambridgeshire, United Kingdom: IT Governance Publishing, 2017), p.193.
[199]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, p. 1–88. Available on:

the chain implies detecting the content and its filtering, as well as changing protocols (which are the consensus mechanism for nodes to validate the transaction[200]) or developing erasure clause in the protocol. [201]

There is an interesting model of regulating unwanted data used by MyHeathMyData (MHMD) project, which is a consortium private blockchain, where all the personal information is filtered and is in possession of the controller inside a central server. [202] The mapping function located outside the chain is a result of recording metadata, which allows the personal data to be mapped to the blockchain.[203] This type of model allows erasing the link between personal data contained in mapping function and the blockchain itself, eliminating the possibility of linking erased data to the chain from the central server. [204]

5.2. Data erasure in blockchain

5.2.1. Pseudonymization

In Article 4(5), the notion of pseudonymization is provided as the processing of the data in a way, when a particular personal data cannot be associated with the particular data subject without being connected to specific additional information that can lead to identification of that data subject. [205] The core idea is that this additional information shall be separated from personal identifiable information in the first place, which is a task of ensuring proper degree of technical and organizational measures, so there is no possibility of the data being attributed to identified or identifiable natural person. [206]

Off-chain data storage may be connected to pseudonymization, where Recital 29 of the GDPR provides that any data that could be attributed to natural person shall be kept separately.[207] Notwithstanding the fact that pseudonymization is used in the blockchain itself

---

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679. Accessed March 4, 2020. Article 5.

[200]Cryptomaniaks.com. Michael R., "What is a Blockchain Protocol?". Available on: https://cryptomaniaks.com/blockchain-protocols-list-explained#h2-0. Accessed March 5, 2020.

[201]Martin Florian, Sophie Beaucamp, Sebastian Henningsen, Björn Scheuermann "Erasing Data from Blockchain Nodes", : 1-10, p.1. arXiv:1904.08901v1 [cs.CR]. Download available at: https://arxiv.org/pdf/1904.08901.pdf.

[202]Global engage. When Blockchain Meets the Right to be Forgotten: Technology Versus Law, available on: http://www.global-engage.com/life-science/when-blockchain-meets-the-right-to-be-forgotten-technology-versus-law/. Published May 2, 2018. Accessed April 13, 2020.

[203]*Ibid.*

[204]*Ibid.*

[205]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, p. 1–88. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679. Accessed January 13, 2019. Article 4(5).

[206]*Ibid.*

[207]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

by means of encryption, it could be also used for the data contained in the off-chain database[208], where pseudonymization of that data would reduce linkability risks and data-identification possibilities to the minimum. As an example, if name and surname, or financial data such as credit card number or wallet data off-chain would be replaced by the set of random numbers or letters, that significantly reduces the risk of identification if the data becomes visible to other apart the controller.[209] Nevertheless, the organization has to understand that if there is a risk of re-identification, even if the data has undergone pseudonymization process, in conformity with Recital 26 of the GDPR it is still personal data.[210]

5.2.2. Anonymization

Anonymization prescribes identifying personal identifiable information that can be linked to individual and protecting it by means of anonymization. [211] To achieve anonymization process correctly, the organization must have a clear-set objectives and technological prerequisites, as well as the controller must monitor the risks arising in connection with data anonymization, since there is no absolute guarantee of anonymous data being impossible to connect to an identifiable person, especially with constant developing technology.[212]

As anonymization may be used as *irreversibl*e prevention of identification of the natural person, it could be a possible solution for mitigation of the enforcement of the Regulation for organization.[213] WP29 in its guidelines on anonymization provides that it could serve as permanent data *erasure* or retention, because it is not possible to connect

---

repealing Directive 95/46/EC (General Data Protection Regulation), *OJ L* 119, 4.5.2016, p. 1–88. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679. Accessed March 14, 2020. Recital 29.

[208]Dr. Dennis-Kenji Kipker, Hauke Bruns, "Blockchains für Versorgungsketten im Lebensmittelsektor und der Datenschutz", *Computer und Recht* 3 (2020): 210-216, p. 216.

[209]Logic2020. GDPR compliance: pseudonymization vs. anonymization, available on: https://www.logic2020.com/insight/gdpr-compliance-pseudonymization-vs-anonymization. Accessed March 25, 2020.

[210]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, p. 1–88. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679. Accessed February 11, 2020. Recital 26.

[211]Muneeb Ul Hassan, Mubashir Husain Rehmani, Dr. Jinjun Chen, "Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions", *Future Generation Computer Systems* 97 (2019): 512-529, p.523. https://doi.org/10.1016/j.future.2019.02.060.

[212]Article 29 Data Protection Working Party. *Opinion 05/2014 on Anonymisation Techniques*, p.3. Available on: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Adopted April 10, 2014. Accessed March 10, 2020.

[213]*Ibid*, p.4.

anonymous data to the data subject or process that data.[214] This makes anonymization sufficient as erasure on the blockchain, whilst physical erasure on immutable ledger may not be possible, organization may rely on different anonymization techniques to be GDPR-compliant, by anonymizing data on the chain.[215] Nevertheless, the controller must be aware of possible ways how to avoid unnecessary costs that could result in overspending of organizations' financial resources and exposing unnecessary personal data by virtue of implementing those anonymization techniques.[216]

5.2.3. GDPR enforcement and off-chain data storage

If the data in private blockchain appears to fall under personal data, off-chain storage would simplify the applicability of the Regulation if the data is of a significant amount and sooner or later may be subject to erasure or modification.[217] Generally, this would mean that information stored in the off-chain would contain specific data that could be accessed when needed, excluding complicated steps of deconstruction and re-building of the chain, or creating new rules for consensus protocol.

Off-chain data storage may include different documentation, sensitive information on the parties, for example the information included in images, PDF, text, WORD documents and similar, that may be personal data containing documents. [218] If organization requires any type of agreement between customers and the company, as well as third parties, there is a possibility to store the contract on the chain. However, the data related to the parties, such as verification of receiving the purchased asset, or any evidence that may be seen as personal data off-chain, whilst the off-chain information would be linked by the hash to the chain.[219]

However, linking data to the chain also creates difficulties, since hash represents a logical link between chain of blocks, thus if the data in one block changes, subsequently the hash value would also change, and, the corresponding hash would still contain traces of

[214]Article 29 Data Protection Working Party. *Opinion 05/2014 on Anonymisation Techniques*, p.7. Available on: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Adopted April 10, 2014. Accessed March 10, 2020.
[215]*Ibid*, *Opinion 05/2014 on Anonymisation Techniques*, Annex: A primer on anonymisation techniques.
[216]Article 29 Data Protection Working Party. *Opinion 05/2014 on Anonymisation Techniques*, p.8. Available on: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Adopted April 10, 2014. Accessed March 10, 2020.
[217]IBM Storage. "Why new off-chain storage is required for blockchains", *International Business Machines Corporation* (2018): 1-11, p.5. Download available on: https://www.ibm.com/downloads/cas/RXOVXAPM. Accessed March 12, 2020.
[218]IBM Storage. "Why new off-chain storage is required for blockchains", *International Business Machines Corporation* (2018): 1-11, p.5. Figure 3: Example off-chain data. Download available on: https://www.ibm.com/downloads/cas/RXOVXAPM. Accessed March 12, 2020.
[219]IBM IT Infrastructure Blog. Storage for blockchain and modern distributed database processing, available on: https://www.ibm.com/blogs/systems/storage-for-blockchain-and-modern-distributed-database-processing/. Published February 8, 2019. Accessed April 13, 2020.

personal data. [220] The solution that could be implemented is the creation of erasure database that would include all of the references to the deleted units (which shall be pseudonymized), that consequently would minimize risk of linkability.[221]

If conducting daily business activities prescribes personal data, all or big part of the data deemed personal shall be stored off-chain, if possible, based on the fact that even the data is encrypted, it may not ensure complete protection of personal data and does not eliminate the risks of data leaks and re-identification in definite circumstances, especially since businesses *do* deal with numbers of personal data related to their customers, partners and employees. [222]

5.2.4. GDPR enforcement and public/private keys

Since public/private keys contain personal data, entity to which the request for data erasure was made by the data subject, can ensure the compliance with the Regulation by using data sanitization. Data sanitization could be described as an intentional process of permanent destruction of personal data in irreversible manner, that prescribes that after the device is undergone the process of data sanitization, even with the intervention of particular tools intended for data recovery, data cannot be restored. [223]

Data sanitization may be achieved by physical destruction of the data, erasure of the data and cryptographic erasure. [224] As per blockchain, cryptographic erasure would erase public or private key, by using encryption software on the entire device that stores the data. [225] This encryption software has to be installed by default, so it can immediately react to erasure of that key replacing it with other, or permanently erasing the original key. [226] It is recommended that private decryption key would be stored in off-chain database with pseudonymized references to it, pursuant to other documents containing personal data, so it could be easily destroyed.[227]

---

[220]Leiyong Guo, Hui Xie, Yu Li, "Data Encryption based Blockchain and Privacy Preserving Mechanisms towards Big Data", *J. Vis. Commun. Image R.* (2019): 1-11, p.3. doi: https://doi.org/10.1016/j.jvcir.2019.102741.

[221]Martin Florian, Sophie Beaucamp, Sebastian Henningsen, Björn Scheuermann, "Erasing Data from Blockchain Nodes": 1-10, p.2. Available at: arXiv:1904.08901v1 [cs.CR]. Download available at: https://arxiv.org/pdf/1904.08901.pdf.

[223]International Data Sanitization Consortium. Data Sanitization Terminology and Definitions, available on: https://www.datasanitization.org/data-sanitization-terminology/. Accessed March 16, 2020.

