BLOCKCHAIN INTEGRATION INTO THE HEALTHCARE SECTOR: NAVIGATING PRIVACY COMPLIANCE, DATA LOCALIZATION, AND CROSS-BORDER DATA FLOWS

Rishabh Jayasimha Iyengar, Jindal Global Law School

ABSTRACT

A rudimentary understanding of blockchain technology will shed light on the pillars of "transparency" and "immutability" that it is built on[1]. These principles paint such technology as the antithesis of protecting personal data of individuals that form part of such blockchains. Once data is recorded within a blockchain, the ledger ensures that no unilateral change can be made by any singular party to the database. Further, this public ledger is heralded for its transparent nature[2].

Such disparities in privacy compliance requirements mandated by the EU's GDPR[3] and India's DPDPA require to be delved into considering the rise in blockchain technology's application within essential sectors like healthcare and finance wherein the protection of sensitive personal data that is processed by corporations in different jurisdictions is paramount[4].

This paper begins with analyzing how the transparency requirements central to blockchain technology are the antithesis to privacy requirements/DSR's mandated by privacy statutes of the EU and India. Furthermore, with the growth of blockchain into essential sectors like finance and healthcare, it will aim to determine the level of compliance to be adhered to in situations of cross-border data flows[5] between the EU and India from corporations processing such sensitive personal data. It also aims to determine the scope of the Indian government's discretion under the DPDPA concerning cross-

[1] *Enhancing MMIS security and transparency with Blockchain technology* (2024) *Enhancing MMIS Security and Transparency with Blockchain*. Available at: https://www.trigyn.com/insights/enhancing-mmis-security-and-transparency-blockchain-technology (Accessed: 12 September 2024).
[2] de Haro-Olmo, F.J., Varela-Vaca, Á.J. and Álvarez-Bermejo, J.A. (2020) *Blockchain from the perspective of privacy and Anonymisation: A systematic literature review*, *MDPI*. Available at: https://www.mdpi.com/1424-8220/20/24/7171 (Accessed: 12 September 2024).
[3] Legal text (2024) General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/ (Accessed: 27 October 2024).
[4] Filippi, P.D., Mannan, M. and Reijers, W. (2020) Blockchain as a confidence machine: The Problem of Trust & Challenges of Governance, Technology in Society. Available at: https://www.sciencedirect.com/science/article/pii/S0160791X20303067 (Accessed: 27 October 2024).
[5] *International Data Transfers* (no date) *International data transfers | European Data Protection Board*. Available at: https://www.edpb.europa.eu/sme-data-protection-guide/international-data-transfers_en (Accessed: 12 September 2024).

border processing of sensitive data arising overseas in the absence of international privacy legislation. Lastly, the paper will also analyze how "sensitive"[6] personal data like health information which has a separate classification under the GDPR[7] will be processed under the DPDPA considering the absence of such classification altogether.

Introduction

Blockchain technology's application has begun to expand beyond its nascent Phase 1 applications within cryptocurrency and immerse itself into more data intensive sectors including healthcare and financial services. With such expansion comes certain concerns including those involving the protection of personal data being processed, transferred across jurisdictions, or even stored remotely on such ledgers.

These systems spark some cause for concern with respect to the permanence of information stored on such ledgers[8]. They are designed to ensure that the stored data cannot be manipulated due to the frequent validation of the "immutable" ledger. As attractive as this transparency is, it exposes all transaction details to potential misuse and scrutiny of actors who have access to the blockchain[9]. Data privacy requirements worldwide preach certain DSR's (Data Subject Rights) that are inalienable in the current day and age. Each of these rights offers data subjects the right to complete access and decision-making capabilities concerning their personal data. Much like the EU's GDPR[10], Section 12 of India's very own DPDPA 2023 also confers the right to erasure/deletion of personal data upon an individual's request. This right is synonymous with the GDPR's[11] "right to be forgotten". These regulations would come in direct conflict with a blockchain ledger's "immutability" concept because the data would not only be publicly accessible on certain public blockchains but also be virtually impossible to alter or delete.

---

[6] *What personal data is considered sensitive?* (no date) *European Commission*. Available at: https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en (Accessed: 12 September 2024).

[7] Legal text (2024) General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/ (Accessed: 27 October 2024).

[8] Habib, G. et al. (2022) Blockchain technology: Benefits, challenges, applications, and integration of blockchain technology with cloud computing, MDPI. Available at: https://www.mdpi.com/1999-5903/14/11/341 (Accessed: 27 October 2024).

[9] Valdeolmillos, D., Martín, Y. and Prieto, J. (2020) Blockchain technology: A review of the current challenges of cryptocurrency | request PDF, Blockchain Technology: A Review of the Current Challenges of Cryptocurrency. Available at: https://www.researchgate.net/publication/333997769_Blockchain_Technology_A_Review_of_the_Current_Challenges_of_Cryptocurrency (Accessed: 27 October 2024).

