UNIVERSITY OF TARTU
SCHOOL OF LAW
Department of Public Law

Anastasia Miller

Data protection on blockchain in the context of the General Data Protection Regulation

Master's thesis

Supervisor
PhD Aleksei Kelli

Tallinn
2019

Table of Contents

1. Introduction

In 1988 Timothy May envisioned "encrypted packets and tamper-proof boxes" [1] – today known as blockchain technology, which is predicted to disrupt industries, such as banking, healthcare, real estate and the legal industry.[2]

The Charter of Fundamental Rights of the European Union Article 8 enshrines the protection of personal data as a fundamental right.[3] Data protection in the European Union is regulated by the General Data Protection Regulation (hereinafter "GDPR")[4], which on the 25th of May 2018 became directly enforceable in all Member States in the European Union. In light of rapid technological developments and globalisation, the European legislator saw new challenges for the protection of personal data. Those developments required a strong and more coherent data protection framework in the Union, backed by strong enforcement in order for the natural persons to regain control over their personal data.[5]

Although the protection of natural persons should be technologically neutral and should not depend on the techniques used[6], it is not clear how several provisions of the GDPR should be complied with in the context of blockchain technology. This uncertainty arises in regard to the defining features of blockchain technology - decentralization, immutability and anonymity – which contradict the centralised and vertical architecture of the GDPR. As such the question arises whether the European data protection regime is suitable for blockchain technology. To conclude, the research problem is the tension of certain elements of the European data protection regime, and the subsequent compliance with it, *vis a vis* the core characteristics of

[1] T. May. Anarchist Manifesto - https://www.activism.net/cypherpunk/crypto-anarchy.html (01.04.2019)
[2] B. Marr. Here Are 10 Industries Blockchain Is Likely To Disrupt - https://www.forbes.com/sites/bernardmarr/2018/07/16/here-are-10-industries-blockchain-is-likely-to-disrupt/#4db6a9fab5a2 (01.04.2019)
[3] Charter of Fundamental Rights of the European Union OJ C 326, 26.10.2012, p. 391–407. Article 8(1) Everyone has the right to the protection of personal data concerning him or her; (2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
[4] 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.
[5] Recital 6-7 GDPR
[6] Recital 15 GDPR

blockchain technology. Subsequently, the purpose of the thesis is to research whether blockchain and the GDPR can be reconciled as well as develop a comprehensive approach on the topic.

In order to research the topic, three research questions will be proposed. First, whether data processing on a blockchain falls within the material scope of the GDPR and thus whether the GDPR applies to blockchain? Second, whether in decentralised data sharing it is possible to attribute responsibility and fulfil the territorial scope? Third, whether selected data protection requirements can be fulfilled in relation to blockchain? Based on the research questions the hypothesis of the thesis is that the data protection regime in the European Union is incompatible with the technology of blockchain.

The research is novel, as the topic has not been researched in Estonia before. Some foreign scientific articles and books have been published on the topic but considering the ever-growing need to protect the privacy of individuals, especially in the context of rapid technological advancement, the topic requires further research.

As due to the limit restrictions, it is not possible to analyse the whole GDPR in relation to blockchain, only the most relevant provisions will be looked at. In addition, although on a national level data protection in Estonia is regulated by the Personal Data Protection Act[7], the focus of this thesis will be solely on the GDPR. The justification being first that the GDPR is directly enforceable in all member states, and second to conduct a wider research.

In order to fully understand how the technological elements relate to the legal elements, a short overview of the technological components must be provided. Blockchain is a form of electronic distributed ledger technology (hereinafter "DLT")[8] which blends together several existing technologies, including peer-to-peer networks, public-private key cryptography, and consensus mechanisms, to create what can be thought of as a highly resilient and tamper-resistant database where people can store data in a transparent and non-reputable manner and engage in a variety of economic transactions pseudonymously.[9] Blockchain, however, is only one, albeit the most know, type of DLT - one that compiles transactions in blocks that are

[7] Personal Data Protection Act - RT I, 04.01.2019, 11.
[8] R. Girasa. Regulation of cryptocurrencies and blockchain technologies : national and international perspectives. Cham : Palgrave Macmillan, 2018. p. 29-30.
[9] P. De Filippi, A. Wright. Blockchain and the law : the rule of code. Cambridge, Massachusetts : Harvard University Press, 2018. p. 2.

then chained to each other.[10] Other DLT's are for example IOTA, where a stream of transactions is entangled together rather than grouped into blocks.[11] Although these new models are not blockchains per se, the term "Blockchain" is now commonly used to refer to distributed ledger technology in general and to the phenomenon surrounding DLT.[12]

A distributed ledger is a type of database that is shared across a peer-to-peer network comprised of independent computers (known as 'peers' or 'nodes'), often scattered across the globe.[13] Blockchains operate on a vertical hierarchical structure as opposed to the client-server model provided by most online service providers today[14] meaning there is no central coordinating authority, for example a bank, for the organization of the network. [15] The information contained on a ledger can be of informative, commercial or legislative significance.[16] Nodes are the devices running the DLT software that collectively maintain the database records[17], having their own identical copy of the ledger. [18] Any changes to the ledger are reflected in all copies in minutes.[19]

Data on the blockchain is encrypted and organized into smaller datasets referred to as "blocks". [20] Each block contains a header used to organize the shared database. The core components of a block's header are a unique fingerprint called hash of all transactions contained in that block, along with a timestamp and a hash of the previous block.[21] Linked together sequentially, these "blocks" form "chains" that make up larger "blockchain"

---

[10] E. Ganne. p. 7.
[11] What is Iota? - https://www.iota.org/get-started/what-is-iota (14.02.2019)
[12] E. Ganne. p. 7.
[13] *Ibid.* p. 2.
[14] P. De Filippi, Blockchain and the law. p. 34.
[15] D. Schoder. *et al.* Core Concepts in Peer-to-Peer Networking - https://pdfs.semanticscholar.org/cb43/290129a3f85455c229285799925d2a794043.pdf (16.01.2019) p. 3.
[16] Krüptograafiliste algoritmide elutsükli uuring. Cybernetica. 2017 - https://www.ria.ee/sites/default/files/content-editors/publikatsioonid/kruptograafiliste_algoritmide_elutsukli_uuring_2017.pdf (12.01.2019)
[17] R. Girasa. p. 29-30.
[18] M. Walport. Distributed ledger technology: Beyond blockchain. London: Government Office for Science, 2016. - https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf (12.01.2019)
[19] *Ibid.*
[20] P. De Filippi, A. Wright. Decentralized Blockchain Technology and the Rise of Lex Cryptographia. March 10, 2015 - https://ssrn.com/abstract=2580664 (06.01.2019)
[21] P. De Filippi, Blockchain and the law. p. 22.

databases of transactions that broadcast a permanent record of transactions whilst maintaining the anonymity of users and specific content exchanged.[22]

A new block of aggregated transactions will only be added to the ledger after the computers on the network reach consensus as to the validity of the transaction. Consensus within the network is achieved through different voting mechanisms, the most common of which is Proof of Work.[23] A proof-of-work consensus model requires the client requesting the service prove that some work has been done in order to process the request. An example of proof-of-work consensus model is the Bitcoin mining, which is a process of solving complex mathematical problems to validate the block. [24]

After a block has been added to the blockchain, it can no longer be deleted and the transactions it contains can be accessed and verified by everyone on the network.[25] A copy of the blockchain is stored on every computer in the network and these computers periodically synchronize to make sure that all of them have the same, shared database. [26] Because blockchains are widely replicated, any data stored in a blockchain is highly resilient and can survive even if a copy of a blokchain is corrupted or if a node on a network fails. [27] Furthermore, blockchains are intended to be maintained by all users in manners meant to be immutable, unless users arrive at a clear consensus to undertake changes.[28]

Because the header of each block incorporates a hash of the preceding block's header, anyone trying to modify the content stored in a block will inevitably break the chain. Even a small alteration will give rise to a new, unique hash tied to the altered block, and will necessarily trigger a change to the hashes of all subsequent blocks. Anyone willing to modify even a single record in the blockchain would have to go through the computationally expensive task of generating new hashes for every subsequent block. The most plausible way to change a record in the blockchain would be to engage in a "51% attack" and effectively take over the

[22] . Campbell-Verduyn. Bitcoin and beyond: cryptocurrencies, blockchains, and global governance. Abingdon, Oxon ; New York, NY : Routledge, an imprint of the Taylor & Francis Group, 2018. p. 1.
[23] De Filippi. Decentralized Blockchain Technology and the Rise of Lex Cryptographia. p. 7.
[24] C. L. Reyes. Moving Beyond Bitcoin to an Endogenous Theory of Decentralized Ledger Technology Regulation: An Initial Proposal – Villanova Law Review. 2016: 61(1), article 5. pp. 191-234 (197-198).
[25] De Filippi. Decentralized Blockchain Technology and the Rise of Lex Cryptographia. p. 8.
[26] *Ibid.* p. 7.
[27] P. De Filippi, Blockchain and the law. p. 2.
[28] M. Campbell-Verduyn. p. 1.

network so that the attackers can approve transactions at a rate that outpaces the rest of the network.[29] Therefore the data on the blockchain is considered immutable. Conte de Leon *et al.* point out that the immutability is, however, a misconception because computational work is needed to modify its data while preserving the soundness, up to the strength of the hash function used. This does not mean that such a blockchain is immutable, but that an agent or set of agents with a sufficient amount of computing power has modified it, perhaps collaboratively.[30] However, as such a modification requires the consensus of over half of the nodes, substantive computational power and financial resource, for the purposes of this thesis the data on blockchains shall be considered immutable.

Furthermore, three types of blockchains exist: public perimissionless where no specific entity or entities manages the platform and which is open to everyone; private blockchains, where the permissions to validate and write data onto the blockchain are controlled by one entity which is highly trusted by the other users, and participants are identified; and a consortium blockchain a subtype of private blockchain that operates under the leadership of a group rather than a single entity and in which participants are identified. [31] For the purposes of the present thesis an example of a private blockchain – the KSI blockchain of Guardtime – and a public blockchain – the Bitcoin blockchain – will be used.

Derived from the research question the thesis is divided into three chapters. The first chapter analyses whether data on a blockchain is personal data and whether the data is processed pursuant to the GDPR. Therefore the chapter answers the question whether the material scope of the GDPR is fulfilled.

The second chapter concentrates on the data protection challenges in decentralised systems. More specifically, whether it is possible to define a controller in decentralized systems, as well as at the problem of territorial scope in decentralized systems. As a processor processes personal data on behalf of the controller, the primary question of the present thesis will be that of controllership. In addition, transfers of personal data to third countries or international organisations will be touched upon as part of the territorial scope in order to highlight the problems of distributed ledgers.

[29] P. De Filippi, Blockchain and the law. p. 25.
[30] D. Conte de Leon, *et al.* Blockchain: properties and misconceptions - Asia Pacific Journal of Innovation and Entrepreneurship. 2017:11(3) pp. 286-300 (290)
[31] E. Ganne. Can blockchain revolutionize international trade?. Geneva : World Trade Organization, 2018. p. 9-11.

The third chapter considers the data protection requirements in the European Union. More specifically, first principles will be looked at as they provide the foundations for European data protection law.[32] Second, the legal ground for processing will be assessed. Third, rights of the data subject will be looked at. As part of the third chapter only the most relevant provisions in relation to blockchain will be analysed.

To answer the research question, mostly systematic and analytical methods have been used in all chapters. The analytical method has been used to analyse the suitability of blockchain technology to the data protection regime.

The basis of this thesis is the GDPR. However, in order to understand the GDPR, the opinions of Article 29 Data Protection Working Party (hereinafter "29WP") and the European Data Protection Board (hereinafter "EDPB"), have been used. Since 25th of May 2018 the 29WP has been succeeded by the EDPB, an independent European body composed of representatives of the national data protection authorities, and the European Data Protection Supervisor.[33] Albeit not legally binding, the opinion of the WP29, now succeeded by the EDPB, possesses undeniable "persuasive authority" and provides the most comprehensive guidelines for data controllers as to how they should apply the concept of personal data in their day-to-day practice. [34] In addition, Judges and Data Protection Authorities often follow their interpretation.[35] However, due to the advisory nature of the opinions, it is also important to look at the interpretation of personal data in the case law of the CJEU of Justice of the European Union (hereinafter "CJEU"). Finally, the research articles by Michele Finck, Matthias Brebereich and Malgorzata Steiner, Lokke Moerel as well as Thomas Buocz *et al.* have been used to construct the legal arguments.

[32] D. Kelleher, K. Murray. EU data protection law. Dublin : Bloomsbury Professional(2018). p. 137.
[33] European Data Protection Board. About EDPB - https://edpb.europa.eu/about-edpb/about-edpb_en (29.04.2019)
[34] N. Purtova. The law of everything. Broad concept of personal data and future of EU data protection law - Law, Innovation and Technology. 2018: 10(1) pp. 40-81 (43)
[35] F. Zuiderveen Borgesius - Singling Out People Without Knowing Their Names – Behavioural Targeting, Pseudonymous Data, and the New Data Protection Regulation. February 16, 2016 - https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2733115 (01.02.2019), p. 10.

The keywords provided by the Estonian Subject Thesaurus that best characterise the current master's thesis are the following: data protection, blockchain technology, personal data, data processing.

2. Personal data processing on blockchain

2.1. Personal data

The material scope of the GDPR is laid down in Article 2, which states "the regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system". Therefore the GDPR applies to data that is (1) personal and (2) being processed by automated means with (3) none of the exceptions in Article 2(2) present.

Personal data is defined as "any information relating to an identified or identifiable natural person ('data subject')".[36] An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[37] The 29WP outlines four elements of the definition of personal data: (1) any information, (2) relating to, (3) identified or identifiable, (4) natural person.

The first element of the definition is "any information" which clearly signals the willingness of the legislator to design a broad concept of personal data. The concept of personal data covers any sort of statements about a person – both objective information, such as the presence of a certain substance in one's blood, and subjective information, such as opinions or assessments. Furthermore, the information does not have to be true or proven. [38] In terms of content "personal data" includes data providing any sort of information, covering both "sensitive data" (corresponding to GDPR Article 9 special categories of data) and more

[36] Article 4(1) GDPR
[37] Article 4(1) GDPR
[38] Article 29 Data Protection Working Party. Opinion 4/2007 on the concept of personal data. WP 136. Brussels: 2007 - https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf (07.02.2019) p. 6.

general data. The term "personal data" includes information touching the individual's private and family life *stricto sensu*, but also information regarding whatever types of activity is undertaken by the individual, like economic behaviour of the individual.[39] Finally, in terms of format, personal data includes information available in whatever form, be it alphabetical, numerical, graphical, photographical or acoustical.[40] It can be on paper, in a computer memory as binary code, structured or in free text or a document.[41] A voice recording or a child's drawing can also be considered personal data.[42]

The CJEU has stated several times in the case law that the scope of the Directive is wide and the personal data covered in that directive is varied.[43] Which ties into the 29WP's opinion of the broad concept of personal data. In the case *Peter Nowak v Data Protection Commissioner* the CJEU assessed whether the written answers submitted by a candidate at a professional examination and any examiner's comments with respect to those answers constitute personal data. The CJEU noted that "any information" is not restricted to information that is sensitive or private, but potentially encompasses all kinds of information, not only objective but also subjective, in the form of opinions and assessments, provided that it "relates" to the data subject.[44]

The second element of the 29WP definition is "relating to". In order to consider that data can "relate" to an individual three elements (content, purpose, result) must be considered as an alternative. If one element is present, it should be considered that the information relates to the individual. The content element is present in those cases where information it is about that individual, for example the information contained in a company's folder under the name of a client. The purpose element can be considered to exist when data is used with the purpose of evaluating, treating in a way or influencing the status or behavior of an individual. The result element entails data being used to have an impact on a certain person's rights or interests.[45]

[39] WP136. p. 6.
[40] *Ibid.* p. 6-7.
[41] WP136. p. 8.
[42] *Ibid.* p. 8.
[43] CJEU C‑553/0 *College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer*, para 59; CJEU C‑434/16, *Peter Nowak v Data Protection Commissioner*, para 33; CJEU C-101/01, *Bodil Lindqvist*, para. 88.
[44] CJEU C‑434/16, *Peter Nowak v Data Protection Commissioner*, para. 34.
[45] WP136. p. 10-11.

