DOI: 10.46924/jihk.v7i2.385

Examining Indonesian Government Accountability and Mitigation Measures in The 2024 Taxpayer Identification Number Data Breach

Hamzah Haikal Riziq Alwi Alatas[1]* & Gunawan Djajaputra[2]

[1,2] Faculty of Law, Universitas Tarumanagara Jakarta, Indonesia

Correspondence

Hamzah Haikal Riziq Alwi Alatas, Faculty of Law, Universitas Tarumanagara Jakarta, Indonesia, Letjen S. Parman St No.1, RT.6/RW.16, Tomang, Grogol petamburan, West Jakarta City, Jakarta 11440, *e*-mail: hamzah.205210145@stu.ac.id

How to cite

Alatas, Hamzah Haikal Riziq Alwi., & Djajaputra, Gunawan. 2026. Examining Indonesian Government Accountability And Mitigation Measures In The 2024 Taxpayer Identification Number Data Breach. *Jurnal Ilmu Hukum Kyadiren*. *7*(2), 1234-1248. https://doi.org/10.46924/jihk.v7i2.385

Original Article

Abstract

This study examines the Indonesian government's accountability for the 2024 Taxpayer Identification Number (NPWP) data breach and evaluates the implementation of personal data protection obligations under the Personal Data Protection Law (PDP Law). Using a normative legal research method with statutory, conceptual, and case-based approaches, the study finds that the Directorate General of Taxes (DGT) has not fully met its duties as a Personal Data Controller. The large-scale breach, involving more than six million records, reveals weaknesses in access control, Data Protection Impact Assessments (DPIAs), privacy-by-design practices, and breach notification procedures. The PDP Law provides administrative, civil, and criminal liability mechanisms for negligent actors, all of which may be applied cumulatively. The findings indicate a significant gap between legal norms and administrative practice, undermining public trust and limiting the effectiveness of the PDP Law in safeguarding personal data.

Keywords: *Personal Data Protection, NPWP Breach, PDP Law, Government Accountability, Legal Liability.*

Abstrak

Penelitian ini mengkaji pertanggungjawaban pemerintah Indonesia atas kebocoran data Nomor Pokok Wajib Pajak (NPWP) tahun 2024 serta menilai penerapan ketentuan perlindungan data pribadi berdasarkan Undang-Undang Perlindungan Data Pribadi (UU PDP). Dengan metode penelitian hukum normatif melalui pendekatan perundang-undangan, konseptual, dan studi kasus, penelitian ini menemukan bahwa Direktorat Jenderal Pajak (DJP) belum sepenuhnya melaksanakan kewajibannya sebagai Pengendali Data Pribadi. Kebocoran lebih dari enam juta data menunjukkan lemahnya pengawasan akses, implementasi Data Protection Impact Assessment (DPIA), integrasi privacy-by-design, serta pemenuhan kewajiban notifikasi sebagaimana diatur dalam UU PDP. Penelitian ini juga menegaskan bahwa pertanggungjawaban hukum atas kelalaian dapat diterapkan melalui mekanisme administratif, perdata, dan pidana secara kumulatif kepada pengendali data, pemroses data, maupun pihak eksternal. Kesimpulannya, terdapat kesenjangan signifikan antara norma hukum dan praktik administrasi, sehingga fungsi perlindungan UU PDP belum optimal. Diperlukan penegakan hukum yang lebih konsisten dan peningkatan kesiapan kelembagaan agar perlindungan data pribadi masyarakat dapat terjamin.

Kata kunci: *Perlindungan Data Pribadi, Kebocoran NPWP, UU PDP, Pertanggungjawaban Pemerintah, Tanggung Jawab Hukum.*

1. INTRODUCTION

The rapid advancement of information and communication technologies over the past two decades has accelerated digital transformation across nearly all facets of Indonesian society.[1] Economic activities, public services, and tax administration increasingly depend on electronic systems that collect, process, and store personal data on a large scale. According to the latest report from the Indonesian Internet Service Providers Association (APJII), by 2024 Indonesia will have more than 221 million internet users, representing an internet penetration rate of approximately 79.5 percent of the national population.[2] These figures reflect the extensive processing of personal data in digital environments and the growing exposure to risks of misuse and data breaches.

In this context, Indonesia has faced several major incidents of data leakage involving population records, public service databases, and information from strategic economic sectors. One case that drew significant public attention was the alleged 2024 Taxpayer Identification Number (NPWP) breach, in which data belonging to millions of taxpayers—including high-ranking state officials—were reportedly traded on hacking platforms such as Breach Forums, along with other sensitive information such as National Identification Numbers (NIK), home addresses, phone numbers, and email addresses.[3] This incident not only triggered public concern but also raised fundamental questions regarding the extent to which the state and electronic system providers fulfill their obligations to safeguard personal data, particularly tax-related data that is inherently confidential and vital to state finances.