[10] Legal text (2024) General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/ (Accessed: 27 October 2024).

[11] Legal text (2024) General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/ (Accessed: 27 October 2024).

Although India has laid the groundwork with the DPDPA in 2023, the act is yet to be notified and is far from comprehensive. Numerous provisions of the act still require refining and lower levels of ambiguity in their inference. Further, the scope and extent of discretion available to the Central Government, especially within the notification of cross-border compliant jurisdictions, lacks clarity. The DPDPA is also silent about any sub-classification of personal data as "sensitive", which leaves the method of processing of cross-border healthcare data that arises from within the EU unaddressed[12].

Large corporations are notorious for decentralizing operations involving the storage and processing of collected personal data worldwide. With the application of blockchain based ledgers that carry such personal information, the new dilemma becomes addressing "how" this personal data, some of which could largely be considered 'sensitive' in nature, is being processed once the data crosses global borders. With processing disparities between the EU's GDPR[13] and India's new DPDPA, there arise concerns about the adequacy of regulation with respect to the processing of more 'sensitive' forms of personal data like health information which is growingly being adapted into blockchain systems globally to ensure seamless accessibility across jurisdictions[14]. Health data on global blockchains speculatively is expected to transform the storage of medical records, revolutionize big pharma supply chain management and possibly even supplement clinical trials more efficiently[15]. Dealing with this sensitive health data as it crosses borders from the EU into India for decentralized storage and processing purposes opens the door to a plethora of new problems concerning privacy compliance with these global blockchains.

Blockchain Technology: The anti-thesis to global privacy norms

Article 5 of the EU's GDPR[16] lays out principles of lawfulness, fairness, transparency, purpose limitation, data minimization, storage limitation, integrity, confidentiality and accountability[17].

[12] Barat, Dr.D. and Gupte, R. (Vaidya) (2024) India's new data protection regime: Tracking updates and preparing for compliance, S&R Associates. Available at: https://www.snrlaw.in/indias-new-data-protection-regime-tracking-updates-and-preparing-for-compliance/ (Accessed: 27 October 2024).
[13] Legal text (2024) General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/ (Accessed: 27 October 2024).
[14] Salzano, F. et al. (2024b) Integrating blockchain technology within an information ecosystem, Blockchain: Research and Applications. Available at: https://www.sciencedirect.com/science/article/pii/S2096720924000381 (Accessed: 27 October 2024).
[15] Agbo, Cornelius C., et al. "Blockchain Technology in Healthcare: A Systematic Review." MDPI, Multidisciplinary Digital Publishing Institute, 4 Apr. 2019, www.mdpi.com/2227-9032/7/2/56.
[16] Legal text (2024) General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/ (Accessed: 27 October 2024).
[17] Regulation - 2016/679 - en - GDPR - EUR-lex (no date) EUR. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj (Accessed: 27 October 2024).

Similarly, Article 15, 16 and 17 of the GDPR[18] lay out integral data subject rights (DSR's) including the right to access, rectification and erasure of personal data, which is synonymous with the right to be 'forgotten'. India's DPDPA shares a fair amount of these foundational DSR's. Section 4 of the act mandates the processing of personal data only in fair, reasonable manners, for purely specified purposes, once the data principal's consent has been acquired[19]. Section 8 further mandates the erasure of personal data by fiduciaries once the purpose for which it was collected has lapsed/fulfilled, while Section 11 & 12 lay out the DSR's like the EU's GDPR[20], i.e., the right to confirmation, access, correction and erasure of personal data[21].

Blockchain technology is built on certain characteristics of transparency wherein all the transactions are made visible to every single node on the network[22]. Logically then, this runs counteractive to the principle of data confidentiality as laid out by the GDPR[23] and the DPDPA[24]. This assumption is reliant on the functioning nature of public blockchains being visible to every participant on the network which is in antithetical to the GDPR's[25] requirements of personal data being processed in manners that ensure the maximal security of personal data collected under Article 5(1)(f) which stipulates protection against any unauthorised processing[26]. Furthermore, once personal data is written into a blockchain ledger, it becomes virtually impossible to erase due to the 'append only' nature of the system. Each block within a blockchain ledger contains a hash of the previous block, thereby creating an 'immutable' chain of such records[27]. These systems were designed with the sole idea that data once recorded cannot be removed. Such a characteristic clashes with the GDPR's[28] right to be

[18] Legal text (2024) General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/ (Accessed: 27 October 2024).
[19]https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf
[20] Legal text (2024) General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/ (Accessed: 27 October 2024).
[21]https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf ' (2003). The Gazette of India.
[22] https://www.researchgate.net/publication/328338366_Blockchain_challenges_and_opportunities_A_survey
[23] Legal text (2024) General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/ (Accessed: 27 October 2024).
[24]'https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf' (2003). The Gazette of India.
[25] Legal text (2024) General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/ (Accessed: 27 October 2024)>
[26] Regulation - 2016/679 - en - GDPR - EUR-lex (no date) EUR. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj (Accessed: 27 October 2024).
[27] Narayanan, A. et al. (2015) Bitcoin and cryptocurrency technologies, Princeton University. Available at: https://bitcoinbook.cs.princeton.edu/ (Accessed: 27 October 2024).
[28] Legal text (2024) General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/ (Accessed: 27 October 2024).

