PRIVACY BETWEEN REGULATION AND TECHNOLOGY: GDPR AND THE BLOCKCHAIN

Asim Jusić*

Abstract

Compliance with the GDPR while using blockchain technology for data processing results in compliance issues, due to the fact that the blockchain and the GDPR employ different methods to ensure privacy-by-design and privacy-by-default. The blockchain is built on disintermediation and relative decentralization, whereas the GDPR aims for re-intermediation and relative centralization of the data protection process. This paper provides an overview of and suggestions on how to secure compliance with the GDPR while processing data using the blockchain. A focus is placed on the data protection impact assessment on the blockchain network, issues in identifying and determining the role(s) of sole and joint data controllers and data processors, obstacles to exercising the right to rectification and right to be forgotten when the data is recorded on the blockchain, GDPR data transfer requirements as applied to the blockchain, and the protection of privacy in the process of creating blockchain-based smart contracts.

Keywords
GDPR · Blockchain · Compliance Privacy

* Asim Jusić is an Attorney at Law and an Adjunct Assistant Professor of Law, International University of Sarajevo.

1. Introduction

The EU's General Data Protection Regulation (GDPR) (EU/2016/679)[1] is considered among the most important privacy protection regulations to have entered into force in recent history. At the same time, the blockchain is considered to be a technological innovation that may well fundamentally alter economies and everyday life by enabling disintermediation and rapid extraction of value from data.[2] However, relatively few sources discuss in detail whether, and how, the processing of data on the blockchain can be organized in such a way so as to comply with the GDPR.[3] This paper has two aims. Firstly, it discusses the main differences between the blockchain and the GDPR. Secondly, it provides practice-oriented suggestions on how to secure compliance with the GDPR while processing data and transferring value using the blockchain.

Part two of the paper provides an overview of the GDPR and blockchain technology. Part three analyses the most important compliance issues that emerge in the process of applying the GDPR to the blockchain: the data protection impact assessment on the blockchain network, issues in identifying and determining the role of sole and joint data controllers and data processors, obstacles to exercising of the right to rectification and right to be forgotten when data is recorded on the blockchain, GDPR data transfer requirements as applied to the blockchain, and the protection of privacy in the process of creating blockchain-based smart contracts. Part four concludes the paper.

2. The GDPR and Blockchain: An Overview

2.1. The General Data Protection Regulation

The GDPR is considered a breakthrough in privacy protection regulations. Three factors make the GDPR one of the most influential privacy protection regulations in existence: the concepts and principles behind it are considered a 'golden standard' of privacy protection; its extraterritorial impact is immense; and its relevance for and impact upon international data transfer flows are equally significant.

[1] Regulation EU/2016/679, European Union, 'General Data Protection Regulation (GDPR) – Official Legal Text' (*General Data Protection Regulation (GDPR),* https://gdpr-info.eu/, accessed 16 May 2021.

[2] McKinsey, 'How Blockchains Could Change the World' (2016), https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/how-blockchains-could-change-the-world#, accessed 19 May 2021.

[3] See Michèle Finck, 'Blockchain and the General Data Protection Regulation', https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf. accessed 14 May 2021; Tom Lyons, Ludovic Courcelas and Ken Timsit, 'Blockchain and the GDPR', https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf, accessed 14 May 2021; and Asim Jusic, 'Dealing with Tensions Between the Blockchain and the GDPR' in Sophia Adams Bhatti, Akber Datoo and Drago Indjic (eds), *The LegalTech Book: The Legal Technology Handbook for Investors, Entrepreneurs and FinTech Visionaries* (John Wiley & Sons 2020), on which this paper builds and expands.

2.1.1. The Gold Standard of Privacy Protection

The GDPR elevated privacy to the level of a fundamental human right, and restricted the collection and processing of the personal data of holders of data rights, i.e. the data subjects.[4] The GDPR achieved this by embracing the concepts of the privacy-by-design and –default, and operationalizing these concepts through six privacy principles for the processing of personal data.

