Pseudonyms just got personal: More complicated than your last relationship

Research into what data is being stored on a public permissionless blockchain and whether this data qualifies as personal data according to Article 4(1) GDPR.

Research paper | Jorie Corten

watsonlaw.

1. Introduction

Blockchain technology has become one of the most revolutionary and disruptive inventions of the digital era in recent years

Blockchain technology has become one of the most revolutionary and disruptive inventions of the digital era in recent years.[1] Its capacity to build open and impenetrable networks has sparked the development of numerous novel use cases in a variety of fields, including supply chain management,[2] voting systems,[3] banking,[4] and healthcare.[5]

However, due to its rapid emergence and wide applicability, blockchain technology is paramount to many legal uncertainties. While there are numerous challenges under the European legal framework that can be identified in connection to blockchain technology, this paper focuses solely on the General Data Protection Regulation (GDPR).[6] Following, this paper aims to explore what data is being stored on public permissionless blockchains and whether this data qualifies as personal data within the meaning of Art. 4(1) GDPR.

2. Blockchain

There is no official legal definition for blockchain.[7] However, it does exist for Distributed Ledger Technology (DLT), which is known as the parental technology of blockchain.[8] DLT means *"a technology that enables the operation and use of distributed ledgers"*. [9] Blockchain is a specific sort of DLT that employs algorithmic and cryptographic techniques to build and verify a continuously expanding, append-only data structure that resembles a chain of so-called *"transaction blocks"* and serves as a distributed ledger.[10] A distributed ledger is "*an information repository that keeps records of transactions and that is shared across, and synchronised between, a set of DLT networks nodes using a consensus mechanism*".[11] Notably, not all distributed ledgers use blockchain technology, and blockchain technology itself can be used in a variety of contexts.[12]

The technological and functional setup, as well as the internal governance systems, of blockchains, do certainly vary greatly

There are many different types of blockchains. The technological and functional setup, as well as the internal governance systems, of blockchains, do certainly vary greatly.[13] Blockchain is thus "a class of technologies" rather than "a single technology" with a set of predetermined qualities.[14] Blockchains are typically divided into two categories: "public and permissionless" and "private and permissioned".[15]

2.1. Private and Permissioned vs. Public and Permissionless

Private permissioned blockchains run on a private network and only nodes[16] that have been preregistered can validate transactions. [17] Permissioned blockchains are frequently designed for a specific purpose and these systems are therefore not open for

anyone to join and use.[18] Similar to private intranets, private and permissioned blockchains are exclusively available to users within that specific organisation.[19]

In public permissionless blockchains,[20] all nodes can validate transactions; no permission is needed.[21] There are no identity constraints for participating in such a permissionless system. [22] Since anybody may download the full ledger and observe transaction data in these systems, transparency is also one of its key features.[23] This is why they are referred to as "public" blockchains. Open-source software is the foundation of permissionless blockchains, allowing anybody to download it and join the network.[24]

Since their highly distributed nature, public and permissionless blockchains pose great compliance issues with the GDPR.[25] This paper, therefore, concentrates on analysing personal data on public and permissionless blockchains.

Source: created by the author using DALL • E

3. The General Data Protection Regulation

The GDPR, as the replacement of the 1995 Data Protection Directive,[26] offers a comprehensive legal framework that harmonises data protection throughout the European Union.

The data protection principles, rights, and obligations only apply when personal data is processed

The GDPR is designed to recognize the tremendous technological advancements of the previous 25 years, particularly the emergence of networked information spaces like the internet.[27] Yet, it was planned and written before blockchain, which is now regarded as one of the most disruptive new information technologies on the horizon.[28]

3.1. Personal Data

According to Article 2(1) GDPR, the GPDR applies *"to the processing of personal data (...)"*. Personal data is one of the fundamental concepts in data protection law that determines the material scope of the GDPR.[29] The data protection principles, rights, and obligations only apply when personal data is processed.[30] Pursuant to Article 4(1) GDPR, personal data means *"any information relating to an identified or identifiable natural person"*. Identifiability is the crucial factor in determining whether data constitutes personal data.[31]

The opposite of personal data is anonymous data and refers to *"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"*.[32] Anonymous data, therefore, does not fall within the scope of the GDPR. Pseudonymous data, however, remains information relating to an identifiable person and is therefore subject to the GDPR.[33] In other words, data is pseudonymous if it is possible to combine data with other available information and can thus identify a person, and it is anonymous if this possibility is non-existent.[34] The resulting notion of personal data is broad, flexible, and adaptable to technological context.[35]