'forgotten' under Article 17 and the DPDPA's[29] requirement to erase data once the purpose limitation has been achieved under Section 8[30].

With the way blockchain systems are decentralized architecturally, there arises a new challenge in enforcing DSR's and imposing accountability onto entities for compliance. Within traditional centralized databases, there are clear demarcations between data controllers who are responsible in managing data and data subjects whose requests are meant to be complied with. In decentralized blockchain networks, there are no controlling entities per se[31]. This clear lack of a data controller makes it doubly hard to enforce DSR's like the right to access or erase data as mandated by the GDPR[32] and the DPDPA[33].

The GDPR[34] lays out the principle of data minimization under Article 5(1)(c) wherein personal data is meant to be adequate, relevant and limited to what is required for the purposes of processing. This is extremely hard to reconcile within the context of blockchain technology. Blockchain technology mandates for data to be replicated on all the nodes of the ledger which leads to personal data being stored and processed on more nodes than necessary for the satisfaction of the original purpose[35]. Coincidentally, there have been certain reservations behind the overall incompatibility of blockchain technology with the GDPR's requirements. While there are technical solutions like Zero Knowledge Proofs, Homomorphic Encryption and Hybrid Blockchain Database Systems that could reconcile the systems with foundational

[29]'https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf
https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf' (2003). The Gazette of India.

[30] Finck, M. (2015) https://edpl.lexxion.eu/data/article/12327/pdf/edpl_2018_01-007.pdf, Blockchains and Data Protection in the European Union. Available at: https://edpl.lexxion.eu/data/article/12327/pdf/edpl_2018_01-007.pdf (Accessed: 27 October 2024).

[31] Kolain, M. and Wirth, C. (2018) (PDF) privacy by Blockchain Design: A Blockchain-enabled GDPR-compliant approach for handling personal data, Privacy by BlockChain Design: A Blockchain-enabled GDPR-compliant Approach for Handling Personal Data. Available at: https://www.researchgate.net/publication/326246922_Privacy_by_BlockChain_Design_A_Blockchain-enabled_GDPR-compliant_Approach_for_Handling_Personal_Data (Accessed: 27 October 2024).

[32] Legal text (2024) General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/ (Accessed: 27 October 2024).

[33]'https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf
https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf' (2003). The Gazette of India.

[34] Legal text (2024) General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/ (Accessed: 27 October 2024).

[35] Fabiano, N. (2017) The internet of things ecosystem: The Blockchain and privacy ..., The Internet of Things ecosystem: The blockchain and privacy issues. The challenge for a global privacy standard. Available at: https://www.researchgate.net/publication/319118738_The_Internet_of_Things_ecosystem_The_blockchain_and_privacy_issues_The_challenge_for_a_global_privacy_standard (Accessed: 27 October 2024).

data protection regimes, they would do little to bypass data protection legislation and would detract from the overall aim of this paper[36].

In addition, there are a couple of conceptual issues between decentralized blockchain systems and centralized forms of control that data protection legislation seeks to implement. Blockchain technology aims at distributing power and control while data protection regimes are predicated on individual rights and centralized control[37]. There have also been arguments made about the possible inclusion of 'data ownership' or 'data property rights' that involve individuals licensing out their rights to blockchain systems[38]. Similarly, there has been some understanding of Decentralized Autonomous Organizations (DAO's) being able to potentially align privacy laws by encoding data protection guidelines into the DAO smart contracts[39] and mandating collective agreement for any alterations to be made[40].

Cross-border data compliance from the EU into India

With blockchain technology seeing a spread into more data intensive sectors like healthcare and financial services, the quantum of data that crosses borders for purposes of processing also rises drastically, which leads to an unanswered question behind the level of compliance that large corporations must adhere to while processing such data overseas, especially health or financial data that is often treated differently across jurisdictions.