'Privacy-by-design' means that privacy and associated data protection issues should be taken into consideration throughout the process of designing any system, service or product. 'Privacy-by-default' requires those governing data processing – primarily data controllers and data processors–to process only such data that is necessary to achieve the specific purpose of data processing.[5] This means that any data processing should be undertaken in line with six core GDPR privacy principles: (a) lawfulness, fairness, and transparency in relation to the data subject (owner of the personal data); (b) purpose limitation; (c) data minimization; (d) accuracy; (e) storage limitation; and (f) integrity and confidentiality.[6]

The concepts of privacy-by-design and -default and the six principles of data processing enshrined in the GDPR became influential even before the GDPR came into force. Presently, the influence of the GDPR is so strong that comparability to the GDPR has become a measure of the quality of non-EU data protection regulations, turning the GDPR into a global 'golden standard' of privacy protection.[7]

2.1.2. The GDPR's Extraterritorial Impact

The GDPR is implemented in the present age of the free flow of data across national borders via the web. For that reason, the GDPR departs from the traditional understanding of the territorial scope of application of law, having instead an extraterritorial reach. Organizations established in the EU are expected to comply with the GDPR, even if they process data outside the EU. Non-EU entities offering goods or services inside the EU must also abide by the GDPR, even if such goods and services are offered free of charge. Further, the GDPR applies to organizations that 'monitor' individuals in the EU, irrespective of the place of registration of such organizations.[8]

To understand the breadth and width of the GDPR's extraterritorial impact, consider the following examples. If a non-EU entity uses one of the official EU languages or the euro as an accepted currency for payments, such a non-EU entity is subject to the GDPR because use of one

[4] PricewaterhouseCoopers, 'Top Policy Trends 2020: Data Privacy' (*PwC*, 2021), https://www.pwc.com/us/en/services/consulting/risk-regulatory/library/top-policy-trends/data-privacy.html, accessed 10 April 2021.
[5] GDPR Art. 25. (1) and (2) and Information Commisioner's Office, "Data Protection by Design and Default" (ICO, February 9, 2021), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/.
[6] GDPR Art. 5. (1).
[7] cf. Asim Jusic, "Practical Guidance: Data Transfers - Gulf Region" (Bloomberg Law, 2018).
[8] GDPR Art. 3 and Freshfields Bruckhaus Deringer, "The Extra-Territorial Scope of the EU's GDPR," accessed April 15, 2021, https://www.freshfields.com/en-gb/our-thinking/campaigns/digital/data/general-data-protection-regulation/.

of the official EU languages or euro as a currency signals that the non-EU entity is 'envisaging' offering goods or services within the EU.[9] Moreover, using cookies to track web traffic and online behavior of individuals in the EU also makes the non-EU entity subject to the GDPR.[10]

2.1.3. International Data Transfers

For the purposes of the GDPR, international data transfers (IDTs)are transfers of data to non-EU countries and countries outside the European Economic Area (third countries) and international organizations, as well as onward data transfers from a third country to another third country or international organization.[11] The main requirement for an IDT is that the protection of rights of data subjects provided by the GDPR shall not be circumvented in the process of such transfer(s). This means that, i.e. data subjects should be informed that their data is to be transferred internationally, and that data processors should comply with their GDPR obligations and retain records of data processing, etc.[12]

Consequently, the GDPR allows IDTs in a limited number of cases. Firstly, an IDT is permitted if an EU Commission adequacy decision exists.[13] Secondly, an IDT can be performed if adequate safeguards for protecting data subjects' rights during the process of data transfer also exist. The GDPR cites standard contractual clauses,[14] binding corporate rules,[15] codes of conduct,[16] and certification mechanisms[17] as methods of IDT that adequately safeguard data subjects' rights. Third, IDTs can be performed in cases of derogations listed in GDPR Art. 49. Finally, IDTs are also permitted if they are sanctioned by international agreements.