[224]*Ibid.*

[225]*Ibid.*

[226]*Ibid.*

[227]Dr. Dennis-Kenji Kipker, Hauke Bruns, "Blockchains für Versorgungsketten im Lebensmittelsektor und der Datenschutz", *Computer und Recht* 3 (2020):210-216, p. 216.

5.2.5. GDPR enforcement and hash function

If the data was disclosed by virtue of hash, the possible solution for an organization willing to modify the data on the chain to comply with the requirements of the GDPR is use chameleon hash functions. [228] The characteristic that makes chameleon hash beneficial is that it allows trusted participants, as it is in private blockchain to have an access to that hash by a particular key called trapdoor, which allows to them to use the key for calculating hash collisions and change the data published without interfering into chain integrity, thus removing the connection between data and the remaining hash. [229] However, this again may be seen as conflicting with blockchain immutability, if the unit on the chain may be modified, it does not make a difference if the database chosen by an organization is blockchain, or other centralized data storage method.

5.2.6. GDPR enforcement and transactional data

In most cases, if the erasure of the data is requested under Article 17, the data had been processed, stored and collected already over some time on the chain.[230] The possible way how the organization can ensure the compliance with the GDPR if the data part is needed to be erased from the transaction is to extend the software used by the node that participates in private blockchain and merely deals with the data subjects' data.[231] That extension would grant a possibility for single or couple of nodes (that would not be problematic for the private chain) to mark the units in the transaction intended for erasure without changing the initial protocol and reaching the consensus between other nodes.[232]

6. GOVERNANCE

6.1. On-chain and off-chain governance

To correctly achieve the erasure of data subjects' personal data within an organization, not all the technological possible solutions have to be implemented, but the crucial factor is to

[228]Martin Florian, Sophie Beaucamp, Sebastian Henningsen, Björn Scheuermann, "Erasing Data from Blockchain Nodes": 1-10, p.2. Available at: arXiv:1904.08901v1 [cs.CR]. Download available at: https://arxiv.org/pdf/1904.08901.pdf.
[229]*Ibid.*
[230]Martin Florian, Sophie Beaucamp, Sebastian Henningsen, Björn Scheuermann, "Erasing Data from Blockchain Nodes": 1-10, p.4. Available at: arXiv:1904.08901v1 [cs.CR]. Download available at: https://arxiv.org/pdf/1904.08901.pdf.
[231]International Data Sanitization Consortium. Data Sanitization Terminology and Definitions, available on: https://www.datasanitization.org/data-sanitization-terminology/. Accessed March 16, 2020.
[232]*Ibid.*

implement correct governance model, as in any other business organization, to ensure communication and cooperation between relevant participants and create the structure that would help them in ensuring compliance. Governance in the sense of private blockchain may be explained as planning the management process of the chain within a particular organization or consortium jointly managing the chain. [233]

For organization, it would be beneficial to distinguish and create two separate governance models, one for the on-chain governance with the focus on rules, duties and responsibilities of the participants, and other for the off-chain, which would include the maintenance of off-chain databases and data.[234] The following governance plan consists of the useful steps that the organization has to follow to implement a particular governance model that would allow complying with the GDPR, same model could be implemented for both on-chain and off-chain, however it has to be interpreted by the organization pursuant to its activity and goal that it wants to achieve.

6.1.1. Appointing responsible authorities

In accessing the entity accountable for data protection requirements, private blockchain has a dominant authority, which may be the creator, owner, and administrator, usually would be responsible for implementing all the necessary measures to comply with data protection requirements.[235] The authority in this case may be compared to a centralized entity that spreads the data between all of the participants, thus, it is its responsibility to uphold to data protection principles by rules that all of the participants have to agree upon.[236] The entity appointed as the controller also is responsible for implementation of erasure measures by *default*, maintaining principle of storage limitation, so the erasure would be done automatically.[237]

---

[233]Vedat Akgiray, "The Potential for Blockchain Technology in Corporate Governance", *OECD Corporate Governance Working Papers*, No. 21, OECD Publishing, Paris (2019):1-32, p.18. Available at https://datubazes.lanet.lv:4876/10.1787/ef4eba4c-en.

[234]BLOCKONOMI. What is Blockchain Governance? Complete Beginner's Guide, available on: https://blockonomi.com/blockchain-governance/. Published 21 September 2018. Accessed April 14, 2020.

[235]International Finance Corporation. John Salmon, Gordon Myers, "Blockchain and Associated Legal Issues for Emerging Markets", p.5, available on: https://www.ifc.org/wps/wcm/connect/da7da0dd-2068-4728-b846-7cffcd1fd24a/EMCompass-Note-63-Blockchain-and-Legal-Issues-in-Emerging-Markets.pdf?MOD=AJPERES&CVID=mxocw9F. Accessed March 19, 2020.

[236]*Ibid.*

[237]European Data Protection Board. *Guidelines 4/2019 on Article 25, Data Protection by Design and by Default*, p. 22, available on: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf. Adopted November 13, 2019. Accessed April 7, 2020.

6.1.2. Planning

Planning requires the organization to understand the overall blockchain system that it uses, how to control that network in a way to comply with the law, and at the same time satisfy the needs of the stakeholders. [238]

Especially, governance planning has to be carefully evaluated when private blockchain is used by the consortium, due to possibility of different perceptions of the use of the chain and goals, nevertheless the consortium shall manage the common functional objectives by dividing responsibilities and creating rules for decision-making process, accountability for the data protection principles, as well as particular plan and technology to address the issues concerning data erasure via cooperation between the organizations.[239]

Up to that point, the organization has to access what it wants to achieve with regard to erasure, whether develop a comprehensive protocol that allows the erasure, extension of the software, or train the controller to implement anonymization techniques, collect metadata or use other available means. Then, the responsibilities have to be allocated to each of the participants in a comprehensive manner, by that creating a particular plan looking at the overall blockchain scope and later dividing it into particular areas for further guidance.

6.1.3. Risk assessment

One of the particular points of the on-chain and off-chain governance that has to be accessed is risks arising from use of private blockchain and erasure of the data on the chain. Mostly, it would be established on its own merits, depending on what data inflows and outflows are in the enterprise, what are the services that it provides, or goods that it sells, some general risks may be discussed in the first place.

Firstly, there is a risk that the participants of the network may not guarantee the full immutability of the data in terms of third-party access to it, due to limited number of participants, which may remove the complexities from consensus mechanism and block validation mechanism compared to public blockchain, for example. [240] Since private blockchain may be seen as closed network managed by single or couple trusted entities, only

[238]PwC. Governance in the Age of Blockchain Distributed Ledger Technology, pp.7-8, available on: https://www.pwc.com/us/en/about-us/new-ventures/assets/pwc-governance-in-the-age-of-blockchain-distributed-ledger-technology.pdf. Accessed April 18, 2020.

[239]International Finance Corporation, World Bank Group. Blockchain Governance and Regulation as an Enabler for Market Creation in Emerging Markets (2018):1-8, pp.4-5. Available on: https://openknowledge.worldbank.org/bitstream/handle/10986/30658/131343-BRI-EMCompass-Note-57-Blockchain-Governance-v1-PUBLIC.pdf?sequence=1&isAllowed=y. Accessed April 23, 2020.

[240]Cédric Hebert, Francesco Di Cerbo, "Secure blockchain in the enterprise: A methodology", *Pervasive and Mobile Computing* 59 (2019): 1-14, p.8, accessed March 5, 2020, https://doi.org/10.1016/j.pmcj.2019.101038. Available at: Science Direct database.

limited and participants assigned to carry the function of validation and participating in consensus mechanism check the integrity of the ledger.[241] That may lead to vulnerability of the chain to hacker attacks and other technological failures of the system. [242] Secondly, there is a risk that even if private blockchain does not permit unauthorized access to personal data, other participants of the chain may see the modification of the data and from that derive the reason of modification, so it has to be evaluated carefully when the erasure of personal data is done on the chain.[243]

Moreover, such risk assessment shall include all of the aspects concerning linkability of pseudonymized, anonymized data to the data subject, thus risks associated with each of the methods of ensuring integrity and safety. Pseudonymizing data in off-chain storage has to be carefully evaluated taking into account the nature of the business, for example, pseudonymizing data may lead to problems in financial and commercial sectors that are usually heavily bound by regulatory requirements. [244] Thus, pseudonymous or anonymous data may be the reason for fraudulent activities from the side of organization or its clients, such as avoiding taxes and money laundering, using the fact that identification possibilities are few. [245]

6.1.4. Identifiability reduction

It is important for organization to access that identification concept is not widened to likelihood of obtaining the data subject's personal data under Article 4(1) GDPR, but as well, potential risk of linkability of the remaining data to erased unit, re-identification and data deduction, hence, provided that the data is identifiable, it is still a subject to data protection norms.[246]

Pseudonymizing data does reduce linkability between the data entry and the data subject, however, it does not exclude the possibility of singling out the data subject by linking multiple datasets together, if the same pseudonym is used for the data subject in multiple

[241]Michèle Finck, "Blockchains: Regulating the Unknown", *German Law Journal* 19, no. 4 (2018): 665-692, p. 670, accessed March 11,2020, DOI:10.1017/S2071832200022847.
[242]International Finance Corporation. John Salmon, Gordon Myers, "Blockchain and Associated Legal Issues for Emerging Markets", p.5, available on: https://www.ifc.org/wps/wcm/connect/da7da0dd-2068-4728-b846-7cffcd1fd24a/EMCompass-Note-63-Blockchain-and-Legal-Issues-in-Emerging-Markets.pdf?MOD=AJPERES&CVID=mxocw9F. Accessed March 19, 2020.
[243]IBM Developer. Private and confidential transactions with Hyperledger Fabric. Elli Androulaki, Sharon Cocco, Chris Ferris, available on: https://developer.ibm.com/tutorials/cl-blockchain-private-confidential-transactions-hyperledger-fabric-zero-knowledge-proof/. Publslihed May 11, 2018. Accessed April 15, 2020.
[244]Greg Kaza, "The Blockchain Revolution," Regulation 41, no. 3 (Fall 2018): 53-57, p.53.
[245] *Ibid.*
[246]Article 29 Data Protection Working Party. *Opinion 05/2014 on Anonymisation Techniques*, p.10. Available on: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Adopted April 10, 2014. Accessed March 10, 2020.

datasets.[247] Identically, if pseudonyms are different but there is a common element that allows to combine all of the datasets and link them to the particular data subject. [248] Up to this point, the organization has to monitor whether the remaining data could be linked to erased or anonymized data, for example, if it before was connected to other dataset, or if it had a common element with the other data and the connection to erased data could be derived from the following information.

