Fordham Intellectual Property, Media and Entertainment Law Journal

Volume 29 *XXIX*
Number 4

Article 5

2019

The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR

Anisha Mirchandani
amirchandani@fordham.edu

The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR

Cover Page Footnote
Associate Editor, Fordham Intellectual Property, Media & Entertainment Law Journal, Volume XXIX; J.D. Candidate, Fordham University School of Law, 2019; B.S., Psychology, Fordham University, 2016. I would like to thank Professor Mark Patterson for his guidance and feedback in developing this Note, along with the IPLJ Editorial Board and staff for their hard work throughout this writing and editing process. I would also like to thank my family and friends for their unconditional love and support.

The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR

Anisha Mirchandani*

When considering the legal landscape emerging after the General Data Protection Regulation went into effect on May 25, 2018, the uncertainty surrounding the Regulation reaches its peak when it is applied to blockchain technology. While the goals of storing personal data on permissioned blockchains may align with the goals of accuracy and transparency emulated by the GDPR, the language of the Regulation makes it likely that blockchain technology, as a whole, violates the GDPR. Permissioned blockchains have promising use cases and developments that have not only streamlined data storage, but also allowed users to have increased control over who accesses their data. Accordingly, this Note proposes that to ensure innovation and technological growth of permissioned blockchains are not stifled, the GDPR must release guidance that exempts permissioned blockchains that store personal data from the daunting violation fines of the GDPR. First, this Note discusses the background of blockchain technology, highlighting the benefits of permissioned blockchains. This Note then discusses the relevant regulations of the GDPR, focusing on the right to rectification, the right to be forgotten, and the right to data portability. Next, this Note discusses how blockchain technology violates users' data access rights. The last part of this Note discusses why permissioned blockchains should be exempt

* Associate Editor, Fordham Intellectual Property, Media & Entertainment Law Journal, Volume XXIX; J.D. Candidate, Fordham University School of Law, 2019; B.S., Psychology, Fordham University, 2016. I would like to thank Professor Mark Patterson for his guidance and feedback in developing this Note, along with the IPLJ Editorial Board and staff for their hard work throughout this writing and editing process. I would also like to thank my family and friends for their unconditional love and support.

from the GDPR and proposes solutions on how to facilitate this exemption, concluding that the most efficient way to ensure that the technological growth of permissioned blockchains is not stifled is immediate guidance from the GDPR that interprets definitions from the Regulation in a way that exempt permissioned blockchains from violations.

INTRODUCTION

> From a blockchain point of view, the GDPR is already out of date. Regulation plays catch up with technology. – John Mathews, CFO of Bitnation[1]

On May 25, 2018, the European Union's General Data Protection Regulation (hereinafter, the "GDPR" or "the Regulation") became effective, increasing the privacy rights of data subjects[2]—or people who entrust businesses with their personal data—around the world.[3] Most notably, the GDPR grants data subjects the right to be forgotten, the right to rectify their data and the right to move their data to another business upon request.[4] While these provisions of the GDPR create transparency and trust between data subjects and businesses, businesses that utilize permissioned blockchains to store personal data violate them, as the core immutable ledger technology of blockchain prevents data subjects from exercising these rights.[5]

According to John Mathews, the Chief Financial Officer of Bitnation, "[f]rom a blockchain point of view, the GDPR is already out of date . . . . Regulation plays catch up with technology."[6] This Note will explore the relevant provisions of the GDPR and how they conflict with the core immutability of blockchain technology, particularly permissioned blockchains. First, this Note will consider the role of businesses using permissioned blockchains to store personal data as data controllers[7] and the possible GDPR

---

1 *See* David Meyer, *Blockchain Technology is on a Collision Course with EU Privacy Law*, INT'L ASS'N OF PRIVACY PROF. (Feb. 27, 2018), https://iapp.org/news/a/blockchain-technology-is-on-a-collision-course-with-eu-privacy-law/ [https://perma.cc/GT9S-9P7S].

2 *See generally* Regulation 2016/679 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, 2016 O.J. L 119, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 [https://perma.cc/AM42-U7KQ] [hereinafter General Data Protection Regulation].

3 While the GDPR is a European regulation, it affects all businesses that collect personal data from European data subjects, thus affecting large-scale businesses in the United States and many other countries.

4 *See generally infra* Section I.B.

5 *See generally infra* Section II.

6 Meyer, *supra* note 1.

7 *See* General Data Protection Regulation, *supra* note 2, at art. 4.

violations when personal data is stored on permissioned blockchains.

Next, this Note will argue that a GDPR exemption for permissioned blockchains must be considered, as businesses are using permissioned blockchains in new and innovative ways to not only secure data subjects' personal data, but also give data subjects more control over their data. While this Note will discuss arguments for why permissioned blockchains should not be exempt from the GDPR, it will ultimately conclude that an interpretation of the GDPR that allows for personal data to be stored on permissioned blockchains, without risking a GDPR violation, not only fosters innovation, but also increases data privacy and security.

I. BLOCKCHAIN TECHNOLOGY AND THE GDPR: A PRIMER

A. Blockchain Technology

Blockchain, popularized by Satoshi Nakamoto and its paradigm for bitcoin in 2008,[8] functions as an information storage system.[9] Designed to deliver internal accuracy of information,[10] blockchain's most valuable characteristic is the fact that it is tamper-proof, thus making it an asset in various areas of business, including cryptocurrency and finance.[11] In addition to being immutable, blockchain allows all users with the same access rights to view and edit records on the chain at the same time, in real time.[12]

---

[8] *See* Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System,* BITCOIN (2008), https://bitcoin.org/bitcoin.pdf [https://perma.cc/CX9V-6RX7].

[9] *See* Mark R. Patterson, *Blockchain: A Conceptual Primer*, LINKEDIN (June 28, 2018), https://www.linkedin.com/pulse/blockchain-conceptual-primer-mark-r-patterson/ [https://perma.cc/F3YB-FSMS].

[10] *Id.*

[11] *See Making Sense of Bitcoin, Cryptocurrency and Blockchain*, PWC, https://www.pwc.com/us/en/industries/financial-services/fintech/bitcoin-blockchain-cryptocurrency.html [https://perma.cc/2Q7S-HBQR] (last visited Jan. 14, 2019).

[12] *See* William Mougayar, *Explaining the Blockchain via a Google Docs Analogy*, STARTUP MGMT. (Sept. 6, 2016), http://startupmanagement.org/2016/09/06/explaining-the-blockchain-via-a-google-docs-analogy/ [https://perma.cc/XY9Q-V2WX]; *see also*

On a basic level, the technology and immutability that blockchain boasts can be compared to a "Google Doc" document.[13] On a Microsoft Word document saved on a computer, without track changes, one party can make changes to a legal document and send it over to another party, but no two parties can be editing the document at the same time.[14] In this scenario, one party has to wait for the other party to finish editing a document, be emailed back a new version on the document, and then add its own changes.[15] Accordingly, two parties cannot be editing the same document at the same time,[16] and versions may get lost as new word documents with titles such as "Version 1(a)" and "Version 1(b)" are saved on various computers. Banks maintain money balances and transfers this way, by locking access to an account when banks decrease the balances and make transfers, then updating the other side's balance, and then reopening access.[17] Like a regular Microsoft Word document, this only allows one party to alter a bank account at a time.[18] A Google Doc, on the other hand, allows all users with access to edit the document at any time they want, while also creating a record of all the changes, if any.[19] Because both parties have access to the document at the same time and can make changes without altering the revision history of the Google Doc, this Google Doc is comparable to a shared ledger on a blockchain.[20] Records stored on a blockchain cannot be altered,[21] similar to how Google Doc users can view the

---

Xen Baynham-Herd, *Blockchain: Decentralized Google Docs on a Grand Scale*, MEDIUM (Aug. 30, 2018), https://medium.com/@xen_26244/blockchain-decentralized-google-docs-on-a-grand-scale-55a2e15c07d1 [https://perma.cc/2XHX-66TY].

13 *See* sources cited *supra* note 12. While this Note will analogize blockchain to Google Drive, Microsoft also has a similar technology called "Microsoft Sharepoint" that has a "OneDrive" feature. *See What is One Drive for Business?*, MICROSOFT, https://support.office.com/en-us/article/what-is-onedrive-for-business-187f90af-056f-47c0-9656-cc0ddca7fdc2 [https://perma.cc/7R7Z-EG6X] (last visited Jan. 8, 2019).

14 *See* sources cited *supra* note 12.

15 *See* sources cited *supra* note 12.

16 *See* sources cited *supra* note 12.

17 *See* Mougayar, *supra* note 12.

18 *See id.*

19 *See* Baynham-Herd, *supra* note 12.

20 *See id.*

21 *See generally* discussion *infra* Section II.A.

complete revision history of a shared Google Doc.[22] All users on a blockchain can view the records on the blockchain in real time, at the same time, just as users on a Google Doc who can view and edit documents in real time.[23] Shared documents and Google Docs are a simplified example of the blockchain; blockchain technology can store any transaction history, including money transfers, property title, and medical history, and cannot alter or delete any transaction history.[24] Thus, the implications of a technology that ensures that transactions and data records are immutable is groundbreaking, and already dynamically affecting finance and business globally.[25]

1. Public Blockchains

In any blockchain, "blocks," or lists of records, are added onto a chain and linked to a previous block, thus beginning the tamper-proof structure of the blockchain.[26] The data on each block of the blockchain, will, ideally, only be data that is relevant to the purpose for which the blockchain was created. For example, if a blockchain is created to store medical records, then the data within each block of a particular blockchain will be the relevant medical records. Blocks of data are linked together, and once they are linked on a blockchain, the data within each block cannot be altered without tipping off users monitoring the blockchain, thus making the whole chain tamper-proof.[27] If the link between two

---

22 *See* sources cited *supra* note 12.