A further limitation on IDTs is the prohibition of the recognition and enforcement of a third-country authority's decisions compelling a data controller or processor subject to the GDPR to transfer or disclose personal data. The data controller or processor subject to the GDPR can comply with such decisions only if an international agreement on the recognition and enforcement of such decisions exists, or if the data transfer and disclosure is undertaken using one of the data transfer mechanisms outlined above.[18]

2.2. Blockchain: What It Is, and Why It Matters

In general, the blockchain can be described as a chain of blocks wherein each block holds data that can be created by multiple originators using multiple internet addresses, while retaining anonymity of the creators in the process of the creation of data. Each new block is attached to a preceding one in a process that is often computationally demanding. The result is the creation of

[9] GDPR, Recital 23.
[10] GDPR, Recital 24 and Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide*, 1st ed. (Springer International Publishing, 2017), 22–29.
[11] GDPR, Art. 44.
[12] Christopher Kuner (editor) et al., *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press, 2020), 757.
[13] GDPR, Art. 45.
[14] GDPR, Art. 46.
[15] GDPR, Art. 47.
[16] GDPR, Art. 40.
[17] GDPR, Art. 42.
[18] Jusic, "Practical Guidance: Data Transfers - Gulf Region," 7.

the 'distributed ledger', i.e. copies of the records of transactions distributed among several participants. There are several types of blockchain. In the permissionless blockchain, for example, records of transactions are transparent, and adding new and removing old records requires the consensus of all participants. In the permissioned type of blockchain, adding and removing new blocks and data need not be based on the consensus of all participants. Regardless, the data recorded in blocks remains private, because it can be accessed only by those in possession of cryptographic keys necessary to decrypt and read the data inside the block.[19]

There are two reasons for blockchain being touted as a revolutionary innovation that will fundamentally alter many industries, and perhaps the entire economy.[20] Firstly, the blockchain is decentralized and disinter mediated, i.e. it allows individuals to directly exchange data without need for an intermediary. Decentralization and disintermediation have made blockchain the technology of choice for the creation of crypto currencies. These crypto currencies enable the direct transfer of value from person to person while bypassing traditional intermediaries such as banks, and, in doing so, 'disrupt' the mainstream financial system and financial industry.[21]

Secondly, the technology behind blockchain provides a significant – albeit not absolute– trustlessness, anonymity and immutability of data records. The participants in blockchain transactions need not know or trust one another in order to enter a transaction. Instead, participants rely on the encryption and immutability of blocks to protect their data from privacy and counterparty risks.[22] The data within blocks is accessible only to those in possession of cryptographic keys, and, in the case of the permissionless blockchain, the immutability of data is protected by the fact that the consensus of all participants is necessary not only for the adding of new blocks to the chain, but also for their removal.[23] From a perspective of privacy protection, the very structure of blockchain *enforces* privacy-by-design and, partially, privacy-by-default.[24]

3. Compliance Issues

As suggested in Part II of this paper, the GDPR and the blockchain share commitment to privacy-by-design and -default. In this part, it is shown that compliance issues have arisen because the blockchain and the GDPR use different methods to ensure privacy-by-design and privacy-by-default. Whereas the blockchain is built on the ideas of disintermediation and decentralization, the philosophy behind the GDPR is the opposite: the GDPR aims for re-intermediation and relative centralization of the data protection process. The focus here is the most significant issues that emerge in the process of ensuring that data transfer using the