As regard anonymization, the technology and legal requirements change over time, thus, the anonymization achieved now may be incomplete or the risk of re-identification may become higher over a certain period. [249] The duties of organization involve maintenance of appropriate technical measures used for anonymization, and if needed, apply them again to reduce the possibility of incomplete erasure. As primary consideration, it is always the question that the data subject has when the data is erased by anonymization, whether in fact the controller *did* erase[250] ones' personal data, without keeping some part of the dataset to the controller. If the set is anonymized, but it is still in possession of the controller, that dataset would still be regarded as personal data.[251] Hence, keeping erased data in anonymized form in possession of the controller has to be eliminated, since there is a possibility of controller deriving that data backwards, thus it may be better to move it to erasure database.

The organization has to focus on contextual legal control, by which the mitigation of risks can be achieved.[252] That would include the knowledge of possibilities of reducing linkability, masking of direct identifiers that can be used also for indirect identifiers that may be linked to the data subject. [253] The primary concern of the organization would be implementing appropriate technical and organizational measures *before* initiating the processing or collecting of the data, that is exclude the possibility of combining couple data

[247]Edited by: Ronald Leenes, Rosamunde van Brakel, Serge Gutwirth, Paul De Hert, *Data Protection and Privacy: The Age of Intelligent Machines* (Oxford,United Kingdom; Portland, Oregon: Hart Publishing 2017),p. 131.
[248]*Ibid*.
[249]Article 29 Data Protection Working Party. *Opinion 05/2014 on Anonymisation Techniques*, p.9. Available on: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Adopted April 10, 2014. Accessed March 10, 2020.
[250]As anonymization may be considered as a way of erasure of ones' personal data, erasure in this case is referred to "means of anonymization" or anonymization in general.
[251]Article 29 Data Protection Working Party, *supra* note 249.
[252]Edited by: Ronald Leenes, Rosamunde van Brakel, Serge Gutwirth, Paul De Hert, *Data Protection and Privacy: The Age of Intelligent Machines* (Oxford,United Kingdom; Portland, Oregon: Hart Publishing 2017),p. 134.
[253]Edited by: Ronald Leenes, Rosamunde van Brakel, Serge Gutwirth, Paul De Hert, *Data Protection and Privacy: The Age of Intelligent Machines* (Oxford,United Kingdom; Portland, Oregon: Hart Publishing 2017),p. 131.

entries in one dataset, do not have the same domain for the same datasets, not to collect elements from existing datasets, manage transferring of the data.[254]

6.1.5. Implement and evaluate

Implementation of that governance model would firstly focus on training the employees, which would include all the aspects related to data erasure, such as how to recognize the request, how to use data protection techniques, how to ensure fast cooperation and response.[255] Implement particular security and organizational measures, depending on the location of the storage, such as pseudonymizing any links to erased data off-chain or on-chain and reducing risks of singling out the data. [256] Manage access controls of who has an access to the erased data if it is impossible to erase it physically, whether it is only in the hands of the controller in central server, or it is allocated between optional nodes chosen to participate in the chain and the measures to erase the data from each of the nodes shall be taken.[257] Create and enforce internal data protection rules, by developing the correct flexible protocol applicable to the participants and the controller of the chain, relevant documentation.[258] The final step would be evaluating the performance and performing audit to establish whether the organization did achieve the objective that it had set to achieve at the beginning or it has to change the governance structure to ensure the compliance with the GDPR.[259]

7. PART IV: GUIDELINES FOR CORRECT IMPLEMENTATION OF ARTICLE 17 FOR THE COMPANIES USING BLOCKCHAIN

To understand Article 17, specifically, how to respond to erasure request, recognize it and whether the company has implemented all the necessary technological and organizational measures when receiving complaints under the GDPR, author suggests that the company shall develop particular structured guidelines.

The guidelines should concern both *external* information, intended to be available for the data subject, and *internal* information, which would serve as rules and steps that the company shall undertake to exclude the possibility of fines under the GDPR and consumers

[254]Edited by: Ronald Leenes, Rosamunde van Brakel, Serge Gutwirth, Paul De Hert, *Data Protection and Privacy: The Age of Intelligent Machines* (Oxford,United Kingdom; Portland, Oregon: Hart Publishing 2017),p. 134-135. Table 6.
[255]*Ibid.*
[256]*Ibid.*
[257]*Ibid.*
[258]*Ibid.*
[259]PwC. Governance in the Age of Blockchain Distributed Ledger Technology, pp.7-8, available on: https://www.pwc.com/us/en/about-us/new-ventures/assets/pwc-governance-in-the-age-of-blockchain-distributed-ledger-technology.pdf. Accessed April 18, 2020.

losing trust in a company that cannot ensure data protection to full extent. The following guidelines are in particular focused on internal rules, with a brief overview of most important points of external rules concerning privacy notice that are necessary to be taken into consideration if the company uses private blockchain.

7.1. Data Protection Impact Assessment (DPIA)

The first step for the company using private blockchain, considering the technological means of immutability and decentralization would probably be to carry out DPIA. WP29 Guidelines describe DPIA as a process for managing the risks that can result from the processing of the personal data to the freedoms and rights of the data subject. In particular, the proportionality, necessity, and description of the processing.[260] It is crucial to determine the measures of the DPIA, to stimulate principle of accountability, helping controllers to comply with the Regulation and demonstrate the appropriate measures under Article 24 GDPR to achieve the aim of proper compliance. [261]

Article 35(1) of the GDPR provides that if the processing of the data is likely to result in a high risk to the rights and freedoms of the data subject, the DPIA shall be carried out prior to the processing. [262] Subsequently, the Article states that especially it applies when the processing is carried out by "using new technology".[263] The concept of "new technology" is vague, thus the controller, when taking into account the scope, nature, content, means and purposes of the processing has to establish particular circumstances that can lead to necessity of DPIA, for example if the processing is automated.[264] DPIA also includes the analysis of security measures undertaken by the controller, such as measures of data protection by design and by default, by using automated algorithms to process data, such as it is processed in the blockchain. [265]

To determine whether the processing is likely to result in a high risk, the organization using private blockchain has to understand whether the DPIA is necessary, taking into account the specialization of the organization, but it is likely that DPIA would be needed, as it

[260]IT Governance Privacy Team, *EU General Data Protection Regulation (GDPR): an implementation and compliance guide* (Ely, Cambridgeshire, United Kingdom: IT Governance Publishing, 2017), p.193.
[261]*Ibid.*
[262]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*, 4.5.2016, p. 1–88. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679. Accessed April 10, 2020. Article 35(1).
[263]*Ibid.*
[264]Edited by: Ronald Leenes, Rosamunde van Brakel, Serge Gutwirth, Paul De Hert, *Data Protection and Privacy: The Age of Intelligent Machines* (Oxford,United Kingdom; Portland, Oregon: Hart Publishing 2017), p.99.
[265]*Ibid.*

provides clarification on means and risks of data processing, that is beneficial for the controller and processor.

7.2. Privacy notice

To exclude uncertainties when using private blockchain as company, the GDPR privacy notice shall be made as the first consideration, thus ensuring compliance and notifying the data subject about its rights, responsibilities of controller and processor and response of the organization in cases of breach of the Regulation.[266] Privacy notice is also used as a proof of data processing activities that are crucial in terms of being beneficial to the organization using private blockchain by justifying the processing and providing specific grounds in a case of a complaint.[267]

Developing the correct privacy notice would eliminate the risks of realization of Article 17 based on unlawful data processing or withdrawal of the consent of the data subject, would give the data subject the overview of the purposes and means of the data processing and how specifically the data would be processed, which is one of the crucial points in privacy policy for organization using private blockchain.[268] It would be efficient to include the brief description of each technological units used by private blockchain such as encryption, hash, public key and other means and purposes, and roles of the participants, so that the data subject understands the actions performed to the data by blockchain algorithm. The description of all the technological facilities of each mathematical function is not necessary, but the fact that personal data is deprived of identifiers, explanation of the information contained in the transaction and its visibility to the controller and other participants of the chain would be necessary.

Privacy notice could be regarded as a first step in ensuring the compliance with the GDPR, because it shows that the organization operating in the EU is aware of lawful personal data processing and the data subject may invoke its rights under the General Data Protection Regulation.

