How to cite item: Putri, Aprialita Ghaisani, and Dyah Permata Budi Asri. "Legal Protection for Victims of Personal Data Misuse by BPJS Kesehatan Under Law Number 27 of 2022" *Jurnal Cakrawala Hukum* 16 no. 3 (2025): 224-238. DOI: 10.26905/idjch.v16i3.16492.

Jurnal Cakrawala Hukum

Volume 16 Issue 3, 2025
P-ISSN: 2356-4962, **E-ISSN**: 2598-6538

Legal Protection for Victims of Personal Data Misuse by BPJS Kesehatan Under Law Number 27 of 2022

Aprialita Ghaisani Putri[1], and Dyah Permata Budi Asri[2].
[1,2.] Faculty of Law, Esa Unggul University, Bekasi, Indonesia.

Article history:
Received 2025-10-03
Received 2025-11-22
Accepted 2025-12-01

Keywords:
Legal Protection; Personal Data; BPJS Kesehatan; Law Number 27 of 2022; Supervisory Mechanism.

DOI:
doi.org/10.26905/idjch.v16i3.16492.

Corresponding Author:
Aprialita Ghaisani Putri.
E-mail: aprialita25@gmail.com.

Abstract: The proliferation of digital data processing in Indonesia's public sector has exposed a critical governance gap between institutional data collection practices and the legal protection afforded to citizens whose personal information is compulsorily surrendered to state-mandated bodies. This study examines the legal protection available to victims of personal data misuse by Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan and evaluates the adequacy of Indonesia's personal data oversight mechanisms, with particular reference to the 2021 data breach involving approximately 279 million participant records. Employing a normative juridical method through statute and conceptual approaches, this study applies the Legal Protection Theory of Philipus M. Hadjon distinguishing preventive and repressive dimensions alongside John Rawls' Theory of Justice as Fairness as its analytical framework. The analysis demonstrates that while Law Number 27 of 2022 on Personal Data Protection establishes a formally comprehensive normative regime, both preventive and repressive legal protections remain substantively deficient due to inadequate institutional data governance, the structural dependence of the supervisory body on the executive branch, and the absence of accessible victim redress mechanisms. Justice as fairness demands that oversight guarantees be equally accessible to the most vulnerable participants. Two reforms are urgently required: the establishment of a structurally independent supervisory commission and the issuance of sector-specific data governance standards for public social security institutions.

1. Introduction

The accelerating pace of digital transformation in the public sector has fundamentally restructured the relationship between the state, its institutions, and the citizens they serve. As governments increasingly migrate core administrative functions to digital platforms, the management of personal data has become one of the most consequential legal and governance challenges of the contemporary era. This shift is particularly pronounced in countries such as Indonesia, where the rapid deployment of integrated electronic systems in public services has proceeded at a pace that

outstrips the development of robust legal safeguards for the personal data of citizens.[1] The asymmetry between technological capacity and legal protection creates a structural vulnerability that is not merely technical in nature but fundamentally juridical: it concerns the scope of state obligations toward individuals whose most sensitive information is collected, processed, and stored by public institutions without adequate accountability frameworks.[2]

Among the institutions that occupy the most critical position in this landscape is Badan Penyelenggara Jaminan Sosial Kesehatan (BPJS Kesehatan), the state-mandated body responsible for administering Indonesia's national health insurance program. Established under Law Number 24 of 2011, BPJS Kesehatan operates as a public legal entity with a mandate to ensure universal health coverage for the Indonesian population. In discharging this mandate, BPJS Kesehatan controls an extraordinarily vast repository of personal data belonging to tens of millions of participants. This data encompasses not merely demographic identifiers such as full names, national identification numbers, and addresses, but also extends to sensitive health information including medical histories, diagnostic records, pharmaceutical transactions, and financial data related to insurance claims.[3] The sheer volume and sensitivity of this data position BPJS Kesehatan as one of the most significant personal data controllers in Indonesia and, by extension, one of the most consequential actors in the national personal data protection ecosystem.

The gravity of this position was starkly revealed by the catastrophic data breach that came to public attention in May 2021. In that incident, approximately 279 million records a number exceeding Indonesia's total population at the time were allegedly leaked from a database attributable to BPJS Kesehatan and offered for sale on an online hacking forum. The leaked data included not only the identifying information of living participants but reportedly also records of deceased individuals, suggesting that the database had been consolidated from multiple sources over an extended period.[4] This incident was not merely a technical failure. It was a systemic failure of institutional accountability, data governance, and regulatory oversight one that exposed the structural inadequacy of Indonesia's then-existing personal data protection framework and catalyzed the legislative process that ultimately led to the enactment of Law Number 27 of 2022 on Personal Data Protection (hereinafter the PDP Law).

The enactment of the PDP Law represents a watershed moment in Indonesian legal history. For the first time, Indonesia possesses a comprehensive, standalone legal instrument dedicated exclusively to the protection of personal data, establishing a unified regime governing the rights of data subjects, the obligations of data controllers and processors, oversight mechanisms, and a graduated system of administrative, civil, and criminal sanctions.[5] The PDP Law formally classifies

---

1 Kurniawan, Teguh, Natalia Carolina Simanjuntak, and Sri Uliana Limbong. "Urgensi Pengesahan Rancangan Undang Undang Perlindungan Data Pribadi Dalam Digitalisasi Pelayanan Publik Guna Mewujudkan Smart Government." *Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal* 2, no. 2 (2022): 264–281. https://doi.org/10.15294/ipmhi.v2i2.55032.

2 Neta, Yulia, Agsel Awanisa, and Melisa. "The Urgency of Establishing Independent Supervisory Authority for Personal Data Protection in Indonesia." *Constitutionale: Jurnal Ilmu Hukum* 3, no. 1 (2022): 19–38. https://doi.org/10.25041/constitutionale.v3i1.2535.

3 Putra, Eduard Awang Maha, Putri Rizkika Bahri, Suci Rizki Ananda, and Baiq Riska Anggi Safitri. "Pelayanan Publik dalam Pelaksanaan Perlindungan Warga Negara melalui Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan." *Indonesia Berdaya* 5, no. 2 (2024): 749–764. https://doi.org/10.47679/ib.2024805.

4 Sorisa, Cinda, Cindi Lusia Kiareni, and Jadiaman Parhusip. "Etika Keamanan Siber: Studi Kasus Kebocoran Data BPJS Kesehatan di Indonesia." *Jurnal Sains Student Research* 2, no. 6 (2024): 586–593. https://doi.org/10.61722/jssr.v2i6.2996.