[19] Joseph J. Bambara and Paul R. Allen, *Blockchain. A Practical Guide to Developing Business, Law and Technology Solutions* (McGrawHill, 2018), 1–13.
[20] Bernardo Nicolletti, *The Future of Fintech: Integrating Finance and Technology in Financial Services* (Palgrave Macmillan, 2017).
[21] Rainer Böhme et al., "Bitcoin: Economics, Technology, and Governance," *Journal of Economic Perspectives* 29, no. 2 (May 2015): 213–38, https://doi.org/10.1257/jep.29.2.213.
[22] William Mougayar and Vitalik Buterin, *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology* (1 edition, Wiley 2016).
[23] Kevin Werbach, "Trust, But Verify: Why the Blockchain Needs the Law," *Berkeley Technology Law Journal* 33 (August 1, 2017): 489, https://doi.org/10.2139/ssrn.2844409.
[24] Silvan Jongerius, 'A Primer to GDPR, Blockchain, and the Seven Foundational Principles of Privacy by Design - Dataconomy', https://dataconomy.com/2019/01/a-primer-to-gdpr-blockchain-and-the-seven-foundational-principles-of-privacy-by-design/, accessed 19 May 2021.

blockchain is compliant with the GDPR: data protection impact assessment, issues in identifying and determining the role of sole and joint data controllers and data processors, obstacles to exercising the right to rectification and right to be forgotten, data transfer requirements, and the protection of privacy in the process of creating blockchain-based smart contracts.

3.1. The Data Protection Impact Assessment and the Blockchain

The data protection impact assessment (DPIA) is an exercise in, as GDPR Art. 35 states, "an assessment of the impact of the envisaged processing operations on the protection of personal data." Data controllers are expected to perform a DPIA if data processing will be performed using new technologies and is likely to create high risks for natural subjects' privacy. The DPIA is obligatory if the personal aspects of data will be used for decision-making in an automated process. In general, a DPIA should include a systematic description of the purpose and processes of data processing, an evaluation of privacy risks, information on the necessity and proportionality of the processing operations in relation to the purpose of processing, and measures in place to ensure compliance with the GDPR and to decrease risks to data subjects' and third parties' privacy.[25]

The application of the text of the GDPR's DPIA requirements to the blockchain yields the following implications and presents several questions for the users of the blockchain network and the data controllers.

Firstly, because it has already existed for two decades, blockchain is not an entirely a new technology. Nevertheless, blockchain is a form of automation, and there are a variety of as-yet-untested ways of using the blockchain. Because automation of data processing in untested ways can create unforeseeable adverse consequences for privacy, from the perspective of the GDPR, the blockchain constitutes a new technology. Hence, entities employing blockchain for the handling of data of natural subjects should conduct a DPIA in advance of creating the blockchain network if the data being processed involves the personal data of natural subjects. If the processing system is deemed unlikely to create heightened privacy risks for natural subjects, the conducting of a DPIA may well be redundant.[26]

Secondly, both the data controllers and the natural subjects could question the usefulness of engaging in the DPIA, for following reasons. The tacit assumption behind the DPIA is that those conducting the DPIA can anticipate most privacy risks with some degree of certainty at the time when the DPIA is performed. The natural subjects whose privacy rights are at stake could argue that such assessment of privacy risks leaves determination of the severity of present and future privacy risks in the hands of those that perform the DPIA. In turn, those conducting the DPIA could protest that the periodical or continuous undertaking of DPIAs is a costly, formalistic and risky exercise in assessment of privacy risks in an "experiment-like" environment that does not reflect real-world situations and privacy risks.

[25] Information Commisioner's Office, "Data Protection Impact Assessments" (ICO, January 11, 2021), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/.
[26] Tamás Bereczki and Ádám Liber, "Blockchain and the GDPR: Addressing the Compliance Challenge," 2018, https://www.lexology.com/library/detail.aspx?g=571106ac-1aaf-4db9-b1a0-0152848fd040.

3.2. Sole and Joint Data Controllers and Data Processors on the Blockchain

If the philosophy of the blockchain is disintermediation, the philosophy behind the GDPR could be labelled 're-intermediation.' This is because protection of data subjects' rights in the GDPR could be said to rest on the activities of two kinds of data intermediaries: the sole and joint data controllers and data processors.