4. Data on a Public Permissionless Blockchain

Many blockchain use cases are examples of pseudonymity

On the surface, a public permissionless blockchain appears to exclusively deal with hashes and encryption rather than names, addresses, or email IDs. Because of this, blockchain data is frequently referred to as "anonymous", particularly in non-legal discussions.[36] As anonymous data is not covered by the GDPR, blockchain may therefore be considered to be beyond the purview of data protection law. However, legally, it is a bit more complex. Often, there are entities that are able to combine data and identify a person behind hashes and encryption.[37] As a result, many blockchain use cases are examples of pseudonymity - in legal terms - rather than anonymity.[38] Since pseudonymous data is still considered personal data, a variety of public permissionless blockchains will fall within the scope of the GDPR.[39]

GDPR compliance is therefore not about the technology, it is about the way the technology is used.[40] There is no such thing as a GDPR-compliant blockchain technology; rather, there are GDPR-compliant use cases and applications, albeit the compliance may change over time.[41]

5. Overarching Problem

Giving people more control over their personal data is one of the main goals of the GDPR.[42] As mentioned, data protection rights apply when personal data is processed.[43] Among those rights are for example the right to access, the right to erasure, and the right to data portability.[44]

Recital 26 GDPR enables the notion of personal data to be a tailored and context-specific analysis determining whether personal data is present.[45] Consequently, a piece of data that was once anonymous may later, just by existing, become personal due to advancements in technology or due to combining new data leading to identifying a person.[46]

This raises the key questions of this paper: How can the legal certainty and data protection rights of citizens be guaranteed when there is uncertainty about the limits of personal data on public permissionless blockchains? And more importantly, to solve this problem, does the GDPR need to change, blockchain technology, or both?

The rights to freedom of expression and data protection must be balanced on a case-by-case basis

6. Conclusion

Blockchain technology has emerged as a game-changer in various fields, but its wide applicability has given rise to numerous legal uncertainties, particularly concerning data protection. This paper has provided a preliminary analysis of data on public permissionless blockchains and whether it qualifies as personal data under the GDPR. Despite the initial impression of anonymity, blockchain data can often be traced back to an identifiable person, making it pseudonymous and thus subject to the GDPR. As such, compliance with the GDPR is not about the technology but rather about the way it handles personal data. Due to this uncertain nature of blockchain technology, it is even more essential to ensure the protection of individuals' personal data in the blockchain ecosystem.

Any questions?
Please contact **Jorie Corten** of Watsonlaw.

Footnotes

[1] Panwar, A., & Bhatnagar, V. (2020, February). Distributed ledger technology (DLT): the beginning of a technological revolution for blockchain. In *2nd International Conference on Data, Engineering and Applications (IDEA), p. 1-5*. IEEE. (Hereafter: Panwar & Bhatnagar (2020)).

[2] See e.g. Chang, S. E., & Chen, Y. (2020). When blockchain meets supply chain: A systematic literature review on current development and potential applications. *Ieee Access, 8*, 62478-62494.

[3] See e.g. Huang, J., He, D., Obaidat, M. S., Vijayakumar, P., Luo, M., & Choo, K. K. R. (2021). The application of the blockchain technology in voting systems: A review. *ACM Computing Surveys (CSUR), 54(3)*, 1-28.

[4] See e.g. Chowdhury, M. U., Suchana, K., Alam, S. M. E., & Khan, M. M. (2021). Blockchain application in banking system. *Journal of Software Engineering and Applications,* 14(7), 298-311.

[5 See e.g. Zhang, P., Schmidt, D. C., White, J., & Lenz, G. (2018). Blockchain technology use cases in healthcare. In *Advances in computers* (Vol. 111, pp. 1-41). Elsevier.

[6] 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).

[7] The technology was first described – although not yet labelled as 'blockchain' in Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized business review,* 21260.

[8] Panwar & Bhatnagar (2020).

[9] Article 2(1) Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology, and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive Panwar, A., & Bhatnagar, V. (2020, February). Distributed ledger technology (DLT): the beginning of a technological revolution for blockchain. In *2nd International Conference on Data, Engineering and Applications (IDEA)*, p. 1-5. IEEE. (Hereafter: Panwar & Bhatnagar (2020)).