23 *See* sources cited *supra* note 12.

24 *See generally* discussion *infra* Section II.A.4.

25 *See* PWC*, supra* note 11.

26 *See* Tom Kulik, *Why Blockchain and the GDPR Collide Over Your Personal Data*, ABOVE THE LAW (Oct. 8, 2018, 5:03 PM), https://abovethelaw.com/2018/10/why-blockchain-and-the-gdpr-collide-over-your-personal-data/ [https://perma.cc/7H95-WUV4].

27 *See* Jimi S., *Blockchain: How Mining Works and Transactions are Processed in Seven Steps*, MEDIUM (May 2, 2018), https://medium.com/coinmonks/how-a-miner-adds-transactions-to-the-blockchain-in-seven-steps-856053271476 [https://perma.cc/K3NQ-JS85] [hereinafter Jimi S., *How Mining Works*]; *see also* Jimi S., *How Does Blockchain Work in 7 Steps – A Clear and Simple Explanation*, MEDIUM (May 6, 2018), https://medium.com/coinmonks/blockchain-for-beginners-what-is-blockchain-519db8c6677a [https://perma.cc/F4CK-RA4R] [hereinafter Jimi S., *How Does Blockchain Work*].

blocks is broken, this is an indication that the blocks, and therefore, the data within the blocks, have been tampered with.[28] In a public blockchain, adding blocks containing data onto a blockchain occurs through a mining process, where users of the blockchain, or miners, use a proof of work model to verify and add blocks to the chain.[29]

The mining process begins when a transaction is broadcasted on an application,[30] such as a bitcoin wallet, that is supported by blockchain.[31] This transaction will then be hovering on the particular public blockchain, such as Bitcoin, in a pool of unconfirmed transactions until a miner has picked it up.[32] Once a miner selects a transaction from this unconfirmed pool, the miner will begin to form this transaction data into a block on the blockchain.[33]

After a miner has decided to add transaction data to a blockchain, it must first verify the previous blocks on the chain in which it decides to add the new block.[34] This verification is done by ensuring that the hash number in the transaction data of a block which the miner decides to build upon (hereinafter "Block N+1")

---

28 *See* PWC*, supra* note 11.

29 *Id.*

30 Users who use bitcoin have a public key and private key to verify their transactions. "When a transaction is initiated by a user to send . . . bitcoins, to another person, the transaction has to be broadcasted to the network where distributed nodes . . . confirm the validity of the transaction before finalizing it and recording it on the blockchain. Before the transaction is broadcasted, it is digitally signed using the private key. The signature proves ownership of the private key, although it does not divulge the details of the private key to anyone. Since a public key is fashioned from the private key, the user's public key is used to prove that the digital signature came from his private key. Once the transaction has been verified as valid, the funds are sent to the recipient's public address . . . [the recipient] will then be able to withdraw [the funds] with his private key." *Public Key*, INVESTOPEDIA, https://www.investopedia.com/terms/p/public-key.asp [https://perma.cc/WD8D-YPSV] (last visited Jan. 14, 2019).

31 *See* sources cited *supra* note 27.

32 The incentive for miners to "pick up" transactions and work on them in public distributed ledgers like blockchain is that they are typically rewarded a transaction fee for verifying previous blocks and adding a new block to the blockchain. *See What is the Bitcoin Mining Reward*, BITCOIN MINING, https://www.bitcoinmining.com/what-is-the-bitcoin-block-reward/ [https://perma.cc/EN5M-PQLE] (last visited Nov. 30, 2018).

33 *See* sources cited *supra* note 27.

34 *See* sources cited *supra* note 27.

matches the hash number of its previous block (hereinafter "Block N"), thus linking the chain.[35] Block N features a timestamp, the data relevant to a particular transaction, and a nonce.[36] A hash function[37] is performed on this data, which alters the data into a random string of numbers that acts as a digital signature, or hash output (hereinafter "Hash Output N").[38] If any data within Block N is ever altered, then Hash Output N would also be altered.[39] Block N + 1, the next block in the chain, also has the same features: a timestamp, the transaction data, which includes Hash Output N, and a nonce.[40] Accordingly, when a miner goes to build on Block N + 1, the miner will verify that Hash Output N present in Block N +1 matches the Hash Output N that is visible on Block N, thus linking the blocks on the chain.[41] If these hash output numbers match, then the miner can verify that the blocks match and thus continue on adding blocks to the blockchain.[42] If the Hash Output N value present in the data of Block N+1 does not match Hash Output N present in Block N, then the miner knows that the data in the block was altered and will not continue to build on that particular blockchain.[43]

When adding a new block to a verified blockchain, a hash of the contents of the new block is taken, a nonce is appended to that hash number, and a new string is hashed with the nonce.[44] This new hash output is compared to the difficulty level provided by the previous block on which the miner is attempting to add the block, which may be something like ensuring that the hash output number

---

35 *See* sources cited *supra* note 27.

36 *See* sources cited *supra* note 27.

37 A cryptographic hash function is used in blockchain transactions because these functions are deterministic, have quick computation, and have pre-image resistance. *See What is Hashing? Under the Hood of Blockchain*, BLOCKGEEKS, https://blockgeeks.com /guides/what-is-hashing/ [https://perma.cc/YN36-9ZJP] (last visited Oct. 25, 2018).

38 *See* sources cited *supra* note 27.

39 *See* sources cited *supra* note 27.

40 *See* sources cited *supra* note 27.

41 *See* sources cited *supra* note 27.

42 *See* sources cited *supra* note 27.

43 *See* sources cited *supra* note 27.

44 "The nonce is an arbitrary string which is concatenated with the hash of a block." BLOCKGEEKS, *supra* note 37.

of the new block has seven consecutive zeros before it.[45] If this new hash is less than the difficulty level, it is one step closer to being added onto the blockchain.[46] If the new hash does not comply with the difficulty level, then the miners must change the nonce, redo the process, and come up with a new hash that is less than the difficulty level.[47] Once a new miner finds a new hash output that complies with the previous block's difficulty level, then it broadcasts its solution to the rest of the miners on the blockchain.[48] This solution acts as the proof of work – the other miners verify that the problem was properly solved by the miner and that the miner's new block corresponds with its previous block by looking at that miner's proof of work.[49] If the other miners agree that the proof of work is accurate, they will reach a consensus that the block is verified and then the new block will be added to the chain.[50] The other miners and "nodes will [then] accept the block and save it to their transaction data," thus successfully completing the mining process for a block.[51]

In sum, this mining process on a public blockchain ensures that public blockchains are fully decentralized peer-to-peer networks.[52] While a public blockchain is accessible by anyone with a computer, there is no central entity that controls the blockchain.[53] By using the Google Doc analogy discussed earlier,[54] a blockchain would operate as though the Google Doc is accessible and editable by any users on the document, but the edits to the document would only be made if a majority of the users agreed to the changes. Accordingly, a public blockchain is a decentralized, practically immutable ledger of information.[55]

---

45 *See id.*

46 *See id.*

47 *See id.*

48 *See* Jimi S., *How Mining Works*, *supra* note 27.

49 *See id.*

50 *See id.*

51 *See id.*

52 *See* Scott A. McKinney, Rachel Landy & Rachel Wilka, *Smart Contracts, Blockchain, and the Next Frontier of Transactional Law*, 13 WASH. J. L. TECH. & ARTS 313, 319–21 (2018).

53 *See id.* at 318.

54 *See generally supra* Section I.A.

55 *See* Nakamoto*, supra* note 8, at 1.

2. Permissioned Blockchains

Permissioned blockchains, the focus of this Note, have one more layer of control than traditional public blockchains: the participants on a permissioned blockchain network have the ability to restrict access.[56] While a public blockchain requires a majority of all nodes, or participants, to determine whether a transaction or block is verified, a consortium blockchain is a permissioned blockchain that allows only specific, pre-selected nodes to determine whether a block is verified.[57] In a consortium blockchain, the right to read the information on the blockchain may be public, but the ability to actually verify transactions and add blocks to the chain is only possessed by a few key groups.[58] For example, financial institutions may exist in a consortium.[59] If there are fifteen financial institutions, each may act as a node, and the blockchain may require ten of these institutions to sign off on a block on the chain for it to be valid.[60] While the institutions may hold the power to sign off on blocks, pre-selected members of the blockchain, such as customers of the bank, may still have the ability to read the transactional history on the blocks, thus ensuring that customers can view the provenance of bank records. Here, the complexities that accompany consensus and verification in a public blockchain dwindle, as most businesses and users that enter into agreements on permissioned blockchains already trust each other.[61] Consensus in consortium blockchains is not achieved by the proof of work method used in public blockchains, but is rather achieved by a method agreed upon by their participants.[62] In sum, a

---

56 *See* Phaedra Boinodiris, *Who Has the Power in Enterprise Blockchains?*, IBM (Feb. 20, 2018), https://www.ibm.com/blogs/blockchain/2018/02/who-has-the-power-in-enterprise-blockchains [https://perma.cc/B846-4562].

57 *See* Vitalik Buterin, *On Public and Private Blockchains*, ETHEREUM BLOG (Aug. 6, 2015), https://ethereum.github.io/blog/2015/08/07/on-public-and-private-blockchains/ [https://perma.cc/Y9FW-LH6B].

58 *See id.*

59 *See id.*

60 *See id.*

61 *See* David Floyd, *Banks Claim They're Building Blockchains. They're Not*, INVESTOPEDIA (July 13, 2018, 6:00 AM), https://www.investopedia.com/news/banks-building-blockchains-distributed-ledger-permission/ [https://perma.cc/7D7U-ZDWU].

