Consent by GDPR vs. Blockchain[1]

Bruno Moslavac[2]

ABSTRACT

The role of consent in personal data protection today is probably the first question for researches on how it impacts in our daily lives, ordinarily or on-line. This paper uses comparative method analyzes seemingly opposed essential parts of consent due to lawfulness of personal data processing versus inclusion of same data in a chain using blockchain technology, with the hypothesis that freewill public announcement of personal data substitute explicit consent for their processing. Finally, the author concludes that the principle of lawfulness stated by GDPR is not violated if the personal data processor using blockchain technology does not obtain consent for the processing of personal data, voluntarily put into the chain by another subject in the same "chain" and the "right to be forgotten" isn't absolute right.

Keywords: Consent. Personal data. Non-personal data. Blockchain. Right to erasure.

1 INTRODUCTION

Blockchain Technology at this moment is the most effective and best way to store and distribute data in an encrypted fashion. Blockchain could be set as an open, usually called public or permission-less either a closed blockchain, also known as private or permissioned

1 Data de Recebimento: 17/03/2020. Data de Aceite: 29/05/2020.
2 Trabalha como procurador há nove anos. É autor de vários livros e livros didáticos sobre Direito Penal e Trabalhista e quase 200 artigos. E-mail: bruno.moslavac@odovt.dorh.hr

blockchain. Public blockchain allegedly is a nightmare for legislator and privacy protection regarding personal data processing. Having more control over our personal data is what Regulation 2016/679 of the European Parliament (EU) 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 what Directive 95/46/EC (General Data Protection Regulation) wants. Two core questions for data privacy protection are: (a) is some data a personal data? And, (b) who is the controller? Those are two things people must have on mind when creating the blockchain. "The conflict between the GDPR and blockchain-based approaches to data privacy is rooted in two fundamentally different philosophies about how best to protect data privacy. The EU's vision, codified in the GDPR, views centralized, governmental authority as essential to protecting consumers and their information against the abuses of private actors, particularly hulking, data-driven technology companies. By contrast, blockchain identity solutions arose out of bitcoin's crypto-libertarian ethos, which scorns centralized authority and believes that privacy rights are best protected not by human institutions but by advanced cryptography and distributed networks that no single actor can control. The GDPR, in some ways, seeks to enhance personal privacy by reordering and further consolidating the balance of power in a familiar paradigm, while blockchain seeks to achieve the same goal by changing the paradigm completely. These foundationally different approaches result in some fundamental inconsistencies of form – but not necessarily of substance – in their two paths to solving the same problem."[3] One of the basic rights from GDPR is right to erase information regarding some individual, while blockchain are immutable, except in a case of so-called "forking[4]".

3 Laura Jehl - BakerHostetler, Robert Musiala - BakerHostetler, Stephanie Malaska – BakerHostetler, May 31, 2018, https://biglawbusiness.com/blockchain-and-the-gdpr-threading-the-needle/

4 In blockchain, a fork is defined variously as: "what happens when a blockchain diverges into two potential paths forward", "a change in protocol" or a situation that "occurs when two or more blocks have the same block height". https://en.wikipedia.org/wiki/Fork_(blockchain)

So, what came first, hen or egg? Another part of the same problem is regulation, or lack of regulation, in a case of a blockchain, what will be also discussed in this paper.

2 LAWFULNESS OF PERSONAL DATA PROCESSING

Principle of lawfulness require that the processing of personal information be lawful, which in practice means that either the processing is explicitly permissible under law or the individual whose personal data is being processed has—after being informed of the reason, context, and purpose of the processing—given consent.[5] Article 6 (1) GDPR provides cases when processing of personal data should be consider legal. Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e) 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; (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, which require protection of personal data, in particular when the data subject is a child.

5 Cate, Fred H. and Mayer-Schönberger, Viktor, "Notice and Consent in a World of Big Data" (2013). Articles by Maurer Faculty. 2662. https://www.repository.law.indiana.edu/facpub/2662.

2.1 Processing of special categories of personal data

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited (Article 9 (1) GDPR). Paragraph 1 shall not apply if, among the others, processing relates to personal data which are manifestly made public by the data subject (Article 9 (2) e GDPR). If data are already public, there is no need to obtain consent. Rightfully, for cited forms of special categories, researcher probably will not ask the subject for consent for processing of personal data. Fairly, situation is practically the same, although fairness and legality are not synonyms.