5 Ayiliani, Fanisa Mayda, and Elfia Farida. "Urgensi Pembentukan Lembaga Pengawas Data Pribadi sebagai Upaya Pelindungan Hukum terhadap Transfer Data Pribadi Lintas Negara." *Jurnal Pembangunan Hukum Indonesia* 6, no. 3 (2024): 431–455. https://doi.org/10.14710/jphi.v6i3.431-455.

entities such as BPJS Kesehatan as "personal data controllers" (*pengendali data pribadi*), imposing upon them affirmative legal obligations to ensure the lawful, transparent, and proportionate processing of personal data, to implement appropriate technical and organizational security measures, and to notify relevant authorities and affected data subjects in the event of a security breach. Non-compliance exposes controllers to administrative sanctions, including fines of up to two percent of annual revenue, as well as potential criminal liability under Articles 57 and 58 of the PDP Law.[6]

Yet the existence of legal instruments, however comprehensive, does not in itself guarantee substantive protection. The gap between normative prescription and institutional implementation has proven to be a persistent and structurally embedded problem in Indonesian administrative law. In the specific context of personal data protection in the health sector, empirical evidence suggests that compliance remains uneven, oversight mechanisms lack independence and effectiveness, and victims of data breaches continue to have limited access to meaningful remedies.[7] The 2021 BPJS Kesehatan data breach proceeded without any public disclosure of accountability measures, criminal prosecution, or compensation to affected participants outcomes that fall manifestly short of the standard of substantive protection that a rights-based legal framework demands.[8]

This normative-empirical gap forms the central problematic that this article seeks to interrogate. Specifically, two interrelated legal questions are addressed. First, what is the legal form and normative content of the protection afforded to victims of personal data misuse by BPJS Kesehatan, analyzed through the lens of Law Number 27 of 2022 on Personal Data Protection? Second, what is the current state of oversight mechanisms governing the protection of personal data in Indonesia's public health insurance sector, and how adequate are these mechanisms in ensuring accountability for personal data breaches? These questions are not merely administrative inquiries but go to the heart of the relationship between institutional power, individual rights, and the obligations of the state in the digital age.[9]

The analytical framework deployed in this study brings together two complementary theoretical traditions that, taken together, provide both a doctrinal and a normative-philosophical foundation for the analysis. The first is the Legal Protection Theory (*Teori Perlindungan Hukum*) of Philipus M. Hadjon, which distinguishes between preventive legal protection mechanisms designed to prevent violations before they occur and repressive legal protection mechanisms that respond to violations after the fact through enforcement, sanctions, and remedies.[10] This binary framework is particularly apt for analyzing the personal data protection obligations of BPJS Kesehatan, which simultaneously bears responsibilities of prevention (through data governance policies, security

---

6 Wardah Yuspin, Trisha Rajput, Abhinayan Basu Bal, Kelik Wardiono, and Absori. "The Regulations of the Supervisory Officer Personal Data Protection-Based Accountability Principle." *Bestuur* 12, no. 1 (2024). https://doi.org/10.20961/bestuur.v12i1.89742.

7 Wira P., Akhmad Afridho, Fitria Esfandiari, and Wasis. "Juridical Analysis of Legal Protection of Personal Data in terms of Legal Certainty." *Indonesia Law Reform Journal* 3, no. 1 (2023): 96–108. https://doi.org/10.22219/ilrej.v3i1.23840.

8 Maulida, One, and Hari Utomo. "Pertanggungjawaban Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan Atas Kebocoran Data Pribadi Pengguna Dalam Perspektif Hukum Pidana." *Indonesian Journal of Law and Justice* 1, no. 2 (2023): 1–10. https://doi.org/10.47134/ijlj.v1i2.2011.

9 Panggabean, Marshanda Vennesa, and Annisa Fitria. "Perlindungan Hukum Data Pribadi Di Indonesia (Kasus Kebocoran Badan Penyelenggara Jaminan Sosial Kesehatan)." *Arus Jurnal Sosial dan Humaniora* 5, no. 2 (2025): 1958–1965. https://doi.org/10.57250/ajsh.v5i2.1487.

10 Bediona, Kornelis, Muhamad Rafly Falah Herliansyah, Randi Hilman Nurjaman, and Dzulfikri Syarifuddin. "Analisis Teori Perlindungan Hukum Menurut Philipus M. Hadjon Dalam Kaitannya Dengan Pemberian Hukuman Kebiri Terhadap Pelaku Kejahatan Seksual." *Das Sollen: Jurnal Kajian Kontemporer Hukum dan Masyarakat* 2, no. 1 (2024). https://doi.org/10.61292/dassollen.v2i1.557.

systems, and internal compliance) and accountability (through disclosure, enforcement, and victim redress). The second theoretical pillar is the Theory of Justice as Fairness articulated by John Rawls, specifically its principles of equal basic liberties and the difference principle, which demand that legal and institutional arrangements be designed so as to protect fundamental rights equally while ensuring that any inequalities in the system operate to the greatest benefit of the most disadvantaged.[11] Applied to the oversight of personal data in public institutions, Rawls' framework insists that supervisory mechanisms must be impartial, structurally independent, and operationally accessible to those citizens who are most vulnerable to the consequences of data abuse including those with limited digital literacy, lower socioeconomic status, and reduced capacity to assert their rights through formal legal channels.[12]

The present study situates itself within an existing body of scholarly inquiry while advancing analytical ground that has not yet been adequately covered in the literature. Prior scholarship on BPJS Kesehatan and data protection has tended to focus on either the criminal liability dimensions of data breaches under the Electronic Information and Transactions Law (Oktaviani et al., 2021) or on broader assessments of personal data protection in Indonesia's health sector without sustained theoretical engagement (Annan, 2023).[13] Research that explicitly applies both Hadjon's legal protection theory and Rawls' theory of justice within an integrated analytical framework and does so against the specific regulatory backdrop of the PDP Law of 2022 remains limited. Furthermore, the literature has yet to adequately interrogate the institutional dimension of oversight failure: not merely whether BPJS Kesehatan has complied with formal requirements, but whether Indonesia's supervisory architecture currently housed within the Ministry of Communication and Digital possesses the structural independence and operational capacity required to enforce meaningful accountability.[14]

The novelty of this study is therefore threefold. First, it offers a theoretically integrated analysis that marshals both Hadjon's doctrinal framework and Rawls' normative philosophy as co-equal analytical tools, rather than treating one as primary and the other as supplementary. Second, it examines the PDP Law of 2022 as the specific regulatory instrument governing BPJS Kesehatan's data protection obligations filling the gap left by earlier studies that relied exclusively on the ITE Law framework, which was neither designed nor adequate for the specific challenges of large-scale public institutional data processing. Third, it advances a normative argument about the institutional design of oversight: that justice as fairness, properly understood, requires the establishment of a structurally independent supervisory authority for personal data protection, and that the current model of ministerially-housed supervision is constitutively inadequate to fulfill this requirement.[15]

---

[11] Consent, Background Justice and Patterned Privacy Principles: "Consent, Background Justice and Patterned Privacy Principles." *Political Studies* 72, no. 2 (2023). https://doi.org/10.1177/00323217231167074.