The GDPR defines a 'data controller' as a natural or legal person or public entity that, alone or jointly with other data controllers, determines the purposes and means of the processing of personal data. The main tasks of the sole or several (joint) data controllers include estimation of privacy risks and implementation of proportionate technical and organizational measures that safeguard data subjects' rights listed in the GDPR. If joint controllers collectively determine the purposes and means of data processing, they should define their roles and responsibilities towards data subjects clearly and in advance. Should joint controllers fail to create a system of distribution of roles and responsibilities, each joint controller becomes responsible for the entirety of the damage to a data subject's privacy rights.[27]

Next in the line of data intermediaries is the data processor, which the GDPR describes as a natural or legal entity that processes personal data on behalf of the data controller. The relationship between the data controller and processor is contractual and largely hierarchical. For example, among many other obligations, the processor is expected to adhere to the controller's documented instructions, preserve data subjects' privacy rights throughout the process of data processing, and control sub-processors, if they are to engage any.[28]

National data protection regulators have suggested that identifying data controllers and processors on the blockchain could be done by classifying those writing on the blockchain as data controllers, while simultaneously treating those validating blockchain entries as data processors.[29] Applying this solution could be relatively straightforward in some cases. Complications ensue, however, when dealing with types of blockchain in which the same entity is simultaneously the data controller and processor.[30] In such cases, according to the GDPR, the data processor could be treated as a data controller, because in this case it is the processor that determines the purpose and means of processing.[31]

If, however, the data subject, controller and processor are merged into a single person or entity, sustaining a distinction between these three roles could be useless. This reveals the extent – and far-reaching impact – of philosophical differences between the blockchain and the GDPR. As boundaries between persons that the GDPR treats as data subject, controller and processor blur, decentralization and disintermediation using the blockchain are more complete. The implication is that the more the data subject, controller and process or merge into one person, the more sovereignty the data subject has over their privacy. At the same time, the regulation of and liability for privacy breaches becomes extremely difficult – if not impossible – to implement.

[27] GDPR Art. 4., 24. and 26.
[28] GDPR Art. 4. and 28.
[29] Commission Nationale Informatique & Libertes, "Premiers éléments d'analyse de la CNIL: Blockchain," 2018, 2, https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf.2018, 2).
[30] Jusic, "Dealing with Tensions Between the Blockchain and the GDPR," 84.
[31] GDPR, Art. 28. (10).

Without employing intermediaries and a setting up a relatively centralized system for the data protection process, regulators lack the capability to deal directly with a myriad of individual data subjects. The world of data subjects' full sovereignty over privacy might be a world without an effective liability for privacy breaches.

3.3. Rectification and the Right to be Forgotten on the Blockchain

A promise of the near-immutability of the data recorded on the blockchain is among the core reasons for the blockchain's attraction to many users. The right to rectification and the right to erasure of data (i.e. the right to be forgotten), however, are among the most important rights of data subjects enshrined in the GDPR. The right to rectification means that a duty is owed by the data controller to the data subject to correct inaccurate personal data, and that the data subject has a right to request that the controller complete any incomplete personal data.[32] The right to be forgotten implies that, in some situations, the data subject can request the complete erasure of their personal data by the data controller.[33] The immutability of data recorded on the blockchain and the GDPR's right to rectification and erasure were often cited as core incompatibilities between the blockchain and the GDPR. Yet, technical and legal reasons suggest that these incongruities are not as insurmountable as might appear. Firstly, not even the permissionless blockchain – the one in which erasing data recorded in the blocks must be approved by all participants in the blockchain – is perfectly immutable.[34] Furthermore, other types of blockchain, such as the private blockchain, are specifically structured so that they are not fully immutable.[35] Secondly, the GDPR does not contain a precise definition of when data can be deemed to have been fully erased.[36] This issue is an important one, as many techniques for deleting data leave a possibility for data recovery, and thus a potential for abuse. A solution that is both applicable to the blockchain and compliant with the GDPR is to consider data to be erased at the point when the probability of recovering and reusing the data is minimal, even if the total physical deletion of such data is impossible.[37]