2.2 Former legal solutions

Until GDPR entry into force on 25 May 2018, Croatia had Law on the protection of Personal Data[6]. In Article 7 (1) it stated, among other, that personal data may be collected and further processed "if the respondent posted this information himself". It was a legislative solution particularly for posting of various content(s) on social networks and on the Internet in general. Especially in that case, subject had the right at any time to withdraw consent and to request the cessation of further processing of his data, except in the case of processing of data for statistical purposes when personal data no longer enable identification of the person to which they refer (Article 7 (2)). The right to withdrawal is not absolute, due to case of processing of data for statistical purposes when personal data no longer enable identification of the person to which they refer. Nevertheless, change

6 O. G. 103/03, 118/06, 41/08, 130/11, 106/12.

of mind should not be applied to blockchain information, because of the principle of immutability. Awareness on the purpose of giving information (personal data) for particular blockchain must take preference in regard to right to erasure.

3 CONSENT: VARIOUS FORMS

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 (Article 4 (11) GDPR). Consent may have various forms with similar flavors, such as informed, explicit, unambiguous or broad, each of these forms is quite diverse in nature and their use have been intensively debated for their utilization in online environments and research projects.[7] Regarding form, consent has to be "proof-able". Written shape is most popular, even has its own various forms, but consent can be verbal. Special case, the situation of clear imbalance between the data subject and the data processing managers (so-called "conditional consent"), especially if the data processor is a public authority[8].

4 POINT OF VIEW TO GIVEN CONSENT

Consent to personal data processing is just a legal instrument and its quality depends on the manner how it is used.[9] Here, we get to the beginning of a whole data protection story: purpose of data

7 Eugenia Politou, Efthimios Alepis, Constantinos Patsakis, Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions, Journal of Cybersecurity, Volume 4, Issue 1, 2018, tyy001, https://doi.org/10.1093/cybsec/tyy001

8 Branka Bet Radelić, Krešimir Rožman, Hrvoje Orešić, Protection of personal dana and the limits of workers' privacy protection, Labour Law, Rosip, Zagreb, 2017, p. 14.

9 Jakub Mišek, Consent to Personal Data Processing – the Panacea or the dead end?, Masaryk University Journal of Law and Technology Vol. 8:1, 2014, pp 69-83.

processing. Consent must fit the purpose for which personal data are being collected, stored, distributed and processed. We can say that there are different "kinds" of formal consent. Within those, we already know as sub-types of consent. So, for example, informed consent will not be structurally the same way in every single case. One must adapt to requests, in a particular case, when processing of personal data is necessary and consent has to be given, respecting principle of lawfulness. Here we do not claim that one has to look for "loopholes" and resort to invented practical solution to fulfill legal form, exactly the opposite. Research must stick to law and, law to science. Have to provide practically solution for daily use, within the content of created consent kinds.

5 CONSENT-BASED DATA PROCESSING IN BLOCKCHAIN CASE

Basic question discussing interrelation between blockchain and personal data protection is whether the consent of the data subject is at all necessary. Conditions for consent stated in Article 7 GDPR don't bring *numerus clausus* of a situation when the controller or processor unconditionally must seek and get subject's consent. Consent should be given unambiguously, but the question is when, in which particular cases or security of personal, data will be endangered. The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that, by default, personal data are not made accessible without the individual's intervention to an indefinite number of natural persons (Article 25 (2) GDPR). Blockchain is independent of the underlying consensus algorithm,

a linked list data structure that uses hash sums over its elements as pointers to the respective elements.[10]

5.1 Amount of personal data collected in "chain"

Only personal data which are necessary for each specific purpose of the processing should be processed. In case of a single "chain" regarding blockchain technology, the amount of personal data collected is significantly small. Not insignificant, but considering the total amount of data, not only personal but also non-personal data, relatively little. Thereby, we should not forget that some categories of formally personal data, such as location data, an online identifier, despite defined as a personal data, very easily can be observed as a non-personal data[11]. Their true "legal" nature, their scope and their contents supports the previous claim. Furthermore, legal standard enforcer is decision-maker if some data is personal or non-personal. Interpretation of certain information as a personal data or non-personal data later will be case for subsequent (re)evaluation by a competent national court, over Constitutional Court until final review by a supranational, European Court of Human Rights.[12]