The CJEU has also assessed the element "relating to". The first time was in the case of *YS and others vs Minister voor Immigratie* where the CJEU assessed whether the data relating to the applicant for a residence permit and the legal analysis included in the application (the "minute") can be considered personal data. The CJEU found that "there is no doubt that the data relating to the applicant for a residence permit and contained in a minute, such as the applicant's name, date of birth, nationality, gender, ethnicity, religion and language, are information relating to that natural person, who is identified in that minute in particular by his name, and must consequently be considered to be 'personal data'".[46] As for the legal analysis, the CJEU stated that it "may contain personal data, it does not in itself constitute such data".[47] Therefore the CJEU appears to interpret "information relating to" narrowly as information about an individual and rejects the broader approach of 29WP's opinion where information can also relate to an individual not by virtue of its content, but by reason of the purpose or effect of it's processing.[48]

However, the CJEU revisited the element in the case *Nowak* where the court stated that information 'relates' to the data subject when the information, by reason of its content, purpose or effect, is linked to a particular person.[49] First the court stated that the content of the answers in the written examination reflect the extent of the candidate's knowledge and competence in a given field and, in some cases, his intellect, thought processes, and judgment. In the case of a handwritten script, the answers contain, in addition, information as to his handwriting.[50] Second, the purpose of collecting the examination answers is to evaluate the candidate's professional abilities and his suitability to practice the profession concerned.[51] And third, use of that information, one consequence of that use being the candidate's success or failure at the examination concerned, is liable to have an effect on his or her rights and interests, in that it may determine or influence, for example, the chance of entering the profession aspired to or of obtaining the post sought.[52] Therefore the CJEU adopted the alternative test of content, purpose or effect used by 29WP, effectively reversing the restrictive view of "information relating to" in *YS and others.*[53]

---

[46] CJEU joined cases C‑ 141/12 and C‑ 372/12, *YS v Minister voor Immigratie, Integratie en Asiel, and Minister voor Immigratie, Integratie en Asiel v M, S,* para. 38.
[47] *Ibid.* para. 39.
[48] N. Purtova. p. 68.
[49] CJEU C‑ 434/16, para. 34-35.
[50] *Ibid.* para. 37.
[51] *Ibid.* para. 38.
[52] *Ibid.* para. 39.
[53] N. Purtova. p. 72.

The third element requires the natural person to be "identified or identifiable". A natural person can be considered as "identified" when, within a group of persons, he or she is "distinguished" from all other members of the group. This also includes the possibility of said distinguishing.[54] Identification is further broken down into direct and indirect. Direct identification is for example someone being identified by name, while indirect identification is when through the collection of unique identifiers a person might still be identifiable even though those identifiers alone will not allow to single out a person.[55]

It is also important to consider the means likely or reasonably used by the controller or third person to identify the data subject. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.[56] All factors should be considered, such as cost conducting identification, the intended purpose, the structuring of processing, the advantage expected by the controller, the interests at stake for the individuals, as well as risk of organizational dysfunctions (e.g. breaches of confidentiality duties) and technical failures.[57] If a possibility to identify does not exist or is negligible, the person should not be considered as identifiable and the information would not be considered "personal data".[58] Furthermore, where the purpose of the processing implies the identification of individuals, it can be assumed that the controller or any other person involved will have the means "likely reasonably to be used" to identify the data subject. Such could be the case for example in video surveillance, as the sole purpose of it is to identify the persons seen in the video images.[59]

The standard for identifiability was set in the *Patrick Breyer v Bundesrepublik Deutschland* case. Static IP addresses are considered personal data[60]. The CJEU ruled that dynamic IP addresses on their own do not constitute personal data, because such an address does not

[54] WP136. p. 12.
[55] *Ibid.* p. 13.
[56] Recital 26 GDPR
[57] WP136. p. 15.
[58] *Ibid.*
[59] WP136. p. 16.
[60] CJEU C-70/10, *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, para. 51.

directly reveal the identity of the natural person.[61] Then the CJEU assesses whether the dynamic IP addresses combined with other information provided by the Internet service provider would render the data subject identifiable. The CJEU proceeded to note that an identifiable person is one who can be identified directly or indirectly.[62] To determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person.[63] The CJEU noted that or information to be treated as 'personal data' it does not have to be in the hands of one person.[64]

The CJEU found that identification would not be possible if the identification of the data subject was prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant.[65] Although in Germany it is not possible for internet service providers (hereinafter "ISP") to transfer the data directly to the online media service provider, in the event of a cyber attack the online media services provider is able to contact the competent authority, so that the latter can take the steps necessary to obtain that information from the ISP and to bring criminal proceedings.[66] Therefore in *Breyer* dynamic IP addresses were found to be personal information.

It is important to note that the CJEU adopted a more restrictive approach to what would reasonably likely than the. Namely identification would not be reasonably likely if prohibited by law. The 29WP names a possibility of organizational dysfunction, meaning also data security breaches resulting from illegal acts, among the relevant factors to be assessed, which is in direct contradiction with the CJEU.[67]

Finally, data protection rules apply to natural persons. This means that information relating to both dead persons and legal persons fall outside the scope of the GDPR. However, in some instances aforementioned information may relate to natural persons and therefore the data

[61] CJEU C‑582/14, *Patrick Breyer v Bundesrepublik Deutschland.* para. 38.
[62] *Ibid.* para. 40.
[63] *Ibid.* para. 42.
[64] *Ibid.* para. 43.
[65] *Ibid.* para. 46.
[66] CJEU C‑582/14, para. 47.
[67] N.Purtova. pp. 64-65.

protection rules would apply indirectly. That would be the case for example where the legal name of the legal person derives from that of a natural person.[68]

Looking at the four criteria in union, it becomes evident that the WP29 leaves the scope of "personal data" very wide. Several authors [69] have argued that in the age of rapid technological advancement and machine data processing, especially big data, the wide scope of personal data could lead to a scenario where everything is personal data. As a result, the intensive compliance regime of the GDPR will become "the law of everything", well meant but impossible to maintain. [70]

The principles of data protection should not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.[71] An important factor is that the processing must be irreversible.[72] Therefore anonymous data falls outside the scope of the GDPR. Pseudonymous data however, still constitutes personal data.[73] Pseudonymisation is the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information. [74] According to the WP29 both encryption and hashing constitute pseudonymisation techniques.[75]

A separate category of personal data is "sensitive data"[76] – data, which is by its nature, particularly sensitive in relation to fundamental rights and freedoms of the data subject.[77] Special data is personal data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data,

[68] WP136. p. 21-23.
[69] See for example: N. Purtova. The law of everything. Broad concept of personal data and future of EU data protection law - Law, Innovation and Technology. 2018: 10(1) pp. 40-81; P. Ohm. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization - UCLA Law Review. 2010:57. p. 1701.
[70] N. Purtova. p. 40.
[71] Recital 26 GDPR
[72] Article 29 Data Protection Working Party. Opinion 05/2014 on Anonymisation Techniques. WP216. Brussels: 2014 - https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf (10.02.2019), p. 5.
[73] Recital 26 GDPR
[74] Article 4(5) GDPR
[75] WP216. p. 20.
[76] Recital 10 GDPR
[77] Recital 51 GDPR

biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.[78]

These personal data are considered as sensitive (as this term is commonly understood) because they are linked to household and private activities (such as electronic communications whose confidentiality should be protected), or because they impact the exercise of a fundamental right (such as location data whose collection questions the freedom of movement) or because their violation clearly involves serious impacts in the data subject's daily life (such as financial data that might be used for payment fraud).[79]

2.2. Data on blockchain

On the blockchain records are stored one after the other in a continuous ledger[80] into "blocks".[81] Each block contains a header used to organize the shared database. The core components of a block's header are a unique fingerprint called hash of all transactions contained in that block, along with a timestamp and a hash of the previous block.[82] Linked together sequentially, these "blocks" form "chains" that make up larger "blockchain" databases of transactions that broadcast a permanent record of transactions whilst maintaining the anonymity of users and specific content exchanged.[83]

DLT's rely on a two-step verification process with asymmetric encryption. Every user has a public key[84], best of thought as an account number that is shared with others to enable transactions. In addition, each user has a private key, which is best thought of as a password that must never be shared with others. Both keys have a mathematical relationship by virtue

[78] Article 9(1) GDPR
[79] Article 29 Data Protection Working Party. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. WP 248. Brussels: 2017 - https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 (29.04.2019), p. 8.
[80] R. Maull, *et al.* p.483
[81] P. De Filippi, A. Wright. Decentralized Blockchain Technology and the Rise of Lex Cryptographia. March 10, 2015 - https://ssrn.com/abstract=2580664 (06.01.2019)
[82] P. De Filippi, Blockchain and the law. p. 22.
[83] . Campbell-Verduyn. Bitcoin and beyond: cryptocurrencies, blockchains, and global governance. Abingdon, Oxon ; New York, NY : Routledge, an imprint of the Taylor & Francis Group, 2018. p. 1.
[84] A string of letters and numbers represeting the user.

of which the private key can decrypt data that is encrypted through the public key. Public keys thus hide the identity of the individual unless they are linked to additional identifiers.[85]

Thus two types of data are stored on a blockchain – the data, which is stored in blocks and the public key. The information contained on a ledger in blocks can be of informative, commercial or legislative significance.[86] Although Guardtime's blockchain is Keyless Signature Infrastructure (KSI), which relies on cryptographic properties of hash functions and the availability of widely published verification codes, rather than the secrecy of private keys[87], it is rather something specific to Guartime's technology.

In the case of Guardtime's KSI blockchain, which is the underlying technology of Estonia's e-Health platform, the blocks contain medical data about a patient, such as blood type, allergies, recent treatments, test results, on-going medication including information about prescriptions or pregnancy.[88] Said data relates to the patient in terms of content, as it is about the data subject. Furthermore, as said data is personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status,[89] the data concerns health pursuant Article 9(1) and merits special protection under the European data protection regime.

The Bitcoin blockchain lists transfers of Bitcoins between different addresses.[90] Every transfer consists of elements that the user determines directly - the input and output addresses and the transferred value, as well as elements containing the metadata, which are the transfer hash and time that the transfer's block was mined.[91] The Bitcoin address is generated from and corresponds to a public key and it is used the same way as the beneficiary name on a

[85] M. Finck. Blockchains and Data Protection in the European Union - European Data Protection Law Review. 2018: 4(1) pp. 17-35 (19).
[86] Krüptograafiliste algoritmide elutsükli uuring. Cybernetica. 2017 - https://www.ria.ee/sites/default/files/content-editors/publikatsioonid/kruptograafiliste_algoritmide_elutsukli_uuring_2017.pdf (12.01.2019)
[87] A. Buldas, *et al.* Keyless signature infrastructure and PKI: hash-tree signatures in pre- and post-quantum world. International Journal of Services Technology and Management. 2017 - https://www.researchgate.net/publication/313235634_Keyless_signature_infrastructure_and_PKI_hash-tree_signatures_in_pre-_and_post-quantum_world (30.04.2019)
[88] e-Estonia. Healthcare - https://e-estonia.com/solutions/healthcare/e-health-record/ (13.04.2019)
[89] Article 4(15) GDPR
[90] T. Buocz, *et al.* p. 185.
[91] T. Buocz, *et al.* p. 185.

cheque (i.e. "Pay to the order of "). [92] It should also be noted that the instruction OP_RETURN allows saving arbitrary data on the Bitcoin blockchain.[93] However, arbitrary data is more of an exception, than a rule, as OP_RETURN transactions constitute ~ 0.96% of the total transactions in the blockchain.[94] Therefore the analysis will focus on the transactional and metadata. Bitcoin users are natural people, thus the data contained on a Bitcoin blockchain is any information, such as information alluding to financial behaviour[95] relating to the user.

As the data stored in blocks is encrypted and encryption is considered a pseudonymisation technique[96], the data stored on a blockchain does not allow for direct identification of the data subject. Similarly public keys are hashed which permits direct identification. Therefore according to the 29WP definition of personal data, it must be assessed whether combined with additional information the data subject could be identified. Applying the *Breyer* standard identification would not be possible if it is prohibited by law or requires disproportionate effort.[97] In the current examples this appears not to be the case.

For example Bitcoin users disclose their addresses intentionally when interacting with online wallet service providers, exchange platform providers, or Bitcoin merchants.[98] Bitcoin users can be identified through mapping their Bitcoin addresses to IP addresses[99] or by clustering the addresses[100]. It should be noted that Bitcoin users could hide their identity using proxy or anonymity services, such as Tor.[101] However, even Tor or other anonymity service can be cut-off.[102]

---

[92] A. M. Antonopoulos. Mastering bitcoin : programming the open blockchain. Sebastopol, Calif. : O'Reilly Media, 2017. p. 61.
[93] M. Bartoletti, L. Pompianu. An analysis of Bitcoin OP RETURN metadata - https://fc17.ifca.ai/bitcoin/papers/bitcoin17-final32.pdf (16.02.2019) p. 1.
[94] *Ibid.* p. 7.
[95] WP136. p. 6.
[96] WP216. p. 20.
[97] *Ibid.* para. 46.
[98] T. Buocz, *et al.* p. 189.
[99] B. Fabian, T. Ermakova, U. Sander. Anonymity in Bitcoin? – The Users' Perspective - https://www.researchgate.net/publication/308648091_Anonymity_in_Bitcoin_-_The_Users'_Perspective (25.02.2019), p. 3.
[100] *Ibid.*
[101] *Ibid.*
[102] A. Biryukov, D. Khovratovich, I. Pustogarov. Deanonymisation of Clients in Bitcoin P2P Network - https://orbilu.uni.lu/bitstream/10993/18679/1/Ccsfp614s-biryukovATS.pdf (26.02.2019)

There are numerous examples where metadata combined with information about person from an outside source allows for the identification of the individual.[103] Therefore drawing a parallel to *Breyer*, data identification should be very likely and thus both data contained on blocks and the public keys should be considered personal data pursuant to Article 4(1).

Such an opinion is shared by Michele Finck who concludes that encrypted and hashed transactional data – data stored on blocks revealing individual behaviour in Internet of Things use cases, digital identities, or financial and medical data – as well as public keys, are considered personal data under the GDPR.[104] Matthias Berberich and Malgorzata Steiner conclude similarly that even if additional information may be necessary to attribute information to the data subject, such information would be merely pseudonymised and count as personal information. Adding that a connection between pseudonymised data and the data subject will usually (and necessarily) arise in blockchain transactions affected for off-chain goods, e.g. conversion into real money payments, purchase of goods or services, registration data, where the transaction parties must be known.[105]

Moubry and others argue that if the precedent set by *Breyer* is to be applied to data, which has undergone pseudonymisation under the GDPR, it should be possible for these data to be rendered anonymous in some circumstances. In their example where Public Authority A provides administrative Research Centre B who strips the data of all identifying information, which is kept separately with technical and organizational controls to prevent the reattribution to the research data. Then the data is shared with an external researcher, who has no relationship with either A or B. Moubry and others argue that the pseudonymised data would not be personal data for the researcher if the researcher has no means reasonably likely to identify the data subjects.[106]

---

[103] See for example: J. Bohannon. Credit card study blows holes in anonymity – Science Magazine. 2015: 347(6221), p. 468; A. Hern. New York taxi details can be extracted from anonymised data, researchers say - https://www.theguardian.com/technology/2014/jun/27/new-york-taxi-details-anonymised-data-researchers-warn (13.04.2019); R. Lemos. Researchers reverse Netflix anonymization - https://www.securityfocus.com/news/11497 (13.04.2019)

[104] M. Finck. p. 22-25.

[105] M. Berberich, M. Steiner. Blockchain Technology and the GDPR - How to Reconcile Privacy and Distributed Ledgers - European Data Protection Law Review (EDPL). 2016: 2(3), pp. 422-426.

[106] M. Moubry, *et al.* Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK - Computer Law & Security Review. 2018: 34(2), pp. 222-233.

If the identification is practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power as pointed by the CJEU in *Breyer*[107], the identification of data subjects by the independent researcher should be denied.