3.4. Data Transfers

Arguably *the* reason for blockchain's popularity is that it provides a seamless direct data transfer via the web, i.e. it allows individuals to directly exchange data across borders without the involvement of an intermediary. A disinter mediated, geographically unbound, free-flowing transfer of data is not entirely condoned by the GDPR; the GDPR only permits the transfer of data to third countries or international organizations and onward if relatively stringent conditions have been met.[38] Because data transfer is vital to both the blockchain and the GDPR, reconciling blockchain and GDPR data transfer requirements is – and will likely remain – a thorny issue, for a number of reasons.

---

[32] GDPR, Art. 16.
[33] GDPR, Art. 16.
[34] Gideon Greenspan, "The Blockchain Immutability Myth," CoinDesk, May 9, 2017, https://www.coindesk.com/blockchain-immutability-myth.
[35] Grant Thornton, "GDPR & Blockchain," 2018, https://blockchain.grantthornton.es/en/blockchain-gdpr-2/.
[36] cf. Matthias Berberich and Malgorzata Steiner, "Blockchain Technology and the GDPR - How to Reconcile Privacy and Distributed Ledgers," *European Data Protection Law Review (EDPL)* 2 (2016): 426.
[37] (Finck 2018).
[38] (Jusic 2018, 7).

Firstly, the structure of the permissionless blockchain consisting of individual nodes transferring data around the globe makes the application of the GDPR's data transfer requirements unworkable. Some GDPR data transfer mechanisms, such as codes of conduct and certifications, can be more readily applied to company- and government entity-operated private and consortium blockchains. But even then, it is questionable whether such GDPR-approved data transfer mechanisms provide real data protection, or merely an appearance of compliance with the GDPR.[39]

Secondly, there are policy issues and trade-offs. The EU rests on and promotes four freedoms (the free movement of capital, people, goods and services) and the rule of law. As the data is already commoditized, it can be questioned whether the benefits of the free flow of data on the internet can be balanced with privacy rights enshrined within the GDPR, and, if not, whether economic interests or privacy will prevail.[40]

The more fundamental question behind this dilemma is whether individuals who act as both consumers and bearers of privacy rights value privacy at all.[41] The future will answer this question. If the pace and reach of technology-driven consumerism are any guide, it can be argued that data subjects will eventually come to use blockchain (or a similar future privacy-enhancing technology) to demand monetary incentives for unavoidable disclosures and sharing of their personal data.

3.5. Smart contracts

The GDPR does not entirely prohibit decisions made using technology without human involvement (automated decision-making).[42] Automated decision-making is permitted when a data subject explicitly consents to it, if it is authorized by the EU or the Member State law applicable to the data controller responsible for safeguarding the data subject's right, or if it is necessary for contractual relations between the data subject and a controller.[43]
Presently, the emerging technology of smart contracts is among the most important forms of automated decision-making based on the blockchain. Smart contracts use executable codes to resolve a 'trust problem', i.e. to facilitate, execute, and enforce a contract between unknown counterparties without engaging an authoritative third party, such as a government.[44] In yet-to-be-developed versions, smart contracts could be used to seamlessly govern contractual

[39] Sonia Daoui, Thomas Fleinert-Jensen, and Marc Lempérière, "GDPR, Blockchain and the French Data Protection Authority: Many Answers but Some Remaining Questions," 2019, https://stanford-jblp.pubpub.org/pub/gdpr-blockchain-france.
[40] Stan Sater, "Blockchain and the European Union's General Data Protection Regulation: A Chance to Harmonize International Data Flows" (Rochester, NY, November 6, 2017), 38, https://doi.org/10.2139/ssrn.3080987.
[41] Joshua Fairfield and Christoph Engel, "Privacy as a Public Good," *Duke Law Journal* 65, no. 3 (December 1, 2015): 456.
[42] Jusic, "Dealing with Tensions Between the Blockchain and the GDPR," 85.
[43] See GDPR Art. 22 and Finck, "Blockchain and the General Data Protection Regulation," 83–84.
[44] Shafaq Naheed Khan et al., "Blockchain Smart Contracts: Applications, Challenges, and Future Trends," *Peer-to-Peer Networking and Applications*, April 18, 2021, https://doi.org/10.1007/s12083-021-01127-0.