62 *See* Anant Kadiyala, *Nuances Between Permissionless and Permissioned Blockchains*, MEDIUM (Feb. 17, 2018), https://medium.com/@akadiyala/nuances-

consortium blockchain functions as a partially decentralized blockchain.[63] When analogized to a Google Doc, a consortium blockchain is a Google Doc where anyone with a link has "Read Only" access, but only the members of the "Team Drive" on which the Google Doc exists can edit the Google Doc.[64]

A private blockchain functions the same way as a consortium blockchain, but *one* central entity controls the transaction execution permissions in the blockchain.[65] Other organizations may have the ability to view or read the blockchain, but they do not have the ability to approve additional blocks on the chain.[66] While there are different levels of permission that participants may have on a private-permissioned blockchain, such as a reader, a writer, or an operator, all participants in the blockchain must still be approved by the centralized authority within the permissioned

---

between-permissionless-and-permissioned-blockchains-f5b566f5d483 [https://perma.cc/28WE-BPWB]. It is important to note that members with verification rights on a consortium blockchain may technically all agree to "rewind" problematic data on a permissioned blockchain, thus restarting the blockchain from the beginning every time data needs to be deleted or altered. *See* Gideon Greenspan, *The Blockchain Immutability Myth*, MULTICHAIN (May 4, 2017), https://www.multichain.com /blog/2017/05/blockchain-immutability-myth/ [https://perma.cc/MQS5-C6MS]. While this hinders the immutability of a permissioned blockchain, this is extremely unlikely to happen for the following reasons: (1) while all members on a permissioned blockchain are participating in the same transaction, they likely do not have all of the same aligned interests in the transaction and will not all want to alter the data on the blockchain; (2) if data subjects and consumers have the right to view the data on the permissioned blockchain, as they do in many current use cases, then they will likely be able to tell when businesses are trying to "rewind" and alter their data on the chain and lose trust in the members of the permissioned blockchain and take their business elsewhere; and (3) rewriting a permissioned blockchain from the beginning is a very timely process and may hinder businesses from processing new incoming network activity, thus making the "rewind" of data not worth it for businesses. *See id.* For the purposes of this Note, it is argued that the above reasons are enough to make permissioned consortium blockchains immutable for the purposes of data storage.

63 *See* Buterin, *supra* note 57.

64 *See generally supra* Section I.A

65 *See* Buterin, *supra* note 57. While private blockchains may be permissioned or permissionless, most private blockchains are permissioned, as there has yet to be a private, permissionless blockchain. *See* Jackson Parsons, *Blockchain Types Explained: It's More Than Public vs Private*, ULEDGER, https://www.uledger.co/blockchain-types-explained-its-more-than-public-vs-private/ [https://perma.cc/Q2TT-VHTW] (last visited Jan. 14, 2019).

66 *See* Buterin, *supra* note 57.

blockchain.[67] Most notably, private-permissioned blockchains do not use Nakamoto's consensus, as a consensus in a private-permissioned blockchain is redundant because actors in these blockchains are chosen by the central authority that uses them.[68] If a Google Doc was analogized to a private-permissioned blockchain, the creator of the Google Doc is the only one who has the ability to share the Google Doc with other users, and, should the creator decide to share it, he or she could only share it with users within the same Google Suite, such as members of an institution that have the same email address ending in ".edu."

3. The Benefits of Blockchain

The benefits of blockchain that make it a viable and desired technology are the following traits: consensus, provenance, immutability, finality, and decentralization.[69] Consensus is particularly important on a public blockchain, as all users must agree to verify the validity of a transaction or block before it is added to the chain.[70] Provenance allows participants on a blockchain network to view the ownership of a block and its data over time, including where the block originated.[71] Immutability ensures that a block cannot be edited or deleted after its added to a ledger.[72] Finality ensures that all data and transaction history is in one trusted source, the blockchain.[73] Decentralization, also particularly important in a public blockchain, ensures that the blockchain ledger is distributed to many nodes, so failure of the blockchain network is not imminent if a few nodes fail.[74]

---

67 *See* Boinodiris, *supra* note 56.
68 *See* Floyd, *supra* note 61.
69 *See* McKinney et al., *supra* note 52, at 319.
70 *See id.*
71 *See id.*
72 *See id.*
73 *See id.*
74 *See id.*

4. The Benefits of Permissioned Blockchains

a) Compliance

Permissioned blockchains are used by businesses like IBM and offer the benefits of blockchain without the disadvantages that come with blockchains on a public ledger, such as thousands of nodes mining and regulating consensus.[75] Specifically, permissioned blockchains greatly benefit compliance and audit teams – when compliance professionals are able to "see" and track the entire provenance of a good or transaction, without any risk of data breaches and alteration, audits become much more efficient, less time consuming, and more reliable.[76]

b) Immutability of Records for Centralized Entities

Permissioned blockchains also can greatly benefit record keeping in current common centralized entities, such as hospitals and banks. People often trust hospitals and banks to store records of their personal data, which are most likely stored on databases.[77] In addition to storing their personal data, people also trust these entities to ensure that their centrally held databases are secure against attacks by hackers and competitors. If these entities fail to properly guard people's information from hackers and competitors, then personal data is lost and susceptible to various types of fraudulent activities.[78] Accordingly, permissioned blockchains are immutable and can only be accessed by entities that are granted access rights, which removes the immense trust that people have in

---

[75] *See Enter an Entirely New Era of Business with IBM Blockchain Solutions*, IBM, https://www.ibm.com/blockchain/solutions [https://perma.cc/K4W2-6BNV] (last visited Oct. 4, 2018); *see also* Christian Auty, *5 Predictions About Blockchain and Compliance*, CORP. COMPLIANCE INSIGHTS (Apr. 9, 2018), https://www.corporatecomplianceinsights.com/5-predictions-blockchain-compliance/ [https://perma.cc/PW4T-8NFT].

[76] *See* Auty, *supra* note 75.

[77] A database is a "usually large collection of data organized especially for rapid search and retrieval (as by a computer)." *See Database*, MERRIAM WEBSTER, https://www.merriam-webster.com/dictionary/database [https://perma.cc/LXY8-2EAJ] (last visited Jan. 9, 2019).

[78] *See* Nolan Bauerle, *What is the Difference Between a Blockchain and a Database?*, COINDESK, https://www.coindesk.com/information/what-is-the-difference-blockchain-and-database [https://perma.cc/Y9YN-9S5S] (last visited Nov. 9, 2018).

centralized entities and replaces it with immutable blockchain technology. The immutability of a permissioned blockchain adds another layer of complexity for hackers and competitors during a cybersecurity attack—even if a hypothetical hacker can gain access rights to a permissioned blockchain, the data on the blockchain itself is immutable, thus preventing any hacker from ever completely erasing or altering records.

While permissioned blockchains have many benefits, it is important to note that they lack one of the main pros of public blockchains—a decentralized system.[79] Even though permissioned blockchains require users to place their personal data with one, or a few, centralized authorities,[80] they still allow for users to be more confident that their data is immutable and secure, compared to data storage on a singular database run by only one administrative party.[81] Because centralized authorities have complete power over their users' data, it may be easier for them to alter users' data and use it for fraudulent purposes, as there are no other entities to hold them accountable. This potential for data alteration is drastically decreased in a consortium blockchain.[82] Accordingly, the immutability aspect of a permissioned blockchain makes it an attractive enough technology to be used for mainstream data storage.

c) Preventing One Party from Hosting a Database in Multiple Party Transactions

"The greatest benefit of permissioned blockchains is not more inclusiveness or transparency, but rather greater consistency and correctness than existing infrastructure, which is incapable of providing a single source of truth for multiple parties in a decentralized fashion."[83] A permissioned blockchain is *designed* as

---

79 *See supra* Section I.A.2.

80 *See supra* Section I.A.2.

81 *See infra* Section I.A.4.c.

82 *See supra* note 62 and accompanying text.

83 *See* Adam Krellenstein, *Smart Contracts on Permissioned Blockchains Pick Up Where Satoshi Left Off*, SYMBIONT (Oct. 23, 2018), https://symbiont.io/blog/2018/10/23/smart-contracts-on-permissioned-blockchains-pick-up-where-satoshi-left-off [https://perma.cc/6SWF-LYPL].

a single ledger that provides accurate records for various parties.[84] The current information storage system between various parties usually features one party hosting a database, while other parties trust that this party is storing the information on the "shared" database accurately.[85] Alternatively, entities in multiple party transactions may also hire a separate, outside party to host a database for information storage.[86] This method adds another unnecessary party to the transaction, or another possible entity could break trust. A permissioned blockchain not only solves this problem, but does so in a way that is cheaper, faster, and more easily verified than public blockchains,[87] while still preserving immutability.[88]

An example of a permissioned blockchain where various entities participate in transactions relating to information storage exists in the healthcare industry.[89] In its white paper, Medicalchain, an organization focused on allowing patients access to their medical data on blockchain, describes its permissioned blockchain as a blockchain with various read and write permissions that stores patients' encrypted medical records.[90] For example, a practitioner may read and write on permissioned electronic health records, a patient may read his or her own electronic health record, permission a practitioner to read his or her electronic health record, and write certain fitness attributes to an electronic health record, and a research institution may read permissioned electronic health records.[91]

---

84 *See* discussion *supra* Section I.A.2.

85 *See* Gideon Greenspan, *Private Blockchains are More Than "Just" Shared Databases*, MULTICHAIN (Oct. 1, 2015), https://www.multichain.com/blog/2015/10/private-blockchains-shared-databases/ [https://perma.cc/Y58S-JWUN].