[12] Wardhono, R. Dwi Tjahja K., Wishnu Badrawani, Ayu Deviana, Melati Pramudyastuti, and Nadhia Shalehanti. "Pelindungan Data Pribadi di Bank Indonesia dan Lembaga Jasa Keuangan: Rekomendasi Kebijakan dan Teknis Pengaturan." Working Paper WP/16/2024, Bank Indonesia, 2024. https://ideas.repec.org/p/idn/wpaper/wp162024.html.

[13] Oktaviani, Shella, Yeremia Juan Dewata, and Aryo Fadlian. "Pertanggung Jawaban Pidana Kebocoran Data BPJS Dalam Perspektif UU ITE." *De Juncto Delicti: Journal of Law* 1, no. 2 (2021): 146–157. https://doi.org/10.35706/djd.v1i2.5732.

[14] Hadiyantina, Shinta, et al. *Perlindungan Data Pribadi dalam Bidang Rekam Medis*. Malang: Universitas Brawijaya Press, 2023. ISBN 978-623-8323-48-5.

[15] Asri, Dyah Permata Budi. "Perlindungan Hukum Hak Kekayaan Intelektual Bagi Produk Kreatif Usaha Kecil Menengah Di Yogyakarta." *Jurnal Hukum Ius Quia Iustum* 27, no. 1 (2020): 130–150. https://doi.org/10.20885/iustum.vol27.iss1.art7.

The significance of this inquiry extends well beyond the specific case of BPJS Kesehatan. Indonesia's national health insurance system, which aims to achieve universal health coverage for a population of over 270 million people, depends structurally on public trust in the integrity of the institutions that administer it.[16] That trust is not automatically secured by the existence of statutory mandates; it must be actively constructed through demonstrable accountability, transparent data governance, and accessible mechanisms for redress. When a state institution responsible for the health security of an entire nation fails to protect the most sensitive personal data of its participants and does so without consequence it does not merely inflict a technical harm. It erodes the foundational legitimacy of the social security system itself.[17]

At a broader normative level, the case of BPJS Kesehatan illustrates a recurring tension in the governance of personal data in the public sector: the tension between the institutional interest in aggregating and utilizing data for administrative efficiency and the individual's fundamental right to informational self-determination.[18] This right, which is increasingly recognized in comparative constitutional jurisprudence as an aspect of the right to privacy and human dignity, demands that data subjects retain meaningful control over the collection, processing, and dissemination of their personal information a demand that is structurally difficult to satisfy in the context of mandatory participation programs such as national health insurance, where individuals have no practical alternative to surrendering their data to the relevant public institution.[19]

It is against this background of acute empirical urgency, normative complexity, and institutional inadequacy that the present study proceeds. By examining the legal protection available to victims of personal data misuse by BPJS Kesehatan through the dual lenses of Hadjon's legal protection theory and Rawls' theory of justice, this article aims to contribute to the development of a more rights-centered, institutionally robust, and philosophically grounded approach to personal data governance in Indonesia's public sector. The analysis is structured as follows: Section 2 examines the legal protection framework applicable to BPJS Kesehatan as a personal data controller, distinguishing between preventive and repressive dimensions; Section 3 assesses the current oversight mechanisms and their adequacy under a Rawlsian standard of justice; and Section 4 draws together conclusions and policy recommendations.[20]

2. Method

This study employs a normative juridical research method, also referred to as doctrinal legal research, which centers on the systematic examination of legal norms, principles, doctrines, and the internal logic of the positive law system. As a mode of inquiry, normative legal research proceeds

[16] Adha, Lalu Adi. "Digitalisasi Industri dan Pengaruhnya Terhadap Ketenagakerjaan dan Hubungan Kerja di Indonesia." *Jurnal Kompilasi Hukum* 5, no. 2 (2020): 267–298. https://doi.org/10.29303/jkh.v5i2.49.

[17] Jayanti, Charisma Septi. "Perlindungan Hukum Terhadap Peserta Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan Atas Kebocoran Data Pribadi." Tesis, Universitas Sebelas Maret, Surakarta, 2023. https://digilib.uns.ac.id/dokumen/detail/99667.

[18] Widjaja, Gunawan, and Hotmaria Hertawaty Sijabat. "Pengesahan Undang-Undang Kesehatan: Kajian Regulasi dan Tantangan Implementasi." *Jurnal Kesehatan* 3, no. 5 (2025): 239–249. https://doi.org/10.61511/jk.v3i5.2025.1247.

[19] Putri, Amelia Natalie, and Ariawan Gunadi. "Legal Consequences of Employer Non-Compliance in Fulfilling Social Security Obligations for Workers Subjected to Unilateral Termination." *Jurnal Al-Dustur* 8, no. 1 (2025). https://doi.org/10.30863/aldustur.v8i1.8702.

[20] Astuti, Nur Rochmah Dyah Puji, et al. *Keamanan Data dalam Revolusi Teknologi*. Indonesia: PT Penerbit Qriset Indonesia, 2025. https://doi.org/10.61722/book.2025.keamanan-data.

from the premise that law is an autonomous normative system whose coherence, consistency, and adequacy can be evaluated through rigorous doctrinal analysis, without resort to primary empirical data collected through fieldwork or interviews.[21] This methodological choice is appropriate to the subject matter of the present study, which concerns the normative adequacy of the legal protection framework applicable to victims of personal data misuse by BPJS Kesehatan and the structural sufficiency of the oversight mechanisms established under Indonesian positive law.

Two principal approaches are employed in conducting the analysis. The first is the statute approach, which involves the systematic examination and interpretation of all relevant legislative instruments bearing on the subject matter of personal data protection and public institutional accountability. The primary statutes subjected to analysis include Law Number 27 of 2022 on Personal Data Protection, Law Number 24 of 2011 on the Social Security Administering Body, Law Number 19 of 2016 on Electronic Information and Transactions, and Law Number 14 of 2008 on Public Information Disclosure, together with their implementing regulations. The statute approach requires not merely the inventorization of applicable norms but their critical evaluation against the constitutional framework and the theoretical benchmarks established by the analytical frameworks deployed in this study.[22] The second approach is the conceptual approach, which involves the engagement with legal doctrines, theoretical constructs, and the academic literature of legal science in order to build a coherent argumentative framework capable of evaluating the normative problems posed by the research questions.[23] The conceptual approach is indispensable in this study given that the central analytical instruments the Legal Protection Theory of Philipus M. Hadjon and the Theory of Justice as Fairness of John Rawls are not derived from positive statutory text but from the doctrinal and philosophical tradition of legal science.