6 SHIFTING BURDEN OF PROOF

Proving facts in any case of illegality is always hard-work. Blockchain is a digital concept to store data. Since blocks are chained together, that makes them (data inside) immutable. Input of data is executed by a person who makes "block" in a chain. That person

10 Judmayer, A. – Stifter, N. – Krombholz, K. –Weippl, E., Blocks and Chains: Introduction to Bitcoin, Cryptocurrencies, and Their Consensus Mechanisms, Morgan & Claypool, 2017, pp. 23-24.
11 Art. 3 (1) Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union (COM/2017/0495 final - 2017/0228 (COD) defines that "data" means data other than personal data as referred to in Article 4 (1) of Regulation (EU) 2016/679.
12 of non-personal Bruno Moslavac, Cyber security Workers' Data, Labour Law Magazine no. 4/2018, pp. 12-22.

has some interest to act on that way and it is fully aware of what information (data) he or she is storing in (public) blockchain. Those data are being stored using cryptographic hash function, so they are not visible "at first". Every string of data has only one unique hash bound to it. Potential abuse of any personal data stored in particular chain requires legal protection based on GDPR rules. First question is who is "plaintiff"? And even more important, second question is who will be "defendant"? Last one is the "victim" of burden of proof, since he or she shall be able to demonstrate that the data subject has consented to processing of his or her personal data. So, the culprit should be detected first and then we can discuss about personal data endangering and protection. Authorized person for consent is a natural person, data subject to who personal data refers to. Processor in a case of a blockchain can be any natural or legal person dealing with or having interest in decentralized applications (DApps). This is where we have to look for "defendant".

7 "RIGHT TO BE FORGOTTEN" AND BLOCKCHAIN

What is on the Internet, stays on the Internet is a well-known fact. This is an argument to support the claim that the willful disclosure of personal data in a "chain", using blockchain technology, does not provide a collision to the protection of personal data in a right way. In particular, a data subject have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary, in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with GDPR. However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information,

for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment to exercise or defense on legal claims[13]. Blockchain should last permanent, so there is no moment when the data inside are no longer necessary. The blockchain, as decentralization, is a revolutionary new computing paradigm. The blockchain is the embedded economic layer the web never had. The blockchain is the coordination mechanism, the line-item attribution, credit, proof, and compensation rewards tracking schema to encourage trustless participation by any intelligent agent in any collaboration. The blockchain is a decentralized trust network. The blockchain is a cloud venue for transnational organizations. The blockchain is a means of offering personalized decentralized governance services, sponsoring literacy, and facilitating economic development. The blockchain is a tool that could prove the existence of exact contents of any document or other digital asset at a particular time.[14] As we can see, blockchain technology is far beyond just the privacy protection or personal data protection regarding the right to be forgotten. General provisions are about right to erasure of personal data, states that "right to be forgotten" shall apply when data are no longer needed for the purposes that they were collected or otherwise processed. Other provisions from Article 17 (1) GDPR notes that the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one, beyond mentioned, of the following grounds applies: the data subject withdraws consent on which the processing is based according to

13 GDPR, Introduction (65).
14 Melanie Swan, Blockchain: Blueprint for a New Economy, O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472, 2015, p. 92.

point (a) of Article 6 (1), or point (a) of Article 9 (2), and where there is no other legal ground for the processing; the data subject objects to the processing pursuant to Article 21 (1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21 (2); the personal data have been unlawfully processed; his personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; the personal data have been collected in relation to the offer of Information Society Services referred to in Article 8 (1).

7.1 Data protection through technology design: Privacy by Design (PdB)

The increasing significance of data protection when creating and operating IT systems creates additional requirements for IT specialists. As a result, data protection must be an essential element in the training of IT professionals.[15] Implementation of PbD will play a significant role in organizations' efforts to respect privacy. In the years to come, we will come across initiatives to specify and apply the concept of PbD during the design process. PbD specification and implementation will go much beyond systems design and will have an impact at different levels. First, it will affect the whole organizational context including stakeholders with diverse interests from different disciplines; and second, the whole supply chain, starting from the component/technology provider and ending at end users.[16] Article 25 GDPR should be seen as a weighty conversation-starter in the necessary dialogue between data protection authorities and privacy advocates. On one side, data controllers, processors and engineers,