2.3. Processing of personal data

Article 4(2) defines "processing" as any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.[108] In order to fall under the material scope of the GDPR processing has to be wholly or partly by automated means. Data is processed by automated means when manual interim steps are not required.[109]

The CJEU has ruled that operation of loading personal data on an internet page must be considered to be such "processing".[110] THE CJEU noted in *Bodil Linqvist* that placing information on an internet page is performed, at least in part, automatically.[111] In addition in *Heinz Huber v Bundesrepublik Deutschland* the CJEU found that the storage and transmission of personal data by the body responsible for the management of the register in which they are kept thus represents the "processing of personal data".[112]

Blockchain is a distributed ledger - a type of database that is shared across a peer-to-peer network comprised of independent computers (known as 'peers' or 'nodes'), often scattered across the globe.[113] Records are stored one after the other in a continuous ledger in blocks and can only be added when the participants reach a quorum.[114] A copy of the blockchain is stored

[107] *Ibid.* para. 46.
[108] Article 4(2) GDPR
[109] T. Buocz, *et al.* Bitcoin and the GDPR: Allocating responsibility in distributed networks - Computer Law & Security Review. 2019: 35(1), pp. 182-198 (190).
[110] CJEU C‑ 131/12, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, para. 26; CJEU C-101/01, para. 25.
[111] CJEU C-101/01, para. 26.
[112] CJEU C‑ 524/06, *Heinz Huber v Bundesrepublik Deutschland*, para. 43.
[113] P. De Filippi, A. Wright. p. 2.
[114] R. Maull, *et al.* p.483

on every computer in the network and these computers periodically synchronize to make sure that all of them have the same, shared database.[115]

For example in the Bitcoin blockchain after a user has created a new transfer, the transfer gets broadcasted to and stored in the network without human intervention. The process is carried out automatically by the nodes of the network according to the blockchain protocol and requires no manual interim steps.[116] As storing constitutes processing and no manual interim steps are required for that process, data on the blockchain is processed by automated means.

The exceptions to the material scope are found in Article 2(2). Pursuant to Article 2(2) the GDPR does not apply to personal data, which is processed: in the course of an activity which falls outside the scope of Union law; by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU; by a natural person in the course of a purely personal or household activity; or by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

Of the selection the "household exception" would be the most relevant to blockchain. A personal or household activity as processing with no connection to a professional or commercial activity, which could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. [117] In the case of a private blockchain, such as Guardtime's KSI blockchain, the processing does not take place in the course of a household activity. Therefore, the exception does not apply. However, the exception could apply in the case of a public blockchain, such as Bitcoin as it can be argued that a natural person who downloads the blockchain and runs it on their computer has no connection to a professional or commercial activity.

The French National Commission on Informatics and Liberty (hereinafter "CNIL") is of the opinion that natural persons who enter personal data on the blockchain, that do not relate to a professional or commercial activity, are not data controllers (pursuant to the "purely personal or household activity" exclusion set out in Article 2 of the GDPR). For example, a natural

[115] *Ibid.* p. 7.
[116] T. Buocz, *et al.* p. 9.
[117] Recital 18 GDPR

person who buys or sells Bitcoin, on his or her own behalf, is not a data controller. However, the said person can be considered a data controller if these transactions are carried out as part of a professional or commercial activity, on behalf of other natural persons.[118]

Furthermore, CJEU ruled that publication of personal data on the internet so that the data is made accessible to an indefinite number of people does not constitute processing in the course of private or family life of individuals.[119] Drawing a parallel to *Bodil Linqvist* it should be concluded that as a public permissionless blockchain, such as Bitcoin, is available for anyone to download and therefore the data will be available to an indefinite number of people, processing data on a public permissionless blockchain does not fall under the household exception pursuant to Article 2(2). Thomas Buocz *et al.* share such an opinion pointing out that the household exemption includes information disclosed to a limited circle of addresses (e.g. in direct messages to one or more recipients). On the contrary, social media posts that are available to an undefined public audience are not included in the household exemption. Thomas Buocz *et al.* conclude that like social media posts, Bitcoin transfers are broadcasted to the entire network. They can be viewed by every internet user and therefore do not fall within the household exemption.[120] Although Buocz *et al.* conclusion is made about Bitcoin exclusively, it applies to all public permissionless blockchains.

3. Decentralised data sharing on blockchain

3.1. Defining the controller

Article 5(2) states that "the controller shall be responsible for, and be able to demonstrate compliance with, [the principles of data protection pursuant to Article 5(1)]". Other provisions point to the controller taking on the responsibility for compliance with the GDPR.[121] According to Article 24(1) the controller shall implement appropriate technical and organisational measures to ensure and be able to demonstrate that processing is performed in accordance with the GDPR. The 29WP has also stressed that clearly identifying the natural or legal person responsible for breaches of data protection law is a perquisite for the effective

[118] Solutions for a responsible use of the blockchain in the context of personal data. CNIL - https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf (12.03.2019)
[119] CJEU C-101/01, *Bodil Lindqvist*, para. 47.
[120] T. Buocz, *et al.* p. 194.
[121] See for example: Articles 7, 12, 13, 16, 17, 18, 19, 20, 22, GDPR

application of the GDPR.[122] Furthermore, the question of controllership is also important in determining the material scope of the GDPR as per Article 3.

It becomes apparent that the GDPR is structured in a vertical hierarchical structure with the controller taking on the accountability for compliance, followed by the processor who acts on behalf of the controller and finally the data subject exercising their rights. However, blockchain technology is a hierarchical structure with the data subject interacting with all the other actors on the network. Thus, distributed ledgers pose a challenge for regulatory approaches that hinge on central intermediaries.[123] The inability to pin-point a controller could have serious implications for the entire data protection framework in the GDPR and many of the data subject's rights would be rendered useless e.g. the right to data retention, access and portability, security breach notifications and most importantly it would be difficult to coerce compliance with the heavy fines.[124] Therefore establishing the controller on a blockchain network is a crucial preliminary step. Furthermore, as a processor processes personal data on behalf of the controller, the primary question of the present thesis is that of controllership.

Article 4(7) of the GDPR defines the controller as "a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data". Therefore the definition contains three key elements.

The first element is "natural or legal person, public authority, agency or other body". This element of the definition refers to the personal side: who can be a controller and is crucial in determining liability and imposing sanctions.[125] The concept of controller is also an essential element in determining which national law is applicable.[126] The 29WP notes that in determining the controller preference should be given to a company or body, rather than a

[122] Article 29 Data Protection Working Party. Opinion 1/2010 on the concepts of "controller" and "processor". WP 169. Brussels: 2010 - https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf (01.03.2019), p. 15.
[123] M. Berberich, M. Steiner. Blockchain Technology and the GDPR - How to Reconcile Privacy and Distributed Ledgers - European Data Protection Law Review (EDPL). 2016: 2(3), pp. 422-426 (424).
[124] S. Kulhari. 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), p. 43.
[125] WP 169. pp. 15-16.
[126] *Ibid.* p. 5.

specific person within the company or body.[127] Likewise the GDPR favours a clear and univocal appointment of the controller, irrespective of whether a formal appointment has been made and publicised.[128] If a natural person working within a company or public body uses data for his or her own purposes, outside the activities of the company, this person shall be considered as *de facto* controller and will be liable as such.[129]

The second element is "alone or jointly with others". Joint controllership, a category, which was not present in the Directive 95/46/EC[130], shall be analysed in the next section.

The final element "determines the purposes and means of the processing of personal data" is the one that requires the most examination. First the word "determines" points to control exercised by the controller. It should be noted that the concept of a controller is based on a factual rather than a formal analysis therefore it is possible to be a controller irrespective of a specific competence or power conferred by law.[131] Control can stem from legal competence, implicit competence, such as the employer in relation to it's employees, and factual influence. The latter is the most problematic and more likely to lead to divergent interpretations. A remedy for this could be the analysis of contractual relationships between parties. Elements, such as the degree of actual control exercised by a party, the image given to data subjects and reasonable expectations of data subjects on the basis of this visibility could all be pointers to the factual controller.[132]

Furthermore, determining the "purposes and means" of the processing amounts to determining the "how" and "why" of processing of personal data. It is also important to consider the level of control someone details as the controller exercises the highest level of control while the processor acts on behalf of the controller.[133] "Purpose" is an anticipated outcome that is intended or that guides one's planned actions, while "means" is how a result is obtained or an end achieved.[134] The controller determines the "purpose" of the processing, as well as substantial questions, which are essential to the core of the lawfulness of

[127] *Ibid.* p. 15.
[128] *Ibid.* p. 15.
[129] Ibid. p. 17.
[130] 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.
[131] WP 169. pp. 8-9.
[132] *Ibid.* pp. 10-12.
[133] *Ibid.* p. 13.
[134] *Ibid.*

processing.[135] Determination of the "means" includes both technical and organizational questions, such as "which data shall be processed?", "which third parties will have access to this data?", "when shall data be deleted?". The decision of the "means" can be delegated to processors.[136] Therefore whoever decides the "purpose" of processing is the *de facto* controller.[137]

3.1.1. Joint controllers

According to Article 26(1) "where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers". Furthermore joint controllers "shall in a transparent manner determine their respective responsibilities for compliance with the obligations under [the GDPR] in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject". The arrangement should duly reflect the respective roles and relationships of the joint controllers *vis-à-vis* the data subjects and its essence shall be made available to the data subject.[138] Such an arrangement requires a clear allocation of the responsibilities.[139] The data subject may exercise their rights in respect of and against each of the controllers, irrespective of the terms of the arrangement.[140]

Joint control will arise when different parties determine with regard to specific processing operations either the purpose or those essential elements of the means, which characterize a controller.[141] The participation of the parties does not need to be equally shared.[142] However, the mere fact that subjects cooperate in processing of personal data, for example in a chain, does not entail that they are joint controllers in all cases, since an exchange of data between to parties without sharing purposes or means in a common set of operations should be

[135] *Ibid.* pp. 15.
[136] WP 169. p. 14.
[137] *Ibid.* p. 15
[138] Article 26(2) GDPR
[139] Recital 79 GDPR
[140] Article 26(3) GDPR
[141] WP 169. p. 19.
[142] CJEU C‑ 210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH,* para. 43.

considered only as a transfer of data between separate controllers.[143] Therefore in order to fulfil the criteria of joint controllership it is important to determine the purpose and means of processing, doing it in a clear and transparent manner by mutual agreement.

3.1.2. Controllership on a blockchain

While centralized solutions rely on pre-established trust between the central authority and the parties in the transaction[144], blockchains operate on a vertical hierarchical structure as opposed to the client-server model provided by most online service providers today.[145] This means that there is no central coordinating authority, for example a bank, for the organization of the network.[146] A copy of the blockchain is shared to each node across a peer-to-peer network. These shared databases operate globally and extend across national borders.[147]

In the traditional client-provider model, it is relatively easy to identify the controller - there is almost always an entity that is offering some product or service, or an agency fulfilling some function, that determines the purpose and means for processing, sets up the systems to do it, and collects and processes the data for the data subject. If several entities are jointly offering a product or service, they can be identified as joint controllers.[148]

The CNIL in their guidelines considers that participants, who have the right to write on the chain and who decide to send data for validation by the miners, can be considered data controllers. More specifically, a natural person and that the personal data processing operation is related to a professional or commercial activity (i.e. when the activity is not strictly personal) or a legal person who registers personal data on a blockchain. For example a notary recording their client's property deed on a blockchain or a bank entering its clients' data onto a blockchain as part of its client management processing – are the controllers.[149]

---

[143] WP 169. p. 19.
[144] D. Conte de Leon, *et al.* Blockchain: properties and misconceptions - Asia Pacific Journal of Innovation and Entrepreneurship. 2017: 11(3) pp.286-300 (294).
[145] P. De Filippi, Blockchain and the law. p. 34.
[146] D. Schoder. *et al.* Core Concepts in Peer-to-Peer Networking - https://pdfs.semanticscholar.org/cb43/290129a3f85455c229285799925d2a794043.pdf (16.01.2019) p. 3.
[147] P. De Filippi, Blockchain and the law. p. 34.
[148] The European Union Blockchain Observatory And Forum. Blockchain and the GDPR. Report - https://www.eublockchainforum.eu/reports (17.04.2019)
[149] Solutions for a responsible use of the blockchain in the context of personal data. CNIL - https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf (12.03.2019)

In case of a private blockchain it is possible to identify a controller (or several controllers in case of a consortium blockchain) – the controller is the natural or legal person who determines the purposes and means of processing. For instance, in the case of the e-Health platform provided by Guardtime's KSI blockchain – the purposes and means of processing are determined by the Ministry of Social Affairs, while the processor is Health and Welfare Information Systems Centre.[150] Several authors support such an interpretation.[151] In a public permissionless blockchain allocating responsibility and thus identifying a controller can be more difficult. Further analysis will try to answer the question of who is the controller on a public permissionless blockchain.

In a public permissionless blockchain there is no central point of control as the network is operated by all nodes in a decentralised fashion.[152] Each node has their own copy of the blockchain stored on their computer on the network and the computers periodically synchronize through the P2P network, the nodes are in charge of carrying out transactions and thus distributing the information to all other nodes.[153] The responsibility for compliance in public networks could thus be attributed to either individual nodes, the nodes collectively or software developers.

Nodes can be divided into participating nodes and validating nodes. Validating nodes are allowed to add data to the ledger, according to the consensus mechanism. Participating nodes store synchronised copies of the data. If a user is connected to a participating note, they can add new data to the ledger, but this data needs to be sent to the participating node first, and then submitted to a validating node.[154] In a public, permissionless network, anyone is allowed to become a participating node or a validating node - there is no network owner, no sign-up procedure, no registration, and no restrictions on who can do this. The open source software is developed and maintained by changing groups of volunteers, and it exists 'in the wild' as a tool that people can choose to use or not.[155] Therefore one interpretation would be to consider

[150] Tervise infosüsteemi põhimäärus RT I, 12.03.2019, 34
[151] M. Finck, p. 26; M. Berberich, M. Steiner, p. 424.
[152] M. Finck. p. 26.
[153] *Ibid.*
[154] The European Union Blockchain Observatory And Forum. Blockchain and the GDPR. Report - https://www.eublockchainforum.eu/reports (17.04.2019)
[155] The European Union Blockchain Observatory And Forum. Blockchain and the GDPR. Report - https://www.eublockchainforum.eu/reports (17.04.2019)

the natural or legal person behind each node to be the controller if they determine the purpose and means of processing.

Downloading the full node, running it and participating in the blockchain network or deciding when to participate, could be considered exercising control by the node. However, a controller must also determine the "purposes and means" of the processing. Due to the immutable properties of blockchain, nodes cannot alter the data of a block, nor delete it. Altering a block would require 51% of the nodes to reach consensus on the alternations, otherwise the deviating block would be rejected from the chain. Running the blockchain application is not enough to constitute deciding the means of processing and if a node has no effect on the processing of data on a block it is doubtful they can determine the purpose of processing. [156] For example in a Bitcoin blockchain, the users determine if a transfer is created and to whom and how much Bitcoin are being transferred.[157] The purpose of data processing is always the transfer of Bitcoin, which cannot be altered by the user.[158] Furthermore, nodes do not decide on the means of processing as they have no effect on which data is processed, which third parties will have access to the data and when will said data be deleted. Therefore each individual node could be considered a controller if they decide on the purpose and means of processing of personal data. However, an individual node does not determine the purpose and means of processing and hence cannot be considered the controller pursuant Article 4(7).

Michele Finck notes in a permissionless setting, either no node qualifies as the data controller in the absence of independent determination of the means and purposes of processing, or more likely, *every* node qualifies as data controller. Finck concludes that as nodes are not subject to external instructions and autonomously decide whether to join the chain, and pursue their own objective, they should be considered controllers. However, determining that each node is a data controller raises considerable complications as the exact number, location and identity of nodes on a chain cannot be established without difficulty. [159] For example in the Bitcoin blockchain there are approximately 10 612 nodes[160] than are known of.[161] Other authors reach a similar conclusion.[162]

[156] J. Erbguth, J. G. Fasching. p. 563.
[157] T. Buocz, *et al.* p. 195.
[158] *Ibid.* p. 194.
[159] M. Finck. p. 26.
[160] Global Bitcoin Nodes Distribution - https://bitnodes.earn.com/#global-bitcoin-nodes-distribution (11.02.2019)

Such conclusion is criticised by Lokke Moerel who compares blockchain technology to the internet – applying the question of controllership to the internet at large would result in a similar conundrum as when applied to public blockchain: either all technical building blocks of the internet would qualify as the controller or none of them would, a result that would pose similar data protection issues under the GDPR. None of these issues have however, hampered the development of the internet, for the simple reason that controllership is not based on the technical level of operation of the relevant technology, but who deploys this technology for a certain purpose. Moerel concludes that blockchain will not make middlemen obsolete but rather replace them. As private and consortium blockchains are emerging to meet business needs, as well as gain social acceptance, these blockchain applications will implement their membership rules. These rules in turn will also provide who the responsible entity is, as well as a choice of law and forum.[163] The critique is relevant but the present analysis focuses on the present state of technology. Whether or not improvements future improvements will alleviate some of the issues with blockchain remains to be seen.