86 *See id.*

87 *See* McKinney et al., *supra* note 52, at 320.

88 *See id.*

89 *See* MEDICALCHAIN, WHITEPAPER 2.1 (2018), https://medicalchain.com/Medicalchain-Whitepaper-EN.pdf [https://perma.cc/XAS9-2M9U].

90 *See id.*

91 *See id.* Interestingly enough, Medicalchain states in its whitepaper that the ways in which personal data is stored on the permissioned blockchain are, "subject to change depending upon regulations and requirements in order to make the Medicalchain platform HIPAA and GDPR compliant." *See id.* Under a strict interpretation of the GDPR, it seems as if this will never be possible. *See infra* Part III.

While Medicalchain is relatively new and is currently in its pilot program,[92] it argues that storing patients' medical data on a blockchain not only keeps it more secure, but allows for a single, central location that features the complete, organized medical history of a patient, rather than multiple records stored in various different offices.[93] By storing these records on a permissioned blockchain, full medical records may be shared with providers and insurers with different access levels without any actual electronic transfer of data.[94] Not only do patients have more control over their data, but crimes like insurance fraud may be prevented.[95] Additionally, outside of just Medicalchain, blockchain can further be implemented in the healthcare industry in a supply chain format, tracking medication and controlled substances and reducing pharmaceutical fraud and theft.[96]

In addition to the healthcare industry, permissioned blockchains have also been considered to record land titles.[97] Dubai and Georgia have implemented permissioned blockchain land registries.[98] In these blockchain registries, permissioned blockchains are replacing central databases and storing records to eliminate operating costs.[99] Private blockchains are used to store personal data, including data about the property and the owner at the time, while a public blockchain is recording land titles.[100] Selective information is available to citizens purchasing land, thus

---

92 *See Partnership*, MEDICALCHAIN, https://medicalchain.com/en/partnership/ [https://perma.cc/LXT2-2UF4] (last visited Jan. 15, 2019).

93 *See The Benefits of Using Blockchain for Medical Records*, HIPAA J. (Sept. 26, 2017), https://www.hipaajournal.com/blockchain-medical-records/ [https://perma.cc/ET9D-BTYY].

94 *See id.*

95 *See* Andrew Arnold, *Is Blockchain the Answer to a Better Healthcare Industry?*, FORBES (Aug. 26, 2018, 3:20 AM), https://www.forbes.com/sites/andrewarnold/2018/08/26/is-blockchain-the-answer-to-a-better-healthcare-industry/#bf92af775a8b [https://perma.cc/7TGB-VHEL].

96 *See id.*

97 *See* J. Michael Graglia & Christopher Mellon, *Blockchain and Property in 2018: At the End of the Beginning*, 12 INNOVATIONS 90, 101 (2018).

98 *See id.*

99 *See id.*

100 *See id.*

reducing fraud in property transfers.[101] This process has successfully been streamlined in Georgia, where a system between a user's mobile phone, smart contracts, and blockchain reduces operational costs of land registries by ninety percent and allows a sale of land to occur within ten minutes, rather than the previous time of about three days.[102] With this blockchain registry,[103] a Georgian citizen can meet the owner of land and verify via blockchain the land title recorded on a mobile application.[104] As of March 2018, approximately one million land titles have been saved in Georgia, each with a unique hash,[105] and the government of Georgia plans to expand this blockchain registry system to other government registry systems across its country.[106]

B. The GDPR

On May 25, 2018, the GDPR came into effect, with goals to transform the way in which personal information is collected, shared, and used by businesses globally.[107] Prior to the GDPR, European data was regulated by the Data Protection Directive (the

---

101 *See id.*

102 *See* Marcell Nimfuehr, *Blockchain Application Land Register: Georgia and Sweden Leading*, MEDIUM (Dec. 3, 2017), https://medium.com/bitcoinblase/blockchain-application-land-register-georgia-and-sweden-leading-e7fa9800170c [https://perma.cc/8TBM-7YYC].

103 *See* Vincent McLeese, *Why Nobody Noticed Blockchain Made the Republic of Georgia World Top 10 in Ease of Business*, LINKEDIN (Nov. 30, 2017), https://www.linkedin.com/pulse/why-nobody-noticed-blockchain-made-republic-georgia-world-mcleese [https://perma.cc/EDT4-QYCU] ("A . . . user simply uses a web interface or application to initiate a request. The application's back-end establishes a smart-contract which is subsequently executed on a private blockchain. The resulting hash is stored on the public bitcoin blockchain, ensuring that the deed is secure, permanent, and easily accessible"). Generally, this system does not come without its flaws. It is important to note that blockchain would likely complicate the bundle of rights that come with land title in many countries.

104 *See* Nimfuehr, *supra* note 102.

105 *See* Shefali Anand, *A Pioneer in Real Estate Blockchain Emerges in Europe*, WALL ST. J. (Mar. 6, 2018, 7:00 AM), https://www.wsj.com/articles/a-pioneer-in-real-estate-blockchain-emerges-in-europe-1520337601?ns=prod/accounts-wsj [https://perma.cc/RB56-KL8T].

106 *See Blockchain Land Registry*, EXONUM, https://exonum.com/napr [https://perma.cc/5MZ8-UKTF] (last visited Nov. 11, 2018).

107 *See* EUROPEAN DATA PROTECTION LAW AND PRACTICE 48 (Eduardo Ustaran ed., 2018).

Directive), which was generally more lenient with businesses and what they did with data subjects' data.[108] The Directive also resulted in legal uncertainty regarding data privacy and storage across the European Union, as it allowed member nations to decide the form and methods of enacting the data privacy regulations in the Directive themselves, rather than having one consistent standard across the European Union (EU).[109] As such, beginning in January 2012, the European Commission, the European Parliament, and the Council of the European began negotiating the provisions that would be included in the GDPR and the GDPR was published in the Official Journal of the European Union in May 2016.[110] Specifically, the key changes incorporated by the GDPR include stronger rights for individuals online, data protection by design and default,[111] and ensuring that organizations remain accountable and can demonstrate compliance with the GDPR.[112]

While the GDPR is a regulation for European businesses, the regulation applies, "wherever the use of personal data by a business relates to the offering of goods or services to individuals in the EU, irrespective of whether a payment is required, or monitoring of those in the EU."[113] The GDPR applies anytime a business, or data controller, collects personal data[114] in the EU relating to an identified or identifiable natural person, or a data subject.[115] If personal data is anonymized, then it is not subject to

---

108 *See id.* at 43.

109 *See id.* at 13, 17.

110 *See id.* at 16–17.

111 *See id.* at 17 (stating that data protection by design and default requires "that data privacy be taken into account when new technologies are being developed.").

112 *See id.* at 17–18.

113 *See id.* at 50.

114 *See* General Data Protection Regulation, *supra* note 2, at art. 4 ("'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); 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.").

115 *See id.* ("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

the GDPR.[116] While pseudonymized data[117] is still subject to the GDPR, the regulation recommends that data be pseudonymized to satisfy data minimization requirements.[118] The GDPR separates businesses that collect personal data into data controllers and data processors.[119] A data controller determines the purposes and means for processing personal data, while a data processor processes data on behalf of the data controller.[120] While the GDPR has many regulations regarding the controlling and processing of personal data by businesses, it also gives data subjects many rights, therefore increasing the autonomy that data subjects have over their personal data.[121] This Note will focus on the right to rectification, the right to be forgotten, and the right to data portability offered to data subjects under the GDPR.

1. The Right to Rectification

The scope of the right to rectification under the GDPR is not particularly new, as this general right existed under the old Directive as well.[122] According to the right to rectification, data subjects have the right to rectify inaccurate personal data.[123] Controllers must ensure that when requested, inaccurate or

---

physical, physiological, genetic, mental, economic, cultural or social identity of that natural person[.]").

116 *See* EUROPEAN DATA PROTECTION LAW AND PRACTICE, *supra* note 107, at 71 ("The [r]egulation does 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.").

117 *See* General Data Protection Regulation, *supra* note 2, at art. 4 ("'Pseudonymisation' means 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, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person[.]").

118 *See* EUROPEAN DATA PROTECTION LAW AND PRACTICE, *supra* note 107, at 72.

119 *See* General Data Protection Regulation, *supra* note 2, at art. 4.

120 *See id.* For the purposes of this Note, businesses will be classified as "controllers" under the GDPR, because businesses are determining what to do with data subjects' data and the means of processing it via a permissioned blockchain.

121 *See* EUROPEAN DATA PROTECTION LAW AND PRACTICE, *supra* note 107, at 159.

122 *See id.* at 162.

123 *See* General Data Protection Regulation, *supra* note 2, at art. 16.

incomplete data is rectified, amended, or removed from a business' storage.[124]

2. The Right to Be Forgotten

The right to be forgotten, or the right to erasure,[125] has been one of the landmark parts of the GDPR, often scrutinized[126] for its rigidity. The right to be forgotten establishes that data subjects may request that their personal data be erased from a business' storage without undue delay.[127] Notably, the GDPR has not yet defined what it means to "erase" data.[128] When a data subject exercises this right to be forgotten, a data controller is required to inform any third parties with which it shared the data subject's personal data that the data subject exercised its right to be forgotten.[129]

3. The Right to Data Portability

The right to data portability gives data subjects the right, upon their request, to receive their own personal data from a data controller in a structured and commonly used, machine-readable format.[130] A "structured, commonly used and machine-readable format" has not been further defined by the GDPR.[131] In addition, this provision of the GDPR allows data subjects the right to request

---

124 *See* EUROPEAN DATA PROTECTION LAW AND PRACTICE, *supra* note 107, at 162.