15 Schaar, P. IDIS (2010) 3: 267. https://doi.org/10.1007/s12394-010-0055-x.
16 Tsormpatzoudi, P., Berendt, B., & Coudert, F. (2016). Privacy by Design: From research and policy to practice - the challenge of multi-disciplinarity. In B. Berendt, T. Engel, D. Ikonomou, D. Le Métayer, & S. Schiffner (Eds.), Privacy Technologies and Policy. Third Annual Privacy Forum, APF 2015. Luxembourg, Luxembourg, October 7-8, 2015. Revised Selected Papers (pp. 199-212).

on the other, are forwarding in the technological and organizational hardwiring of privacy-related interests.[17] Legislative changes have the potential, sometimes inadvertently, to make data access and thus research more difficult. Continuing technological developments demand constant, refinement of physical and technical infrastructure.[18] At this point, there are not judgment(s) of the European Court of the Human Rights concerning privacy and adjusted with the growth of blockchain technology.

7.2 "Place" of data storing

By storing the personal data off-the-chain (not in actual blockchain), the system complied with the GDPR rule (right to be forgotten). Misuse, mismanagement and lesser scope for personally identifiable information (PII) tracking were identified as major causes of privacy breaching. Using an off-chain blockchain with data hash checking, the proposed system successfully addressed those pitfalls. Privacy by design should apply in blockchain development for efficient privacy preservation.[19] Personal data and sensitive data in general, should not be trusted in the hands of third-parties, where they are susceptible to attacks and misuse. Instead, users should own and control their data without compromising security or limiting companies' and authorities' ability to provide personalized services. Furthermore, with a decentralized platform, making legal and regulatory decisions about collecting, storing and sharing sensitive data should be simpler. Moreover, laws and regulations could be programmed into the blockchain

17 Lee A. Bygrave, Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements, Oslo Law Review, Volume 4, Nº 2-2017, pp. 105–120.
18 Caitlin Pencarrick Hertzman, Nancy Meagher, Kimberlyn M McGrail, Privacy by Design at Population Data BC: a case study describing the technical, administrative, and physical controls for privacy-sensitive secondary use of personal information for research in the public interest, Journal of the American Medical Informatics Association, Volume 20, Issue 1, January 2013, Pages 25–28, https://doi.org/10.1136/amiajnl-2012-001011
19 Onik, M., Kim, C., Lee, N., et al. (2019). Privacy-aware blockchain for personal data sharing and tracking. Open Computer Science, 9(1), pp. 80-91. Retrieved 16 Aug. 2019, from doi:10.1515/comp-2019-0005.

itself, so that they are enforced automatically. In other situations, the ledger can act as legal evidence for accessing (or storing) data, since it is (computationally) tamper-proof.[20] To fully adopt and implement the paradigm of "Privacy by Design", we must recognize transparency as an important attribute of not only the data itself but also the code handling of personal data (open-source). Knowing what a system does with our data is the only way of allowing educated data subjects to identify risks to them. For this reason, we have deliberately chosen to represent the concept of the data subject's consent such as the responsibility of providing personal data lies, both legally and technically, in his or her own hands. By representing the consent of the data subject in a smart contract ecosystem, we make the processing of personal data a question of control rather than trust.[21]

8 ANONYMITY DUE TO GDPR AND BLOCKCHAIN

Personal data protection is GDPR mainstream. True question, when parsing personal data protection related to blockchain, is either they "must" be discovered on the Internet. Blockchain as a new technology aim to anonymity, but through or up to privacy. Anonymity is simply privacy or the security of one's personal data. The anonymity issue has merged into the online privacy issue, and the online privacy issue is merged into the offline privacy issue, and in fact has become just the issue with no adjectives[22]. Does anonymity just mean hiding your identity? Blockchain anonymity rises from the fact that ledger, record of all transactions in the chain, be available to "public", everyone and all transactions in blockchain are/be public knowledge. That

20 Guy Zyskind, Oz Nathan, Alex 'Sandy' Pentland, Decentralizing Privacy: Using Blockchain to Protect Personal Data, https://enigma.co/ZNP15.pdf.
21 Wirth C, Kolain M (2018) Privacy by blockchain design: a blockchain-enabled GDPR-compliant approach for handling personal data. In: Proceedings of 1st ERCIM blockchain workshop 2018. European Society for Socially Embedded Technologies (EUSSET).
22 A. Michael Froomkin, From Anonymity to Identification, Journal of Self-Regulation and Regulation, Volume 01 (2015), pp. 120-139.