Buocz *et al.* outline that although users running full nodes make essential contributions to the functioning of network, they cannot determine the purposes and means of these activities by themselves as the consensus building functions automatically according to code. They conclude that because individual users running full nodes cannot change the protocol by themselves or choose a different protocol, they cannot be considered controllers.[164] Erbguth and Fasching conclude similarly that nodes decide whether to participate in a network or not but this has no effect on the functioning of the blockchain. Thus if a node has no influence on the processing, it is doubtful whether they determine the purposes of the processing.[165]

Therefore it appears that the debate whether individual nodes constitute controllers and if so, whether they decide the purposes and means of processing, is on going. According to the

---

[161] *Ibid.* Those are the nodes which have been reached through sending getaddr messages recursively to find all the reachable nodes in the network. Nodes running protocol version older than 70001 will be skipped.
[162] See for example: M. Berberich, M. Steiner. p. 424; M. Martini, O. Weinzierl. Die Blockchain-Technologie und das Recht auf Vergessenwerden - Neue Zeitschrift für Verwaltungsrecht. 2017: 17, pp. 1251-1259 (1253).
[163] L. Moerel. Blockchain & Data Protection … and Why They Are Not on a Collision Course - European Review of Private Law. 2018: 26(6), pp. 825–851 (833-835).
[164] T. Buocz, *et al.* p. 195.
[165] J. Erbguth, J. G. Fasching. Wer ist Verantwortlicher einer Bitcoin-Transaktion? - https://erbguth.ch/ZD12-2017.pdf (26.02.2019), p. 563.

European Commission's EU Blockchain Observatory and Forum it is not desirable to categorise nodes a controllers, as the debate has not been settled, as well as problems with enforcement.[166]

It would be possible to classify all the nodes collectively as joint controllers under article 26(1) if the nodes meet two conditions. First, it would require for all the participating nodes to "jointly determine the purposes and means of processing". However, if an individual node has no control over the purpose and means of processing, then it is doubtful that the collective of nodes will. Theoretically the nodes could coordinate their actions to reach a 51% consensus and alter the blocks on the chain. The author would argue that in this case two or more controllers would at least determine the "how" or the "means" of processing.

But as a second condition Article 26 also requires the determination of respective responsibilities for compliance in a transparent manner by means of arrangement between the nodes. The arrangement between joint controllers requires a "clear allocation of the responsibilities".[167] The GDPR does not specify the format of such an agreement but it can be assumed that the burden of proof will be on the joint controllers to demonstrate the clear allocation of responsibilities.[168] The rules of a blockchain network stem not from an agreement of the nodes, but ultimately from the sum of their independent behaviour.[169] Thus it is not enough that several parties act in union, but they must determine the purpose together. Between the node operators, however, there is usually no agreement on the purpose.[170] The lack of shared purpose means the processing will result in qualifying two entities as two separate data controllers.[171]

The discussion in academia about whether nodes can constitute joint controllers is on going.[172] The author believes that in a public permissionless scenario where the exact number and location of nodes is unknown and the sum of the independent behaviour of the nodes dictates the rules of the network, not their cooperation, the collective of nodes does not

[166] The European Union Blockchain Observatory And Forum. Blockchain and the GDPR. Report - https://www.eublockchainforum.eu/reports (17.04.2019)
[167] Recital 79 GDPR
[168] For example Recital 42, 69, 74 GDPR.
[169] R. Böhme, P. Pesch. Technische Grundlagen und datenschutzrechtliche Fragen der Blockchain-Technologie - Datenschutz und Datensicherheit (DuD). 2017: 41(8) pp. 473–481 (479)
[170] J. Erbguth, J. G. Fasching. p. 563.
[171] WP 169. p. 20.
[172] M. Finck; M. Berberich, M. Steiner; T. Buocz, *et al.*; L. Moerel; S. Kulhari.

qualify as joint controllers pursuant Article 26 because there is no arrangement between the nodes. For example there is no coordination between the nodes of a Bitcoin blockchain. A remedy to this could be determining the respective responsibilities already in the design phase of the blockchain. Then it would be possible to classify nodes as joint controllers pursuant Article 26. Some authors believe considering the liability side of data protection in the design phase would lead to a huge downfall for the adaptation of blockchain-networks and hamper the innovative potential of decentralization behind blockchain technology.[173]

Further it would be possible to argue that software developers are controllers as they are the ones who write the code of the blockchain. For example in the Bitcoin blockchain the programmer[174] would be Satoshi Nakomoto, fulfilling the personhood criterion. It can be argued that by writing the code, the developer determines how the blockchain should operate. However, as the software is open source, it is produced collaboratively, shared freely, published transparently, and developed to be a community good rather than the property or business of a single company or person.[175] Furthermore, it is developed by a developed and maintained by changing groups of volunteers, who in many cases are not directly compensated for their efforts and are in essence simply creating a useful tool, not prescribing how this tool should be used.[176] Thus after the publication of the program code, the software developer relinquishes control over the means and purposes of the processing.[177] Similar to other programmers, blockchain developers only supply a means for the processing of personal data, even though occasionally they play an important role in the further technical advancement of the blockchain.[178] An example of this would be the DAO hack on the Etherum blockchain.[179] However, solving technical problems is not considered as a

[173] C. Wirth, M. Kolain. Privacy by BlockChain Design: A Blockchain-enabled GDPR-compliant Approach for Handling Personal Data - https://dl.eusset.eu/bitstream/20.500.12015/3159/1/blockchain2018_03.pdf (16.04.2019)

[174] For the present analysis it shall be considered that there is one person behind the pseudonym.

[175] https://coincenter.org/entry/what-is-open-source-and-why-is-it-important-for-cryptocurrency-and-open-blockchain-projects (27.04.2019)

[176] The European Union Blockchain Observatory And Forum. Blockchain and the GDPR. Report - https://www.eublockchainforum.eu/reports (17.04.2019)

[177] M. Martini, O. Weinzierl. p. 1253.

[178] J. Kaufmann. Blockchain meets Data Privacy - https://legal-revolution.com/images/pdf/Blockchain-meets-Data-Privacy_Blockchain-and-the-Data-Controller.pdf (27.02.2019)

[179] Ethereum Executes Blockchain Hard Fork to Return DAO Funds - https://www.coindesk.com/ethereum-executes-blockchain-hard-fork-return-dao-investor-funds (27.02.2019)

determination of the purposes and means of the processing of personal data.[180] Therefore as the programmers do not determine the purposes and means of the processing, which is an important element of the controllership, they cannot be considered controllers as per Article 4(7).

In conclusion, it is not clear whether individual nodes or nodes collectively should be considered controllers. Each individual node does not determine the purposes and means of processing, therefore does not qualify as controller pursuant to Article 4(7). If over 51% of the nodes would reach consensus and alter the blocks on the chain, they would at least determine the means of processing. If the nodes would jointly determine the purposes and means of processing in a mutual arrangement, they would qualify as joint controllers pursuant to Article 26. However, in public permissionless blockchains, such as Bitcoin, there is no coordination between the nodes. Finally, software developers should not be considered controllers as they relinquish control of the open source software once it is published, thus they have no effective control on the purposes and means of processing.

3.2. Territorial scope

The territorial scope of the GDPR is laid down in Article 3. Article 3 defines the territorial scope on the basis of two main criteria: (1) the "establishment" criterion, as per Article 3(1), and the "targeting" criterion as per Article 3(2).[181] In addition, as per Article 3(3) the GDPR applies where a controller is not established in the Union, but Member State law applies by virtue of public international law. Similarly as in section 2.1 this section will look at the guidelines 3/2018 on the territorial scope of the GDPR published by the EDPB, as well as European case law and apply these criterions to blockchain. As the third criterion applies to diplomatic mission or consular post cases[182], the first two are most relevant to blockchain technology.

[180] J. Erbguth, J. G. Fasching. p. 563.
[181] European Data Protection Board. Guidelines 3/2018 on the territorial scope of the GDPR (Article 3). Brussels: 2018 - https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_en.pdf (21.03.2019), p. 3.
[182] Recital 25 GDPR

3.2.1. ‘Establishment’ criterion

As per Article 3(1) the GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. The EDPB establishes a threefold approach in determining whether the processing of personal data falls within the scope of Article 3(1).

The first element is “an establishment in the Union”. In order to define the establishment criterion, it is important to identify who is the controller or processor for a given processing activity.[183] As seen in chapter 3.1 defining the controller in decentralised systems is more straightforward when private blockchains are used but more complex in public blockchains.

The GDPR Article 4(16)(a) defines “main establishment” as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment.

Recital 22 further clarifies that establishment “implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect”. Furthermore Recital 36 states that “the main establishment of a controller in the Union should be the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union, in which case that other establishment should be considered to be the main establishment”. The main establishment should be determined according to objective criteria irrespective of location and imply the effective and real exercise of management activities determining the main decisions as to the purposes and means of processing through stable arrangements.[184]

In several rulings the CJEU has broadened the term “establishment”, departing from a formalistic approach whereby undertakings are established solely in the place where they are

[183] Guidelines 3/2018, p. 4.
[184] Recital 36 GDPR

registered.[185] In order to establish whether a company has an establishment in a Member State other than the Member State or third country where it is registered, both the degree of stability of the arrangements and the effective exercise of activities in that other Member State must be interpreted in the light of the specific nature of the economic activities and the provision of services concerned. [186] This is particularly true for undertakings offering services exclusively over the Internet.[187] The 29WP notes the threshold for "stable arrangement" in the context of services online provided by non-EU entity's can be as low as a single employee if the employee acts with a sufficient degree of stability.[188] The nationality of the persons concerned by such data processing is irrelevant.[189] The legal form of the establishment, whether simply a branch or a subsidiary with a legal personality, is not the determining factor.[190]

The second consideration is "processing in the context of the activities of an establishment in the Union". Article 3(1) confirms that is not necessary that the processing is carried out "by" the establishment concerned itself, but only that it be carried out "in the context of the activities" of the establishment.[191] The EDPB recommends determining this consideration on a case-by-case basis, in the light of relevant case law.[192] The CJEU has noted that "[to ensure] effective and complete protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data, [this criterion] cannot be interpreted restrictively"[193]. However, on the other hand it should not be concluded that the existence of any presence in the EU would trigger compliance.[194] Two factors should be looked at when assessing this consideration. First, the relationship between the data controller or processor outside the Union and a local establishment in the Union – if the data processing activities are inextricably linked, the data protection may be triggered, even if that local establishment is not actually taking any role in the data processing itself.[195] Second, whether revenue raising is present in the Union by the local establishment to the extent that these activities can be considered "inextricably linked" to the processing of

[185] See for example: Guidelines 3/2018, p. 5; CJEU C‑131/12, CJEU C‑210/16; CJEU C‑230/14, *Weltimmo s. r. o. v Nemzeti Adatvédelmi és Információszabadság Hatóság.*
[186] CJEU C‑230/14, para. 29.
[187] CJEU C‑230/14, para. 29.
[188] Guidelines 3/2018, p. 5.
[189] CJEU C‑230/14, para. 40.
[190] CJEU C‑131/12, para. 48.
[191] *Ibid.* para. 52.
[192] Guidelines 3/2018, p. 6.
[193] CJEU C‑131/12, p. 53.
[194] Guidelines 3/2018, p. 6.
[195] Guidelines 3/2018, p. 6-7.

personal data taking place outside the Union.[196] For example, a foreign operator with a sales office or some other presence in the EU, even if that office has no role in the actual data processing, such as a Chinese owned e-commerce website with an office in Berlin to lead marketing campaigns towards the EU.[197]

Finally the GDPR applies to processing in the context of the activities in the Union "regardless of whether the processing takes place in the Union or not". More specifically this means the place of processing is not relevant in determining whether or not the processing, carried out in the context of the activities of an EU establishment, fall into the scope of the GDPR.[198] For example in an instance where a French car-sharing company addressed to customers of Tunisia and Morocco exclusively but with the processing being carried out in France, would trigger the compliance of the GDPR.[199]

In the *Google Spain* case the intention of Google Spain, Google Inc.'s establishment in the EU, to promote and sell advertising space in a Member State, which served to make the service offered by [the controller] profitable was considered processing in the context of the activities of that establishment.[200] The CJEU found that the activities of Google Inc. and Google Spain were inextricably linked since the activities relating to the advertising space constituted the means of rendering the controller economically profitable and that engine is, at the same time, the means enabling those activities to be performed.[201]

3.2.2. 'Targeting' criterion

As per Article 3(2) the GDPR also applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union. The EDPB recommends a twofold approach when analysing the 'targeting' criterion. First, whether the processing relates to subjects in the Union, and second whether it relates to the

[196] *Ibid.* p. 7
[197] *Ibid.*
[198] *Ibid.* p. 8.
[199] *Ibid.* p. 8.
[200] CJEU C‑ 131/12, para. 55.
[201] *Ibid.* para. 56

offering of goods and services *or* to the monitoring of data subjects' behaviour in the Union.[202] The two conditions must be present together in order for the processing to qualify under Article 3(2).

Article 3(2) applies to "data subjects in the Union" irrespective of their citizenship, residence or other type of legal status.[203] This fact is also confirmed by Recital 14 which states "protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence*".* The requirement for the data subject to be located in the Union must be assessed when the triggering activity takes place, i.e. the at the moment of offering of goods or services or the moment the behaviour is being monitored, regardless of the duration of the offer made or monitoring undertaken.[204]

The first alternative of the second condition of Article 3(2) is the "offering of goods and services". It should be noted that the criterion applies irrespective of whether a payment has been made for said goods and services. A controller or processor is offering goods or services to data subjects who are in the Union if it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union.[205] Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.[206] Therefore conditions, such as a processor's website in the Union, cannot exist in isolation and trigger Article 3(2). Rather it should be ascertained whether the combination of factors show that the controller envisages offering goods or services to data subjects in the Union.

Envisages offering goods or services – this approach has already triggered criticism, mainly revolving around the fact that targeting focuses on the subjective intentions of the controller and therefore compromise legal certainty. Instead, exclusive reliance on objective criteria,

[202] Guidelines 3/2018, p. 13
[203] *Ibid.* p. 13.
[204] *Ibid.* p. 13
[205] Recital 23 GDPR
[206] Recital 23 GDPR

such as the concrete outcome of businesses' activities directed to the EU territory, is preferred for the determination of the territorial scope of the GDPR.[207]

The second alternative is the "monitoring the data subjects behaviour". In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.[208] While Recital 24 makes reference of tracking through the Internet, the EDPB considers that tracking through other types of network technology involving personal data processing, such as wearable or smart devices, should also be taken into account.[209]

Although Article 3(2) does not mention the intention of the controller as part of this criterion, the EDPB notes the purpose of the processing needs to be still taken into account.[210] Examples of monitoring of activities include behavioural advertisement or studies, geo-location activities, online tacking through cookies or fingerprinting, personalized diet and health analytic services online and CCTV.[211]

3.2.3. Territorial scope of a blockchain

Determining the territorial scope depends largely on determining the controller and subsequently establishing the applicable jurisdiction. In addition, the EPDB has stressed the importance of identifying the controller or processor of a given processing activity.[212] The fact that blockchains operate on a decentralised structure means personal data could be processed across multiple jurisdictions. This in turn poses a risk to the protection of personal data of the subjects. Given that recital 13 of the GDPR stresses how technology should further facilitate the free flow of personal data within the Union and the transfer to third countries and

[207] M. Gömann. The new territorial scope of EU data protection law: Deconstructing a revolutionary achievement - Common Market Law Review. 2017:5(2), pp. 567–590 (586).
[208] Recital 24 GDPR
[209] Guidelines 3/2018, p. 17-18.
[210] Guidelines 3/2018, p. 18.
[211] *Ibid.*
[212] *Ibid.* p. 4.

international organisations, while ensuring a high level of the protection of personal data,[213] blockchains could be problematic.

An example of a private blockchain would be the Guardtime blockchain. Given that Guardtime's headquarters are situated in Amsterdam, the Netherlands[214] and one example of Guardtime's blockchain solutions are government e-services run on blockchain techology, such as in Estonia and the Netherlands[215], the Guardtime blockchain falls under Article 3(1).

A public permissionless blockchain is public by definition, meaning anyone in any jurisdiction can download the software and run it on their computer. In addition, in a public permissionless blockchain the question of controllership is more nuanced. This in turn raises considerable questions as to how to determine the territorial scope of the GDPR.