125 *See* General Data Protection Regulation, *supra* note 2, at art. 17.

126 *See* EUROPEAN DATA PROTECTION LAW AND PRACTICE, *supra* note 107, at 162.

127 *See* General Data Protection Regulation, *supra* note 2, at art. 17. Specifically, the right to be forgotten establishes that data subjects have the right to have their personal data erased if: (1) the data is no longer needed for its original purpose and no new lawful purpose exists; (2) the lawful basis for the processing is the data subject's consent, the data subject withdraws the consent, and no other lawful ground exists; (3) the data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing; (4) the data has been processed unlawfully; or (5) erasure is necessary for compliance with the EU law or the national law of the relevant member state. *See* EUROPEAN DATA PROTECTION LAW AND PRACTICE, *supra* note 107, at 162–63.

128 *See* Jeffrey Neuburger, *Blockchain, Personal Data and the GDPR Right to be Forgotten*, LEXOLOGY (Apr. 17, 2018), https://www.lexology.com/library/detail.aspx?g=fa1eda71-dc77-46f5-b7b6-fde35e85dd03 [https://perma.cc/2XNH-T2GA].

129 *See* EUROPEAN DATA PROTECTION LAW AND PRACTICE, *supra* note 107, at 163.

130 *See* General Data Protection Regulation, *supra* note 2, at art. 20; *see also* EUROPEAN DATA PROTECTION LAW AND PRACTICE, *supra* note 107, at 165.

131 *See* EUROPEAN DATA PROTECTION LAW AND PRACTICE, *supra* note 107, at 165.

that their data be transmitted from one data controller to another, without any hindrance from the original data controller.[132]

4. Violations

When a business violates the GDPR, it may be fined up to twenty million euros, or four percent of the worldwide annual revenue of its previous financial year, whichever is higher.[133] Accordingly, violating the GDPR is not something that businesses want to risk, as the fines are astronomical and could devastate a new business.

II. PERMISSIONED BLOCKCHAINS THAT STORE PERSONAL DATA LIKELY VIOLATE THE GDPR, BUT SHOULD THEY?

A. Permissioned Blockchains, Personal Data Storage, and GDPR Violations

"When it comes to data privacy law and your personal data, the [blockchain] technology represents the proverbial round peg that does not fit squarely within the four corners of the law (yet)."[134] Due to the immutability of the blockchain, the GDPR's right to rectification, right to be forgotten, and right to data portability are all likely violated when a data subject's personal data is stored on a permissioned blockchain.[135] Generally, because data cannot be removed from a blockchain, only added to, it is not possible for data subjects to request that their personal data on the chain be

---

[132] *See* General Data Protection Regulation, *supra* note 2, at art. 20; *see also* EUROPEAN DATA PROTECTION LAW AND PRACTICE, *supra* note 107, at 165.

[133] *See* General Data Protection Regulation, *supra* note 2, at art. 83.

[134] Kulik, *supra* note 26.

[135] While this Note focuses on the ways in which permissioned blockchains violate the GDPR, it is important to note that public-key cryptography violates the right to be forgotten, the right to rectification, and the right to data portability. In his white paper, Satoshi Nakamoto identified the risk associated with the reuse of public keys. *See* Nakamoto*, supra* note 8, at 6. Nakamoto's paper stated that while blockchain achieves a newer level of privacy by limiting the access that trust third parties have to information, some linking of users to their public key was still unavoidable. *See id.* For multi-input transactions in bitcoin, public keys may reveal that inputs are done by the same owner by linking multiple transactions to the same owner. *See id.*

altered, deleted, or transferred to another business.[136] The most that a permissioned blockchain node can do is supersede old, inaccurate data, with new data.[137] It cannot alter or delete previously entered data.[138] Even though old data is not physically deleted from the chain,[139] it becomes a part of an older block and is not added upon directly and monitored by nodes.[140] Therefore, a business that stores data subjects' personal data on a permissioned blockchain cannot remove a data subject's personal data from the chain for rectification purposes, erasure purposes, or data portability purposes without violating the GDPR.

B. An Argument Against a Permissioned Blockchain Exemption from the GDPR

1. Permissioned Blockchains are Too Similar to Databases to Warrant an Exemption from the GDPR

Some blockchain experts argue that permissioned blockchains are just "gussied-up" alternatives to company databases, rather than having significant benefits of their own.[141] Accordingly, one may argue that if a database already performs the main function of a permissioned blockchain, personal data storage, then confronting the legal complications of attempting to exempt permissioned blockchains from the GDPR is simply too much unnecessary trouble. Additionally, cryptocurrency and blockchain experts also argue the blockchains are slower than traditional databases,[142]

---

136 *See supra* Section I.B.

137 This is barring the highly unlikely principle that the members of a consortium blockchain would decide to rewrite the entire blockchain every time a single data subject exercises any right that requires a change in data on the blockchain. *See supra* note 62 and accompanying text.

138 *See supra* note 62 and accompanying text.

139 *See* HOGAN LOVELLS, A GUIDE TO BLOCKCHAIN AND DATA PROTECTION 15 (2017), https://www.hlengage.com/_uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf [https://perma.cc/P9R4-CMMD] ("In a blockchain environment, erasure is technically impossible because the system is designed to prevent it.").

140 *See* Kulik, *supra* note 26.

141 *See* John Potter, *The Unfortunate Rise of Permissioned Blockchains*, XTRABYTES (Sept. 13, 2018), https://blog.xtrabytes.global/technology/the-unfortunate-rise-of-permission-blockchains/ [https://perma.cc/8UBB-6W3C].

142 *See* Floyd, *supra* note 61.

which also makes the case for exempting permissioned blockchains that store personal data from the GDPR weaker, for efficiency and speed may be lost when personal data is stored on permissioned blockchains. Therefore, permissioned blockchains may not be beneficial enough to warrant an exemption from the GDPR.

2. The Process of Storing Personal Data on a Permissioned Blockchain Does Not Comply with the GDPR

a) Personal Data on a Blockchain Cannot be "Erased"

The GDPR does not define "erasure" in its regulation, despite requiring personal data to be "erased" when requested by a data subject under the right to be forgotten.[143] Permissioned blockchain businesses will likely err on the safe side and follow a strict interpretation of "erasure" as to avoid risking a GDPR violation. As the core function of blockchain is the fact that its immutable, physically erasing personal data is not possible and thus violates the GDPR. It may be argued that an immutable blockchain ledger inherently contradicts the pivotal right to be forgotten, or right of "erasure," under the GDPR, which is too significant of a right granted to data subjects to be compromised for blockchain technology.

b) Hashed Personal Data is Likely Pseudonymized Data

While blockchain experts are still debating whether hashed personal data classifies as anonymized or pseudonymized data under the GDPR, a strict interpretation of the GDPR classifies hashed personal data as pseudonymized data, thus violating the GDPR. A hash function alters personal data stored on a blockchain into a random string of numbers that act as a digital signature.[144]

---

[143] *See generally* General Data Protection Regulation, *supra* note 2, at arts. 4, 17; Andries Van Humbeeck, *The Blockchain-GDPR Paradox*, MEDIUM (Nov. 21, 2017), https://medium.com/wearetheledger/the-blockchain-gdpr-paradox-fc51e663d047 [https://perma.cc/U3J3-BK56].

[144] *See* BLOCKGEEKS, *supra* note 37 (stating that cryptographic hash function is used in blockchain transactions because these functions are deterministic, have quick computation, and have pre-image resistance).

While hash functions are typically considered one way and unable to be reverse engineered,[145] thus making personal data that is inputted into the hash function unrecognizable in the hash output, there is still some inherent link between hashed personal data and the identity of the data subject.[146] Additionally, working backwards from a hashed output to obtain a data subject's personal data is not impossible, just infeasible. [147] The brute force attack method, while tedious and extremely time consuming, may technically reveal a data subject's original personal data.[148] Blockchain experts have argued that under a strict interpretation of the GDPR, if this technical revelation of personal data is possible, then hashed personal data is merely pseudonymous and thus susceptible to the GDPR.[149] Accordingly, the use of permissioned blockchains similar to Medicalchain and Georgia's land registry system[150] violate the GDPR if they store any personal data from European Union citizens, as the personal data hashes stored on the blockchain are pseudonymized and thus rob data subjects of not just one, but three of their rights under the GDPR: the right to be forgotten, the right to rectification, and the right to data portability. When considering sheer quantity, one may argue that under the current, strict interpretation of the GDPR, permissioned

---

145 *See* LOVELLS, *supra* note 139, at 9.

146 *See* Chris Middleton, *Banking: Is Blockchain GDPR Compliant—Yes or No?*, INTERNET OF BUS. (June 6, 2018), https://internetofbusiness.com/banks-is-blockchain-gdpr-compliant-yes-or-no/ [https://perma.cc/3S6R-CDKY] ("Meanwhile, hashing can be used to verify that data on a chain has, or has not, been modified – because any altered data would result in a different hash. However, this means that hash itself could still be considered personal data if it could be linked to a person and traced across a distributed system, even if the original data is inaccessible.").

147 *See* BLOCKGEEKS, *supra* note 37 ("We already know that it is not impossible to determine the original input from its hash value.").

148 *See* Pavitra Shankdhar, *Popular Tools for Brute-Force Attacks [Updated for 2018]*, INFOSEC INST. (Feb. 17, 2018), https://resources.infosecinstitute.com/popular-tools-for-brute-force-attacks/#gref [https://perma.cc/G4P3-K7Q8].

149 *See* Middleton, *supra* note 146.