The flow of personal data across EU borders and into India sees an overlap between the application of the GDPR and the DPDPA[41]. As under Article 3(2), the GDPR[42] has a higher standard of protection and extraterritorial application by governing the processing of personal data of individuals based in the EU even when the processor is not established within the EU. This would also then include Indian companies that process personal data concerning EU

[36] Ibanez, L.-D., O'Hara, K. and Simperl, E. (2018) On blockchains and the General Data Protection Regulation, King's College London. Available at: https://kclpure.kcl.ac.uk/portal/en/publications/on-blockchains-and-the-general-data-protection-regulation (Accessed: 27 October 2024).
[37] Buocz, T. et al. (2019) Bitcoin and the GDPR: Allocating responsibility in Distributed Networks, SSRN. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3297531 (Accessed: 27 October 2024).
[38] Ibáñez, Luis Daniel, et al. "(PDF) on Blockchains and the General Data Protection Regulation." On Blockchains and the General Data Protection Regulation, July 2018, www.researchgate.net/publication/326913146_On_Blockchains_and_the_General_Data_Protection_Regulation.
[39] Buocz, T. et al. (2019) Bitcoin and the GDPR: Allocating responsibility in Distributed Networks, SSRN. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3297531 (Accessed: 27 October 2024).
[40] Buocz, T. et al. (2019) Bitcoin and the GDPR: Allocating responsibility in Distributed Networks, SSRN. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3297531 (Accessed: 27 October 2024).
[41] 'https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf' (2003). The Gazette of India.
[42] Legal text (2024) General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/ (Accessed: 27 October 2024).

residents in connection with any good/service offered therein although there is no actual physical presence within the EU[43]. On the Indian flipside, Section 3(b) of the DPDPA[44] aims to govern personal data outside the territory of India that is in connection with 'any activity' related to goods and services that are being offered to data principals 'within Indian territory'.

With respect to the transfer of such personal data to other countries, the GDPR has very strict demarcations under Chapter V[45]. Article 45 is the primary mechanism to ratify transfers of personal data to a third country, i.e., through an 'adequacy' decision by the Commission that is based on the level of data protection the country has to offer. The Commission has not declared India 'adequate' under Article 45's scope and thus transfers justified on adequacy decisions cannot be ratified right now[46]. The secondary mechanism to ratify such flows fall under Article 46(2)(c) of the GDPR, i.e., Standard Contractual Clauses (SCC's) and Article 47 of the GDPR, i.e., Binding Corporate Rules (BCR's). SCC's tend to involve model clauses/contracts between parties to protect individual rights when personal data crosses borders and are usually used to govern the relationship between data importers and exporters. These clauses also contain little/no scope for alteration and are pre-approved by the Commission. BCR's on the other hand are used within large corporations and used to transfer data across borders to further operational processes. They require formal authorization and cover entire organizations/corporates[47].

However, the CJEU's Schrems II judgement from 2020[48] clarified that SCC's alone may not be enough for data exporters[49]. They must determine on a case-by-case basis whether any additional safeguards should be put in place to ensure an equivalent level of data protection as guaranteed within the EU, especially if the third country's privacy laws permit the government to have a disproportionate access to personal data. The European Data Protection Board (EDPB) has also issued some recommendations that are aimed at supplementing the transfer

[43] "Guidelines 3/2018 on the Territorial Scope of the GDPR (Article ..." Guidelines 3/2018 on the Territorial Scope of the GDPR, Nov. 2019, www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en.pdf.

[44]https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

[45] Legal text (2024) General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/ (Accessed: 27 October 2024).

[46] "Data Protection Adequacy for Non-EU Countries." European Commission, commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. Accessed 27 Oct. 2024.

[47] "Understanding Standard Contractual Clauses (SCCS): A Complete Guide." Kiteworks, 2 Aug. 2024, www.kiteworks.com/risk-compliance-glossary/standard-contractual-clauses-sccs/.

[48] "CJEU - C-311/18 - Facebook Ireland and Schrems." GDPRhub, gdprhub.eu/index.php?title=CJEU_-_C-311%2F18_-_Schrems_II. Accessed 27 Oct. 2024.

[49] "Lex - 62018CJ0311 - En - EUR-Lex." EUR, eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62018CJ0311. Accessed 27 Oct. 2024.

of personal data across borders and ensure some level of EU compliance[50]. These are purely technical through techniques of pseudonymization, other contractual measures including challenging government access, transparency and accountability measures.

India's data localization discourse begins with the Srikrishna committee report in 2018, that emphasised the need for data localization of certain sensitive categories of data, along with certain ancillary obligations[51]. The implications of such data localization for corporations functioning globally would involve local storage of personal data which would inevitably raise compliance costs. The Reserve Bank of India further mandated data localization, stipulating that all payment data generated within the country must be stored exclusively on local servers[52]. However, the DPDPA[53] does not explicitly require companies operating in India to mandatorily store the relevant data within the country. In fact, it allows data to flow freely across jurisdictions unless prohibited by a statutory authority. For instance, the RBI prohibits payment system providers operating in India to transfer any data related to payment systems outside India. Additionally, the Indian government has been given the power to restrict the transfer of data to identified territories outside India. Thus, the scope of this discretion is still blurry as the legislature has adopted a 'blacklist' approach wherein the government has been provided the power to notify jurisdictions to which such transfers will not be permitted.