If every individual node would be considered a controller, then a node running the blockchain in Germany would fall under Article 3(1) as the processing of personal data in the context of the activities of an establishment in the Union. However, as the author already established, an individual node cannot be considered the controller, as it does not determine the purpose and means of processing pursuant Article 4(7).

In the case of a public permissionless blockchain it would be possible to classify the nodes as joint controllers if they jointly determine the purposes and means of processing. In such case if the nodes are in the European Union, then the processing of personal data on a blockchain falls under Article 3(1). However, if one or more of the nodes is not established in the Union, it should be assayed whether such processing falls under Article 3(2). More specifically, first whether the processing relates to subjects in the Union, and second whether it relates to the offering of goods and services *or* to the monitoring of data subjects' behaviour in the Union.[216] The two conditions must be present together in order for the processing to qualify under Article 3(2).

---

[213] Recital 13 GDPR

[214] S. Hankewitz. Estonian Guardtime launches a personal care record platform for the UK NHS patients - http://estonianworld.com/technology/estonian-guardtime-launches-a-personal-care-record-platform-for-the-uk-nhs-patients/ (30.03.2019)

[215] Guardtime. Dutch Government deploys Guardtime's KSI Blockchain for integrity assurance - https://guardtime.com/blog/dutch-government-deploys-guardtime-s-ksi-blockchain-for-integrity-assurance (30.03.2019)

[216] Guidelines 3/2018, p. 13.

The webpage www.Bitcoin.org is offered in several European Union languages, such as among others German, French, Italian, Dutch and Spanish.[217] According to the EDPB one of the factors of the intention to offer goods or services can be the use of language or a currency other than generally used in the trader's country, especially a language or currency of one or more EU member states.[218] Although the language criterion is not determining in isolation, based on the use of multiple European languages, it can be concluded that the processing applies to data subjects in the Union. Bitcoin is described as "an innovative payment network". [219] Thus the Bitcoin blockchain provides a platform for the trading of cryptocurrency. Therefore offering a platform for the trading of cryptocurrency in several member states constitues offering of good and services as per Article 3(2). Even if the joint controllers are not established in the European Union, the processing of personal data falls under Article 3(2) thus fulfilling the territorial scope of the GDPR and triggering compliance.

Finck outlines that unpermissioned blockchain run on nodes located in various jurisdictions across the globe, leaving creators with no control over the geographic spread of the network, which makes DLTs inherently transnational in nature, triggering a range of jurisdictional issues.[220] However, several authors have concluded that the broad territorial scope will apply to DLTs like blockchain.[221] Moerel argues that similarly to the internet due to the lack of government regulated supervision, the stakeholders involved in blockchain will implement their own contractual self-regulatory mechanisms to ensure adequate dispute resolution.[222] This shall provide relief to the jurisdictional issues. Similarly as with the question of controllership, Moerel's argument is oriented towards the future, while the present analysis focuses on the technology available today. Either way, as the present analysis demonstrated the territorial scope of the GDPR is broad and even data processing on decentralised systems will trigger compliance.

3.2.4. Transfers of personal data to third countries or international organisations

[217] Bitcoin - https://bitcoin.org/en/ (30.03.2019)
[218] Guidelines 3/2018, p. 16.
[219] Bitcoin - https://bitcoin.org/en/ (30.03.2019)
[220] M. Finck, p. 27.
[221] See for example: M. Finck, p. 27; M. Berberich, M. Steiner, p. 423; T. Buocz, *et al.* pp. 190-192.
[222] L. Moerel. p. 837.

Closely connected to the question of territorial scope are the transfers of personal data to third countries or international organisations. The transfer of personal data is permitted to the 28 Member States of the European Union and to the European Economic Area member countries (Norway, Iceland, Lichtenstein). The rest of the foreign countries are often referred to as "third countries". It is permitted to transfer personal data to a third country, if its level of data protection is deemed to be sufficient by the European Commission.[223]

The GDPR encourages transfers of personal data to third countries or internal organisations, as they are necessary for the expansion of international trade and international cooperation. But in case of such transfers the level of protection of natural persons ensured in the Union by this Regulation should not be undermined and transfers to third countries and international organisations may only be carried out in full compliance with the GDPR. [224]

Chapter V of the GDPR establishes rules regarding the transfers of personal data to third countries or international organisations. According to Article 44 data transfer to a country or organisation outside the Union shall take place only if the controller and processor comply with the conditions in chapter V of the GDPR. Moreover, according to Article 44 all provisions in chapter V of the GDPR shall be applied in order to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined. Such transfers are allowed based on an adequacy decision [225] , appropriate safeguards [226] or specific derogations.[227] Chapter V suggests that this is not a list but rather a hierarchy with adequacy decisions at the top and derogations at the bottom.[228]

So far the European Commission has issued adequacy decisions to Andorra[229], Argentina[230], Canada[231], Faroe Islands[232], Guernsey[233], Israel[234], Isle of Man[235], Japan[236], Jersey[237], New

[223] Estonian Data Protection Inspectorate. Transfer of personal data to a foreign country - https://www.aki.ee/en/guidelines/transfer-personal-data-foreign-country (29.04.2019)
[224] Recital 101 GDPR
[225] Article 45 GDPR
[226] Articles 46, 47 GDPR
[227] Article 49 GDPR
[228] D. Kelleher, K. Murray. p. 117.
[229] Commission Decision 2010/625/EU of 19 October 2010 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Andorra (notified under document C(2010) 7084), OJ L 277, 21.10.2010, p. 27–29.
[230] Commission Decision 2003/490/EC of 30 June 2003 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina, OJ L 168, 5.7.2003, p. 19–22.

Zealand[238], Switzerland[239], Uruguay[240] and the United States (limited to the Privacy Shield framework).[241] Previously personal data transfers to the United States were considered adequate under the Safe Harbour decision[242], which was invalidated in the *Maximillian Schrems v Data Protection Commissioner* case.[243]

---

[231] Commission Decision 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (notified under document number C(2001) 4539), OJ L 2, 4.1.2002, p. 13–16.

[232] Commission Decision 2010/146/ of 5 March 2010 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection provided by the Faeroese Act on processing of personal data (notified under document C(2010) 1130), OJ L 58, 9.3.2010, p. 17–19.

[233] Commission Decision 2003/821/EC of 21 November 2003 on the adequate protection of personal data in Guernsey (notified under document number C(2003) 4309), OJ L 308, 25.11.2003, p. 27–28.

[234] Commission Decision 2011/61/EU of 31 January 2011 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data (notified under document C(2011) 332), OJ L 27, 1.2.2011, p. 39–42.

[235] Commission Decision 2004/411/EC of 28 April 2004 on the adequate protection of personal data in the Isle of Man, OJ L 151, 30.4.2004, p. 48–51.

[236] Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information, OJ L 76, 19.3.2019, p. 1–58.

[237] Commission Decision 2008/393/EC of 8 May 2008 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Jersey (notified under document number C(2008) 1746), OJ L 138, 28.5.2008, p. 21–23.

[238] Commission Implementing Decision 2013/65/EU of 19 December 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by New Zealand (notified under document C(2012) 9557), OJ L 28, 30.1.2013, p. 12–14.

[239] Commission Decision 2000/518/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland (notified under document number C(2000) 2304), OJ L 215, 25.8.2000, p. 1–3.

[240] Commission Implementing Decision 2012/484/EU of 21 August 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the Eastern Republic of Uruguay with regard to automated processing of personal data (notified under document C(2012) 5704), OJ L 227, 23.8.2012, p. 11–14.

[241] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176), OJ L 207, 1.8.2016, p. 1–112.

[242] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441), OJ L 215, 25.8.2000, p. 7–47.

[243] CJEU C‑362/14, *Maximillian Schrems v Data Protection Commissioner,* para. 107.

Similarly as observed in chapter 3.2.3 decentralised systems such as blockchain are problematic from the perspective of data protection because anyone can download the blockchain from different parts of the world. Subsequently personal data can be shared to any location. In such a scenario the rules set forth in chapter V of the GDPR should be complied with but are more difficult to enforce in the case of DLTs.

Finck opines that in theory the chain's protocol could be designed to account for these accounts, yet the substantive requirements of data protection cannot easily be reconciled with DLT. A more realistic solution is enshrined in Article 49(1)(1) that foresees the possibility of a data subject providing explicit consent for such a transfer, subject to being informed about possible risk. Adding also that this could be achieved on a private blockchain, but it is not obvious how such consent should be acquired in respect of a permissionless chain. [244] Informed consent is particularly decisive in the context of transfers of personal data to third countries.[245] The relevance of consent pursuant to Article 49(1)(1)(a) depends on whether to consider using the blockchain as giving *de facto* consent to the processing of personal data. The author would refrain from reaching such a conclusion.

[244] M. Finck. p. 28.
[245] WP187, p. 20.

4. Data protection requirements and core characteristics of blockchain

4.1. Principles

The principles relating to processing of personal data set out the basic rules that apply to the processing of personal data – they provide foundations for European data protection law.[246] The principles relating to processing of personal data are laid down in Article 5(1). Pursuant to Article 5(2) the controller shall be able to demonstrate compliance with the principles set out in Article 5(1).

The most relevant principles in relation to blockchain technology are the data minimisation principle pursuant to Article 5(1)(c), storage limitation principle pursuant Article 5(1)(e) and the data protection by design and default principle pursuant to Article 25.

4.1.1. Data minimisation and privacy by design and default

Data minimisation is defined in Article 5(1)(c), which states "personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". The principle of data minimisation must be read in conjunction with the obligations of data protection by design and default set out in Article 25.[247]

Data minimisation was considered in *Google Spain* where the CJEU noted "even initially lawful processing of accurate data may, in the course of time, become incompatible with the directive where those data are no longer necessary in the light of the purposes for which they were collected or processed. That is so in particular where they appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes and in the light of the time that has elapsed".[248] As 12 years had passed since the publication of the newspaper mentioning the complainant's name, the CJEU ruled that the operator of the search engine – Google - must erase said links to Mr González's name.[249]

[246] D. Kelleher, K. Murray. p. 137.
[247] *Ibid.* p. 142.
[248] CJEU C‑131/12, para. 93.
[249] CJEU C‑131/12, para. 94.

Article 25 contains the data protection by design and default obligation. Article 25(1) states that "taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects".

Thus controllers must account for the GDPR's objectives already in the design phase. To demonstrate compliance the controller should adopt internal policies and implement measures, which meet in particular the principles of data protection by design and data protection by default. [250] Such measures include minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features.[251]

4.1.2. Storage limitation

The storage limitation principle is defined in Article 5(1)(e). Personal data must be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed".[252] This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum.[253] Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by [the GDPR] in order to safeguard the rights and freedoms of the data subject.[254] In order to ensure that the personal

[250] Recital 78 GDPR
[251] *Ibid.*
[252] Article 5(1)(e)
[253] Recital 39 GDPR
[254] Article 5(1)(c) GDPR

data are not kept longer than necessary time limits should be established by the controller for erasure or for periodic review.[255]

The CJEU considered storage limitation principle in the Nowak case ruling that the retention of the written answers submitted by a candidate and the examiner's comments "is, a priori, no longer necessary as soon as the examination procedure is finally closed and can no longer be challenged, so that those answers and comments have lost any probative value". [256] Conversely to the *Nowak* case in *Camera di Commercio,Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni* [257]the CJEU stated "it seems impossible, at present, to identify a single time limit, as from the dissolution of a company, at the end of which the inclusion of such data in the register and their disclosure would no longer be necessary".[258]

4.1.3. Principles and blockchain

Although the GDPR should be a technology neutral law, it can be argued that the core characteristics of the blockchain technology are in tension with the minimisation principle pursuant to Article 5(1)(c), storage limitation principle pursuant Article 5(1)(e) and the data protection by design and default principle pursuant to Article 25.

Firstly, as each node has their own copy of the blockchain stored on their computer on the network [and the computers periodically synchronize through the P2P network,] the nodes are in charge of carrying out transactions and thus distributing the information to all other nodes.[259] Therefore the data is replicated in every node – replicated in each computer running the blockchain software. This in turn is difficult to reconcile with the data minimisation principle, which entails keeping personal data limited to what is necessary in relation to the purposes for which they are processed.[260]

Michele Finck considers the data minimisation principle to be profoundly at odds with data storage on a DLT as distributed ledgers are by definition ever-growing creatures, which augment and accumulate further data with each additional block. In addition, integral copies

[255] Recital 39 GDPR
[256] CJEU C‑ 434/16, para. 55.
[257] CJEU C-398/15, *Camera di Commercio,Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni*
[258] *Ibid.* para. 55.
[259] M. Martini, O. Weinzierl. p. 1254.
[260] Article 5(1)(c) GDPR

of the chain are stored on each full node, contradicting the data minimisation.[261] Shraddha Kulhari notes that digital identity platforms built on blockchain would fall foul of the traditional understanding of the data minimisation principle and such contradiction would arise from the structure of the blockchain technology whereby data is replicated on each node.[262]

Secondly, Article 25 requires for the controller to implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing. Encryption is one of the measures, which the controller should adopt to comply with the principles of data protection by design and data protection by default.[263] As data on blockchain is encrypted, it can be argued that at least one element towards compliance is accounted for. Furthermore, as data on the blockchain is immutable, a case could be made for the security of the data - said data is tamper-resistant and every change is traceable. However, as the replication of data is counter to data minimisation principle, a case could be made that the principle data protection by design and default has not been accounted for in the developing stage of the technology. Such a conclusion could have implications on the compliance of controller using blockchain.

Matthias Berberich and Malgorzata Steiner opine that the fact that the current architecture of blockchain runs counter to data minimisation, storage limitations and clearly determined data controller, may raise the question whether it is in line with the privacy by design principle. Berberich and Steiner find it doubtful that the aforementioned features of blockchain are incompatible with Article 25, as views diverge whether Article 25 generally brings additional "hard obligations". Furthermore, Article 25 does not set out absolute requirements – implementing the principle will take account of state-of-the-art technology, implementation costs, nature, scope, context and purposes of data processing as well as the likelihood of privacy risks. It does not strictly rule out that a balance may be struck between legitimate policy objectives.[264] Adding that it would also make a difference in respect to Article 25 whether public or private blockchains are used, as well as implementing additional technology, such as adding noise to blockchains to prevent re-identification.[265] Such a

[261] M. Finck, p. 28.
[262] S. Kulhari. p. 45.
[263] Recital 78 GDPR
[264] M. Berberich, M. Steiner. pp. 424-425.
[265] *Ibid.* p. 425.

conclusion makes sense, as the elements of data protection are more clear-cut in private blockchains, while public permissionless blockchains remain challenging for regulators.

Furthermore, Michele Finck expresses the view that while data minimisation will always be challenging on DLTs, Article 25(1) underlines that encryption can be a desirable feature, which may be reason for regulators and CJEUs to look favourably at the technology.[266] Finck concludes however, that Article 25 cannot be complied with in respect to public keys as each full node holds a complete copy of each blockchain and given that a new block is added to the complete preceding chain. The only way to ensure compliance in this respect would be to recognize specific key-handling techniques such as particularly strong encryption formulas or zero-knowledge proof as GDPR compliant.[267]

Thirdly, after a block has been added to the blockchain, it can no longer be deleted and the transactions it contains can be accessed and verified by everyone on the network.[268] Unless the nodes engage in a "51% attack" to alter the chain, the data on the chain is immutable. This raises the question of how the immutability should be reconciled with the storage limitation principle pursuant Article 5(1)(e)? As the period for which the personal is stored should be limited to a strict minimum and the controller should establish time limits for erasure or periodic review[269], the question of compliance arises when on blockchain data is stored indefinitely.

Considering that the controller shall be responsible for, and must be able to demonstrate compliance with the core principles as per Article 5(2), the tension with the core principles of the GDPR might result in noncompliance of all actors using blockchain technologies and the subsequent heavy fines of the GDPR. A similar problem has been observed in relation to Big Data.[270]

---

[266] M. Finck. p. 32.
[267] *Ibid.*
[268] P. De Filippi, A. Wright. Decentralized Blockchain Technology and the Rise of Lex Cryptographia. p 8
[269] Recital 39 GDPR
[270] See for example: T. Zasky. Incompatible: The GDPR in the Age of Big Data - https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3022646 (30.03.2019); B-J. Koops. Forgetting Footprints, Shunning Shadows: A Critical Analysis of the 'Right to Be Forgotten' in Big Data Practice - https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1986719 (16.04.2019)

However, there are several methods to overcome the tension with the core principles of the GDPR. One solution would be storing data off-chain and merely linked to the blockchain through a hash pointer.[271] The MIT-ENIGMA project combines off-chain and on-chain storage for more sensible data using the blockchain only as a "pointer" to centrally stored data.[272] Another solution is the zero knowledge proof, a technique by which an entity, or prover, with private data provides a verifiable proof to a verifier that certain property holds true for that data without revealing any additional information other than the truth of verified property.[273] Off-chain storage solution could however, require the reintroduction of a trusted third party[274], which would undermine the decentralization of a blockchain. In any case the author believes that it is possible to overcome the tension with principles through technological development.