[266] Gdpr.eu. Writing a GDPR-compliant privacy notice (template included), available on: https://gdpr.eu/privacy-notice/. Accessed April 10, 2020.
[267] *Ibid.*
[268] *Ibid.*

7.3. Ground-by-ground analysis

As the last step, to recognize whether the situation falls within Article 17, the analysis of each ground has to be conducted. Although there is no particular analysis regarding private blockchain, it is possible to interpret current guidelines published by EDPB "Guidelines on the Right to Be Forgotten in Search Engine Cases", by that providing an organization the guidance on possible scenarios and grounds on which the data subject can rely on in relation to personal data contained on the chain or off-chain, and the exceptions that the organization can apply to reject the received request. [269] The following analysis template is included in Annex Ⅰ.

7.4. Erasure request

Firstly, the company needs to acknowledge how to recognize the erasure request, therefore the staff needs to be trained accordingly. The company needs to understand the conditions where the right to erasure and right to be forgotten is applicable, as well as exceptions under the right to refuse the erasure or right to be forgotten.

7.4.1. Erasure request template

As established before, it is important for the company to acknowledge the request for erasure and for the data subject to understand how the request for erasure may be made. Regarding the form of erasure request, General Data Protection Regulation does not specify how the request should be made, thus the template contained in Annex Ⅱ is a combination of the erasure request template from the official DPA of the Republic of Latvia "Datu Valsts Inspekcija"[270] and modified in accordance with erasure request template suggested by *gdpr.eu.*[271] Since there is no single form, this template taken from the Member State of the Union official DPA may be used for erasure requests in any other Member State respectively. For organization using private blockchain, the following erasure request can be added to the company's website with availability of download, by that simplifying the erasure process for both the company and the data subject.

[269] European Data Protection Board. *Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR*, available on: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201905_rtbfsearchengines_forpublicconsultation.pdf. Adopted December 2, 2019. Accessed April 13, 2020.

[270] Datu Valsts Inspekcija. Veidlapas un formas, *Pieprasījuma par datu labošanu, papildināšanu vai datu apstrādes pārtraukšanu paraugs*, available on : https://www.dvi.gov.lv/lv/datu-aizsardziba/organizacijam/veidlapas-un-formas/. Accessed March 21, 2020.

[271] Gdpr.eu. Right to erasure request form, available on: https://gdpr.eu/wp-content/uploads/2019/01/RIGHT-TO-ERASURE-REQUEST-FORM.pdf Accessed March 21, 2020.

7.5. Keeping record of the data

As the last step, keeping the record of data erasure may be useful for monitoring the compliance of the organization with the Regulation, determining the most effective means of erasure that achieved the expected result of irreversible action.[272] Keeping record of the data would also demonstrate that technical and organizational measures of the controller are efficient, as well that the controller can use the record to evaluate the performance based on metrics that the controller had chosen to include in the record.[273] Of high importance is that the record *shall not include any personal data* that had been erased or reference to it, but may include the technical unit (such as public/private key, transactional data, hash, off-chain storage unit etc.). Followed by, location of the unit, whether it was stored on the chain or off-chain, grounds for erasure, thus which of the conditions under Article 17 apply to this particular unit[274], means of achieving the erasure, thus anonymization, physical destruction, putting data beyond use, software overwriting or other chosen by the organization.

The next step would be to add some additional information, such as whether the unit did contain personal data, is there a risk of re-identifying the data, whether the data is accessible to the controller, as well as include the time, specifically, how long did the erasure process take, to later re-evaluate the efficiency. If the erasure request was lawfully declined on grounds listed in Article 17[275], author suggests that for keeping record to later analyze company's overall performance regarding the compliance with data protection legal requirements, in section provided for additional information the brief explanation for refusal[276], as well as grounds should be listed too. If there is joint-controllership or consortium of companies, author suggests that each of the controllers keep similar record of any personal data erasure related actions, taking into account their duties and responsibilities conferred

[272]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, p. 1–88. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679. Accessed March 15, 2020. Article 30 in conjunction with Recital 82.

[273]European Data Protection Board. *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, p.7, available on: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf. Adopted November 13, 2019. Accessed April 24, 2020.

[274]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, p. 1–88. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679. Accessed March 15, 2020. Article 17.1.

[275]*Ibid*, Article 17.3.

[276]The request in this case may be brief, since the main ground for refusal has to be provided and explained in detail to the data subject. Whereas this record is kept only within the company, mainly data controller, thus to eliminate possible connection to particular data subject, the information in the record has to be kept to the minimum, for purposes of evaluation of the performance.

upon them. The document that could be used for keeping record of erased data on private blockchain and determine risks is contained in Annex Ⅲ.

CONCLUSION

When observing right to erasure or right to be forgotten *per se*, even if the organization decided to use private blockchain, which in its essence is decentralized and immutable, the organization has to understand that the GDPR is a binding Regulation that creates an immediate obligation of the controller or joint-controllers under Article 17 to erase personal data if the request for erasure is made, understanding the availability of the technology, that as well includes the erasure of links connected to the data, copies and replications.[277] Given consideration to obligations arising under Article 17, the organization using private blockchain shall *not* be an exception in terms of applicability of the Regulation if the scope of applicability is satisfied, regardless of complex structure of the chain.

It may be derived that the compliance with the General Data Protection Regulation while using blockchain may not be achieved straightforwardly and it may require vast resources to achieve it correctly. Consequently, if the company needs or decides to use private blockchain, it has to access all the possible risks associated with data protection and issue specific regulatory guidance on each point that potentially may pose obstacles to sufficient data protection requirements within the organization.

When examining relationship of GDPR with private blockchain, *de facto* the system remains decentralized, but with central scrutinizing authority and still immutable by the consensus protocol. However, private blockchain allows exceptions for data erasure, which depends on the rules developed by the authority scrutinizing the chain. Therefore, presents alternative options that may allow for modification of the chain and erasure of the data, if implemented by default or included in the set of governing rules created by the responsible entity binding on the participants, thus undermining the strict immutability and decentralization that is assumed.

With regard given to the compliance of organization with right to erasure or right to be forgotten, whether the compliance may be ensured in immutable and decentralized system by design, erasure of the data on blockchain network still remains a complicated concept. The

[277]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, p. 1–88. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679. Accessed March 15, 2020. Article 17.

absence of the notion of erasure creates uncertainties whether erasure would be satisfied only via physical destruction of the data, which technologically would be possible only in exceptional cases, or, limitation of data visibility achievable through anonymization and pseudonymization may satisfy the result of data erasure or a "right to be forgotten" under Article 17 to full extent. Consequently, creating additional risks of particular identification units left on the chain after the erasure, with the possibility of singling out the erased data or having particular connection to the data, if implemented incorrectly.

On the subject of the mitigation of applicability of Article 17 in organization using private blockchain, coordination of tasks and creating a sequential model of actions between all participants of the chain is of the utmost importance. It allows to analyze fundamental aspects of defining responsibilities and the main entity accountable for compliance, providing effective technical, corporate and legal solutions for implementation of the Regulation and organization reacting *effectively* and *immediately* if the erasure request has been made.

Creating blockchain governance plan on-chain and off-chain would provide clarity on the roles of the participants, determine whether blockchain creator, administrator, owner, is the controller or whether there are joint-controllers. Inevitably, that would simplify the process of notification of other controllers about the data erasure, and, most importantly, allow nodes that are affected by right to erasure or right to be forgotten exercised by the data subject to cooperate. Therefore, reach the consensus on possible erasure of personal data, as well as help the organization to maintain the chain in accordance with particular rules to comply with the Regulation.

To mitigate the enforcement of Article 17, the organization needs to access the risks connected with data erasure, find the most suitable storage for the data, implement the governance model, constantly monitor the erasure process, and carefully evaluate its performance. Organization must create particular data erasure rules, accordingly compromised with available technology and options, such as destroying off-chain data, deleting private key, using chameleon hashes, metadata, destroying or anonymizing the component that does include personal data and pseudonymize potential identifiers or links to the data.

As a result, compliance process with Article 17 shall be planned by each organization individually, depending on available financial, human, technological resources, amount of possible personal data circulating on the chain and is subject to assessment on its own merits. Regardless, complete compliance with the Regulation when using private blockchain would *not* be possible, since there will always be risk of re-identifying the data unless erased by

physical destruction, due to technological fundamentals of the chain itself. In any event, the choice of private blockchain as the main network that the company operates on has to be accordingly estimated from the perspective of its potential benefits to the company balanced with the potential problems arising from applicability and realization of the provisions of the General Data Protection Regulation.

ANNEXES

Annex Ⅰ Guidelines: Ground-by-ground analysis.

NOTICE FOR THE ORGANIZATION: ON CASE-TO-CASE BASIS, THE RIGHT TO ERASURE HAS TO BE IN ADDITION EVALUATED SUBJECT TO SPECIAL NATIONAL LEGAL ACTS OF THE MEMBER STATE TO WHICH THE COMPANY IS SUBJECT.[278]

PART 1: RIGHTS OF THE DATA SUBJECT

1. **Ground one (Article 17.1 a): personal data anymore is not necessary for purposes that it was originally collected or otherwise processed.**

The organization must closely monitor the conditions of data storage and data disclosure, especially in cases concerning this specific ground of Article 17. Couple of the conditions that the organization must be aware of to mitigate the enforcement of Article 17.1.a:

▪ If the public register removes the information about the data subject from that public register, but the information is still held by the organization. This particular point implies that the organization has to check not only whether their partners (which could be in the consortium or the ones that the organization provides services or sells goods via blockchain) are in compliance with the legal framework, but as well closely monitor whether they are still contained in the public register, so that the data that had been removed is not left *on* the chain, but all the agreements and information about the fulfilled transactions are already moved to off-chain.

▪ If the private blockchain concerns information about the person that is no longer linked to that organization, such as no longer employed, no longer participates in consensus, no longer uses the services or purchases goods provided by that organization via blockchain.