build anonymity and privacy concerns. Among other data, a blockchain can house the code which could make an individual identifiable. There are many technologies helping secure anonymity when using blockchain, the most common are Tor and VPNs. Transactions stored in a blockchain are anonymous and irreversible. Although parties in the network release no private information, their transactions are traceable and visible network-wide. Although, blockchains preserve anonymity and privacy, the security of assets depends on safeguarding the private key, a form of digital identity. If one's private key is acquired or stolen, no third party can recover it. Cryptographic keys and anonymous transactions make blockchain vulnerable to account takeover and digital identity theft, because an identity is protected only by its private key.[23] Even though, the blockchain foundationally contradicts certain principles in the GDPR, such as rectification and removal. The blockchain strongly conforms to the technical data protection principles according to the GDPR, as the blockchain has proven to be one of the most secure structures. The biggest conflict between the blockchain and the GDPR is the blockchain's immutability. However, its biggest strength originates from that. This immutability and the purposes of having an immutable object are in line with some of the GDPR's purposes, namely integrity, security and transparency, but do result in the data subject losing the retroactive control over their personal data. The GDPR assesses these principles as absolute but, does not discuss if alternative usage would provide the most security for the individual. The blockchain provides one of the highest security standards to date regarding the integrity of data but, at the cost of data being non-removable. It might be required to address if there is a breaking point where security is achievable at the cost of other principles, enter the blockchain.[24]

23 Xu, J.J. Financ Innov (2016) 2: 25. https://doi.org/10.1186/s40854-016-0046-5.
24 Sebastian Ramsey, The General Data Protection Regulation vs. The Blockchain - A legal study on the compatibility between blockchain technology and the GDPR, FAculty of LAw Stockholm University, 2018, https://pdfs.semanticscholar.org/c231/c390f1bb345a2f6ebceee792264f227f9d32.pdf.

9 BLOCKCHAIN "LEGALIZATION" (REGULATION)

Every legal regulation implies the activities of social institutions and institutions of public authority. There is no (general) legal act or law that provides legality for Internet, let alone blockchain technology. The whole blockchain idea is about privacy and decentralization, beyond the reach of the authorities. To declare something unlawful, it should be legalized on the first place. Those conditions are not executed when talking about blockchain. Causative consequence is that simply there cannot be "unlawful processing" of personal data in a blockchain case. The area for possible illegal acts, including potential criminal offenses, almost does not exist when applying blockchain technology. On the other hand, privacy protection in case of a personal data is "fertile ground" for criminals of various kinds with various measures. Future "Blockchain Law" should resolve lack of regulation of new technology occurrence and became a counterbalance to existing GDPR. At that point, we will have two equivalent regulations and challenge for lawyers to resolve regulations conflict using legal instruments.

10 FINAL CONSIDERATIONS

The right to be forgotten (right to erasure), as an integral part of personal data security and the inseparable part of European Privacy Law, is actually, not the opposite of the blockchain idea. The entire personal data protection system at first, or at least in one huge part, starts from the consent. Anyone involved in any part of the blockchain at start, gives the free-willing consent for posting certain information that does not necessarily represent personal data. The subsequent request for removal of personal data from a legal point of view does not affect the legitimacy and authenticity of the earlier disclosure of the relevant information, so there is no "conflict of interest" or a derogation from GDPR due to, or "in favor" of, blockchain technology.

Lack of blockchain legal (law) regulation is a problem, so we cannot use the principle lex posterior derogate legi priori. Already more and more opinions and researchers are emerging and creating solutions to prove that GDPR and blockchain are not opposed. Permission from users before processing their personal data is not needed when individual in his "free will and common sense" voluntarily gets involved in a blockchain. The right to be forgotten is not absolute right, after all, neither is the right to the protection of personal data, even it is a fundamental (human) right. Public interest for and out of blockchain technology has to overwhelm private interest of personal data protection.