4.2. Lawfulness of processing

4.2.1. General grounds

In order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law.[275] In addition, one of the main principles of the GDPR is that personal data should be processed lawfully, fairly and in a transparent manner in relation to the data subject.[276]

The grounds for processing are laid down in Article 6(1) of the GDPR, which provides that processing is lawful if at least one of the following applies:

1) processing is based on consent;
2) processing is necessary for the performance of a contract;
3) processing is necessary for compliance with a legal obligation;
4) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

[271] M. Finck, p. 23.
[272] M. Berberich, M. Steiner. p. 425.
[273] V. Pandit, P. Dayama. Privacy in blockchain collaboration with zero knowledge proofs – https://www.ibm.com/blogs/blockchain/2019/01/privacy-in-blockchain-collaboration-with-zero-knowledge-proofs/ (31.03.2019)
[274] *Ibid.*
[275] Recital 40 GDPR
[276] Article 5(1)(a) GDPR

5) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
6) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party.[277]

The author considers processing based on consent in relation to the public permissionless blockchain and processing necessary for the compliance with a legal obligation in relation to KSI blockchain. Therefore for the purposes of the present thesis only these grounds will be analysed.

4.2.2. Conditions for consent

The definition of consent is found in Article 4(11) which states that consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The 29WP has noted that the order in which the legal grounds in Article 7 is relevant, but it does not mean consent is always the most appropriate ground to legitimize the processing of personal data.[278] If consent is not used in the right context, it provides a weak legal basis for processing.[279] Therefore the elements of consent are (1) it is given freely, (2) it is specific, (3) informed, (4) unambiguous and (5) explicit.

The first element is freely given. This element implies real choice and control for data subjects.[280] Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.[281] Consent can be valid is the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences if he or she does not consent.[282] In a case of clear imbalance between a data subject and controller, like when the controller is a

[277] Article 6(1)(a)-(f) GDPR
[278] Article 29 Data Protection Working Party. Opinion 5/2011 on the definition of consent. WP187. Brussels: 2011 - https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf (17.04.2019) p. 7.
[279] *Ibid.* p. 10.
[280] Article 29 Data Protection Working Party. Guidelines on consent under Regulation 2016/679. WP259. Brussels: 2017- https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 (17.04.2019), p. 5.
[281] Recital 42 GDPR
[282] WP187, p. 12.

public authority, consent should not provide a legal ground for processing.[283] Any element of inappropriate pressure or influence upon the data subject shall render the consent invalid.[284]

The second element is the consent must be specific. This means that blanket consent without specifying the exact purpose of the processing is not acceptable. To be specific, the consent must be intelligible: it should refer clearly and precisely to the scope and the consequences of the data processing.[285] To comply the controller must apply purpose specifications as a safeguard against function creep, granularity in consent requests and clear separation of information related to obtaining consent for data processing activities from information about other matters.[286]

The third element is the informed character of the consent. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended.[287] At least the following information is required for obtaining a valid consent:

1. the identity of the controller;
2. the purpose of each processing of operations for which consent is sought;
3. what type of data will be collected and used;
4. the existence of the right to withdraw consent;
5. information about the use of data for automated decision-making in accordance with Article 22(2)(c);
6. on the possible risks of data transfers due to absence of an adequacy decision and of appropriate safeguards as described in Article 46.[288]

The information provided must be sufficient to guarantee that individuals can make well-informed decisions about the processing of their personal data. This translates into giving information in appropriate language for the subject to understand and providing the information in a clear and sufficiently conspicuous manner so that users cannot overlook it.[289]

[283] *Ibid.* p. 43.
[284] WP259, p. 6.
[285] WP187, p. 17.
[286] WP259, p. 11.
[287] Recital 42 GDPR
[288] WP259, p. 13.
[289] WP187, p. 35.

The fourth element is that consent must be unambiguous meaning that the procedure to seek and give consent must leave no doubt as to the data subject's intention to deliver consent. Data controllers are *de facto* encouraged to have in place procedures and mechanisms to leave no doubt that consent has been given, either on the basis of an express action carried out by the individual or by being clearly inferred from an action carried out by an individual. [290]

Finally, the consent must be explicit or an indication of the wish of the subject by a statement of clear, affirmative action. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent.[291]

Furthermore, conditions for consent are laid down in Article 7 and as per Article 7(1) the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data where processing is based on consent. Pursuant to Article 7(3) the data subject has the right to withdraw consent at any time. This distinguishes processing based on consent from other lawful bases.[292]

4.2.3. Consent as a lawful basis of processing on public permissionless blockchain

Given that in order to use the public blockchain, a person – the node – has to download the blockchain and run the software on their computer, one possible interpretation could be that by doing so the data subject consents to the processing of personal data and thus the legal basis for processing is Article 6(1)(a). However, the as outline in chapter 4.2.2 the GDPR sets very specific conditions for consent. Thus the conditions need to be analysed separately.

In the case of a public permissionless blockchain it is the user's choice to download the full node on their computer, run it and therefore participate in the blockchain network. Therefore the question whether consent is given freely should be answered in the affirmative. Furthermore, downloading the blockchain and running it on the computer constitutes an

[290] WP187, pp. 24-25.
[291] Recital 32 GDPR
[292] D. Kelleher, K. Murray. p. 155.

affirmative action. However, "a clear affirmative act" means that the data subject must have taken a deliberate action to consent to the particular processing.[293]

More problematic are the elements of being informed and specific. Firstly, in order for the consent to be informed, the data subject should at least be aware of the identity of the controller and the purposes of the processing for which the personal data are intended.[294] This is problematic in a public permissionless setting as the question of controllership is not so clear. WP29 notes that in a case where the consent sought is to be relied upon by multiple (joint) controllers or if the data is to be transferred or processed by other controllers, who wish to rely on the original consent, these organisations should all be named.[295] If one would follow the argumentation that all the nodes on the network constitute joint controllers pursuant Article 26, this would be again problematic.

Furthermore, the GDPR does not prescribe the form or shape in which information should be provided in order to fulfil the requirements of informed consent. However, the GDPR puts several requirements for informed consent in place, predominantly in Article 7(2) and Recital 32, which leads to a higher standard for the clarity and accessibility of the information.[296]

Secondly, for the consent to be specific, obtaining valid consent is always preceded by the determination of a specific, explicit and legitimate purpose of the intended processing activity pursuant to Article 5(1)(b) GDPR.[297] Again it is in a public permissionless setting it is not clear as to what the specific the consent is given. The controller is expected to separate clearly information related to obtaining consent for data processing activities from information about other matters.[298]

In can be concluded that not every criterion of the conditions for consent is met. Similarly, the European Commission's EU Blockchain Observatory and Forum, comprised of specialists in the field, in their report have noted that it could be argued that by choosing to use a decentralised network, like Bitcoin, the user is *de facto* providing consent. GDPR however,

[293] WP259, p.16.
[294] Recital 42 GDPR
[295] WP259, p. 13.
[296] WP259, p. 14
[297] *Ibid.* p. 12.
[298] *Ibid.* p. 11.

stipulates that consent be specific and unambiguous, which seems to imply active granting of permission, not a passive one.[299]

In addition, a separate and additional consent should be requested to allow for the sending of the individual's data to third parties[300] and that informed consent is particularly decisive in the context of transfers of personal data to third countries.[301] These criterions are difficult to enforce in a decentralised structure. Blockchains as technology however, are good mechanisms for giving and withdrawing consent if the law is used as a base requirement.[302]

4.2.4. Legal obligation as a lawful basis of processing on private blockchain

The controller of data on the e-Health platform is the Ministry of Social Affairs and the processor is Health and Welfare Information Systems Centre.[303] Where processing is carried out in accordance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, the processing should have a basis in Union or Member State law.[304] The legal basis for the processing of personal data comes from the Health Services Organisation Act[305] Thus the legal basis for processing is Article 6(1)(c).

In addition, as discussed in chapter 2.1 special data pursuant Article 9(1) merits special protection in the European data protection regime as the processing of such data could create significant risks to the fundamental rights and freedoms of the data subject.[306] The GDPR sets a general prohibition of the processing of special data.[307] The processing of special data is only allowed when the conditions in Article 9(2) are met.[308] In addition to specific

[299] The European Union Blockchain Observatory And Forum. Blockchain and the GDPR. Report - https://www.eublockchainforum.eu/reports (17.04.2019)
[300] WP187, p. 18.
[301] WP187, p. 20.
[302] See for example: C. Wirth, M. Kolain. Privacy by BlockChain Design: A Blockchain-enabled GDPR-compliant Approach for Handling Personal Data - https://dl.eusset.eu/bitstream/20.500.12015/3159/1/blockchain2018_03.pdf (17.04.2019); K. Rantos. Blockchain-based Consents Management for Personal Data Processing in the IoT Ecosystem - https://www.scitepress.org/papers/2018/69110/69110.pdf (16.04.2019)
[303] Tervise infosüsteemi põhimäärus - RT I, 12.03.2019, 34
[304] Recital 45 GDPR
[305] Health Services Organisation Act - RT I 2001, 50, 284
[306] Recital 51 GDPR
[307] Article 9(1) GDPR
[308] Article 9(2)(a)-(j) GDPR

requirements of the processing of special categories of personal data, the general principles of the GDPR should apply, in particular as regards to the conditions for lawful processing.[309] A margin of manoeuvre is left to Member States to specify the rules concerning the processing of special categories of personal data.[310]

Guardtime's KSI blockchain contains personal data concerning health pursuant to Article 9(1). The processing of such special data is prohibited unless the exceptions in Article 9(2) apply. The applicable exception could be Article 9(2)(h) which states that processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3.

According to Recital 52 the derogation from "the general prohibition may be made for health purposes, including […] the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system".[311] Furthermore, special categories of personal data which merit higher protection should be processed for health-related purposes only where necessary to achieve those purposes for the benefit of natural persons and society as a whole, in particular in the context of the management of health or social care services and systems, including processing by the management and central national health authorities of such data for the purpose of quality control, management information and the general national and local supervision of the health or social care system, and ensuring continuity of health or social care and cross-border healthcare or health security.[312] The KSI blockchain is used in Estonia's e-Health platform thus it is used for the management of health or social care systems and services on the basis of Union or Member State law. Furthermore, the blockchain is used to process personal data by the national health authority for the management of information. Therefore the exception of Article 9(2)(h) is applicable in the case of Guartime's blockchain. The Bitcoin blockchain as a rule does not process special data, more specifically data concerning health. However, if it did, then the abovementioned exception would not be applicable.

[309] Recital 51 GDPR
[310] Recital 10 GDPR
[311] Recital 52 GDPR
[312] Recital 53 GDPR

4.3. Rights of the data subject and data persistence

4.3.1. Right to rectification

The right to rectification is contained in Article 16. Pursuant to Article 16 the data subject first has the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Second, taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Every reasonable step must be taken by the controller to ensure that data, which does not meet the requirements of Article 16, is erased or rectified.[313] In the *Schrems* case the CJEU noted that the data subjects had no administrative or judicial means of redress enabling, in particular, the data relating to them to be accessed and, as the case may be, rectified or erased.[314] Therefore outlining the importance of such procedures.

4.3.2. Right to erasure

The right to erasure or the "Right to be forgotten" is laid down in Article 17(1) according to which the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay if one of the conditions of Article 17(1) applies. Said conditions include that data is no longer necessary, withdrawal of consent, objection pursuant Article 21, unlawful processing, a legal obligation to erase the personal data and the collection of personal data in relation to information society services referred to in Article 8(1).[315] A data subject should have the right to have personal data concerning him or her rectified and a "right to be forgotten" where the retention of such data infringes this Regulation or Union or Member State law to which the controller is subject.[316]

[313] CJEU C‑ 131/12, para. 72.
[314] CJEU C‑ 362/14, *Maximillian Schrems v Data Protection Commissioner*, para. 90.
[315] Article 17(1)(a)-(f) GDPR
[316] Recital 65 GDPR

The right to erasure did not exist in the Directive 95/46/EC.[317] The Directive 95/46/EC did however contain references to erasure of data.[318] The intellectual roots of the "right to be forgotten" in Europe can be found in French law, which recognises *le droit á l'oubli* or the "right to oblivion" – a right that allows a convicted criminal who has served his time and been rehabilitated to object to the publication of the facts of his conviction and incarceration.[319] The introduction of said right in the GDPR constitutes an attempt of the EU to facilitate the erasure of obsolete personal data and thereby respond to the challenges posed by the digital remembering.[320] The right has is the most controversial and has been discussed in literature[321] and also criticized as the biggest threat to free speech on the Internet in the coming decade.[322] Furthermore, the extent to which the right to be forgotten may be enforceable in practice remains unclear[323] and whether any item of data can ever be fully or properly erased is very much open to question.[324] However, further analysis on this topic would be out of the scope of this thesis.

If a controller has made personal data public and is obliged to erase personal data pursuant to Article 17(1), the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.[325] Such measures are to be taken to "strengthen the right to be forgotten in the online environment".[326]

---

[317] Directive 95/46/EC.
[318] See for example: Article 12(b) Directive 95/46/EC.
[319] J. Rosen. The Right to be Forgotten - Stanford Law Review Online. 2012: 64 - https://www.stanfordlawreview.org/online/privacy-paradox-the-right-to-be-forgotten/ (16.04.2019)
[320] E. Politou, *et al.* Backups and the right to be forgotten in the GDPR: An uneasy relationship – Computer Law & Security Review. 2018: 34(6) pp. 1247-1257 (1248)
[321] See for example: B-J. Koops; J. Rosen; J. Ausloos. The 'Right to be Forgotten' - Worth Remembering? - Computer Law & Security Review. 2012: 28(2), pp. 143-152; M. L. Ambrose, J. Ausloos. The Right to Be Forgotten Across the Pond - Journal of Information Policy. 2013: 3, pp. 1-23; A. Bunn. The curious case of the right to be forgotten - Computer Law & Security Review. 2015: 31(3), pp. 336-350.
[322] J. Rosen, p. 88.
[323] Opinion of the European Data Protection Supervisor on the data protection reform package - https://edps.europa.eu/sites/edp/files/publication/12-03-07_edps_reform_package_en.pdf (16.04.2019)
[324] D. Kelleher, K. Murray. p. 208.
[325] Artilce 17(2) GDPR
[326] Recital 66 GDPR

The right to erasure in not an absolute right and shall not apply if processing is necessary for exercising the right of freedom of expression and information, for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, for public interest in the area of public health, for archiving purposes in the public interest and the establishment, exercise or defence of legal claims.[327] That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child.[328]

Methods by which to restrict the processing of personal data could include, inter alia, temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website.[329] In automated filing systems, the restriction of processing should in principle be ensured by technical means in such a manner that the personal data are not subject to further processing operations and cannot be changed. The fact that the processing of personal data is restricted should be clearly indicated in the system.[330]

The right to be forgotten was considered by the CJEU in the *Google Spain* case. However, it should be noted that the CJEU found that the links to Mr. González's name in the Google Search should be removed, even when its publication in itself on those pages is lawful[331] as the processing by the publisher of a web page consisting in the publication of information relating to an individual may, in some circumstances, be carried out "solely for journalistic purposes" and thus fall under an exception, whereas that does not appear to be so in the case of the processing carried out by the operator of a search engine. [332] Thus the CJEU did not oblige the daily newspaper to remove the original content. The CJEU also held that the right to private life and protection of personal data should be balanced against economic interest of the operator of the search engine but also the interest of the general public in finding that information upon a search relating to the data subject's name. The CJEU found that in the present case Mr. González's rights overrode the economic interests and public interests.

[327] Article 17(3)(a)-(e) GDPR
[328] Recital 65 GDPR
[329] Recital 67 GDPR
[330] *Ibid.*
[331] CJEU C‑ 131/12, para. 88.
[332] Ibid. para. 85.