[10] Natarajan, H., Krause, S., & Gradstein, H. (2017). Distributed ledger technology and blockchain, p. 1. (Hereafter: Natarajan et al (2017)); Panwar & Bhatnagar (2020).

[11] Article 2(2) DLT Pilot Regulation.

[12] Natarajan et al (2017), p. VII; Panwar & Bhatnagar (2020).

[13] Panel fort he Future of Science and Technology (STOA). (2019). *Blockchain and the General Data Protectie Regulation: Can distributed ledgers be squared with European data protection law?* European Parliament. Retrieved 28 March 2023, from https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf, p. 4-5. (Hereafter: STOA (2019)).

[14] Beck, R., Müller-Bloch, C., & King, J. L. (2018). Governance in the blockchain economy: A framework and research agenda. *Journal of the Association for Information Systems,* 19(10), 1, p. 3.

[15] STOA (2019), p 4-5; The European Union Blockchain Observatory and Forum. (2018). *Blockchain and the GDPR*. Retrieved 28 March 2023, from https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf, p. 14. (Hereafter: EU Blockchain Forum (2018)).

[16] Nodes are usually referred to as the computers that store a local version of the distributed ledger; STOA (2019), p. 3.

[17] STOA (2019), p 4-5; Peters, G. W., & Panayi, E. (2016). *Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money,* p. 239-278. Springer International Publishing.

[18] STOA (2019), p 4-5.

[19] EU Blockchain Forum (2018), p. 15; STOA (2019), p 4-5.

[20] The public permissionless blockchain was invented to power Bitcoin.

[21] Peters, G. W., & Panayi, E. (2016). *Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money,* p. 239-278. Springer International Publishing; STOA (2019), p 4-5.

[22] EU Blockchain Forum (2018), p. 15; STOA (2019), p 4-5.

[23] Ibid.

[24] STOA (2019), p 4-5.

[25] EU Blockchain Forum (2018), p. 16.

[26] 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.

[27] EU Blockchain Forum (2018), p. 7-8.

[28] Ibáñez, L. D., O'Hara, K., & Simperl, E. (2018, June). On blockchains and the general data protection regulation. In *EU Blockchain Forum and Observatory,* p. 3.

[29] Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology, 10*(1). Retrieved 29 March 2023, from https://doi.org/10.1080/17579961.2018.1452176, p. 43-44. (Hereafter: Purtova (2018)).

[30] Purtova (2018), p. 43-44.

[31] STOA (2019), p. 19.

[32] Recital 26 GDPR.

[33] Recital 26 and Article 4(5) GDPR.

[34] 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), p. 7-8. (Hereafter: Wirth & Kolain (2018)).

[35] Schwartz, P. M., & Solove, D. J. (2014). Reconciling personal information in the United States and European Union. *Calif. L. Rev., 102,* p. 886-887. (Hereafter: Schwartz & Solove (2014)); Purtova (2018), p. 44.

[36] Wirth & Kolain (2018), p. 7-8.

[37] Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques (WP 216) 0829/14/EN, 20; Article 29 Working Party, Opinion 05/2012 on Cloud Computing (WP 196) 01037/12/EN; STOA (2019), p. 31. Examples of such entities are Chainalysis and Elliptic.

[38] Wirth & Kolain (2018), p. 7-8.

[39] Ibid.

[40] EU Blockchain Forum (2018), p. 4.

[41] Ibid.

[42] Giessen, D. (2019). *Blockchain and the GDPR's right to erasure* (Bachelor's thesis, University of Twente), p. 2.

[43] Purtova (2018), p. 43-44.

[44] Articles 15, 17, and 20 GDPR.

[45] Schwartz & Solove (2014), p. 886; Purtova (2018), p. 65.

[46] Purtova (2018), p. 44.

Questions?

Feel free to ask our specialists.






This paper is written by Jorie Corten, one of the blockchain experts of Watsonlaw. Whether you have questions regarding your crypto-oriented company, or have specific questions regarding the implementation of MiCA, do not hesitate to contact us. Watsonlaw is your partner in blockchain, tokenization and the crypto-market in the Netherlands and abroad, with a broad network of collaborating law firms throughout various countries to provide national as well as international advice. Not only do we possess extensive knowledge regarding the new MiCA regulation, we can also guide your company every step of the way to becoming a leading blockchain enterprise.

watsonlaw.nl

watsonlaw.