With 'Sensitive' data in the EU and India, as discussed above, there arise some sectoral regulations that impose additional requirements on cross border transfers. The EU's eHealth Network has guidelines in place for the interoperability of health data including those on cross border transfers[54]. Similarly, the guidelines under India's draft Digital Information Security in Healthcare Act (DISHA) proposes stricter requirements in the collection, storage and transfer

[50] "Recommendations 01/2020 on Measures That Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data." Recommendations 01/2020 on Measures That Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data | European Data Protection Board, 18 June 2021, www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en.

[51] Gupta, Aditya. "Data Localization in India: Regulations, Impact, and the Future." Data Localization In India: Regulations, Impact, And The Future - Privacy Protection - Privacy - India, 25 Sept. 2024, www.mondaq.com/india/privacy-protection/1522118/data-localization-in-india-regulations-impact-and-the-future.

[52] Burman, Anirudh, and Upasana Sharma. "How Would Data Localization Benefit India? - Carnegie Endowment for International Peace | Carnegie Endowment for International Peace." How Would Data Localization Benefit India?, 14 Apr. 2021, carnegieendowment.org/research/2021/04/how-would-data-localization-benefit-india.

[53] 'https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf' (2003). The Gazette of India.

[54] Guidelines on Minimum/Non- Exhaustive Patient Summary ..., Nov. 2013, health.ec.europa.eu/system/files/2019-02/guidelines_patient_summary_en_0.pdf.

of digital health data[55]. Thus, compliance while dealing with healthcare specific data which is 'sensitive' in nature becomes two-fold, i.e., adherence to general privacy regulation and sector specific guidelines.

For corporations operating between both jurisdictions, implementing BCR's can ensure a more streamlined approach to cross border transfers due to a more structured compliance regime dealing with transfers within the same group of companies functioning in jurisdictions that do not extend the same level of privacy protection[56]. Apart from this, anonymization and pseudonymization mechanisms can only logically be used to reduce compliance issues as they fall outside the scope[57] of the GDPR[58] and the DPDPA[59]. This would only stand true if the anonymization is not reversible and any risk of re-identification is low and unlikely to identify/link the individual[60]. The GDPR[61] lays out technical measures for organisations to comply with as well under Article 24, i.e., internal data protection policies, audits and privacy sensitisation[62]. Similarly, Section 8 of the DPDPA[63] lays out the obligations of a data fiduciary regarding accountability and security safeguards. Article 25 of the GDPR[64] and Section 10(2)(c)(i) hint at the concepts of 'privacy by design' which requires companies to begin integrating data protection principles and approaches into their business practices and processing activities from the lowest level[65]. This approach ensures that any data collected to

[55] Panda, Additi. "Digital Information Security in Healthcare Act: Estartindia." Https://Www.Estartindia.Com/, Sept. 2023, www.estartindia.com/knowledge-hub/blog/digital-information-security-in-healthcare-act.
[56]"Article 29 Data Protection Working Party." Recommendation on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, Apr. 2018, www.edpb.europa.eu/sites/default/files/files/file2/wp264_art29_wp_bcr-c_application_form.pdf.
[57] Hintze, Mike. "Viewing the GDPR through a De-Identification Lens: A Tool for Compliance, Clarification, and Consistency." OUP Academic, Oxford University Press, 19 Dec. 2017, academic.oup.com/idpl/article/8/1/86/4763693.
[58] Legal text (2024) General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/ (Accessed: 27 October 2024).
[59]'https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf' (2003). The Gazette of India.
[60] "Article 29 Data Protection Working Party." Opinion 05/2014 on Anonymisation Techniques, 10 Apr. 2014, ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.
[61] Legal text (2024) General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/ (Accessed: 27 October 2024).
[62] Bovens, Mark, et al. Academic.Oup.Com, Aug. 2014, academic.oup.com/edited-volume/28191.
[63]'https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf' (2003). The Gazette of India.
[64] Legal text (2024) General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/ (Accessed: 27 October 2024).
[65] Cavoukian, Ann. "Privacy by Design: Origins, Meaning, and Prospects for Assuring Privacy and Trust in the Information Era." Privacy by Design: Origins, Meaning, and Prospects for Assuring Privacy and Trust in the Information Era, Jan. 2011, www.researchgate.net/publication/289769458_Privacy_by_Design_Origins_Meaning_and_Prospects_for_Assuring_Privacy_and_Trust_in_the_Information_Era.

be processed from the very beginning is purely what is necessary to achieve the specified purpose[66].

Indian Government's scope of discretion under Section 16 of the DPDPA

The use of the word 'may' under Section 16 of the DPDPA[67] indicates the discretionary nature of the power available to the government in determining restrictions over jurisdictions wherein transfer can be barred. The lack of statutory guidelines raises concerns about arbitrary decision making which can in turn harm systems that rely on the cross-border flows of personal data for processing purposes. Section 16 of India's DPDPA[68] provides the government a substantial power in terms of the discretion available to restrict the transfer of personal data across borders by 'blacklisting' jurisdictions. Through this, the government can notify certain jurisdictions to which personal data cannot be transferred[69]. With no mention as to what the parameters of such power is, there now exists scope for an unbridled exercise of such discretionary power[70]. The section effectively places a bar on the issue of data localization under the guise of what can only be justified on the grounds of national security. However, the section is clear about the exclusion of other statutory agencies and their mandatory localization requirements[71].