However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of inclusion in the list of results, access to the information in question.[333]

4.3.3. Rights and blockchain

Similarly to chapter 4.1 it can be argued that the core characteristic of blockchain technology – data immutability – is in tension with the right to rectification pursuant Article 16 and right to erasure pursuant Article 17.

Firstly, pursuant to Article 16 the data subject has the right to obtain without undue delay the rectification of inaccurate personal data. Article 16 does not provide any exceptions to this right but the purposes of the processing should be taken into account.

Secondly, as per Article 17(1) any data subject has right to obtain from the controller the erasure of personal data concerning him or her without undue delay if one or several of the Article 17(1) conditions apply. That could be the case for example if a financial transaction has been carried out and the personal data is no longer necessary in relation to the purposes of which it was collected as per Article 17(1)(a), the data subject withdraws consent as per Article 17(1)(b) or the data subject objects to the processing as per Article 17(1)(c) and there are no overriding legitimate grounds for the processing. Given that none of the exceptions apply, the controller of the blockchain would have to delete the personal data, which infringes the data subject's rights from a block.

As immutability is a core feature of the technology, both erasure and rectification would be practically impossible. As outlined above, changing a block would be possible if 51% of the nodes engaged in a "51% attack" which would require extensive computational power and financial resources. This would result in breaking the chain and altering a block. However, as the blockchain would be completely 'blocked' before it can even resume its function of adding new transactions, it appears at the moment almost unfeasible from an operational and technical perspective to change blockchain content subsequently in practical operation.[334] Therefore the controllers of blockchain technology could not comply with the requirements set forth in Article 16 and Article 17 due to the persistence of data on a blockchain. Still as set

[333] CJEU C‑ 131/12, para. 97
[334] M. Berberich, M. Steiner. p. 426.

forth in the case *Google Spain* the right to erasure is not an absolute right, it would have to be balanced with other rights. For example in line with the *Manni* ruling registering limited personal data in a blockchain for public registers like land ownership, trademark ownership, company registers, may well be justified.[335]

Michele Finck notes that pursuant to Article 16 the data subject could address any or all nodes with a request to rectify personal data subject to the provided conditions. However, identification of all full nodes is problematic and data stored on them cannot be changed except in very exceptional circumstances.[336] With regards to erasure, Finck opines whether the reference to "available technology" could lead to an interpretation of the GDPR that dispenses from outright erasure in light of blockchains' technical limitations in favour of an alternative solution, such as transmitting a key to the data subject or deletion of the private key.[337]

Other possible solutions include adding to the blockchain a transaction that contains a reference to the block that is being erased or amended that semantically invalidates it. However, the applicability of such a solution depends on the significance of erroneous data being still visible, even if the blockchain attests its amendment. For example, if blockchain is used to store data about sexual offenders and due to a mistake, a record of someone that has not committed such a crime appears in the blockchain. This citizen invokes his right to amendment, and a transaction on the blockchain is pushed such that the record is "invalidated". Would that be enough? [338] The author believes preference should be given to other solutions. Or perhaps soon a high enough level of anonymisation of personal data within blockchain systems is achieved, that the GDPR could be sidestepped from its very beginning.[339]

From the perspective of erasure, another promising solution is the editable blockchain, which has been patented by Accenture. Accenture's editable blockchain allows designated authorities to edit, rewrite or remove previous blocks of information without breaking the

[335] L. Moerel, p. 846.
[336] M. Finck. p. 29.
[337] *Ibid.* p. 30.
[338] L-D. Ibáñez, *et al.* On Blockchains and the General Data Protection Regulation - https://eprints.soton.ac.uk/422879/1/BLockchains_GDPR_4.pdf (16.04.2019)
[339] *Ibid.*

chain under extraordinary circumstances using a "chameleon" hash.[340] However, removing the immutability feature comes at a price – other measures should be implemented to retain (or gain) sufficient trust in the blockchain application for individuals and organisations to use it as a record of their transactions.[341]

Shraddha Kulhari makes a point that the immutability of blockchains should be left intact and regulators should not adopt a very restrictive interpretation and rather strike a balance between protecting privacy and the understanding of how technology shapes up.[342] The author agrees with this view, as with all emerging technologies a balance should be struck between regulation on one hand and innovation, on the other. An example of this is Article 35(1) of Germany's Federal Data Protection Act, which states that the subject shall not have the right to erasure if erasure would be impossible or would involve a disproportionate effort due to the specific mode of storage.[343]

Berberich and Malgorzata Steiner argue that under Article 17(1)(a) personal data could be still necessary for the processing purpose, as blockchain by design requires persistent and continuously written chain.[344] It is doubtful whether such an interpretation is in line with the purpose limitation principle and thus with the objectives of the GDPR as a whole.

[340] Accenture. Editing The Uneditable - https://www.accenture.com/us-en/insight-editing-uneditable-blockchain (30.04.2019)
[341] L. Moerel, p. 849.
[342] S. Kulhari. p. 47.
[343] Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097) - https://www.gesetze-im-internet.de/englisch_bdsg/ (16.04.2019)
[344] M. Berberich, M. Steiner. p. 426.

5. Conclusion

As data protection of natural persons should be technologically neutral and should not depend on the techniques used, it was not clear how several provisions of the GDPR should be complied with in the context of blockchain technology. Thus the purpose of the present thesis was research whether blockchain and the GDPR can be reconciled as well as develop a comprehensive approach on the topic. The current master's thesis aimed to answer three research questions.

Firstly, whether the data processing on a blockchain falls within the material scope of the GDPR and thus whether the GDPR applies to blockchain? The first chapter was dedicated to answering this question. In order to understand the definition of personal data the author looked at guidelines of 29WP and the case law of CJEU. From this analysis it became apparent that the definition of personal data is broad, encompassing four main elements: (1) any information, (2) relating to, (3) identified or identifiable, (4) natural person. Two types of data are stored on a blockchain - the data, which is stored in blocks and the public key. The data stored on blocks is encrypted, while the public keys are hashed. Principles of data protection do not apply to anonymous information. However, both encryption and hashing are considered pseudonymisation techniques. Therefore as direct identification of the data subject is not possible, the author looked at whether the identification of data subjects would be possible with additional information. For example Bitcoin users disclose their addresses voluntarily when interacting with other participants, but can also be identified through mapping their Bitcoin addresses to IP addresses or by clustering the addresses. The standard for identification was set forth in the case of *Patrick Breyer v Bundesrepublik Deutschland* according to which the identification is practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power. Applying the standard set forth in the case *Breyer*, it was concluded that data identification should be very likely and thus both data contained on blocks and the public keys should be considered personal data pursuant to Article 4(1).

Furthermore, blockchain is a type of database where records are stored one after the other in a continuous ledger. Storing data on a blockchain constitutes processing pursuant to Article 4(2) of the GRPR. Furthermore, processing personal data on a blockchain is carried out automatically, thus fulfilling the material scope if no exceptions apply. The most relevant of the exceptions in relation to blockchain was the "household exception" which was relevant in

relation to a public blockchain. No exceptions applied in the case of Guardtime's private blockchain. However, it was concluded that the household exception pursuant to Article 2(2) does not apply as demonstrated by the *Bodil Linqvist* case because a public permissionless blockchain, such as Bitcoin, is available for anyone to download and therefore the data will be available to an indefinite number of people. Thus as none of the exceptions were applicable, the processing of personal data on a blockchain was within the material scope of the GDPR.

The second chapter assessed decentralised data sharing on a blockchain. First determining the question of controllership on a blockchain as it is important in terms of allocating responsibility, as well as the material scope. As per Article 4(7) the three elements of the definition of controller were looked at: (1) natural or legal person, public authority, agency or other body, (2) alone or jointly with others and (3) determines the purposes and means of the processing of personal data. Further the author analysed the elements of joint controllership pursuant to Article 26, which included multiple controllers jointly determining the purposes and means of processing with a transparent arrangement between each other.

The author concluded that in case of a private blockchain it is possible to identify a controller (or several controllers in case of a consortium blockchain) – the controller is the natural or legal person who determines the purposes and means of processing. In a public permissionless blockchain there is no central point of control as the network is opetated by all nodes in a decentralised fashion. Thus allocating responsibility and thus identifying a controller can be more difficult. The debate about controllership in public blockchains is still on-going and has not been settled. One solution would be to consider natural or legal person behind each node (the user) to be the controller if they determine the purpose and means of processing. However, nodes do not decide on the means of processing as they have no effect on which data is processed, for how long and when will said data be deleted. If over 51% of the nodes would reach consensus and alter the blocks on the chain, they would at least determine the means of processing.

The second solution would be to classify all the nodes collectively as joint controllers under article 26(1) if the nodes "jointly determine the purposes and means of processing", as well as determine their respective responsibilities for compliance in a transparent manner by means of arrangement. If the criteria are fulfilled, joint controllership should be affirmed. However, in scenarios, such as Bitcoin the rules of the network stem not from an agreement of the nodes, but ultimately from the sum of their independent behaviour. Thus it is doubtful that the nodes

determine their respective responsibilities. Finally, software developers should not be considered controllers as they relinquish control of the open source software once it is published, thus they have no effective control on the purposes and means of processing.

Next the territorial scope of the GDPR was assessed in relation to blockchain technology. The fact that blockchains operate on a decentralised structure means personal data could be processed across multiple jurisdictions. This in turn poses a risk to the protection of personal data of the subjects. The territorial scope of the GDPR as per Article 3 is comprised of two criteria. Firstly, the "establishment" criterion as per Article 3(1) meaning the GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. Second, the "targeting" criterion as per Article 3(2) meaning the GDPR applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to either the offering of goods or services or the monitoring of the subjects' behaviour.

It was concluded that in case of a private blockchain, which is established in the European Union, such as Guardtime, the processing falls within Article 3(1). In public blockchains anyone can download the software from anywhere in the world, meaning if the controller is not established in the European Union, the GDPR would apply if the conditions of Article 3(2) were met. The author found that in the case of Bitcoin the webpage was offered in several European languages and provides a platform for the trading of cryptocurrency. Therefore the conditions of Article 3(2) were met. It was concluded that the territorial scope of the GDPR is broad and even data processing on decentralised systems will trigger compliance. In addition, as part of the territorial scope the problem of data transfers to third countries and international organisations was touched upon. The GDPR allows for such transfers only when specific conditions in chapter V of the GDPR are met but they more difficult to enforce in the case of DLTs.

The final chapter compared data protection requirements and core characteristics of blockchain technology. First, a tension with the minimisation minimisation principle pursuant to Article 5(1)(c), storage limitation principle pursuant Article 5(1)(e) and the data protection by design and default principle pursuant to Article 25, was found. This is due to the ever-growing nature of data on blockchains and data persistence due to the immutable nature of the technology. The author considered whether due to said core characteristics of blockchain the

technology was at odds with the core principles of the GDPR. However, blockchains personal data on blockchains is encrypted and encryption is one of the measures, which the controller should adopt to comply with the principles of data protection by design and data protection by default. The author outlined solutions such as off-chain storage and zero knowledge proofs, which could also be of help in overcoming this tension.

Then the criterion for lawfulness of processing was looked at. The author considered consent to be the most plausible legal ground for processing in public permissionless blockchain setting. As in order to use the public blockchain, a person – the node – has to download the blockchain and run the software on their computer, this could be considered *de facto* consenting. Although downloading the blockchain and running it on the computer constitutes a freely given, affirmative action, the other necessary conditions for consent – such as being informed and specific – were not met. Blockchains did constitute good mechanisms for giving and withdrawing consent if the law was used as a base in the design phase. In the example of the private blockchain – Guardtime's KSI blockchain – the author found the lawful basis for processing to be compliance with a legal obligation.

Finally, the rights of the data subject and data persistence were analysed. Similarly as observed with the principles, as immutability is a core feature of the technology, it was outlined that both erasure and rectification are problematic in the blockchain context. Erasure would be possible if the nodes engaged in a "51% attack" but this would require extensive computational power and financial resources. This action would block the chain from functioning thus would not be a viable possibility for erasure. Therefore the controllers of blockchain technology could not comply with the requirements set forth in Article 16 and Article 17 due to the persistence of data on a blockchain. Still as set forth in the case *Google Spain* the right to erasure is not an absolute right, it would have to be balanced with other rights. Further, the author outlined several solutions, which have been proposed either in literature or have been seen in the market. It remains to be seen whether any of the solutions provide any relief to the tension with enforcement of the data subjects' rights and blockchain data persistence. However, a wider interpretation of "erasure", such as in Germany's Data Protection Act, would be of benefit for blockchain compliance.

In the light of the above, the hypothesis was correct partially – stemming from core characteristics of blockchain certain rights, such as the right to erasure and rectification, as well as principles are difficult to enforce. However, the fact that blockchain technology is still

new and developing should also be considered. As the present analysis demonstrated some solutions are already being deployed in order to respond to the data protection challenges. The present analysis also confirmed that it makes a difference in terms of compliance whether public or private blockchains are used, as for example the questions of controllership and jurisdiction are more clear in private structures.

Plokiahela tehnoloogia andmekaitse üldmääruse kontekstis

Resümee

Õigus andmete kaitsele on Euroopa Liidus reguleeritud andmekaitse üldmäärusega, mis jõustus kõikides Euroopa Liidu liikmesriikides 25. mail 2018. aastal. Kuigi määrusest tulenevad andmekaitse põhimõtted ja õigused peaksid olema neutraalsed kasutatava tehnoloogia osas, siis ei ole selge kuidas tagada määrusega vastavus plokiahela tehnoloogia kontekstis. Nimelt plokiahela tehnoloogia iseloomulikud jooned, nagu detsentraliseeritus, pidevalt kasvav andmete hulk ja nende püsivus samuti ühe kindla vastutava töötleja kinldaksmääramise probleem, on fundamentaalselt vastuolus andmekaitse määrusest tulenevate põhimõtete ja sätetega. Nii õiguskirjanduses, kui ka kohtupraktikas puudub veel vastus kuidas eelnimetatud vastuolu lahendada. Seega on kasoleva magistritöö uurimisprobleemiks vastuolu plokiahela iseloomulike joonte ja andmekaitse üldmääruse elementide ja neile vastavuse vahel. Magistritöö eesmärgiks on uurida kas neid kahte pealtnäha vastandlikku elementi on võimalik omavahel ühendada ja luua valdkonnas terviklik käsitlus. Tulenevalt töö eesmärgist, püstitab autor hüpoteesi, et Euroopa Liidu andmekaitse režiim ei ole sobiv kohalduma plokiahela tehnoloogiale.

Selleks, et teemat uurida on autor esitanud kolm uurimisküsimust. Esiteks, andmekaitse üldmääruse sisuline kohaldamisala kohaldub andmete töötlemisele plokiahelal? Sisulise kohaldamisala kohustuslikeks elementideks on isikuandmed, nende automatiseeritud töötlemine ja Arikkel 2(2) välistavate asjaolude puudumine. Andmed, mida plokiahelal töödeldakse on krüpteeritud andmed ahelal ja avalikud võtmed, mis on räsitud. Andmekaitse üldmäärus ei kohaldu anonüümsetele andmete ehk andmetele, kuid kuna nii krüpteerimist, kui räsimist, käsitletakse, kui pseudonümiseerimist, siis on andmed ahelal isikuandmed. Lisaks on plokiahela puhul tegemist automatiseeritud andmete töötlemisega, seega on täidetud sisulise kohaldamisala kohustuslikud elemendid.

Teiseks uurimisküsimuseks on kas plokiahelal on võimalik määrata kindlaks vastutav töötleja ja täita territoriaalset ulatust? Autor uurib desentraliseeritud struktuuride problemaatikat. Täpsemini on plokiahela puhul raske tuvastada andmete töötlejat, kuna plokiahel on ülesehitatud horisontaalses struktuuris, kus andmete töötlemine ja edastamine toimub igas arvutis, kes plokiahela alla laeb. Analüüs näitab, et loalise plokiahela puhul on vastutavat töötlejat kergem tuvastada. Avalike plokiahelate puhul aga, nagu näiteks Bitcoini plokiahela puhul on see küsimus problemaatilisem. Õiguskirjanduses ei ole seda debatti veel lahendatud.