▪ If public key of an individual was disclosed by organization or voluntarily for a particular time for fulfillment of the legal obligation, over specific period of time (or, intended for single or couple transactions *only*), this implies that the organization has to monitor the fulfillment of the transaction and after it is done, operatively move anything that contains personal data and is no longer needed off-chain or anonymize by default.

The company has to pay attention, since same applies if the data subject wants to erase the data that is not up to date or goes contrary to original purposes of the processing. The data that

[278]This may provide for setting time limitations for the erasure, whether the data can be erased at all depending on the functioning of the organization, whether the data erasure goes contrary to AML framework etc.

is outdated or inaccurate may be the private key which has been disclosed or changed, public key which is no longer used by the data subject, financial information that had changed over the time, whilst the outdated financial information is still contained in one of the important transactions or functions, wallet, information which is stored on the chain to monitor customers' behavior, hash that includes outdated or inaccurate information about the data subject. As well, same applies if for example public and private key is used for anything beyond the initial purpose.

The fact to consider here is that the examination of original purposes of the processing is required, cooperation between relevant authorities, clear measures shall be implemented, and time period for data erasure or "right to be forgotten" has to be set. [279]

2. **Ground two (Article 17.1.b): erasure of the data when the data subject withdraws the consent where the legal basis for the processing is Articles 6.1.a or 9.2.a GDPR and where there is no other legal basis for the processing.**

This ground is in particular connected with creating the right Privacy Policy and consent given by the data subject about processing and collecting his or her data via blockchain algorithm. Consequently, when the data subject withdraws the consent given at the beginning of initiation of the processing and collecting the data by organization, the consent is considered to be utilized, thus there is no other legal basis to continue definite processing. Before dealing with erasure requests based on this point, author suggests the controller to read all the necessary provisions related to the consent, as well as analyze the types of the consent to understand the difference and scope.

Here, if the data subject withdraws the consent, it is an obligation of the data controller appointed by the organization to inform all of the other participants of the chain that store parts of the data subjects' personal data, and agree on the rules of erasure of the data from each of the nodes. That erasure may constitute anonymizing each of the pieces of the data until it is impossible to restore it, or, apply suggested software extension that allows nodes to mark units for erasure. As well, it is crucial to stop *all the actions* with the data when the blockchain participant withdraws the consent.[280]

[279]Template is based on: European Data Protection Board. *Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR*, pp. 6-7. Available on: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201905_rtbfsearchengines_forpublicconsultation.pdf. Adopted December 2, 2019. Accessed April 13, 2020.

[280]European Data Protection Board. *Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR*, pp. 7-8. Available on: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201905_rtbfsearchengines_forpublicconsultation.pdf. Adopted December 2, 2019. Accessed April 13, 2020.

Ground three (Article 17.1.c): erasure can be requested when the data subject exercises the right to object to the processing and collecting of his or her personal data either pursuant to Article 21(1) with no overriding legitimate grounds for the processing, or the data pursuant to Article 21(2).

The core factor to be taken into account here is that the controller has to understand and provide legitimate grounds for the processing, if there are no any, the controller is obliged to erase the data. [281]

Recital 47 provides clarification on when the company may present other legal basis to justify the relationship of the data subject with the controller. Although each situation shall be accessed individually, in situations when the data subject is the client or is in the service of the controller (thus, the company using private chain), controller can rely on legitimate interest, which would constitute the prevention of fraud (as an example, the company using private blockchain for financial purposes would not want to anonymize the data of the participants in some cases, to prevent money-laundering, hindering the transactions) or direct marketing purposes, where this information plays an important role. Whereas, fundamental rights of the data subject are primary concern.[282] As well, if private blockchain within the company would be influenced by the following provision, by *influenced*, meaning that the erasure of this data would lead to malfunction in data security (for example threat to immutability), integrity (if by erasure of that data the significant value of the chain or the transaction would change in a way affecting other pieces of data) and accessibility of the data, this may constitute a legitimate interest of the controller.[283]

Ground four (Article 17.1.d): erasure can be requested when personal data has been unlawfully processed.

[281]European Data Protection Board. *Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR*, pp. 8-9. Available on: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201905_rtbfsearchengines_forpublicconsultation.pdf. Adopted December 2, 2019. Accessed April 13, 2020.

[282]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, p. 1–88. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679. Accessed April 15, 2020. Recital 47.

[283]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, p. 1–88. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679. Accessed April 15, 2020. Recital 49.

Although it is unlikely that the erasure request to the company using private blockchain would be based on this specific ground, since the assumption is that before the participant is admitted to the chain (received invitation from the organization, owner, administrator or creator of the chain with conditions such as the consent for data processing, and as well got acquainted with Privacy Policy) or uses the chain for goods and services, the data subject has given his or her consent to the following actions with their data based on blockchain algorithm. This ground also includes the obligation of the company to monitor that each of the actions performed via blockchain by the participants is based on the data subject giving consent to the actions with his or her data.[284]

Ground five (Article 17.1.e): erasure of personal data may be requested as being in compliance with the legal obligation.

This imposes the obligation on organization to understand that the erasure of particular data may be requested by national law or EU law, which organization using private blockchain is subject to. This includes the assessment of the relevant field of the law by the organization, depending on its purpose to find regulatory provisions related to erasure of the data and the conditions.

One of the factors that the controller appointed by the organization has to consider that this point of Article 17 may be also applied if the controller does not uphold the period the organization had set in its rules for the data erasure, such as the data must be erased within 30 days from receiving the request. [285] Identically, if retention period is laid out in national law, but the controller did not uphold the period for data erasure.

Ground six (Article 17.1.f): erasure of personal data, which has been collected for the purposes of offering of information society services (ISS) to a child.

Firstly, if the erasure of personal data is requested based on this point, the duty of the controller is to be acquainted with Article 8 of the GDPR.

The organization has to be prepared, since the scope of this point is only limited to ISS, but for this to apply the blockchain has to be qualified as an ISS. The GDPR has no definition of information society services, thus the interpretation is provided by European Law, specifically as the EDPB suggests the interpretation of ISS in recital 18 of the Directive 2000/31/CE.[286]

[284]European Data Protection Board. *Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR*, pp. 9-10. Available on: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201905_rtbfsearchengines_forpublicconsultation.pdf. Adopted December 2, 2019. Accessed April 13, 2020.
[285]*Ibid*, p.10.
[286]*Ibid*.

ISS in accordance with recital 18 constitute a broad range of economic activity that is online, mainly selling goods and providing services online.[287] Therefore, the activity that would fall under ISS from the perspective of the organization would be sales of goods and provision of services via private blockchain, including the wide range of remunerated and non-remunerated activities, blockchain contracting, tools of the chain allowing the transmission of the information by the transaction or any means from point A to point B, access to the network and obtaining particular data, information online and communications that may have commercial aim within the chain.[288] For more clarity on whether blockchain does in certain circumstances fall under ISS (again, depending on the organization) the author suggests the organization to deeply analyze the following provisions of the Directive 2000/31/CE and their interpretation.

PART 2: EXCLUSIONS UNDER ARTICLE 17.

Given that right to erasure "right to be forgotten" is not of an absolute nature, the organization needs to access the grounds when exercise of this right would not be possible for the data subject.

Ground one (Article 17.3.a): erasure may be refused based on freedom of expression and information.

This ground specifically emphasizes the *balance* between public interest and fundamental rights of the data subject.

If organization had received an erasure request, but it thinks that, it would be sufficient to decline it based on the following ground, firstly, the balance test (weighting public interest and fundamental rights of the data subject) shall be performed, as well asking questions similar to:

1. What would the impact of erasure of certain data on the public (e.g. impact on the access of information)?
2. Would that influence the freedom of information of the chain users?

This ground would be accessed on its own merits, depending on what type of data is in question, whether the data on or off-the chain constitutes sensitive data, that is connected in particular with private life of the data subject and whether this data is actually in the interest

[287] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), *OJ L* 178, 17.7.2000, p. 1–16. Available on: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32000L0031. Accessed April 17, 2020. Recital 18.

[288] *Ibid.*

of the public. However, fundamental rights of the data subject should prevail in most of the cases (and will prevail in general), so the organization must consider this.

For the balance test the author advises to check the judgments of *Costeja* and *Google 2*.[289]

Ground two (Article 17.3.b): erasure may be refused for compliance with a legal obligation that requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Article 17.3.b).

As for legal obligation, business organization may be a subject to legal obligation of the national or EU law. That legal obligation may cover the duty to publish particular reports on its activities, hand over the information on its customers, audit and similar documents that may contain personal data.

That legal obligation is not widened only to publicly reported information; there is also a possibility on having legal obligation as the organization to submit particular information to official authorities in private, depending on the functioning of organization. If the data contained on-chain or off-chain is one of the data that has to be included in the report that has to be published or handed over pursuant to law, organization may refuse to erase this data.

At the same time, there may be a time limitation set for the period for which that data may be kept. If the organization had already provided data in accordance with the law and it is no longer needed due to particular reasons, the organization would be bound by the erasure request and is obliged to erase the data.[290]

Ground three (Article 17.3.c.): erasure may be refused if the processing is a necessity because of reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3).

This ground would in particular concern organizations using private blockchain for healthcare purposes. Although, it is unlikely that this ground would be used for erasure refusal, since in positive scenario all of the data, which is related to health, may be put into category of sensitive data, hence cryptography on the chain would secure the data and risks of

[289]European Data Protection Board. *Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR*, pp. 11-12. Available on: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201905_rtbfsearchengines_forpublicconsultation.pdf. Adopted December 2, 2019. Accessed April 13, 2020.