150 While Georgia is not a member of the European Union, if European Union member nations were to adapt a similar, successful blockchain land registry like that of Georgia, then those nations would violate the GDPR. *See List of non-EU Countries*, EUR. COMM'N, https://ec.europa.eu/taxation_customs/business/calculation-customs-duties/rules-origin/introduction/list-noneu-countries_en [https://perma.cc/D2RB-W6HW] (last visited Dec. 13, 2018).

blockchains violate too many data subjects' rights for an exemption from the GDPR to even be considered.

C. An Argument for a Permissioned Blockchain Exemption from the GDPR

1. A Loose Interpretation of the GDPR May Already Permit the Storage of Personal Data on Permissioned Blockchains

While businesses may currently follow a strict interpretation of the GDPR, a looser interpretation of its provisions may already permit the storage of personal data in permissioned blockchains without risking violations. For example, if a looser interpretation of "erasure" of data is employed under the GDPR, it may be argued that restricting access rights to a data subject's personal data so that only the data subject can view the data may comply with the GDPR.

Additionally, if the GDPR is interpreted in a less strict manner and classifies hashed personal data as anonymized data, then permissioned blockchains that store personal data via a hash function do not violate the GDPR. The debate about hashed personal data, when considered with the purpose of the GDPR, centers around the concept of traceability. When considering the intent of the GDPR, are the drafters more likely to care about the technical anonymity of data subjects' data, or the lack of traceability of the data to the data subject? According to David Post, traceability is "the ease with which additional information [about a sender of information] can be obtained."[151] While Post does not necessarily focus further on this theory in terms of blockchain, it is an interesting definition to consider and apply to how personal data may be linked to a data subject on a permissioned blockchain. Because hashed functions are almost impossible to reverse engineer, the traceability level of a data subject's personal data on a permissioned blockchain is extremely

---

[151] David G. Post, *Pooling Intellectual Capital: Thoughts on Anonymity, Pseudonymity, and Limited Liability in Cyberspace*, 1996 U. CHI. LEGAL F. 139, 150 https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1202&context=uclf [https://perma.cc/3Z5C-ZWUW].

low. Is an extremely low, even "infeasible,"[152] traceability level of personal data to a data subject not enough to allow permissioned blockchains that store personal data to comply with the GDPR? When weighed against the advantages of permissioned blockchains and the desire to foster technological growth, it should be. If anonymity is looked at through the lens of traceability, then the mere technicality of extremely unlikely reverse engineering of a hash output should not immediately classify permissioned blockchains as violating the GDPR.

Because the GDPR was written in 2016,[153] before many of the permissioned blockchain use cases and developments that exist now, the GDPR's language is not equipped to consider newer uses of permissioned blockchains that may increase data privacy and security if they have a chance to be employed on a large scale. Under a strict interpretation of the GPDR's language, personal data on these blockchains will likely be classified as pseudonymized data, deterring businesses from actually employing permissioned blockchain use cases on a grand scale, as they do not want to risk high GDPR violation fines. Therefore, the European Union must pass guidance to clarify the language of GDPR and how it applies to personal data on the permissioned blockchains, for the current strict interpretation of the language greatly hinders technological growth.

2. Blockchain Technology and the GDPR Have Similar Goals

The GDPR values accountability of the use of data subjects' personal data and advises businesses to employ methods of data protection by design and data protection by default to comply with record keeping obligations.[154] In fact, the principles of the GDPR, listed in Article 5 of the Regulation, include fairness, transparency, integrity, and accuracy.[155] Specifically, the immutable ledger of

---

152 *See* BLOCKGEEKS, *supra* note 37.

153 *See Background and Introduction to the General Data Protection Regulation*, LK SHIELDS (Sept. 19, 2017), https://www.lkshields.ie/news-insights/publication/background-and-introduction-to-the-general-data-protection-regulation [https://perma.cc/J2JG-W2YP].

154 *See* EUROPEAN DATA PROTECTION LAW AND PRACTICE, *supra* note 107, at 51.

155 *See id.* at 61.

blockchain increases transparency,[156] integrity,[157] and accuracy,[158] while the ability to gain consent from users to utilize blockchain emulates fairness.[159] The provenance and finality of blockchain[160] ensure that personal data on a chain is unaltered and accurate.[161] Additionally, in permissioned blockchains that allow users read and viewing access, the GDPR goal of transparency is also achieved, as data subjects can "see" their personal data. Accordingly, permissioned blockchains like Medicalchain and Georgia's land registry system act as a form of privacy by design.[162] Because permissioned blockchains can add granularity to personal data and encode restrictions, permissions, and conditions for its use,[163] they increase data security and privacy. Unfortunately, even though the goals of both the GDPR and blockchain align, a strict interpretation of the GDPR prohibits data

---

156 *See id.* at 102–03 (stating that transparency is accomplished when data controllers are open and clear towards data subjects and provide clear and accessible information).

157 *See id.* at 109 (stating that the principle of integrity may be accomplished when data controllers protect against unauthorized processing of data, accidental loss of data, or destruction or damage of data).

158 "Controllers must take reasonable measures to ensure that the data is accurate and, where necessary, kept up to date. Reasonable measures should be understood as implementing processes to prevent inaccuracies during the data collection process (i.e. verifying the data is accurate, complete and not misleading), as well as during the ongoing processing in relation to the specific use for which the data is processed." *See id.* at 108; *see also* McKinney et al., *supra* note 52, at 321, 324.

159 *See* discussion *infra* Section IV.B.2.

160 *See* McKinney et al., *supra* note 52, at 319.

161 *See* Kulik, *supra* note 26 (arguing that immutability on the blockchain via a hash function is a big plus for data privacy).

162 Privacy by design integrates privacy into the creation and operation of new devices and networked infrastructures. *See Privacy by Design*, TREND MICRO USA, https://www.trendmicro.com/vinfo/us/security/definition/privacy-by-design [https://perma.cc/GM8S-GMMN] (last visited Dec. 13, 2018). Permissioned blockchains function as privacy by design systems because the network infrastructure of a permissioned blockchain is powered by an immutable ledger technology, which ensures that hackers cannot easily alter the personal data of users on the blockchain, thus increasing privacy of data. Another way in which privacy by design and default may be accomplished under the GDPR is by allowing data subjects greater visibility over the process of their data. *See* EUROPEAN DATA PROTECTION LAW AND PRACTICE, *supra* note 107, at 204. A permissioned blockchain with viewing access for data subjects accomplishes this.

163 *See Editing the Uneditable Blockchain*, ACCENTURE (2016), https://www.accenture.com/t00010101T000000__w__/es-es/_acnmedia/PDF-33/Accenture-Editing-Uneditable-Blockchain.pdf [https://perma.cc/6YNY-X7QX].

subjects from storing personal data on permissioned blockchains, costing them the ability to take advantage of a technology that not only has the possibility to give them more control over their data, but keeps their personal data immutable.[164] The similarity of the goals of blockchain and GDPR, compared to the likely illegality of blockchain under the GDPR, not only creates a GDPR-blockchain paradox[165] that needs to be solved, but also hinders large scale employment of permissioned blockchains and further technological developments and use cases for permissioned blockchains.

3. Off-Chain Personal Data Storage Sacrifices the Benefits of Permissioned Blockchains

While some businesses have attempted to comply with the GDPR by storing personal data in an off-chain database, rather than on the blockchain itself, this method sacrifices many of the benefits of using a blockchain in the first place.[166] In these off-chain database systems, hashes of personal data are stored on the blockchain itself and in a separate, off-chain database, the same hash of personal data is stored next to the original personal data that was put through the hash function.[167] Proponents of this system contend that when a data subject exercises its right to be forgotten, the hash and corresponding personal data in the off-chain database will be destroyed.[168] Once the information in the off-chain database is destroyed, the link between the hashed data on the chain and the data located in the off-chain database is also destroyed.[169] This makes the hashed data on the blockchain useless for purposes of identification.[170] The right to rectification and the right to data portability may also be exercised by data subjects under this system, as all personal data is stored off-chain and can easily be altered.

---

164 *See* Van Humbeeck, *supra* note 143.

165 *See id.*

166 *See* Neuburger, *supra* note 128.

167 *See* Carol R.W. De Meijer, *Blockchain Versus GDPR and Who Should Adjust the Most*, FINEXTRA (Oct. 9, 2018), https://www.finextra.com/blogposting/16102/blockchain-versus-gdpr-and-who-should-adjust-most [https://perma.cc/W4N9-CENE].

168 *See id.*

169 *See id.*

170 *See id.*

While this method complies with GDPR, it ignores the key benefit of blockchain: immutability.[171] Functionally, this off-chain database has the same features as a regular, editable database, so what is the point of employing blockchain technology and essentially just making the system more complex and inefficient? By storing data subjects' personal data in the off-chain database, the database still has the same cybersecurity issues as a regular database. Transparency is also reduced because when personal data is stored off-chain, data subjects have no way of knowing who is accessing their data on the off-chain database.[172] Adding an off-chain database increases the complexity of the system, thus increasing the risk of errors and adding another part of a data information system that is susceptible to an attack and breach.[173] The off-chain database also increases the cost of the technology, thus generally decreasing the efficiency and return calculations of utilizing a permissioned blockchain system in the first place.[174] Additionally, if hashed personal data still qualifies as merely pseudonymized data under the GDPR, then even the presence of hashed personal data on the permissioned blockchain still classifies as a GDPR violation, despite the possibility of erasing personal data off-chain.[175] Therefore, storing data subjects' personal data off-chain not only defeats many of the general data security goals of permissioned blockchains, such as making sure that personal data is immutable and transparent to users on the blockchain, but also likely violates the GDPR because the system still stores hashed personal data "on-chain."

---

171 *See* Kulik, *supra* note 26 (confirming that storing personal data outside of a database starts defeating the purpose of using a blockchain in the first place).