transactions of, for example, transfer of property deeds, currencies, and intellectual property rights.[45]

As the GDPR is not opposed to automated decision making as such, presently the application of the GDPR to smart contracts is an issue of risk management and adjustments to technological advancement. If smart contracts become widely used, however, privacy issues will become more pronounced. In such a scenario, smart contracts will comprise a part of longer transaction chains. Within such transaction chains, it will become progressively more difficult for data subjects to exercise their right to be informed of the use of their data and to ensure that potential data errors can be rectified via exercise of their right to human intervention.[46]

4. Conclusion

The GDPR and the blockchain could be said to be on a same mission: to increase individuals' sense of privacy and autonomy. Methods used to fulfill that mission – re-intermediation and relative centralization in the case of the GDPR, disintermediation and decentralization in the case of the blockchain –differ significantly, however, and may also come into direct conflict with one another. In this paper, it was shown that ensuring compliance with the GDPR while using the blockchain for data processing is not necessarily impossible, despite the seeming irreconcilability. Future research and, more importantly, developments in industry and practice should lead to an investigation of other means of ensuring a heightened level of GDPR-compatible privacy protection when data is processed using the blockchain.

[45] Balázs Bodó, Daniel Gervais, and João Pedro Quintais, "Blockchain and Smart Contracts: The Missing Link in Copyright Licensing?," *International Journal of Law and Information Technology* 26, no. 4 (December 1, 2018): 311–36, https://doi.org/10.1093/ijlit/eay014.
[46] Jusic, "Dealing with Tensions Between the Blockchain and the GDPR," 85.

LIST OF REFERENCES

Books and Book Chapters (Printed Version)

- Bambara, Joseph J., and Paul R. Allen. *Blockchain. A Practical Guide to Developing Business, Law and Technology Solutions*. McGrawHill, 2018.
- Jusic, Asim. "Dealing with Tensions Between the Blockchain and the GDPR." In *The LegalTech*
- *Book: The Legal Technology Handbook for Investors, Entrepreneurs and FinTech Visionaries*, edited by Sophia Adams Bhatti, Akber Datoo, and Drago Indjic, 83–86. John Wiley & Sons, 2020.
- Kuner, Christopher (editor), Lee A. Bygrave (editor), Christopher Docksey (editor), and Laura Drechsler (editor). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press, 2020.
- Mougayar, William, and Vitalik Buterin. *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*. 1 edition. Hoboken, New Jersey: Wiley, 2016.
- Nicolletti, Bernardo. *The Future of Fintech: Integrating Finance and Technology in Financial Services*. Palgrave Macmillan, 2017.
- Voigt, Paul, and Axel von dem Bussche. *The EU General Data Protection Regulation (GDPR): A Practical Guide*. 1st ed. Springer International Publishing, 2017.