[290]European Data Protection Board. *Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR*, pp. 13-14. Available on: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201905_rtbfsearchengines_forpublicconsultation.pdf. Adopted December 2, 2019. Accessed April 13, 2020.

identification would be relatively low. However, there could be some grounds, which have to be accessed by the controller of the organization by analyzing provisions of Article 9 GDPR.[291]

Ground four (Article 17.3.d): erasure may be refused for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing.

If the organization participates in particular scientific, statistical or historical research purposes, which are assumed to be of a public interest, the organization may refuse to erase particular data. Although it is *only* relevant in cases, where it would result in significant impact on the outcome of the research. Such as if, the organization uses private blockchain for particular academic purposes (such as storing and verification of academic credentials, by which later conducting statistical research) and erasure of the data would potentially hinder the result to a big extent. Nevertheless, it all depends on balance of rights of the data subject and importance of that data to the public.[292]

Ground five (Article 17.3.e): erasure of the data may be refused because it is needed to establish, exercise or defend legal claims.

In positive scenario, the situation under Article 17.3.e is unlikely to occur, however, if the organization faces lawsuit and has to establish, exercise or defend legal claim, where personal data contained in the private chain presents a particular important piece of information related to the case, or is an important evidence, the organization can refuse to erase the data in exceptional cases. Again, in most cases that would be determined by relevant law of the Member State to which the organization is subject to, or relevant EU law.[293]

[291] European Data Protection Board. *Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR*, p. 15. Available on: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201905_rtbfsearchengines_forpublicconsultation.pdf. Adopted December 2, 2019. Accessed April 13, 2020.
[292] *Ibid.*
[293] *Ibid.*

Annex Ⅱ Guidelines: Erasure request template.

To (organization name), the controller

(to legal entity, state or local authority -

name, registration number and address, for natural person-

name and address.)

_____

_____

_____

_____

Request for erasure of personal data

We *(name of organization)* acknowledge that under General Data Protection Regulation Article 17 you have a right to have your personal data that we hold erased upon request.

IMPORTANT NOTICE: We use private blockchain for actions with your data, which means that your data may not be available for physical erasure or modification in some cases. However, we will try to implement necessary measures in accordance with General Data Protection Regulation to satisfy your request by hiding your data and possible information, as well as any links related to it. For clarification, the information about erasure techniques used by our organization can be found on our website (link) in section (name, link).

For additional information about erasing data on blockchain, please contact the person responsible for data protection in our organization: (name, surname, email, phone).

We oblige, that the data will be erased within 30 (thirty) days from the time of receiving the request:

- based on this template

- verbally
- any form

The information you provide in this document would only be used to identify the component of data intended for erasure. You are not obliged to fill out this request; however it would help us to process the request as soon as possible.

1. **Please provide your contact details:**

- Name, surname:
- Address:
- Email:
- Phone:

2. **Are you a data subject?**

□ **YES**

□ **NO**, acting on behalf of the data subject. (Then, the written proof of authority given from the data subject is required, as well as proof of the data subject identity and identity of the person acting on data subject's behalf)

- Proof of identity included (passport, ID card, driver's license[294], birth certificate).

- Proof of address (may be provided in your passport, utility bill, credit card information, ID card, driver's license etc.)

- Proof of identity, if you represent the data subject (please include proof of data subject's identity in point 1.)

If we do not receive the suitable proof of identity, we can refuse to erase the data.

3. **Data erasure under Article 17 GDPR**

Please tell us *in detail* what information do you want us to erase (such as public key, corresponding private key, wallet number, credit card details, etc.) if possible, provide

[294]This has to be evaluated pursuant to national law, because driver's licence may not be considered as an official document for proving ones' identity.

additional information about any of the units (number of the transaction, location etc.). If possible, send us the URL or provide the location where the data can be found.

I, *(name, surname)* ask *(name of organization or the controller)* to erase the personal data at your disposal,

_____

_____

_____

_

Please explain how this information relates to you, or the data subject you represent, and briefly, state other reasons not provided in point 3. (if any) why do you want us to erase it.

_____

_____

_____

_

Please note, that relying on Article 17 GDPR, right to erasure ('right to be forgotten'), the erasure of your data can be refused, if it goes contrary to conditions stated in Article 17(3), the right of freedom of expression and information, fulfillment of legal obligation, public health and interest reasons, research and statistical purposes, if it relates to establishment, defense and exercise of legal claims. In case the erasure of the data contradicts one of these principles, you will receive a notification that we are unable to erase your data, with explanation of the refusal.

If we are unable to physically erase/destroy your data because of technological contradictions of our system, you will be notified about other means available to us that can erase your data and the result.

Please pick the following grounds that you feel apply to your data that we hold and process,

(Tick the desired)

□ you feel that the data is no longer needed for original purpose of collecting and processing.

□ you no longer consent to us processing, storing and collecting your data. □ □ □

□ you object to data processing in accordance with your right under Article 21 GDPR.

□ you think that we are obliged to erase your personal data in accordance with EU law or law of the Member State we operate in.

□ you are a child, or representative of the child, or you were a child when the data was originally collected and processed, and you feel that we are trying to offer you information society related services.

4. Declaration

I confirm that I have read and understood the terms of this document and that the information presented to *(name of organization)* is true, and any purposeful misleading of information may result in prosecution.

I acknowledge that the information I state in this document is necessary for (name of organization) to establish my identity as the data subject (or data subject and its representative), establish the data that is needed to be erased, as well as its location and any other relevant information that may be connected to that data. [295]

Name, surname:…… Signature:…… Date:……..

Documents to be attached:

- Document proving your identity, address, contact information.
- Document of data subject's identity, address, contact information. (if applicable)
- Authorization from the data subject. (if applicable)

<u>You can describe points 4, 5 of this document on a separate PDF format document, if you feel that it is necessary.</u>

[295] This template is based on: Gdpr.eu. Right to erasure request form, available on: https://gdpr.eu/wp-content/uploads/2019/01/RIGHT-TO-ERASURE-REQUEST-FORM.pdf Accessed March 21, 2020.

Annex Ⅲ Guidelines: Record of erasure template[296].

Organization		**Controller**		**Joint-controller (if so, indicate the existence of agreement, area of responsibility)**		**Agreement, Area of responsibility**
Name		Name		Name		
Address		Address		Address		
Contact e-mail		Contact e-mail		Contact e-mail		
Phone		Phone		Phone		

IN ACCORDANCE WITH DATA ERASURE POLICY OF ORGANIZATION, (document number)

Reference 1. (date)	Unit intended for erasure 1.	Location (off-chain, on the chain (to be anonymized), etc.)	Technical and organizational measures of erasure	Grounds for erasure (Article 17)	Additional information	Time of performance (1-30 days).	Grounds for refusal of erasure request

[296]This template is based on: Wolfgang Braun, Susanne Dehmel, Heiko Gossen, Dr. Hartmut Hässig, Lars Kripko, Ilona Lindemann, Christian Wagner, Stephan Weinert, "The Processing Records: Records of Processing Activities according to Art. 30 General Data Protection Regulation (GDPR)", *Bitkom e. V. Federal Association for Information Technology, Telecommunications and New Media* (2017): 1-42, pp. 13-18. Available on: https://www.bitkom.org/sites/default/files/file/import/180529-LF-Verarbeitungsverzeichnis-ENG-online-final.pdf. Accessed April 18, 2020.

Reference 2. (date)	Unit intended for erasure 2.	Location (off-chain, on the chain, etc.)	Technical and organizational measures of erasure	Grounds for erasure (Article 17)	Additional information	Time of performance (1-30 days)	Grounds for refusal of erasure request
Reference 3. (date)	Unit intended for erasure 3.	Location (off-chain, on the chain, etc.)	Technical and organizational measures of erasure	Grounds for erasure (Article 17)	Additional information	Time of performance (1-30) days	Grounds for refusal of erasure request
Reference 4. (date)	Unit intended for erasure 4.	Location (off-chain, on the chain, etc.)	Technical and organizational measures of erasure	Grounds for erasure (Article 17)	Additional information	Time of performance (1-30) days	Grounds for refusal of erasure request [297]

[297] 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, p. 1–88. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679. Accessed April 15, 2020. Article 30. The document template is created in accordance with Article 30, which implies the maintenance of records of processing activities.

BIBLIOGRAPHY

Primary Sources

Legislation

1. 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, *OJ L* 281, 23.11.1995, p. 31–50. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046. Accessed October 19, 2019.
2. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), *OJ L* 178, 17.7.2000, p. 1–16. Available on: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32000L0031. Accessed April 17, 2020.
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, p. 1–88.* Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679. Accessed October 19, 2019.

Case law

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.

Secondary Sources

Books

1. Edited by: Leenes, Ronald, Rosamunde van Brakel, Serge Gutwirth, Paul De Hert. *Data Protection and Privacy: The Age of Intelligent Machines*. Oxford, United Kingdom; Portland, Oregon: Hart Publishing 2017.
2. *Handbook on European data protection law*. Luxembourg: Publications Office of the European Union, 2018. Available on: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-

protection_en.pdf. Published May 24, 2018. Accessed October 31, 2019, doi:10.2811/343461.

3. IT Governance Privacy Team. *EU General Data Protection Regulation (GDPR): an implementation and compliance guide*. Ely, Cambridgeshire, United Kingdom: IT Governance Publishing, 2017.
4. Shraddha, Kulhari. "The Midas touch of Blockchain: Leveraging It for Data Protection." in *Building-Blocks of a Data Protection Revolution: The Uneasy Case for Blockchain Technology to Secure Privacy and Identity*. Baden-Baden, Germany: Nomos Verlagsgesellschaft MbH, 2018.
5. Voigt, Paul, Axel von dem Bussche. *The EU General Data Protection Regulation (GDPR): a practical guide*. Hamburg, Berlin, Germany: Springer Publishing, 2017.