The legal materials used in this study are classified into three categories. Primary legal materials consist of binding normative sources, including the 1945 Constitution of the Republic of Indonesia, all relevant statutes and government regulations, and official decisions of state institutions with normative force.[24] Secondary legal materials encompass the scholarly literature of legal science, including peer-reviewed journal articles, legal monographs, and research reports bearing on the topics of personal data protection, public institutional accountability, and the theoretical frameworks applied in the analysis.[25] Tertiary legal materials, including legal dictionaries and encyclopedias, are employed where clarification of technical legal terminology is required.

The collection of legal materials is conducted through a systematic library research technique, which entails the identification, inventorization, and classification of relevant legal materials from

---

21 Wira P., Akhmad Afridho, Fitria Esfandiari, and Wasis. "Juridical Analysis of Legal Protection of Personal Data in terms of Legal Certainty." *Indonesia Law Reform Journal* 3, no. 1 (2023): 96–108. https://doi.org/10.22219/ilrej.v3i1.23840.

22 Budiono, Indro, Anindya Yustika, Mevlana El Rumi Abimanyu, and Raditya Nur Syabani. "Internalization Free, Prior, and Informed Consent as Indigenous Alienation Resistance in Structural Agrarian Conflict." *Jurnal Cakrawala Hukum* 14, no. 3 (2023): 279–290. https://doi.org/10.26905/idjch.v14i3.11486.

23 Neta, Yulia, Agsel Awanisa, and Melisa. "The Urgency of Establishing Independent Supervisory Authority for Personal Data Protection in Indonesia." *Constitutionale: Jurnal Ilmu Hukum* 3, no. 1 (2022): 19–38. https://doi.org/10.25041/constitutionale.v3i1.2535.

24 Wardah Yuspin, Trisha Rajput, Abhinayan Basu Bal, Kelik Wardiono, and Absori. "The Regulations of the Supervisory Officer Personal Data Protection-Based Accountability Principle." *Bestuur* 12, no. 1 (2024). https://doi.org/10.20961/bestuur.v12i1.89742.

25 Kurniawan, Teguh, Natalia Carolina Simanjuntak, and Sri Uliana Limbong. "Urgensi Pengesahan Rancangan Undang Undang Perlindungan Data Pribadi Dalam Digitalisasi Pelayanan Publik Guna Mewujudkan Smart Government." *Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal* 2, no. 2 (2022): 264–281. https://doi.org/10.15294/ipmhi.v2i2.55032.

primary and secondary sources, including domestic and international legal databases, and open-access repositories of peer-reviewed scholarship.[26] Once collected, the legal materials are subjected to qualitative analysis through two primary techniques: legal interpretation, applied to ascertain the meaning and scope of the relevant legal norms in the context of the PDP Law and related statutes, and legal construction, applied to build systematic arguments where the positive law does not explicitly resolve the normative problems under examination. The analytical process proceeds through a deductive syllogistic method, moving from the major premises established by the theoretical frameworks and relevant legal norms to specific conclusions regarding the legal protection of BPJS Kesehatan participants and the adequacy of existing oversight mechanisms.[27]

3. Results and Discussion

3.1. Legal Protection for Victims of Personal Data Misuse by BPJS Kesehatan

The normative foundation for assessing the legal protection available to victims of personal data misuse by BPJS Kesehatan rests on the intersection of two regulatory frameworks: Law Number 24 of 2011 on the Social Security Administering Body, which defines the institutional mandate and public law character of BPJS Kesehatan, and Law Number 27 of 2022 on Personal Data Protection (PDP Law), which establishes a comprehensive regime governing the rights of data subjects and the obligations of data controllers. Read together, these two instruments position BPJS Kesehatan unambiguously as a *personal data controller* (*pengendali data pribadi*) within the meaning of Article 1 point 4 of the PDP Law an entity that determines the purposes and means of personal data processing and bears primary legal responsibility for the security, accuracy, and lawful handling of that data.[28] This classification is not merely taxonomic; it generates a substantial and enforceable body of legal obligations that extend far beyond the institutional mandate conferred by Law Number 24 of 2011 and constitute the primary normative basis for the legal protection of BPJS Kesehatan participants.

Applying the Legal Protection Theory of Philipus M. Hadjon to the present context, legal protection assumes two analytically distinct but functionally complementary forms: preventive legal protection and repressive legal protection.[29] Preventive protection operates *ex ante*, seeking to forestall violations before they occur through regulatory requirements, institutional policies, and technical safeguards. Repressive protection operates *ex post*, providing mechanisms for accountability, enforcement, and redress once a violation has materialized. The adequacy of legal protection for BPJS Kesehatan participants must be assessed along both dimensions and the analysis demonstrates that, while normative instruments for both forms of protection exist under the PDP Law, their practical implementation remains systemically deficient.

---

[26] Ayiliani, Fanisa Mayda, and Elfia Farida. "Urgensi Pembentukan Lembaga Pengawas Data Pribadi sebagai Upaya Pelindungan Hukum terhadap Transfer Data Pribadi Lintas Negara." *Jurnal Pembangunan Hukum Indonesia* 6, no. 3 (2024): 431–455. https://doi.org/10.14710/jphi.v6i3.431-455.

[27] Asri, Dyah Permata Budi. "Perlindungan Hukum Hak Kekayaan Intelektual Bagi Produk Kreatif Usaha Kecil Menengah Di Yogyakarta." *Jurnal Hukum Ius Quia Iustum* 27, no. 1 (2020): 130–150. https://doi.org/10.20885/iustum.vol27.iss1.art7.

[28] Wira P., Akhmad Afridho, Fitria Esfandiari, and Wasis. "Juridical Analysis of Legal Protection of Personal Data in terms of Legal Certainty." *Indonesia Law Reform Journal* 3, no. 1 (2023): 96–108. https://doi.org/10.22219/ilrej.v3i1.23840.

[29] Asri, Dyah Permata Budi. "Perlindungan Hukum Hak Kekayaan Intelektual Bagi Produk Kreatif Usaha Kecil Menengah Di Yogyakarta." *Jurnal Hukum Ius Quia Iustum* 27, no. 1 (2020): 130–150. https://doi.org/10.20885/iustum.vol27.iss1.art7.