Esimeseks võimaluseks on lugeda igat kasutajat vastutavaks töötlejaks, kui kasutajad määravad kindlaks isikuandmete töötlemise eesmärgid ja vahendid. Kuid üksik kasutaja ei saa plokiahela toimimist mõjutada, seega tuleks teda vastutavaks töötlejaks mitte lugeda. Teine võimalus on lugeda kasutajaid kaasvastutavateks töötlejateks juhul, kui nad määravad ühiselt kindlaks isikuandmete töötlemise eesmärgid ja vahendid. Autor leiab, et süsteemide, nagu Bitcoin, reeglid tulenevad üksikute kasutajate summaarsest käitumisest, mitte nende koordinatsioonist. Seega on kaheldav kas kasutajaid saaks lugeda kaasvastutavateks töötlejateks.

Seejärel analüüsitakse territoriaalset kohaldamisala. Detsentraliseeritud struktuurides toimub andmete töötlemine ja jagamine üle mitme jurisdiktsiooni. Analüüs näitab, et Euroopa Liidus asutatud loaliste polkiahelate puhul kohaldub andmekaitse üldmääruse artikkel 3(1), seega on territoriaalne kohaldamisala täidetud. Avalike plokiahelate puhul on igaühel võimalik tarkvara ükskõik millisest maailma otsast alla laadida. Seega kui vastutav töötleja ei paikne Euroopa Liidus, peab analüüsima kas andmekaitse üldmääruse artikkel 3(2) tingimused on täidetud. Autor jõuab järeldusele, et andmekaitse üldmääruse territoriaalne kohaldamisala on väga lai ning kohaldub igal juhul ka desentraliseeritud struktuuridele.

Kolmandaks otsitakse vastust küsimusele kas andmekaitse üldmäärusest tulenevaid nõudeid on võimalik täita plokiahelaga seoses? Vaadeldakse printsiipe, õigusi ja sikuandmete töötlemise seaduslikku alust. Täpsemini uuritakse õimalikult väheste andmete kogumise printsiipi, säilitamise piirangut ning lõimitud andmekaitse ja vaikimisi andmekaitse printsiipe. Plokiahela iseloomulikke jooni, nagu andmete püsivust ja pidevalt kasvavat andmete hulka on raske ühildada andmekaitse üldmäärusest tulenevate printsiipidega. Siiski leiab autor, et lahendused, nagu *zero knowledge proof* või andmete säilitamine plokiahela väliselt, võivad leevendada seda vastuolu. Samuti kirjeldatakse andmekaitse üldmäärusest tulenevaid õigusi, nagu õigus andmete kustutamisele ja parandamisele, mida on raske maksma panna tulenevalt plokiahela andmete püsivusest. Kaardistatakse võimalikud lahendused sellele probleemile. See, kas mõni neist lahendustest leevendab plokiahela ja andmekaitse üldmääruse vastuolu, selgub tulevikus.

Kokkuvõttes, uuritav hüpotees pidas paika osaliselt. Tulenevalt tulenevalt plokiahela iseloomulikest joontest, on andmesubjektil raske teatud õigusi, nagu õigust andmete kustutamisele ja parandamisele, maksma panna. Samuti on ka prinitsiipide puhul. Siiski tuleks arvestada, et plokiahela tehnoloogia on veel uus ja arenev. Käesolev analüüs näitas, et

andmekaitse väljakutsetele vastamiseks on juba kasutusel mõned tehnilised lahendused. Käesolev analüüs kinnitas ka seda, et loaliste plokiahelate puhul on paljud andmekaitse küsimused selgemad.

List of abbreviations

CJEU	CJEU of Justice of the European Union
DLT	Distributed ledger technology
GDPR	General Data Protection Regulation
ISP	Internet Service Provider
P2P	Peer-to-peer
WP29	Article 29 Data Protection Working Party
CNIL	French National Commission on Informatics and Liberty
EDPB	European Data Protection Board

List of bibliography

1. Antonopoulos, A. M. Mastering bitcoin : programming the open blockchain. Sebastopol, Calif. : O'Reilly Media, 2017.
2. Ambrose, M. L, Ausloos, J. The Right to Be Forgotten Across the Pond - Journal of Information Policy. 2013: 3, pp. 1-23.
3. Aste, T. *et al.* Blockchain Technologies: The Foreseeable Impact on Society and Industry - IEEE Computer. 2017:50(9) pp. 18-28.
4. Ausloos, J. The 'Right to be Forgotten' - Worth Remembering? - Computer Law & Security Review. 2012: 28(2), pp. 143-152.
5. Berberich, M. Steiner, M. Blockchain Technology and the GDPR - How to Reconcile Privacy and Distributed Ledgers - European Data Protection Law Review (EDPL). 2016: 2(3), pp. 422-426.
6. Bohannon, J. Credit card study blows holes in anonymity – Science Magazine. 2015: 347(6221), p. 468.
7. Bunn, A. The curious case of the right to be forgotten - Computer Law & Security Review. 2015: 31(3), pp. 336-350.
8. Buocz, T. *et al.* Bitcoin and the GDPR: Allocating responsibility in distributed networks - Computer Law & Security Review. 2019: 35(1), pp. 182-198.
9. Böhme, R. Pesch, P. Technische Grundlagen und datenschutzrechtliche Fragen der Blockchain-Technologie - Datenschutz und Datensicherheit (DuD). 2017: 41(8) pp. 473–481.
10. Campbell-Verduyn, M. Bitcoin and beyond: cryptocurrencies, blockchains, and global governance. Abingdon, Oxon ; New York, NY : Routledge, an imprint of the Taylor & Francis Group, 2018.
11. Christidis, K. Devetsikiotis. M. Blockchains and Smart Contracts for the Internet of Things. – Access IEEE. 2016:4. pp. 2292-2303.
12. Conte de Leon, D. *et al.* Blockchain: properties and misconceptions - Asia Pacific Journal of Innovation and Entrepreneurship. 2017: 11(3) pp.286-300.
13. De Filippi, P. Wright, A. Decentralized Blockchain Technology and the Rise of Lex Cryptographia. March 10, 2015 -https://ssrn.com/abstract=2580664 (06.01.2019)
14. De Filippi, P. Wright, A. Blockchain and the law : the rule of code. Cambridge, Massachusetts : Harvard University Press, 2018.
15. Finck, M. Blockchains and Data Protection in the European Union - European Data Protection Law Review. 2018: 4(1) pp. 17-35

16. Fulmer, N. Exploring the Legal Issues of Blockchain Applications - Akron Law Review. 2019: 52(1), article 5, pp. 161-192.
17. Ganne, E. Can blockchain revolutionize international trade?. Geneva : World Trade Organization, 2018.
18. Girasa, R. Regulation of cryptocurrencies and blockchain technologies : national and international perspectives. Cham : Palgrave Macmillan, 2018.
19. Gömann, M. The new territorial scope of EU data protection law: Deconstructing a revolutionary achievement - Common Market Law Review. 2017:5(2), pp. 567–590.
20. Herian, R. Blockchain and the (re)imagining of trusts jurisprudence - Strategic Change. 2017: 26(5) pp. 453–460.
21. Kelleher, D. Murray, K. EU data protection law. Dublin : Bloomsbury Professional(2018).
22. Kulhari, S. 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).
23. Koops, B-J. Forgetting Footprints, Shunning Shadows: A Critical Analysis of the 'Right to Be Forgotten' in Big Data Practice. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1986719 (16.04.2019)
24. Martini, M. Weinzierl, O. Die Blockchain-Technologie und das Recht auf Vergessenwerden - Neue Zeitschrift für Verwaltungsrecht. 2017: 17, pp. 1251-1259
25. Maull, R. *et al.* Distributed ledger technology: Applications and implications – Strategic Change. 2017; 26(5) pp. 481- 489.
26. Moerel, L. Blockchain & Data Protection … and Why They Are Not on a Collision Course - European Review of Private Law. 2018: 26(6), pp. 825–851.
27. Moubry, M. *et al.* Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK - Computer Law & Security Review. 2018: 34(2), pp. 222-233.
28. Ohm, P. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization - UCLA Law Review. 2010:57. p. 1701.
29. Politou, E. *et al.* Backups and the right to be forgotten in the GDPR: An uneasy relationship – Computer Law & Security Review. 2018: 34(6) pp. 1247-1257.
30. Purtova, N. The law of everything. Broad concept of personal data and future of EU data protection law - Law, Innovation and Technology. 2018: 10(1) pp. 40-81.

31. Reyes, C. L. Moving Beyond Bitcoin to an Endogenous Theory of Decentralized Ledger Technology Regulation: An Initial Proposal – Villanova Law Review. 2016: 61(1), article 5. pp. 191-234 (197-198).
32. Rosen, J. The Right to be Forgotten - Stanford Law Review Online. 2012: 64. Available at: https://www.stanfordlawreview.org/online/privacy-paradox-the-right-to-be-forgotten/ (16.04.2019)
33. Voss, D. N. Porter, J. E. Why Napster matters to writing: Filesharing as a new ethic of digital delivery - Computers and Composition. 2006: 23(2) pp. 178-210.
34. Zasky, T. Incompatible: The GDPR in the Age of Big Data. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3022646 (30.03.2019)

List of normative material

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.

36. 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.

37. Charter of Fundamental Rights of the European Union OJ C 326, 26.10.2012, p. 391–407.

38. Personal Data Protection Act - RT I, 04.01.2019, 11.

39. Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097). Available at: https://www.gesetze-im-internet.de/englisch_bdsg/ (16.04.2019)

40. Tervise infosüsteemi põhimäärus RT I, 12.03.2019, 34

41. Health Services Organisation Act - RT I 2001, 50, 284

List of cases

42. CJEU C‑553/0, *College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer*

43. CJEU C-101/01, *Bodil Lindqvist*

44. CJEU C‑524/06, *Heinz Huber v Bundesrepublik Deutschland*

45. CJEU C-70/10, *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*

46. CJEU C‑131/12, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*

47. CJEU joined cases C‑141/12 and C‑372/12, *YS v Minister voor Immigratie, Integratie en Asiel, and Minister voor Immigratie, Integratie en Asiel v M, S*

48. CJEU C‑230/14, *Weltimmo s. r. o. v Nemzeti Adatvédelmi és Információszabadság Hatóság*

49. CJEU C‑362/14, *Maximillian Schrems v Data Protection Commissioner*

50. CJEU C‑582/14, *Patrick Breyer v Bundesrepublik Deutschland*

51. CJEU C-398/15, *Camera di Commercio,Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni*

52. CJEU C‑434/16, *Peter Nowak v Data Protection Commissioner*

53. CJEU C‑210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*

Other sources

54. Article 29 Data Protection Working Party. Opinion 4/2007 on the concept of personal data. WP 136. Brussels: 2007. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf (07.02.2019)
55. Article 29 Data Protection Working Party. Opinion 05/2014 on Anonymisation Techniques. WP216. Brussels: 2014. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf (10.02.2019)
56. Article 29 Data Protection Working Party. Opinion 5/2011 on the definition of consent. WP187. Brussels: 2011 - https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf (17.04.2019)
57. Article 29 Data Protection Working Party. Guidelines on consent under Regulation 2016/679. WP259. Brussels: 2017- https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 (17.04.2019)
58. Article 29 Data Protection Working Party. Opinion 1/2010 on the concepts of "controller" and "processor". WP 169. Brussels: 2010. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf (01.03.2019)
59. European Data Protection Board. Guidelines 3/2018 on the territorial scope of the GDPR (Article 3). Brussels: 2018. Available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_en.pdf (21.03.2019)
60. Commission Decision 2010/625/EU of 19 October 2010 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Andorra (notified under document C(2010) 7084), OJ L 277, 21.10.2010, p. 27–29.
61. Commission Decision 2003/490/EC of 30 June 2003 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina, OJ L 168, 5.7.2003, p. 19–22.
62. Commission Decision 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (notified under document number C(2001) 4539), OJ L 2, 4.1.2002, p. 13–16.
63. Commission Decision 2010/146/ of 5 March 2010 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection provided by

the Faeroese Act on processing of personal data (notified under document C(2010) 1130), OJ L 58, 9.3.2010, p. 17–19.

64. Commission Decision 2003/821/EC of 21 November 2003 on the adequate protection of personal data in Guernsey (notified under document number C(2003) 4309), OJ L 308, 25.11.2003, p. 27–28.
65. Commission Decision 2011/61/EU of 31 January 2011 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data (notified under document C(2011) 332), OJ L 27, 1.2.2011, p. 39–42.
66. Commission Decision 2004/411/EC of 28 April 2004 on the adequate protection of personal data in the Isle of Man, OJ L 151, 30.4.2004, p. 48–51.
67. Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information, OJ L 76, 19.3.2019, p. 1–58.
68. Commission Decision 2008/393/EC of 8 May 2008 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Jersey (notified under document number C(2008) 1746), OJ L 138, 28.5.2008, p. 21–23.
69. Commission Implementing Decision 2013/65/EU of 19 December 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by New Zealand (notified under document C(2012) 9557), OJ L 28, 30.1.2013, p. 12–14.
70. Commission Implementing Decision 2012/484/EU of 21 August 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the Eastern Republic of Uruguay with regard to automated processing of personal data (notified under document C(2012) 5704), OJ L 227, 23.8.2012, p. 11–14.
71. Commission Decision 2000/518/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland (notified under document number C(2000) 2304), OJ L 215, 25.8.2000, p. 1–3.
72. Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of

the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176), OJ L 207, 1.8.2016, p. 1–112.

73. Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441), OJ L 215, 25.8.2000, p. 7–47.
74. Ethereum Executes Blockchain Hard Fork to Return DAO Funds - https://www.coindesk.com/ethereum-executes-blockchain-hard-fork-return-dao-investor-funds (27.02.2019)
75. J. Kaufmann. Blockchain meets Data Privacy - https://legal-revolution.com/images/pdf/Blockchain-meets-Data-Privacy_Blockchain-and-the-Data-Controller.pdf (27.02.2019)
76. B. Fabian, T. Ermakova, U. Sander. Anonymity in Bitcoin? – The Users' Perspective. Available at: https://www.researchgate.net/publication/308648091_Anonymity_in_Bitcoin_-_The_Users'_Perspective (25.02.2019)
77. A. Biryukov, D. Khovratovich, I. Pustogarov. Deanonymisation of Clients in Bitcoin P2P Network. Available at: https://orbilu.uni.lu/bitstream/10993/18679/1/Ccsfp614s-biryukovATS.pdf (26.02.2019)
78. J. Erbguth, J. G. Fasching. Wer ist Verantwortlicher einer Bitcoin-Transaktion? Available at: https://erbguth.ch/ZD12-2017.pdf (26.02.2019)
79. L-D. Ibáñez, *et al.* On Blockchains and the General Data Protection Regulation. Available at: https://eprints.soton.ac.uk/422879/1/BLockchains_GDPR_4.pdf (16.04.2019)
80. Guardtime Technology. Available at: https://guardtime.com/technology (30.03.2019)
81. Global Bitcoin Nodes Distribution. Available at: https://bitnodes.earn.com/#global-bitcoin-nodes-distribution (11.02.2019)
82. Solutions for a responsible use of the blockchain in the context of personal data. CNIL. Available at: https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf (12.03.2019)
83. T. May. Anarchist Manifesto. Available at: https://www.activism.net/cypherpunk/crypto-anarchy.html (01.04.2019)

84. B. Marr. Here Are 10 Industries Blockchain Is Likely To Disrupt. Available at: https://www.forbes.com/sites/bernardmarr/2018/07/16/here-are-10-industries-blockchain-is-likely-to-disrupt/#4db6a9fab5a2 (01.04.2019)
85. S. Hankewitz. Estonian Guardtime launches a personal care record platform for the UK NHS patients - http://estonianworld.com/technology/estonian-guardtime-launches-a-personal-care-record-platform-for-the-uk-nhs-patients/ (30.03.2019)
86. Guardtime. Dutch Government deploys Guardtime's KSI Blockchain for integrity assurance - https://guardtime.com/blog/dutch-government-deploys-guardtime-s-ksi-blockchain-for-integrity-assurance (30.03.2019)
87. Bitcoin - https://bitcoin.org/en/ (30.03.2019)
88. Krüptograafiliste algoritmide elutsükli uuring. Cybernetica. 2017 - https://www.ria.ee/sites/default/files/content-editors/publikatsioonid/kruptograafiliste_algoritmide_elutsukli_uuring_2017.pdf (12.01.2019)
89. What is Iota? - https://www.iota.org/get-started/what-is-iota (14.02.2019)
90. V. Pandit, P. Dayama. Privacy in blockchain collaboration with zero knowledge proofs – https://www.ibm.com/blogs/blockchain/2019/01/privacy-in-blockchain-collaboration-with-zero-knowledge-proofs/ (31.03.2019)