172 *See* Van Humbeeck, *supra* note 143.

173 *See id.*

174 *See* Quincy Gomez, *No, GDPR-Compliant Blockchains are not a Myth*, EVERIS (Aug. 13, 2018), http://insights.everis.co.uk/post/102f0lf/no-gdpr-compliant-blockchains-are-not-a-myth [https://perma.cc/F2ZE-FB8A].

175 *See* Jim Lee, *GDPR & Blockchain: At the Intersection of Data Privacy and Technology*, BDP BLOG, https://www.bdpinternational.com/blog/gdpr-blockchain-at-the-intersection-of-data-privacy-and-technology [https://perma.cc/RX99-2KHE] (last visited Jan. 26, 2019).

4. Blockchain Redaction Sacrifices the Benefits of Permissioned Blockchains

In 2016, Accenture tried to solve the GDPR-blockchain paradox by creating a permissioned blockchain redaction system.[176] Accenture patented a special hash function entitled the "chameleon hash," which is added to the hash function that links two blocks on a chain and provides a secret key "that allows the link between blocks to be unlocked so blocks may be edited and relocked."[177] If a change has been made to a block, the original hash will be broken, but the chameleon hash will still remain intact to maintain the link between edited and existing blocks, indicating that the block itself was edited.[178] Similar to the off-chain database, what is the point of Accenture's chameleon hash if it removes immutability from the blockchain? Accenture's chameleon hash functionally turns a permissioned blockchain into a database. Accenture's "solution" to the GDPR-blockchain paradox makes the usage of a blockchain paradigm to store personal data pointless and unnecessary.

5. The Possible "Public Interest" Exception Under the GDPR Is Unclear

While there is yet to be any official enforcement on this aspect of the GDPR, the GDPR states that the right to be forgotten and the right to data portability do not apply in certain public interest exceptions.[179] Specifically, the right to be forgotten does not apply when "processing is necessary for reasons of public interest in the area of public health, such as . . . ensuring high standards of quality and safety of health care,"[180] or when "processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes."[181] The right to data

---

176 *See Blockchain Redaction*, ACCENTURE, https://www.accenture.com/t20180810T060600Z__w__/us-en/_acnmedia/PDF-44/Accenture-Blockchain-Redaction-Infographic.pdf [https://perma.cc/S5AT-3QX5] (last visited Dec. 13, 2018).

177 *Id.*

178 *See id.*

179 *See* General Data Protection Regulation, *supra* note 2, at arts. 17(3)(c)–(d), 20(3), & 89(3).

180 *Id.* at art. 9(2)(i).

181 *Id.* at art. 9(2)(j).

portability does not apply "to processing necessary for the performance of a task carried out in the public interest."[182] Accordingly, one may argue that businesses like Medicalchain and blockchain land registries may, in fact, be exempt from the GDPR, as both exist for public interest reasons. Medicalchain ensures a higher quality and more organized health care system, while blockchain land registries exist for archiving purposes and are utilized for public interest, as they act as an efficient and transparent method of tracking land titles.

On the other hand, the right to rectification does not seem to have a public interest exception.[183] According to the right to rectification, a data subject shall have the right to have incomplete personal data completed by means of providing a supplementary statement.[184] In this situation, a data subject may rectify its personal data by providing a supplementary statement with correct personal data, but this supplementary statement will likely be stored off-chain, which defeats the purpose of storing personal data on the blockchain anyway.[185] Medicalchain and blockchain land registries are utilizing blockchain to store personal data not only for greater transparency, but also to mend filing systems that feature copious amounts of paper records.[186] Allowing supplementary statements to personal data on permissioned blockchains not only acts as the first step towards returning back to paper records, but also defeats many of the core features of permissioned blockchains: immutability of records that are stored on the blockchain.

While Medicalchain and blockchain land registries may fit into a public interest exception under the GDPR, it seems unlikely that the GDPR will allow all businesses to fit other blockchain paradigms and use cases under this exception. Regulators are more likely to consider blockchain uses by government entities as public interest exceptions, but what about other businesses, not limited to the healthcare and government regulation industry, that want to

---

182 *Id.* at art. 20(3).
183 *See id.* at art. 16.
184 *See id.*
185 *See generally supra* Section II.C.3.
186 *See generally* Arnold, *supra* note 95.

utilize permissioned blockchains to store personal data? Will they be prevented from doing so under the public interest exception because they are for-profit entities? Regardless, at this stage, the public interest exception is merely conjecture. The GDPR's guidelines are not clear enough for an entire growing technological industry to rely on a possible public interest exception, especially with the fines for violating the regulation so high. Most businesses utilizing blockchain technologies are startups that cannot afford risking a fine of upwards of twenty million euros, so making these startups developing new uses for blockchain subject to the GDPR, and then subsequently risk violating it, hinders innovation drastically.[187]

6. Even If Permissioned Blockchains are Relatively New Technology, the GDPR Should Not Stifle Technological Growth

Many permissioned blockchain use cases are currently in early development and use case stages.[188] Accordingly, one may ask why GDPR regulators should devote time and energy to make blockchain compatible with the GDPR, when the full benefits of permissioned blockchains have not even been adopted to the mainstream yet? The answer to this is simple – developers should make permissioned blockchain exempt from the GDPR and its violations so that innovators are not deterred from further developing the technology. The language of the GDPR is too ambiguous for developers to merely take a chance and begin storing data subjects' personal data on blockchains, as they risk millions of euros in fines if their technology ends up violating the GDPR.[189] This theory is expanded upon by Sepehr Shahshahani, who argues, based on case studies about past litigation against new emerging technologies, that when courts rule in favor of emerging technologies, this eventually leads to a subsequent compromise between the law and the new and emerging technologies.[190] When

---

187 *See* Sepehr Shahshahani, *The Role of Courts in Technology Policy*, 61 J. L. & ECON. 37, 56–57 (2018).

188 *See generally supra* Section I.A.4.

189 *See* General Data Protection Regulation, *supra* note 2, at art. 83(4)–(6).

190 *See* Shahshahani, *supra* note 187, at 57.

courts rule against new and emerging technologies, this leads to the technological newcomer being shut out from influencing subsequent policymaking.[191] Applying this theory to future enforcement actions under the GDPR, if permissioned blockchains are held to be completely incompatible with the GDPR, this will hinder future innovation and any chance at mainstream use of permissioned blockchains, as policymakers will fail to recognize the technology's potential. As such, to solve the GDPR-blockchain paradox and ensure that technological developments are not stifled, the GDPR must immediately be interpreted in a way that allows permissioned blockchain startups like Medicalchain to continue to develop more use cases that benefit data storage, data security, and data privacy.

7. Businesses Will Not Take Undue Advantage of a Blockchain Exemption from GDPR

While one may argue that exempting permissioned blockchains from the GDPR may catalyze businesses to just use blockchain to field any GDPR violations, this seems unlikely, as implementing a new system of data storage on a permissioned blockchain requires planning and takes time to develop. Additionally, implementing a new data storage system is expensive and requires businesses to not only hire blockchain experts, but lawyers who know how blockchain works to constantly advise on this data storage system and GDPR compliance.

In fact, even if businesses began utilizing blockchain to field possible GDPR liabilities, how much should this actually matter? If the goals of blockchain and GDPR align, isn't using permissioned blockchains to store personal data achieving exactly what GDPR wants: no misuse of data subjects' personal data and increased transparency? If the use of a data subject's personal data is truly more transparent and less susceptible to alteration by third parties in permissioned blockchains, then why shouldn't businesses utilize permissioned blockchains to further the goals of the GDPR and transform the landscape of data protection? Utilizing permissioned blockchains to provide greater security and

191 *See id.*

transparency should not be considered as abuse of the technology to field GDPR liability, but, rather, as a way of furthering the accuracy and transparency goals of the GDPR.

III. WAYS TO EXEMPT PERMISSIONED BLOCKCHAINS THAT STORE PERSONAL DATA FROM THE GDPR

While the GDPR still remains in the early stages of its enforcement, blockchain experts are confident that there are bound to be changes in the GDPR to accommodate blockchain, as they simply do not see blockchain going away anytime soon.[192] Blockchain experts contend that once people understand what blockchain is, including its benefits in recording transactions and documents, massive changes to the GDPR will be underway.[193] To ensure that people are actually exposed to blockchain technology, businesses need to employ blockchain in the mainstream, rather than just citing use cases. Until businesses receive clarity about whether permissioned blockchains violate the GDPR's right to rectification, right to be forgotten, and right to data portability, they likely will not employ blockchain in the mainstream, as they do not want to risk the GDPR violation fines. If the European Union fails to take action promptly, the GDPR risks stifling innovations and further technological developments of permissioned blockchains, such as the Medicalchain, and ultimately causing the full potential of blockchain technology to go untapped. As such, the GDPR must either: (1) alter its provisions to definitively allow personal data to be stored on permissioned blockchains; (2) allow data subjects to decide whether they would like to store their personal data on permissioned blockchains; or (3) provide guidance and clarification about its provisions, specifically the definition of "erasure" and the classification of hashed personal data as pseudonymized data under the GDPR.

---

192 *See* Darryn Pollock, *How Can Blockchain Thrive in the Face of European GDPR Blockade?*, FORBES (Oct. 3, 2018, 4:07 AM), https://www.forbes.com/sites/darrynpollock/2018/10/03/how-can-blockchain-thrive-in-the-face-of-european-gdpr-blockade/#69978c8f61df [https://perma.cc/FQS7-BPJH].