In the domain of preventive legal protection, the PDP Law imposes upon BPJS Kesehatan a set of affirmative obligations that constitute the primary normative architecture for the pre-emptive protection of participants' personal data. Article 35 mandates that data controllers implement technical and organizational measures proportionate to the risks of the data processing activities conducted, including encryption, access controls, and integrity verification systems. Article 39 specifically requires that controllers ensure the accuracy, completeness, and currency of personal data throughout its processing lifecycle, and mandates the appointment of a Personal Data Protection Officer in circumstances where the scale or sensitivity of the processing warrants such oversight.[30] In the context of BPJS Kesehatan which processes the sensitive health and financial data of tens of millions of participants on a continuous basis these requirements are not aspirational standards but binding legal obligations whose breach carries legal consequences. The institution has sought to comply with these obligations through the adoption of an information security management framework aligned with ISO/IEC 27001 standards, the implementation of role-based access controls, and the conduct of periodic cybersecurity training for personnel.[31] However, the 2021 data breach, in which approximately 279 million personal data records were reportedly extracted from a database attributable to BPJS Kesehatan and traded on a public online forum, constitutes compelling evidence that these preventive measures were inadequate in practice either in their technical implementation, their organizational enforcement, or both. The mere existence of a security policy does not discharge the legal obligation of effective data protection; the PDP Law's preventive framework demands operational effectiveness, not merely formal compliance.

The preventive obligations of BPJS Kesehatan under the PDP Law extend beyond purely technical measures to encompass the structural principle of *privacy by design and by default* a doctrine that requires data protection considerations to be embedded in systems and processes from the outset, rather than retrofitted as an afterthought.[32] Under this principle, the default settings of any data processing system must be calibrated to the minimum data collection necessary for the stated purpose, the shortest retention period consistent with that purpose, and the most restricted access consistent with operational needs. In a public institution of the scale of BPJS Kesehatan, the systemic failure to implement privacy by design principles as evidenced by the reported breadth of the 2021 data breach points to a structural governance deficit that transcends individual technical failures and reflects an institutional culture in which data protection has not been internalized as a core operational value.[33] This finding carries significant normative weight under the PDP Law: Article 40 provides that data controllers who fail to implement adequate technical and organizational measures may be subjected to administrative sanctions, including written warnings and the temporary suspension of data processing activities.

---

30 Yuspin, Wardah, Trisha Rajput, Abhinayan Basu Bal, Kelik Wardiono, and Absori. "The Regulations of the Supervisory Officer Personal Data Protection-Based Accountability Principle." *Bestuur* 12, no. 1 (2024). https://doi.org/10.20961/bestuur.v12i1.89742.

31 Putra, Eduard Awang Maha, Putri Rizkika Bahri, Suci Rizki Ananda, and Baiq Riska Anggi Safitri. "Pelayanan Publik dalam Pelaksanaan Perlindungan Warga Negara melalui Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan." *Indonesia Berdaya* 5, no. 2 (2024): 749–764. https://doi.org/10.47679/ib.2024805.

32 Setyoko, Agus, Moh. Fadly, and Noor Fatimah. "Petugas/Pejabat Pelindungan Data Pribadi dalam Ekosistem Perlindungan Data Pribadi: Indonesia, Uni Eropa dan Singapura." *Business Economic, Communication, and Social Sciences Journal (BECOSS)* 4, no. 2 (2022): 111–120. https://doi.org/10.21512/becossjournal.v4i2.8377.

33 Sorisa, Cinda, Cindi Lusia Kiareni, and Jadiaman Parhusip. "Etika Keamanan Siber: Studi Kasus Kebocoran Data BPJS Kesehatan di Indonesia." *Jurnal Sains Student Research* 2, no. 6 (2024): 586–593. https://doi.org/10.61722/jssr.v2i6.2996.

The dimension of repressive legal protection that which responds to violations that have already occurred is addressed in the PDP Law through a tiered system of administrative, civil, and criminal sanctions. Administratively, Article 57 authorizes the competent supervisory authority to impose fines of up to two percent of annual revenue for violations of data security obligations, a figure that, in the case of BPJS Kesehatan, would represent a substantial deterrent if enforced. Civilly, data subjects who suffer material or immaterial harm as a result of a data breach are entitled to claim compensation from the responsible controller under the general civil liability framework, supplemented by the specific provisions of Article 67 of the PDP Law, which affirm the data subject's right to redress.[34] Criminally, Articles 67 through 69 of the PDP Law establish offenses carrying imprisonment of up to six years and fines of up to six billion rupiah for the unlawful disclosure, use, or falsification of personal data. The PDP Law thus provides, on paper, a formidable arsenal of repressive legal instruments that could, in principle, be deployed to hold BPJS Kesehatan accountable for the consequences of the 2021 data breach.

Yet the critical weakness of the existing repressive protection framework lies not in the insufficiency of its normative prescriptions but in the near-total absence of enforcement in the aftermath of the 2021 incident. No administrative fine was publicly announced against BPJS Kesehatan. No criminal prosecution was initiated. No compensation mechanism was established for the 279 million individuals whose data were reportedly compromised. This pattern of enforcement failure is not merely a case of procedural omission; it reflects a structural problem in the architecture of personal data protection in Indonesia. At the time of the breach, Indonesia lacked a dedicated, independent supervisory authority for personal data protection; the supervisory function was dispersed across multiple ministerial and institutional actors without the institutional focus, legal mandate, or operational capacity to mount a coherent enforcement response.[35] The PDP Law has sought to address this gap through the establishment of a supervisory authority under Articles 58 through 60, but the operationalization of this body remains incomplete. In its absence, the repressive protection framework guaranteed to participants by the PDP Law remains largely notional.

The inadequacy of both preventive and repressive legal protection in the BPJS Kesehatan context is further compounded by the structural power asymmetry that characterizes the relationship between individual participants and a public institution mandated by the state. Unlike consumers in a commercial relationship who retain, at least in theory, the freedom to withdraw from a data controller's services BPJS Kesehatan participants are legally required to be enrolled in the national health insurance program. Their data is collected, processed, and retained not through a voluntary contractual relationship but through a statutory compulsion that leaves them with no realistic alternative. This structural compulsion heightens the legal obligation of BPJS Kesehatan to ensure the highest standard of data protection, and correspondingly heightens the culpability of institutional failures that expose participants to data breach harms.[36] A truly adequate regime of legal

[34] Soemitro, Dian Purwaningrum, Muhammad Arvin Wicaksono, and Nur Aini Putri. "Penal Provisions in the Personal Data Protection Law: A Comparative Legal Study between Indonesia and Singapore." *SIGn Jurnal Hukum* 5, no. 1 (2023): 155–167. https://doi.org/10.37276/sjh.v5i1.272.

[35] Ayiliani, Fanisa Mayda, and Elfia Farida. "Urgensi Pembentukan Lembaga Pengawas Data Pribadi sebagai Upaya Pelindungan Hukum terhadap Transfer Data Pribadi Lintas Negara." *Jurnal Pembangunan Hukum Indonesia* 6, no. 3 (2024): 431–455. https://doi.org/10.14710/jphi.v6i3.431-455.