Periodicals

- Berberich, Matthias, and Malgorzata Steiner. "Blockchain Technology and the GDPR - How to Reconcile Privacy and Distributed Ledgers." *European Data Protection Law Review (EDPL)* 2 (2016): 422.
- Bereczki, Tamás, and Ádám Liber. "Blockchain and the GDPR: Addressing the Compliance Challenge," 2018. https://www.lexology.com/library/detail.aspx?g=571106a c-1aaf-4db9-b1a0- 0152848fd040.
- Bodó, Balázs, Daniel Gervais, and João Pedro Quintais. "Blockchain and Smart Contracts: The Missing Link in Copyright Licensing?" *International Journal of Law and Information Technology* 26, no. 4 (December 1, 2018): 311–36. https://doi.org/10.10 93/ijlit/eay014.
- Böhme, Rainer, Nicolas Christin, Benjamin Edelman, and Tyler Moore. "Bitcoin: Economics, Technology, and Governance." *Journal of Economic Perspectives* 29, no. 2 (May 2015): 213–38. https://doi.org/10.1257/jep.29.2.213.
- Fairfield, Joshua, and Christoph Engel. "Privacy as a Public Good." *Duke Law Journal* 65, no. 3 (December 1, 2015): 385–457.
- Jusic, Asim. "Practical Guidance: Data Transfers - Gulf Region." Bloomberg Law, 2018.
- Khan, Shafaq Naheed, Faiza Loukil, Chirine Ghedira-Guegan, Elhadj Benkhelifa, and Anoud Bani-Hani. "Blockchain Smart Contracts: Applications, Challenges, and Future Trends." *Peer-to-Peer Networking and Applications*, April 18, 2021. https://doi.org/10. 1007/s12083-021-01127-0.

- Sater, Stan. "Blockchain and the European Union's General Data Protection Regulation: A Chance to Harmonize International Data Flows." Rochester, NY, November 6, 2017. https://doi.org/10.2139/ssrn.3080987.
- Werbach, Kevin. "Trust, But Verify: Why the Blockchain Needs the Law." *Berkeley Technology Law Journal* 33 (August 1, 2017): 489. https://doi.org/10.2139/ssrn.2844409.

Reports

- Commission Nationale Informatique & Libertes. "Premiers éléments d'analyse de la CNIL: Blockchain," 2018. https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf.
- Finck, Michèle. "Blockchain and the General Data Protection Regulation." European Parliamentary Research Service, 2019. https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf.
- Information Commisioner's Office. "Data Protection by Design and Default." ICO, February 9, 2021. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/dataprotection-by-design-and-default/.
- "Data Protection Impact Assessments." ICO, January 11, 2021. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/.
- Lyons, Tom, Ludovic Courcelas, and Ken Timsit. "Blockchain and the GDPR." The EU European Union Blockchain Observatory Forum, 2018. https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf.

Web Sources

- Daoui, Sonia, Thomas Fleinert-Jensen, and Marc Lempérière. "GDPR, Blockchain and the French Data Protection Authority: Many Answers but Some Remaining Questions," 2019.
- https://stanford-jblp.pubpub.org/pub/gdpr-blockchain-france.
- Freshfields Bruckhaus Deringer. "The Extra-Territorial Scope of the EU's GDPR." Accessed April 15, 2021. https://www.freshfields.com/en-gb/our-thinking/campaigns/digital/data/general-data-protection-regulation/.
- Grant Thornton. "GDPR & Blockchain," 2018. https://blockchain.grantthornton.es/en/blockchain-gdpr-2/.
- Greenspan, Gideon. "The Blockchain Immutability Myth." CoinDesk, May 9, 2017. https://www.coindesk.com/blockchain-immutability-myth.
- Jongerius, Silvan. "A Primer to GDPR, Blockchain, and the Seven Foundational Principles of Privacy by Design - Dataconomy." Accessed May 19, 2021. https://dataconomy.com/2019/01/a-primer-to-gdpr-blockchain-and-the-seven-foundational-principles-of-privacy-by-design/.
- McKinsey. "How Blockchains Could Change the World," 2016. https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/how-blockchains-could-change-the-world#.

– PricewaterhouseCoopers. “Top Policy Trends 2020: Data Privacy.” PwC, 2021. https://www.pwc.com/us/en/services/consulting/risk-regulatory/library/top-policy-trends/data-privacy.html.

Laws

– European Union. “General Data Protection Regulation (GDPR) – Official Legal Text.” General Data Protection Regulation (GDPR). Accessed May 16, 2021. https://gdpr-info.eu/.