The drawbacks of such a 'blacklist' approach are apparent through the complete lack of any guiding principles whatsoever. This essentially leads to large corporations being constantly unsure about when a data importing jurisdiction is likely to be flagged under the list. Without any principles to guide this practice, and the possible circumvention of this regulation altogether through a mere transfer first to a viable jurisdiction and then to a blacklisted one, the discretion seemingly seeks to serve no purpose. Rather, an approach like the EU's adequacy requirements or other conditional approaches that can be achieved through contractual

[66] "Art. 25 GDPR – Data Protection by Design and by Default." General Data Protection Regulation (GDPR), 28 Mar. 2018, gdpr-info.eu/art-25-gdpr/.

[67]'https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf' (2003). The Gazette of India.

[68]'https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf' (2003). The Gazette of India.

[69] Burman, Anirudh, and Upasana Sharma. "How Would Data Localization Benefit India? - Carnegie Endowment for International Peace | Carnegie Endowment for International Peace." How Would Data Localization Benefit India?, 14 Apr. 2021, carnegieendowment.org/research/2021/04/how-would-data-localization-benefit-india.

[70] Burman, Anirudh, and Upasana Sharma. "How Would Data Localization Benefit India? - Carnegie Endowment for International Peace | Carnegie Endowment for International Peace." How Would Data Localization Benefit India?, 14 Apr. 2021, carnegieendowment.org/research/2021/04/how-would-data-localization-benefit-india.

[71] Narain, Anahad. "Cross Border Data Transfers under the DPDP Act." Cross Border Data Transfers under the DPDP Act, 10 July 2014, www.leegality.com/consent-blog/cross-border-data-transfer.

arrangements seem to be more rational alternatives. Any further restrictions can be made based on the 'form' of personal data being processed, however the DPDPA[72] doesn't recognise differential treatment of more 'sensitive' forms of personal data either[73].

These restrictions logically would lead to the limitation of blockchain ledgers' abilities to leverage their own decentralized architecture in the processing of sensitive personal data. This would push corporations to start localizing their data processing which would rise operational costs and diminish the interoperability that global blockchain systems boast of. With overly restrictive data localization tactics that are seeking to be pushed with the wide scope of discretion available to the government, there arises a chance of local blockchain networks being isolated by the global ecosystem, lower opportunities within cross border collaboration and innovation. For instance, an argument could be made regarding blockchain's potential in changing the management of health records, secure sharing between providers and even medical research through the anonymization techniques that the ledger can offer. Cross border restrictions would lead to a loss in a unified network thereby hindering the quality of the ledger[74].

Thus, depending on how the government decides to exercise the discretion provided under Section 16[75], it could impact the transfer of Indians' personal data abroad for processing purposes. Any arbitrary blacklist would destroy existing processing agreements, and without any criteria to determine blacklisted jurisdictions, there are naturally concerns about the use of this power for non-technical reasons which do not provide certainty for setting up such networks. Arguments about discriminatory trade barriers could also be made if the discretionary power is abused with no actual justification and merely to serve political ends.

---

[72]'https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf' (2003). The Gazette of India.

[73] Raghavan, Malavika. "Rulemaking for Data Protection: Implementing India's Digital Personal Data Protection Act, 2023." IJLT, IJLT, 5 July 2024, www.ijlt.in/post/rulemaking-for-data-protection-implementing-india-s-digital-personal-data-protection-act-2023.

[74] Gaur, Sreekumar. "A Dawn of a New Era for Data Protection in India: An in-Depth Analysis of the Digital Personal Data Protection Act, 2023." A Dawn Of A New Era For Data Protection In India: An In-Depth Analysis Of The Digital Personal Data Protection Act, 2023 - Data Protection - Privacy - India, 15 Aug. 2023, www.mondaq.com/india/data-protection/1355250/a-dawn-of-a-new-era-for-data-protection-in-india-an-in-depth-analysis-of-the-digital-personal-data-protection-act-2023.

[75]'https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf' (2003). The Gazette of India.