[36] Roihan Ba'abud, Mohammad Fadel, and Dodik Setiawan Nur Heriyanto. "Application of the Principles of Extraterritorial Jurisdiction Towards Personal Data Breach Committed Cross-Country Borders." *Uti Possidetis: Journal of International Law* 5, no. 1 (2024): 106–137. https://doi.org/10.22437/up.v5i1.28300.

protection for BPJS Kesehatan participants therefore requires not merely the formal existence of normative instruments which the PDP Law now provides but the active, institutional commitment to implementing preventive measures with operational rigor and to pursuing repressive remedies with enforcement seriousness. The gap between these requirements and the current reality constitutes the central normative deficit that Indonesian personal data protection law must urgently address.

3.2. Oversight Mechanisms and the Adequacy of Personal Data Protection in Indonesia's Public Health Insurance Sector

The question of whether the legal protection framework for BPJS Kesehatan participants is structurally sufficient cannot be answered without examining the institutional architecture through which oversight is exercised. Legal norms, however carefully drafted, remain inert without credible enforcement mechanisms; and enforcement, in the domain of personal data protection, depends critically on the independence, capacity, and operational effectiveness of the supervisory bodies entrusted with that function. Applying the Theory of Justice as Fairness developed by John Rawls specifically its first principle of equal basic liberties and the difference principle, which holds that institutional arrangements must operate to the greatest benefit of the least advantaged the oversight of personal data in public institutions must be evaluated not only by its formal design but by its substantive accessibility to those citizens who are least equipped to assert their rights without institutional support.[37] In the context of Indonesia's national health insurance system, this standard demands a supervisory architecture that is structurally independent from the political branches of government, operationally resourced to conduct proactive audits and respond effectively to breach notifications, and institutionally designed to receive and process complaints from individual participants without erecting barriers of procedural complexity or digital literacy that systematically disadvantage lower-income and less-educated populations.[38]

The current supervisory framework for personal data protection in Indonesia falls substantially short of this standard. Under Articles 58 through 60 of the PDP Law, oversight authority over personal data controllers including BPJS Kesehatan is assigned to an institution designated by the President. At the time of writing, this supervisory function has been provisionally housed within the Directorate General of the Application of Digital Space under the Ministry of Communication and Digital. This institutional arrangement is problematic on both structural and functional grounds. Structurally, a supervisory body that operates within the hierarchy of a government ministry is subject to the political oversight and budgetary control of the executive branch the same branch that, as the owner of BPJS Kesehatan, has a direct institutional interest in minimizing the reputational and financial consequences of data breaches attributed to that institution.[39]

---

[37] Neta, Yulia, Agsel Awanisa, and Melisa. "The Urgency of Establishing Independent Supervisory Authority for Personal Data Protection in Indonesia." *Constitutionale: Jurnal Ilmu Hukum* 3, no. 1 (2022): 19–38. https://doi.org/10.25041/constitutionale.v3i1.2535.

[38] Kurniawan, Teguh, Natalia Carolina Simanjuntak, and Sri Uliana Limbong. "Urgensi Pengesahan Rancangan Undang Undang Perlindungan Data Pribadi Dalam Digitalisasi Pelayanan Publik Guna Mewujudkan Smart Government." *Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal* 2, no. 2 (2022): 264–281. https://doi.org/10.15294/ipmhi.v2i2.55032.

[39] Wahyudi, Reza, Yogi Prasetyo, and Rena Yulia. "Urgensi Pembentukan Lembaga Pengawas Pelindungan Data Pribadi di Indonesia Berdasarkan Pasal 58 Juncto Pasal 59 dan Pasal 60 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi." *SINERGI: Jurnal Riset Ilmiah* 1, no. 4 (2024): 234–242. https://doi.org/10.62335/8qf44b59.

The absence of structural independence creates a constitutive conflict of interest that undermines the supervisory body's capacity to act impartially and effectively. This is not merely a theoretical concern; the complete absence of enforcement action against BPJS Kesehatan following the 2021 data breach despite clear evidence of a large-scale breach attributable to an institution under the supervisory authority's jurisdiction demonstrates precisely the kind of supervisory failure that structural independence is designed to prevent.[40]

The urgency of establishing a genuinely independent supervisory authority for personal data protection in Indonesia has been widely recognized in academic and policy discourse. Comparative analysis consistently demonstrates that the effectiveness of data protection oversight is closely correlated with the degree of institutional independence of the supervising body. The European Union's General Data Protection Regulation (GDPR), which serves as a global benchmark, requires that each member state's supervisory authority operate with complete independence from government direction, exercise its powers with full legal personality, and possess sufficient human and financial resources to discharge its mandate effectively.[41] Indonesia's current supervisory arrangement satisfies none of these requirements. The supervisory body lacks formal institutional independence, operates with a mandate that encompasses a far broader range of digital governance functions beyond personal data protection, and has not demonstrated the enforcement profile in terms of investigations initiated, fines imposed, and prosecutions supported that would be expected of a credible data protection regulator.[42] The establishment of an independent supervisory commission with a specialized mandate, security of tenure for its members, a dedicated budget appropriated directly by the legislature, and explicit authority to conduct ex officio investigations and impose administrative sanctions without ministerial approval is therefore a prerequisite for the effective operationalization of the PDP Law's protection framework.

The functional inadequacy of the existing oversight framework is compounded by the specific characteristics of BPJS Kesehatan's data processing environment, which present supervisory challenges of exceptional complexity. Unlike a private sector data controller whose data processing activities can be benchmarked against commercial industry standards, BPJS Kesehatan operates at the intersection of public law, social insurance law, and healthcare data governance domains each governed by distinct regulatory frameworks with partially inconsistent requirements.[43] The PDP Law's general framework must be integrated with the specific requirements of Law Number 36 of 2009 on Health, the Minister of Health Regulation Number 24 of 2022 on Electronic Medical Records, and the cybersecurity standards established under Government Regulation Number 71 of 2019 on Electronic System and Transaction Organization. The current supervisory body has not articulated sector-specific guidance for the health insurance sector that would clarify how these

[40] Sorisa, Cinda, Cindi Lusia Kiareni, and Jadiaman Parhusip. "Etika Keamanan Siber: Studi Kasus Kebocoran Data BPJS Kesehatan di Indonesia." *Jurnal Sains Student Research* 2, no. 6 (2024): 586–593. https://doi.org/10.61722/jssr.v2i6.2996.

[41] Setyoko, Agus, Moh. Fadly, and Noor Fatimah. "Petugas/Pejabat Pelindungan Data Pribadi dalam Ekosistem Perlindungan Data Pribadi: Indonesia, Uni Eropa dan Singapura." *Business Economic, Communication, and Social Sciences Journal (BECOSS)* 4, no. 2 (2022): 111–120. https://doi.org/10.21512/becossjournal.v4i2.8377.