Scholarly articles

1. "GDPR, Blockchain and the French Data Protection Authority: Many Answers but Some Remaining Questions," *Stanford Journal of Blockchain Law & Policy* 2, no. 2 (2019): 1-14. Available on: Hein Online database.
2. Allessie, David, Sobolewski Maciej, Vaccari Lorenzino, "Blockchain for digital government", *Publications Office of the European Union* (2019):1-88. Accessed November 12, 2019. doi:10.2760/942739.
3. Casino, Fran, Politou Eugenia, Efthymios Alepis, Constantinos Patsakis, "Immutability and Decentralized Storage: An Analysis of Emerging Threats" (2019): 4737-4744, p.4739. Accessed March 3, 2020. doi : 10.1109/ACCESS.2019.2962017.
4. Finck, Michèle, "Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?", *European Parliamentary Research Service* (2019) :1-101. Accessed November 1, 2019. doi: 10.2861/535.
5. Finck, Michèle, "Blockchains: Regulating the Unknown", *German Law Journal* 19, no. 4 (2018): 665-692. Accessed March 11, 2020. doi:10.1017/S2071832200022847.
6. Frizzo-Barker, Julie, Peter A.Chow-White, Philippa R.Adams, Jennifer Mentanko, Dung Ha, Sandy Green,"Blockchain as a disruptive technology for business: A systematic review", *International Journal of Information Management* 51 (2020): 1-14. Accessed March 4, 2020. https://doi.org/10.1016/j.ijinfomgt.2019.10.014.
7. Gilbert, Francoise, "European Data Protection 2.0: New Compliance Requirements in Sight - What the Proposed EU Data Protection Regulation Means for U.S. Companies," *Santa Clara Computer & High Technology Law Journal* 28, no. 4 (2011-2012): 815-864.

8. Goldenfein, Jake, Dan Hunter, "Blockchains, Orphan Works, and the Public Domain," *Columbia Journal of Law & the Arts* 41, no. 1 (2017): 1-44.
9. Gudkov Aleksei, "Control on Blockchain Network," *Nova Law Review* 42, no. 3 (Spring 2018): 353-374.
10. Guo, Leiyong, Hui Xie, Yu Li, "Data Encryption based Blockchain and Privacy Preserving Mechanisms towards Big Data", *J. Vis. Commun. Image R.* (2019): 1-11. Accessed March 18, 2020. doi: https://doi.org/10.1016/j.jvcir. 2019.102741.
11. Hebert, Cédric, Francesco Di Cerbo, "Secure blockchain in the enterprise: A methodology", *Pervasive and Mobile Computing* 59 (2019): 1-14. Accessed March 5, 2020, https://doi.org/10.1016/j.pmcj.2019.101038.
12. Helo, Petri, Yuqiuge Hao "Blockchains in operations and supply chains: A model and reference implementation", *Computers & Industrial Engineering*, Vol.136 (2019): 242-251. Accessed December 19, 2019. https://doi.org/10.1016/j.cie.2019.07.023.
13. Kaza, Greg "The Blockchain Revolution," *Regulation* 41, no. 3 (Fall 2018): 53-57.
14. Kipker, Dr. Dennis-Kenji, Hauke Bruns, "Blockchains für Versorgungsketten im Lebensmittelsektor und der Datenschutz", *Computer und Recht* 3 (2020):210-216.
15. Kwik, Justin, "In Light of the Technical Impracticality of the Right to Erasure, What Answers Can Actor-Network Theories Provide," *Singapore Comparative Law Review* 2019 (2019): 48-65.
16. Mirchandani, Anisha, "The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR," Fordham Intellectual Property, *Media & Entertainment Law Journal* 29, no. 4 (Summer 2019): 1201-1242.
17. Morkunas, Vida J., Jeannette Paschen, Edward Boon, "How Blockchain Technologies Impact Your Business Model", *Kelley School of Business, Indiana University* (2019):1-12. Accessed February 10, 2020. https://doi.org/10.1016/j.bushor.2019.01.009. Published by Elsevier Inc. Available on: https://fardapaper.ir/mohavaha/uploads/2019/08/Fardapaper-How-blockchain-technologies-impact-your-business-model.pdf.
18. 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 (2019): 80-91. Accessed January 20, 2020. https://doi.org/10.1515/comp-2019-0005.
19. Pehlivan Ceyhun Necati, Inés Isidro Read "Blockchain and Data Protection: A Compatible Couple?" (The Netherlands: Kluwer Law International BV, 2020), *Global Privacy Law Review*, Vol. 1, Issue 1 (2020): 39-48.

20. Ul, Muneeb Hassan, Mubashir Husain Rehmani, Dr. Jinjun Chen, “Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions”, *Future Generation Computer Systems* 97 (2019): 512-529. Accessed December 5, 2019. https://doi.org/10.1016/j.future.2019.02.060.
21. Van Eecke, Patrick, Anne-Gabrielle Haie, "Blockchain and the GDPR: The EU Blockchain Observatory Report," *European Data Protection Law Review* (EDPL) 4, no. 4 (2018): p. 531-534.
22. Zahay, Debra, James Peltier, Don Schultz, Abbie Griffin, “The Role of Transactional versus Relational Data in IMC Programs: Bringing Customer Data Together”, *Journal of Advertising Research* 44 no.1 (2004): 3-18. Accessed February 27, 2020. https://doi.org/10.1017/S0021849904040188.
23. Zetzsche, Dirk A., Ross P. Buckley, Douglas W. Arner, "The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain," *University of Illinois Law Review* 2018, no. 4 (2018): 1361-1406.
24. Zheng, Rongyue, Jianlin Jiang, Xiaohan Hao ,Wei Ren , Feng Xiong, and Yi Ren, “bcBIM: A Blockchain-Based Big Data Model for BIM Modification Audit and Provenance in Mobile Cloud”, *Hindawi Mathematical Problems in Engineering* (2019) : 1-14. Accessed March 2, 2020. https://doi.org/10.1155/2019/5349538.

Internet resources

1. Amelia Wallace “Protection of Personal Data in Blockchain Technology - An investigation on the compatibility of the General Data Protection Regulation and the public blockchain”, *Master’s Thesis*, Stockholm University, p. 10. Download available at: http://www.diva-portal.org/smash/get/diva2:1298747/FULLTEXT01.pdf.
2. Anderberg, Alexandre, Amanda Andonova, Elena Bellia Mario, Calès Ludovic, Inamorato Dos Santos Andreia, Kounelis Ioannis, Nai Fovino Igor, Petracco Giudici Marco, Papanagiotou Evangelia,Sobolewski Maciej,Rossetti Fiammetta, Spirito Laura, ed. By Figueiredo Do Nascimento and Susana Roque Mendes Polvora, “Blockchain Now and Tomorrow” (Publications Office of the European Union, Luxembourg, 2019). Table 1: Examples of blockchain types. Accessed November 3, 2019. doi:10.2760/901029. Download available on: https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/blockchain-now-and-tomorrow.
3. Article 29 Data Protection Working Party. *Guidelines on Personal data breach notification under Regulation 2016/679*. Available on:

https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052. Last adopted on February 6, 2018. Accessed February 18, 2020.

4. Article 29 Data Protection Working Party. *Opinion 05/2014 on Anonymisation Techniques*. Available on: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Adopted April 10, 2014. Accessed March 10, 2020.
5. Article 29 Data Protection Working Party. *Statement of the WP29 on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU*. Available on: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622229. Published April 11 2018. Accessed February 16, 2020.
6. Article 29 Working Party. *Opinion 1/2010 on the concepts of "controller" and "processor" (WP 169)*. Available on: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf. Adopted February 16, 2010. Accessed March 2, 2020.
7. Blockchain.com. Public and private keys, available on: https://support.blockchain.com/hc/en-us/articles/360000951966-Public-and-private-keys. Accessed February 19, 2020.
8. Blockgeeks. Ameer Rosic, "What Is Hashing? [Step-by-Step Guide-Under Hood of Blockchain]", available on: https://blockgeeks.com/guides/what-is-hashing/. Accessed: March 2, 2020.
9. BLOCKONOMI. What is Blockchain Governance? Complete Beginner's Guide, available on: https://blockonomi.com/blockchain-governance/. Published 21 September 2018. Accessed April 14, 2020.
10. Cambridge Business English Dictionary. Definition of *filing system*, available on: https://dictionary.cambridge.org/dictionary/english/filing-system Accessed January 24, 2020.
11. Christian Cachin, Marko Vukolic "Blockchain Consensus Protocols in the Wild", IBM Research (2017): 1-24, p. 5 (Section 3.1. para., 4.). Download available at: https://arxiv.org/pdf/1707.01873. Accessed December 30, 2019.
12. Cindy Compert, Maurizio Luinetti, Bertrand Portier, "Blockchain and GDPR: How blockchain could address five areas associated with GDPR compliance", *IBM Corporation (IBM Security) white paper* (2018): 1-8. Download available on: https://www.ibm.com/downloads/cas/2EXR2XYP. Accessed February 9, 2020.