Processing 'Sensitive' EU sourced personal health data under the DPDPA

The GDPR[76], under Article 9 recognises certain 'special' kinds of personal data which includes Health, Genetic and Biometric data[77]. The act bars the processing of such data altogether unless certain specific conditions are met, which include obtaining explicit consent from the data subject and processing purely for essential health related purposes. This level of protection for health data reflects the acknowledgement of certain forms of personal data posing greater risks to individuals' privacy rights with respect to processing[78]. In stark contrast, the DPDPA[79] lays no mention of any distinction between the processing of personal data and more sensitive forms of personal data. The absence of this specific classification causes some confusion pertaining to the protection of sensitive personal data arising from the EU, flowing into India for processing purposes. This regulatory grey-area becomes more concerning while dealing with the establishment of global blockchain ledgers being implemented within the healthcare sector to deal with secure sharing and storage of medical records, pharmaceutical supply chain management, and even clinical trial data management and storage[80]. The DPDPA's[81] lack of specific procedures to deal with 'sensitive' personal data creates inherent cross border compliance issues between the GDPR's[82] high standards for data arising from the EU and India's lack of standard for the processing of cross border data.

Due to the absence of such specific provisions under the DPDPA[83], large corporations processing EU sourced healthcare data in India will have to rely on extensive contractual arrangements and other binding corporate rules to maximise compliance with the provisions of the GDPR[84].

---

[76] Legal text (2024) General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/ (Accessed: 27 October 2024).
[77] Regulation (EU) 2016/ 679 of the European ..., Apr. 2016, eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.
[78] *Statement on the Role of a Risk-Based Approach in Data ...*, May 2014, ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf.
[79]'https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf' (2003). The Gazette of India.
[80] Agbo, Cornelius C., et al. "Blockchain Technology in Healthcare: A Systematic Review." MDPI, Multidisciplinary Digital Publishing Institute, 4 Apr. 2019, www.mdpi.com/2227-9032/7/2/56.
[81]'https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf' (2003). The Gazette of India.
[82] Legal text (2024) General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/ (Accessed: 27 October 2024).
[83]'https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf
[84] Legal text (2024) General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/ (Accessed: 27 October 2024).

First, corporations transferring health data outside the EU to India will have to ensure compliance with Chapter V of the GDPR[85]. Due to the absence of an adequacy decision for India by the Commission, the provisions of Article 46 as already discussed earlier in this paper will come into play, i.e., Standard Contractual Clauses or Binding Corporate Rules. Each of these agreements will need to be tailored to address the risks associated with the cross-border transfer of health specific data, through the implementation of clauses mandating data minimization, purpose limitation, storage limitation and other inalienable Data Subject Rights (DSR's)[86].

Second, these corporations will need to lay out better organizational mechanisms to maximise security of the health data processed under their respective ledgers. This will require technical implementations including encrypting health data through homomorphic or multi-party computation methods which essentially allow for encrypted data to be processed without sacrificing the integrity of the underlying data[87]. Within organizational blockchains, advanced access control mechanisms will restrict the availability of such data to unauthorized entities[88].

Third, clearer governance and accountability frameworks need to be put in place for blockchains containing health data that span across multiple jurisdictions. This essentially involves the designation of data protection officers, conducting data protection assessments, and other audits including the establishment of data breach notifications as under Article 33 of the GDPR[89]. This includes the clear allotment of data controller, processor and subject roles within the global blockchain network as mandated by the GDPR[90].

Fourth, as a statutory obligation to data subjects, corporations are mandated to provide information to data subjects regarding the purposes of processing health data, recipients of such

[85] Legal text (2024) General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/ (Accessed: 27 October 2024).
[86] "Guidelines 05/2021 on the Interplay between the Application of Article 3 and the Provisions on International Transfers as per Chapter V of the GDPR." Guidelines 05/2021 on the Interplay between the Application of Article 3 and the Provisions on International Transfers as per Chapter V of the GDPR | European Data Protection Board, 24 Feb. 2023, www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052021-interplay-between-application-article-3_en.
[87] Raj, Rahul, et al. "Blockchain and Homomorphic Encryption for Data Security and Statistical Privacy." MDPI, Multidisciplinary Digital Publishing Institute, 1 Aug. 2024, www.mdpi.com/2079-9292/13/15/3050.
[88] Dubovitskaya, Alevtina. "Secure and Trustable Electronic Medical Records Sharing Using Blockchain." AMIA ... Annual Symposium Proceedings. AMIA Symposium, U.S. National Library of Medicine, 2018, pubmed.ncbi.nlm.nih.gov/29854130/.
[89] Finch, Michèle. "Blockchains and Data Protection in the European Union." Blockchains and Data Protection in the European Union, 2018, edpl.lexxion.eu/data/article/12327/pdf/edpl_2018_01-007.pdf.
[90] Legal text (2024) General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/ (Accessed: 27 October 2024).

data and other safeguards in place for cross-border transfers. Data subjects are required to be made aware of their rights to access, rectify and erase their health data and even object to its processing to the extent that is made applicable to blockchain based systems[91].

Lastly, corporations are expected to conduct regular audits and assessments of their blockchain systems that process health data to ensure compliance with the GDPR's 'sensitive' data guidelines. As already discussed, this could involve the application of Zero Knowledge Proofs (ZKP's) or other secure methods to depict compliance without revealing allied sensitive information[92].