[42] Dewi, Sri Wahyuni, and others. "Independent Supervisory Authority to Protect Social Media Users' Personal Information in Indonesia." *Ius Poenale* 3, no. 1 (2022): 39–48. https://doi.org/10.25041/ip.v3i1.2531.

[43] Ishak, Nurfaika. "Guarantee of Information and Communication Technology Application Security in Indonesia: Regulations and Challenges?" *Audito Comparative Law Journal (ACLJ)* 4, no. 2 (2023): 108–117. https://doi.org/10.22219/aclj.v4i2.26098.

overlapping regulatory frameworks are to be reconciled, nor has it issued binding sector-specific data protection standards applicable to public social security institutions. This regulatory lacuna leaves BPJS Kesehatan without clear operational benchmarks and leaves participants without clear knowledge of the standards against which the institution's data governance practices can be assessed.[44]

A further dimension of inadequacy in the existing oversight framework concerns the mechanisms available to individual BPJS Kesehatan participants to assert their rights under the PDP Law. Article 5 of the PDP Law establishes a comprehensive catalog of data subject rights, including the right to receive information about the purposes of data processing, the right to access and correct personal data, the right to withdraw consent, the right to object to automated processing, and the right to claim compensation for data breach harms. These rights, however, are effectively unenforceable in the absence of accessible complaint mechanisms, clear timelines for institutional response, and an independent supervisory authority empowered to adjudicate disputes between data subjects and controllers.[45] The Rawlsian framework is particularly instructive here: justice as fairness demands that basic rights be guaranteed in a manner that is genuinely accessible to all members of society, including those with limited digital literacy, limited legal knowledge, and limited financial capacity to pursue formal legal remedies. A rights regime that is formally generous but practically inaccessible to the most vulnerable does not satisfy the requirements of justice; it constitutes, in Rawls' terms, a failure of the basic structure of society to function fairly. The institutional design of Indonesia's personal data protection regime with its multiple overlapping authorities, unclear complaint pathways, and absence of accessible, low-cost dispute resolution mechanisms fails precisely this test.[46]

The inadequacy of oversight mechanisms in the personal data protection field reflects a broader pattern of governance deficit in Indonesia's digital regulatory landscape. The rapid pace of digital transformation in the public sector has consistently outpaced the development of regulatory capacity, creating enforcement gaps that private and state actors have been able to exploit with impunity.[47] Addressing this deficit in the specific context of BPJS Kesehatan requires a multi-layered institutional response. At the normative level, the government must expedite the issuance of a Presidential Regulation (*Peraturan Presiden*) establishing a fully independent personal data protection supervisory commission with a clear mandate, institutional independence guarantees, and the operational capacity to exercise meaningful oversight of major public data controllers. At the institutional level, BPJS Kesehatan must be required to implement a comprehensive data governance framework aligned with both the PDP Law's requirements and international best practices,

---

44 Ayiliani, Fanisa Mayda, and Elfia Farida. "Urgensi Pembentukan Lembaga Pengawas Data Pribadi sebagai Upaya Pelindungan Hukum terhadap Transfer Data Pribadi Lintas Negara." *Jurnal Pembangunan Hukum Indonesia* 6, no. 3 (2024): 431–455. https://doi.org/10.14710/jphi.v6i3.431-455.

45 Wira P., Akhmad Afridho, Fitria Esfandiari, and Wasis. "Juridical Analysis of Legal Protection of Personal Data in terms of Legal Certainty." *Indonesia Law Reform Journal* 3, no. 1 (2023): 96–108. https://doi.org/10.22219/ilrej.v3i1.23840.

46 Wardah Yuspin, Trisha Rajput, Abhinayan Basu Bal, Kelik Wardiono, and Absori. "The Regulations of the Supervisory Officer Personal Data Protection-Based Accountability Principle." *Bestuur* 12, no. 1 (2024). https://doi.org/10.20961/bestuur.v12i1.89742.

47 Roihan Ba'abud, Mohammad Fadel, and Dodik Setiawan Nur Heriyanto. "Application of the Principles of Extraterritorial Jurisdiction Towards Personal Data Breach Committed Cross-Country Borders." *Uti Possidetis: Journal of International Law* 5, no. 1 (2024): 106–137. https://doi.org/10.22437/up.v5i1.28300.

including the appointment of a dedicated Personal Data Protection Officer, the conduct of regular privacy impact assessments, and the establishment of a transparent breach notification and victim redress procedure. At the societal level, investment in digital literacy and public legal education is essential to ensure that participants are aware of their rights and equipped to assert them a dimension of the oversight problem that is frequently neglected in regulatory reform debates but is indispensable to the realization of justice as fairness in the digital domain.[48]

4. Conclusion

This study has demonstrated that the legal protection available to victims of personal data misuse by BPJS Kesehatan operates on two normatively distinct but functionally interdependent dimensions preventive and repressive as theorized by Philipus M. Hadjon. While Law Number 27 of 2022 on Personal Data Protection has, for the first time, established a comprehensive normative framework governing the obligations of BPJS Kesehatan as a personal data controller, the analysis reveals that both dimensions of protection remain substantively inadequate in practice. Preventive protection is undermined by structural deficiencies in institutional data governance, the absence of operationalized privacy-by-design principles, and the lack of binding sector-specific standards for the public health insurance sector. Repressive protection is rendered largely notional by the absence of enforcement action, the non-existence of accessible victim redress mechanisms, and the structural dependence of the supervisory body on the executive branch whose institutional interests conflict with rigorous oversight. Evaluated through the lens of John Rawls' Theory of Justice as Fairness, the current supervisory architecture fails the fundamental requirement that institutional arrangements guarantee basic rights in a manner equally accessible to the most disadvantaged members of society. The mandatory character of BPJS Kesehatan participation amplifies this failure, as participants bear the full risks of institutional data misuse without a meaningful institutional recourse. Two policy reforms are therefore imperative: first, the immediate establishment of a structurally independent personal data protection supervisory commission; and second, the issuance of sector-specific data governance standards applicable to public social security institutions, accompanied by accessible dispute resolution mechanisms for affected participants.

References

Asri, Dyah Permata Budi. "Perlindungan Hukum Hak Kekayaan Intelektual Bagi Produk Kreatif Usaha Kecil Menengah Di Yogyakarta." *Jurnal Hukum Ius Quia Iustum* 27, no. 1 (2020): 130–150. https://doi.org/10.20885/iustum.vol27.iss1.art7.