CONSENTIMENTO DO GDPR VS. BLOCKCHAIN

RESUMO

Atualmente, o papel do consentimento na proteção de dados pessoais é provavelmente a primeira pergunta das pesquisas sobre como isso afeta nosso dia a dia, na normalidade ou on-line. Este artigo usa análises comparativas de métodos, aparentemente opostos a partes essenciais do consentimento, devido à legalidade do processamento de dados pessoais versus a inclusão dos mesmos dados em uma cadeia, usando a tecnologia Blockchain, com a hipótese de que o anúncio público voluntário de dados pessoais substitui o consentimento explícito pelo processamento. Finalmente, o autor conclui que o princípio da legalidade declarado pelo GDPR não é violado se o processador de dados pessoais que usa a tecnologia Blockchain não obtiver consentimento para o processamento de dados pessoais, caso esses sejam voluntariamente colocados em cadeia por outro sujeito da mesma "cadeia" e o "direito de ser esquecido" não é um direito absoluto.

Palavras-chave: Consentimento. Dados pessoais. Dados não pessoais. Blockchain. Direito de exclusão.

REFERENCES

Jehl, Laura; BakerHostetler, Robert Musiala - BakerHostetler, Stephanie Malaska – BakerHostetler, May 31, 2018, https://biglawbusiness.com/blockchain-and-the-gdpr-threading-the-needle/

Cate, Fred H. and Mayer-Schönberger, Viktor, "Notice and Consent in a World of Big Data" (2013). Articles by Maurer Faculty. 2662. https://www.repository.law.indiana.edu/facpub/2662.

Eugenia Politou, Efthimios Alepis, Constantinos Patsakis, Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. **Journal of Cybersecurity**, Volume 4, Issue 1, 2018, tyy001, https://doi.org/10.1093/cybsec/tyy001

Radelić, Branka Bet; Rožman, Krešimir; Orešić, Hrvoje. **Protection of personal dana and the limits of workers' privacy protection**, **Labour Law, Rosip, Zagreb**, 2017, p. 14.

Jakub Mišek, Consent to Personal Data Processing – the Panacea or the dead end?, **Masaryk University Journal of Law and Technology**, Vol. 8:1, 2014, pp 69-83.

Judmayer, A. – Stifter, N. – Krombholz, K. –Weippl, E. **Blocks and Chains**: Introduction to Bitcoin, Cryptocurrencies, and Their Consensus Mechanisms, Morgan & Claypool, 2017, pp. 23-24.

Moslavac,Bruno. Cyber security Workers' Data. **Labour Law Magazine**, no. 4/2018, pp. 12-22.

Swan, Melanie. **Blockchain:** Blueprint for a New Economy, O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472, 2015, p. 92.

Tsormpatzoudi, P., Berendt, B., & Coudert, F. (2016). **Privacy by Design**: From research and policy to practice - the challenge of multi-disciplinarity. In B. Berendt, T. Engel, D. Ikonomou, D. Le Métayer, & S. Schiffner (Eds.), Privacy Technologies and Policy. Third Annual Privacy Forum, APF 2015. Luxembourg, Luxembourg, October 7-8, 2015. Revised Selected Papers (pp. 199-212).

Lee A. Bygrave. **Data Protection by Design and by Default**: Deciphering the EU's Legislative Requirements, Oslo Law Review, Volume 4, No. 2-2017, pp. 105–120.

Caitlin Pencarrick Hertzman, Nancy Meagher, Kimberlyn M McGrail, Privacy by Design at Population Data BC: a case study describing the technical, administrative, and physical controls for privacy-sensitive secondary use of personal information for research in the public interest, **Journal of the American Medical Informatics Association**, Volume 20, Issue 1, January 2013, Pages 25–28, https://doi.org/10.1136/amiajnl-2012-001011

Onik, M., Kim, C., Lee, N., et al. (2019). blockchain Privacy-aware for personal data sharing and tracking. **Open Computer Science**, 9(1), pp. 80-91. Retrieved 16 Aug. 2019, from doi:10.1515/comp-2019-0005.

Guy Zyskind, Oz Nathan, Alex 'Sandy' Pentland, Decentralizing Privacy: Using Blockchain to Protect Personal Data, https://enigma.co/ZNP15.pdf.

Froomkin, A. Michael. **From Anonymity to Identification, Journal of Self-Regulation and Regulation**. Volume 01 (2015), pp. 120-139.

Xu, J.J. **Financ Innov.** (2016) 2: 25. https://doi.org/10.1186/s40854-016-0046-5.

Sebastian Ramsey. **The General Data Protection Regulation vs. The Blockchain - A legal study on the compatibility between blockchain technology and the GDPR**. FAculty of LAw Stockholm University, 2018, https://pdfs.semanticscholar.org/c231/c390f1bb345a2f6ebceee792264f227f9d32.pdf.