13. COINDESK. Gideon Greenspan, “The Blockchain Immutability Myth”, available on: https://www.coindesk.com/blockchain-immutability-myth. Published May 9, 2017. Accessed February 10, 2020.
14. Cryptomaniaks.com. Michael R., “What is a Blockchain Protocol?”, available on: https://cryptomaniaks.com/blockchain-protocols-list-explained#h2-0. Accessed March 5, 2020.
15. Datu Valsts Inspekcija. Veidlapas un formas, *Pieprasījuma par datu labošanu, papildināšanu vai datu apstrādes pārtraukšanu paraugs*, available on : https://www.dvi.gov.lv/lv/datu-aizsardziba/organizacijam/veidlapas-un-formas/. Accessed April 1, 2020.
16. Dr Garrick Hileman & Michel Rauchs “Global Blockchain Benchmarking Study”, Cambridge Centre for Alternative Finance, University of Cambridge: Judge Business school, (2017):1-121. Available on: https://www.crowdfundinsider.com/wp-content/uploads/2017/09/2017-Global-Blockchain-Benchmarking-Study_Hileman.pdf . Accessed February 8, 2020.
17. European Data Protection Board. *Guidelines 4/2019 on Article 25, Data Protection by Design and by Default*. Available on: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf. Adopted on 13 November 2019. Accessed April 7, 2020.
18. European Data Protection Board. *Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR*. Available on: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201905_rtbfsearchengines_forpublicconsultation.pdf. Adopted December 2, 2019. Accessed April 13, 2020.
19. European Data Protection Supervisor, Agencia Española de Protección de Datos | AEPD. Introduction to the Hash Function as a Personal Data Pseudonymisation Technique, available on: https://edps.europa.eu/sites/edp/files/publication/19-10-30_aepd-edps_paper_hash_final_en.pdf, Accessed March 10, 2020.
20. Fergal Reid, Martin Harrigan “An Analysis of Anonymity in the Bitcoin System”, *Clique Research Cluster, Complex & Adaptive Systems Laboratory University College Dublin, Ireland* (2012): 1-26. Available at: arXiv:1107.4524v2 [physics.soc-ph]. Download available at: https://arxiv.org/pdf/1107.4524.pdf.
21. GDPR Report. Data masking: anonymization or pseudonymization?, available on: https://gdpr.report/news/2017/09/28/data-masking-anonymization-pseudonymization/ . Published September 28, 2017. Accessed February 15, 2020.

22. Gdpr.eu. Right to erasure request form, available on: https://gdpr.eu/wp-content/uploads/2019/01/RIGHT-TO-ERASURE-REQUEST-FORM.pdf Accessed March 21, 2020.
23. Gdpr.eu. Writing a GDPR-compliant privacy notice (template included), available on: https://gdpr.eu/privacy-notice/. Accessed April 10, 2020.
24. Global engage. When Blockchain Meets the Right to be Forgotten: Technology Versus Law, available on: http://www.global-engage.com/life-science/when-blockchain-meets-the-right-to-be-forgotten-technology-versus-law/. Published May 2, 2018. Accessed April 13, 2020.
25. GOCODING. Barry Allen, "Transaction Data in Blockchain". Available on: https://gocoding.org/transaction-data-in-blockchain/. Published June 30, 2019. Accessed March 12, 2020.
26. IBM Developer. Private and confidential transactions with Hyperledger Fabric. Elli Androulaki, Sharon Cocco, Chris Ferris, available on: https://developer.ibm.com/tutorials/cl-blockchain-private-confidential-transactions-hyperledger-fabric-zero-knowledge-proof/. Pubslihed May 11, 2018. Accessed April 15, 2020.
27. IBM IT Infrastructure Blog. Storage for blockchain and modern distributed database processing, available on: https://www.ibm.com/blogs/systems/storage-for-blockchain-and-modern-distributed-database-processing/. Published February 8, 2019. Accessed April 13, 2020.
28. IBM Storage. "Why new off-chain storage is required for blockchains", *International Business Machines Corporation* (2018): 1-11. Download available on: https://www.ibm.com/downloads/cas/RXOVXAPM. Accessed March 12, 2020.
29. Information Commissioner's Office. Guide to the General Data Protection Regulation (GDPR) (2018):1-295. Available on: https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf. Published April 2, 2018. Accessed March 3, 2020.
30. Information Commissioner's Office. Right to erasure, available on: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/. Accessed October 24, 2019.
31. Information Commissioner's Office. What are identifiers and related factors, available on: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-are-identifiers-and-related-factors/. Accessed January 5, 2020.

32. Information Commissioner's Office. What is personal data, available on: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/. Accessed March 3, 2020.
33. Information Commissioner's Office. What is personal data, available on: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/. Accessed March 3, 2020.
34. International Data Sanitization Consortium. Data Sanitization Terminology and Definitions, available on: https://www.datasanitization.org/data-sanitization-terminology/. Accessed March 16, 2020.
35. International Finance Corporation, World Bank Group. Blockchain Governance and Regulation as an Enabler for Market Creation in Emerging Markets (2018):1-8. Available on: https://openknowledge.worldbank.org/bitstream/handle/10986/30658/131343-BRI-EMCompass-Note-57-Blockchain-Governance-v1-PUBLIC.pdf?sequence=1&isAllowed=y. Accessed April 23, 2020.
36. International Finance Corporation. John Salmon, Gordon Myers, "Blockchain and Associated Legal Issues for Emerging Markets", available on: https://www.ifc.org/wps/wcm/connect/da7da0dd-2068-4728-b846-7cffcd1fd24a/EMCompass-Note-63-Blockchain-and-Legal-Issues-in-Emerging-Markets.pdf?MOD=AJPERES&CVID=mxocw9F. Accessed March 19, 2020.
37. Jessica Schroers, "Are public keys personal data?", available on: https://www.law.kuleuven.be/citip/blog/are-public-keys-personal-data/. Accessed January 29, 2020. Published May 8, 2018.
38. Logic2020. GDPR compliance: Pseudonymization vs. anonymization, available on: https://www.logic2020.com/insight/gdpr-compliance-pseudonymization-vs-anonymization. Accessed March 25, 2020.
39. Martin Florian, Sophie Beaucamp, Sebastian Henningsen, Björn Scheuermann, "Erasing Data from Blockchain Nodes": 1-10. Available at: arXiv:1904.08901v1 [cs.CR]. Download available at: https://arxiv.org/pdf/1904.08901.pdf.
40. Michel Rauchs, Apolline Blandin, Keith Bear, Stephen McKeon "2nd Global Enterprise Blockchain Benchmarking Study", *Cambridge Centre for Alternative Finance, University of Cambridge: Judge Business school* (2019): 1-72. Available on: https://www.crowdfundinsider.com/wp-content/uploads/2019/09/2019-ccaf-second-global-enterprise-blockchain-report.pdf . Accessed February 8, 2020.

41. Nodes.com. Blockchain Nodes: An In-Depth Guide. Available on: https://nodes.com/. Accessed December 30, 2019.
42. Pritesh Shah, Daniel Forester, Davis Polk & Wardwell Llp, Matthias Berberich, Carolin Raspé, Hengeler Mueller, with Practical Law Data Privacy Advisor, "Blockchain Technology: Data Privacy Issues and Potential Mitigation Strategies", *Thomson Reuters* (2019): 1-8. Available on : https://www.davispolk.com/files/blockchain_technology_data_privacy_issues_and_potential_mitigation_strategies_w-021-8235.pdf. Accessed March 27, 2020.
43. PwC. Governance in the Age of Blockchain Distributed Ledger Technology, available on: https://www.pwc.com/us/en/about-us/new-ventures/assets/pwc-governance-in-the-age-of-blockchain-distributed-ledger-technology.pdf. Accessed April 7, 2020.
44. The CNIL (Commission nationale de l'informatique et des libertés). *Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data*. Published November 6, 2018. Download available on: https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf. Accessed December 15, 2019.
45. Tom Lyons, Ludovic Courcelas, Ken Timsit, "Blockchain and the GDPR", thematic Report for *The European Union Blockchain Observatory and Forum*. Published 16 October 2018. Available on: https://www.eublockchainforum.eu/reports. Accessed December 29, 2019.
46. Tom Lyons, Ludovic Courcelas, Ken Timsit, "Legal and regulatory framework of blockchains and smart contracts", thematic report for *The European Union Blockchain Observatory and Forum*. Published 27 September 2019. Download available on: https://www.eublockchainforum.eu/reports. Download available: Accessed February 1, 2020.
47. Vedat Akgiray, "The Potential for Blockchain Technology in Corporate Governance", *OECD Corporate Governance Working Papers*, No. 21, OECD Publishing, Paris (2019):1-32, p.18. Available at https://datubazes.lanet.lv:4876/10.1787/ef4eba4c-en.
48. Verypossible.com. Brian Zambrano, "Blockchain Explained: How Does Immutability Work?", available on: https://www.verypossible.com/blog/blockchain-explained-how-does-immutability-work. Published February 27, 2018. Accessed February 5, 2020.
49. White & Case LLP. Dr. Detlev Gabel, Tim Hickman, "Chapter 9: Rights of data subjects – Unlocking the EU General Data Protection Regulation", available on: https://www.whitecase.com/publications/article/chapter-9-rights-data-subjects-unlocking-

eu-general-data-protection-regulation. Accessed November 5, 2019. Published April 5, 2019.

50. Wolfgang Braun, Susanne Dehmel, Heiko Gossen, Dr. Hartmut Hässig, Lars Kripko, Ilona Lindemann, Christian Wagner, Stephan Weinert, "The Processing Records: Records of Processing Activities according to Art. 30 General Data Protection Regulation (GDPR)", Bitkom e. V. Federal Association for Information Technology, Telecommunications and New Media (2017): 1-42, pp. 13-18. Available on: https://www.bitkom.org/sites/default/files/file/import/180529-LF-Verarbeitungsverzeichnis-ENG-online-final.pdf. Accessed April 18, 2020.