Furthermore, corporations that process overseas health data locally could begin adopting GDPR[93] compliant consent mechanisms, which go over and above the DPDPA's requirements[94]. This includes the obtaining of explicit and informed consent prior to the processing of health data and the provision of withdrawing such consent at any point in time. This maximizes DSR awareness and ensures compliance with the GDPR's statutory requirements[95]. On a similar tangent, large data processors could conjointly establish regulatory sandboxes with Indian regulatory authorities that allow organizations to test and implement solutions for 'sensitive' personal data processing which could eventually contribute to the creation of a more comprehensive set of guidelines/practices to manage consent, ensure DSR's, and securely handling sensitive data on blockchains[96].

Noting the proviso to Section 16 of the DPDPA[97] that permits sector specific legislation to take precedence over the DPDPA[98] when more stringent measures regarding cross-border data processing are proposed to be imposed, the need for sector specific legislation to govern

[91] "India's Digital Personal Data Protection Act 2023 vs. The ..." India's Digital Personal Data Protection Act 2023 vs. the GDPR: A Comparison, Dec. 2023, www.lw.com/admin/upload/SiteAttachments/Indias-Digital-Personal-Data-Protection-Act-2023-vs-the-GDPR-A-Comparison.pdf.
[92] J, Andrew, et al. "Blockchain for Healthcare Systems: Architecture, Security Challenges, Trends and Future Directions." Journal of Network and Computer Applications, Academic Press, 3 Apr. 2023, www.sciencedirect.com/science/article/pii/S1084804523000528.
[93] Legal text (2024) General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/ (Accessed: 27 October 2024).
[94]'https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf' (2003). The Gazette of India.
[95] "Guidelines 05/2020 on Consent under Regulation 2016/679 ..." Guidelines 05/2020 on Consent under Regulation 2016/679, May 2020, www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.
[96] Chumak, Alona. "Cross-Border Health Data Transfer Rules around the World." InCountry, 6 Feb. 2024, incountry.com/blog/cross-border-health-data-transfer-rules-around-the-world/.
[97]'https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf' (2003). The Gazette of India.
[98]'https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf' (2003). The Gazette of India.

sensitive personal data cannot be overstressed. Sector specific legislation that considers sectoral nuances could provide a roadmap detailing better consent practices and technical safeguards specific to blockchain technology. More importantly, with the sheer lack in uniformity within privacy statutes globally, some level of regulatory consensus would make cross-border data flows a lot more compliant[99].

Conclusion

The expansion of blockchain technology into the management of healthcare data globally includes challenges involving compliance with antithetical privacy requirements that the GDPR[100] and the DPDPA lay out. Moreover, this compliance arrangement causes concern while navigating EU-India data flows in the absence of the requisite adequacy decision under Article 45 of the GDPR. In this situation, corporations must take it upon themselves to chart out compliance frameworks involving consent backed SCC's or BCR's along with the supplemental organizational safeguards[101]. The DPDPA's[102] delegation of governmental discretion under Section 16 of the act however seems to cause some pending concern to established global blockchain networks and will continue to do so until the legislature clarifies its scope in further notifications. The paper most importantly has laid out the DPDPA's[103] absence of specific regulation concerning more sensitive forms of personal data which once again places the onus on corporations that process this health data to take up the role of ensuring frameworks rooted in better consent mechanisms, detailed DSR's, frequent impact assessments and other GDPR[104] pro practices to balance blockchain technology's promising potential with mandated regulatory guidelines[105]. Lastly, the paper notes the discord between global privacy statutes and standards, and in the absence of a more universal privacy law, it becomes important to harmonize cross border data compliance through sector specific regulation wherever

[99]"Data Protection Regulations and International Data Flows." Data Protection Regulations and International Data Flows: Implications for Trade and Development, unctad.org/system/files/official-document/dtlstict2016d1_en.pdf. Accessed 27 Oct. 2024.
[100] Legal text (2024) General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/ (Accessed: 27 October 2024).
[101] Taherdoost, Hamed. "Privacy and Security of Blockchain in Healthcare: Applications, Challenges, and Future Perspectives." MDPI, Multidisciplinary Digital Publishing Institute, 30 Oct. 2023, www.mdpi.com/2413-4155/5/4/41.
[102]'https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf' (2003). The Gazette of India.
[103]'https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf' (2003). The Gazette of India.
[104] Legal text (2024) General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/ (Accessed: 27 October 2024).
[105] Priyansh Sharma, Rujhan Khandelwal. "Cryptocurrency to Cryptography: Analyzing the DPDP Act Vis-à-Vis Blockchain Startups." IRCCL, IRCCL, 25 Sept. 2023, www.irccl.in/post/cryptocurrency-to-cryptography-analyzing-the-dpdp-act-vis-%C3%A0-vis-blockchain-startups.

possible to maximize blockchain networks' data sharing capabilities within the healthcare sector.