193 *See id.*

A. Alter the Language of the GDPR

The most extreme way to make permissioned blockchains compatible with the GDPR is to create an exception for permissioned blockchains within the GDPR. This exception could be established by adding the following provision to Article 16 (the right to rectification), Article 17 (the right to be forgotten), and Article 20 (the right to data portability): "Where the controller has stored personal data on a permissioned blockchain, then the controller shall not be required to delete the data subject's personal data from the blockchain."

While this method may exempt businesses that are utilizing permissioned blockchains from GDPR violations, it is too soon after the GDPR has come into effect to advise such a sweeping change to the regulation. With very few enforcement actions for violating the GDPR published, it is reckless to alter a regulation that many businesses are still struggling to comply with and interpret.[194] Accordingly, amending the language of the GDPR is too radical to solve GDPR and permissioned blockchain compatibility issues, when the same could be done by merely passing guidance on the ways in which the GDPR defines certain terms, thus allowing businesses that have already been developing permissioned blockchain use cases for years to go forth and employ them on a large scale without risking colossal GDPR fines.

B. Obtain Consent from Data Subjects to Store Personal Data on Permissioned Blockchains

While altering the language of the GDPR to allow all permissioned blockchains to be exempt from GDPR violations is too radical, passing guidance that allows data subjects to merely consent to the use of permissioned blockchains to store their personal data, when prompted, is a less extreme solution. The GDPR requires that when personal data is collected from a data subject, the data subject must be told, in plain language, what its

---

[194] *See* Edward Gately, *80 Percent of Companies Still Not GDPR-Compliant*, CHANNEL PARTNERS (July 13, 2018, 1:08 PM), https://www.channelpartnersonline.com/2018/07/13/80-percent-of-companies-still-not-gdpr-compliant/ [https://perma.cc/DK7K-JC3K].

data is being used for and how that data is being stored.[195] In this solution, if a data subject consents to storing its personal data on a permissioned blockchain for greater transparency and security, a business should be able to do so without risking a GDPR violation. If one of the GDPR's goals is to ensure that individuals regain control over their data, then shouldn't they be able to relinquish this control to a permissioned blockchain via their affirmative consent?[196] Indeed, obtaining consent exemplifies the GDPR's goal of fairness, as fairness is linked to the idea that data subjects must be aware of how their data is being collected, kept, and used and be able to exercise their data protection rights as they make informed decisions about whether they agree with businesses' data storage collection and storage methods.[197] While it may be difficult for consumers to anticipate the implications of blockchain right now, assuming that its popularity increases and permissioned blockchains become more mainstream, people are more likely to understand the implications of this technology and thus, consent to its use.

Accordingly, the GDPR can pass guidance that allows businesses to be exempt from GDPR violations when a data subject affirmatively consents to store its personal data on a permissioned blockchain in exchange for revoking its right to exercise the right to be forgotten, the right of data portability, and the right of rectification. Here, not only is a data subject on notice of the use of blockchain technology, but the data subject has also provided its affirmative consent to the business to use a permissioned blockchain.[198] Therefore, this solution complies with one of the main goals of the GDPR – giving individuals control over their personal data.

---

195 *See* EUROPEAN DATA PROTECTION LAW AND PRACTICE, *supra* note 107, at 50–51.

196 *See* Samuel Martinet, *GDPR and Blockchain: Is the New EU Data Protection Regulation a Threat or an Incentive?*, COINTELEGRAPH (May 27, 2018), https://cointelegraph.com/news/gdpr-and-blockchain-is-the-new-eu-data-protection-regulation-a-threat-or-an-incentive [https://perma.cc/9G85-3YJL] ("Data rights can be managed exclusively via the blockchain and trusted hardware, by users; returning control and privacy of their data back to them.").

197 *See* EUROPEAN DATA PROTECTION LAW AND PRACTICE, *supra* note 107, at 101.

198 In this situation, if a data subject does not want to store its information on a permissioned blockchain, then it may simply not consent to do so.

A drawback to this solution is that most data subjects may not understand the benefits or costs of storing their personal data on a permissioned blockchain, thus making them hesitant to consent to a business' use of this technology. While detailed information in businesses' privacy policies and Terms of Use may clarify the benefits and costs of blockchain, privacy policies are often not read and understood by users.[199] Therefore, burying information about how permissioned blockchains function in a privacy policy do not align with the GDPR's goals of fairness and transparency. While obtaining affirmative consent from data subjects may seem like a solution to the GDPR-blockchain paradox, it should not be the only barrier between utilizing permissioned blockchains and risking GDPR violations until blockchain is a more mainstream technology and data subjects know of its benefits *and* costs.

C. Clarify the Definition of "Erasure" Under the GDPR

As mentioned earlier, the GDPR has yet to clarify what exactly "erasure" of data is under the right to be forgotten.[200] If "erasure" of data allows moving onto a new block, or creating a "fork" within a permissioned blockchain when data is requested to be forgotten, blockchain may comply with the GDPR.[201] If "erasure" of data is interpreted to allow restricting the access rights to a data subject's personal data such that only the data subject has access to it, then permissioned blockchains may not violate the GDPR. But, as there has been no guidance as of yet, blockchain experts have interpreted "erasure" as literally as possible, assuming that it means actual physical and logical deletion of personal data.[202] Thus, a clarification of this definition by the GDPR would assist permissioned blockchain businesses to decide when personal data is truly "erased" from their blockchain and whether their blockchain use violates the GDPR.

---

199 *See* John A. Rothchild, *Against Notice and Choice: The Manifest Failure of the Proceduralist Paradigm to Protect Privacy Online (Or Anywhere Else)*, 66 CLEV. ST. L. R. 559, 626–28 (2018).

200 *See supra* Section II.B.2.a.

201 *See* Kulik, *supra* note 26 (stating that forking to a new chain may be a way for data subjects to delete or remove personal data stored in a blockchain).

202 *See* Neuburger, *supra* note 128.

The GDPR should interpret limiting the access rights to personal data on a blockchain to only the data subject as "erasure" of data, for doing so makes the personal data of the data subject untraceable. In situations where a data subject has control over who accesses its data on a permissioned blockchain, such as the paradigm discussed in Medicalchain, limiting the access rights in this manner leaves the personal data untraceable, as the data subject is the only one who owns it. Alternatively, in consortium blockchains where the data subject is not the only administrator, other businesses in the consortium could agree, prior to receiving the data subject's personal data, that if the data subject requests "erasure" of its data, the businesses in the consortium blockchain will reach consensus to limit access on the part of the blockchain with the data subject's personal data to only the data subject. While the GDPR's clarification of the term "erasure" in this manner may solve the issues with violating the right to be forgotten, the GDPR must provide further clarity to permissioned blockchain developers so that they may comply with the right to rectification and the right to data portability and continue to create new uses for permissioned blockchains that benefit data privacy and security.

D. Classify Hashed Personal Data as Anonymized Data Under the GDPR

By classifying hashed personal data as anonymized data under the GDPR, permissioned blockchains like Medicalchain and Georgia's data land registry do not violate data subjects' right to be forgotten, right to rectification, and right to data portability under the GDPR.[203] A whole technological industry should not be deterred from further developing use cases because of an infeasible possibility that may lead to a data subject's personal data on a blockchain to be linked to its identity. Blockchain technology has the ability to alter the way that personal data is stored globally and this potential should be fully explored, rather than abandoned because of a mere infeasible technicality. The low traceability of hashed personal data to a data subject, when weighed against the current and potential benefits of permissioned blockchains in data

---

[203] *See supra* Section I.A.4.b.

security, should be enough to classify hashed personal data as anonymous. Thus, by merely releasing guidance that defines the terms "erasure" and "anonymized" in ways that will, rightfully, allow permissioned blockchains to comply with the GDPR, the European Union can foster, rather than stifle, innovation in use cases like Medicalchain and the Georgia land registries that promote data provenance, transparency, immutability, and thus, privacy.

While it seems difficult to have the core technology of blockchain reconcile with the current interpretation of the GDPR, this reconciliation is crucial to ensure that the full potential of permissioned blockchain uses do not go untapped. As Sepehr Shahshahani concludes, it is necessary for the courts and the legal community to rule in favor of new technologies to reach compromise between the law and technological innovations and growth.[204] If the legal community fails to do so and passes restrictive rulings regarding new technologies, then these technologies fail to influence subsequent policymaking.[205] The use of permissioned blockchains to date, specifically in areas such as the healthcare industry and land title registries, have demonstrated that the implications of an immutable ledger are vast in the realm of data privacy, security, and provenance. By releasing clarifying guidance that supports the use of permissioned blockchains to store personal data, the GDPR can promote innovation and technological growth in a way that exemplifies its goals of fairness, transparency, integrity, and accuracy.[206]

CONCLUSION

Because GDPR and blockchain technology are both new to the legal landscape, the regulations and enforcement them needs to be clarified before businesses can confidently turn their use cases into mainstream development. Permissioned blockchains, like Medicalchain and blockchain land registries, benefit society

---

[204] *See* Shahshahani, *supra* note 187, at 37, 57.

[205] *See id.*

[206] *See* EUROPEAN DATA PROTECTION LAW AND PRACTICE, *supra* note 107, at 99.

because they streamline data storage and increase data protection. While these innovative uses of blockchain foster data protection, they paradoxically violate the new data protection regime under the GDPR. Accordingly, permissioned blockchains that store personal data need to be exempt from the GDPR not only because the goals of the GDPR and permissioned blockchain technology align, but also to foster technological growth and innovation within the blockchain community. While many solutions to exempt the permissioned blockchains from the GDPR exist, GDPR guidance that allows the definitions of "erasure" and "anonymized data" to include permissioned blockchains that store personal data is the most efficient way to solve the GDPR-blockchain paradox.