Ayiliani, Fanisa Mayda, and Elfia Farida. "Urgensi Pembentukan Lembaga Pengawas Data Pribadi sebagai Upaya Pelindungan Hukum terhadap Transfer Data Pribadi Lintas Negara." *Jurnal Pembangunan Hukum Indonesia* 6, no. 3 (2024): 431–455. https://doi.org/10.14710/jphi.v6i3.431-455.

[48] Budiono, Indro, Anindya Yustika, Mevlana El Rumi Abimanyu, and Raditya Nur Syabani. "Internalization Free, Prior, and Informed Consent as Indigenous Alienation Resistance in Structural Agrarian Conflict." *Jurnal Cakrawala Hukum* 14, no. 3 (2023): 279–290. https://doi.org/10.26905/idjch.v14i3.11486.

Bediona, Kornelis, Muhamad Rafly Falah Herliansyah, Randi Hilman Nurjaman, and Dzulfikri Syarifuddin. "Analisis Teori Perlindungan Hukum Menurut Philipus M. Hadjon Dalam Kaitannya Dengan Pemberian Hukuman Kebiri Terhadap Pelaku Kejahatan Seksual." *Das Sollen: Jurnal Kajian Kontemporer Hukum dan Masyarakat* 2, no. 1 (2024). https://doi.org/10.61292/dassollen.v2i1.557.

Budiono, Indro, Anindya Yustika, Mevlana El Rumi Abimanyu, and Raditya Nur Syabani. "Internalization Free, Prior, and Informed Consent as Indigenous Alienation Resistance in Structural Agrarian Conflict." *Jurnal Cakrawala Hukum* 14, no. 3 (2023): 279–290. https://doi.org/10.26905/idjch.v14i3.11486.

Dewi, Sri Wahyuni, et al. "Independent Supervisory Authority to Protect Social Media Users' Personal Information in Indonesia." *Ius Poenale* 3, no. 1 (2022): 39–48. https://doi.org/10.25041/ip.v3i1.2531.

Ishak, Nurfaika, et al. "Guarantee of Information and Communication Technology Application Security in Indonesia: Regulations and Challenges?" *Audito Comparative Law Journal* 4, no. 2 (2023): 108–117. https://doi.org/10.22219/aclj.v4i2.26098.

Kurniawan, Teguh, Natalia Carolina Simanjuntak, and Sri Uliana Limbong. "Urgensi Pengesahan Rancangan Undang Undang Perlindungan Data Pribadi Dalam Digitalisasi Pelayanan Publik Guna Mewujudkan Smart Government." *Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal* 2, no. 2 (2022): 264–281. https://doi.org/10.15294/ipmhi.v2i2.55032.

Maulida, One, and Hari Utomo. "Pertanggungjawaban Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan Atas Kebocoran Data Pribadi Pengguna Dalam Perspektif Hukum Pidana." *Indonesian Journal of Law and Justice* 1, no. 2 (2023): 1–10. https://doi.org/10.47134/ijlj.v1i2.2011.

Neta, Yulia, Agsel Awanisa, and Melisa. "The Urgency of Establishing Independent Supervisory Authority for Personal Data Protection in Indonesia." *Constitutionale: Jurnal Ilmu Hukum* 3, no. 1 (2022): 19–38. https://doi.org/10.25041/constitutionale.v3i1.2535.

Oktaviani, Shella, Yeremia Juan Dewata, and Aryo Fadlian. "Pertanggung Jawaban Pidana Kebocoran Data BPJS Dalam Perspektif UU ITE." *De Juncto Delicti: Journal of Law* 1, no. 2 (2021): 146–157. https://doi.org/10.35706/djd.v1i2.5732.

Panggabean, Marshanda Vennesa, and Annisa Fitria. "Perlindungan Hukum Data Pribadi Di Indonesia (Kasus Kebocoran Badan Penyelenggara Jaminan Sosial Kesehatan)." *Arus Jurnal Sosial dan Humaniora* 5, no. 2 (2025): 1958–1965. https://doi.org/10.57250/ajsh.v5i2.1487.

Putra, Eduard Awang Maha, Putri Rizkika Bahri, Suci Rizki Ananda, and Baiq Riska Anggi Safitri. "Pelayanan Publik dalam Pelaksanaan Perlindungan Warga Negara melalui Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan." *Indonesia Berdaya* 5, no. 2 (2024): 749–764. https://doi.org/10.47679/ib.2024805.

Roihan Ba'abud, Mohammad Fadel, and Dodik Setiawan Nur Heriyanto. "Application of the Principles of Extraterritorial Jurisdiction Towards Personal Data Breach Committed Cross-Country Borders." *Uti Possidetis: Journal of International Law* 5, no. 1 (2024): 106–137. https://doi.org/10.22437/up.v5i1.28300.

Setyoko, Agus, Moh. Fadly, and Noor Fatimah. "Petugas/Pejabat Pelindungan Data Pribadi dalam Ekosistem Perlindungan Data Pribadi: Indonesia, Uni Eropa dan Singapura." *Business Economic, Communication, and Social Sciences Journal (BECOSS)* 4, no. 2 (2022): 111–120. https://doi.org/10.21512/becossjournal.v4i2.8377.

Soemitro, Dian Purwaningrum, Muhammad Arvin Wicaksono, and Nur Aini Putri. "Penal Provisions in the Personal Data Protection Law: A Comparative Legal Study between Indonesia and Singapore." *SIGn Jurnal Hukum* 5, no. 1 (2023): 155–167. https://doi.org/10.37276/sjh.v5i1.272.

Sorisa, Cinda, Cindi Lusia Kiareni, and Jadiaman Parhusip. "Etika Keamanan Siber: Studi Kasus Kebocoran Data BPJS Kesehatan di Indonesia." *Jurnal Sains Student Research* 2, no. 6 (2024): 586–593. https://doi.org/10.61722/jssr.v2i6.2996.

Wahyudi, Reza, Yogi Prasetyo, and Rena Yulia. "Urgensi Pembentukan Lembaga Pengawas Pelindungan Data Pribadi di Indonesia Berdasarkan Pasal 58 Juncto Pasal 59 dan Pasal 60 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi." *SINERGI: Jurnal Riset Ilmiah* 1, no. 4 (2024): 234–242. https://doi.org/10.62335/8qf44b59.

Wira P., Akhmad Afridho, Fitria Esfandiari, and Wasis. "Juridical Analysis of Legal Protection of Personal Data in terms of Legal Certainty." *Indonesia Law Reform Journal* 3, no. 1 (2023): 96–108. https://doi.org/10.22219/ilrej.v3i1.23840.

Yuspin, Wardah, Trisha Rajput, Abhinayan Basu Bal, Kelik Wardiono, and Absori. "The Regulations of the Supervisory Officer Personal Data Protection-Based Accountability Principle." *Bestuur* 12, no. 1 (2024). https://doi.org/10.20961/bestuur.v12i1.89742.