Normatively, the recognition of personal data protection as a legal imperative is grounded in the human rights guarantees of the 1945 Constitution of the Republic of Indonesia.[4] Article 28G paragraph (1) affirms that every person has the right to protection of themselves, their family, their honor, dignity, property, and personal security. The rights to privacy and personal data protection are commonly understood as extensions of these constitutional guarantees. Numerous studies have positioned personal data protection as an essential component of human rights that must be upheld by a state governed by the

[1] Juan Matheus and Ariawan Gunadi, "Pembentukan Lembaga Pengawas Perlindungan Data Pribadi Di Era Ekonomi Digital: Kajian Perbandingan Dengan KPPU," *JUSTISI* 10, no. 1 (2024): 20–35, https://doi.org/https://doi.org/10.33506/jurnaljustisi.v10i1.2757.

[2] Benyamin Maduwu, Nancy Nopeline, and Martin Luter Purba, "Analisis Pengaruh Pengguna Internet Dan Transaksi E-Commerce Terhadap Pertumbuhan Ekonomi Indonesia Tahun 2011-2023," *Jurnal Eknomi Dan Bisnis Islam* 4, no. 3 (2025): 389–405, https://doi.org/10.62668/attariiz.v4i03.1712.

[3] Muhammad Ali, Ni Putu Yundari, and Ahnaf Tsaqif, "Analisis Risiko Keamanan Siber Dalam Transformasi Digital Pelayanan Publik Di Indonesia," *Cosmos: Jurnal Ilmu Pendidikan, Ekonomi, Dan Teknologi* 6, no. 2 (2025): 1–12, https://doi.org/10.7454/jkskn.v6i2.10082.

[4] Pemerintah Republik Indonesia, "Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 Pasal 27 Ayat (2)" (Jakarta: Pemerintah Republik Indonesia, n.d.) Lihat Pasal 28G ayat (1).

rule of law (rechtsstaat). Consequently, the state is required to establish clear, coherent, and effective legal mechanisms to prevent and address violations of citizens' personal data.

Before the enactment of Law No. 27 of 2022 on Personal Data Protection (the PDP Law), Indonesia's regulatory framework for personal data was sectoral and dispersed across multiple statutes, including the Electronic Information and Transactions Law, the Population Administration Law, the Banking Law, and various sector-specific regulations. This fragmented approach resulted in normative gaps and regulatory overlaps, as no overarching framework governed the principles, obligations, and responsibilities of personal data controllers and processors. As a consequence, legal certainty for data subjects—including citizens whose information is administered by state institutions as part of digital public services—remained weak.[5]

To address these deficiencies, the government and the House of Representatives (DPR) enacted the PDP Law in 2022 as Indonesia's first comprehensive data protection legislation. The law defines personal data as information relating to an identified or identifiable individual and underscores its protection as part of safeguarding constitutional rights.[6] It establishes core principles, articulates the rights and obligations of data subjects, regulates the duties of data controllers and processors, outlines data processing and transfer mechanisms, mandates the creation of a supervisory authority, and stipulates administrative, civil, and criminal sanctions for violations. Several scholars regard the PDP Law as a pivotal milestone in Indonesia's data governance landscape, marking a shift toward viewing personal data not merely as an economic asset but also as an object of human rights protection that must be ensured by the state.[7]

Nevertheless, various academic studies suggest that the implementation of the Personal Data Protection Law continues to encounter significant challenges. Research by Asep Mahbub Juanedi, for instance, underscores the persistent ambiguity in several provisions of the law, which may hinder effective enforcement, particularly when assessed against international standards such as the European Union's General Data Protection Regulation (GDPR).[8] Other studies further point to institutional and enforcement-related issues, including the incomplete development of supervisory bodies, limited capacity

[5] Beni Kharisma Arrasuli and Khairul Fahmi, "Perlindungan Hukum Positif Terhadap Kejahatan Penyalahgunaan Data Pribadi," *Unes Journal of Swara Justisia* 7, no. 2 (2023): 369–92, https://doi.org/10.31933/ujsj.v7i2.351.

[6] DPR RI, "Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi," Pub. L. No. 27, 1 (2022).

[7] Shafa Salsabila and Sidi Ahyar Wiraguna, "Pertanggungjawaban Hukum Atas Pelanggaran Data Pribadi Dalam Perspektif Undang-Undang Pelindungan Data Pribadi Indonesia," *Konsensus: Jurnal Ilmu Pertahanan, Hukum Dan Ilmu Komunikasi* 2, no. 2 (2025): 145–57, https://doi.org/10.62383/konsensus.v2i2.736.

[8] Asep Mahbub Junaedi, "Urgensi Perlindungan Data Pribadi Dalam Era Digital: Analisis Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi," *Knowledge Jurnal Inovasi Hasil Penelitian Dan Pengambangan* 5, no. 2 (2025): 247–57, https://doi.org/10.51878/knowledge.v5i2.5269.

among law enforcement personnel, and low levels of personal data literacy among both the public and data managers.

In practice, the obligations placed on personal data controllers and processors under the Personal Data Protection Law require adequate data security and governance measures, including the implementation of technical and organizational safeguards to prevent unauthorized access, loss, or leakage of data. Recent legal scholarship on personal data protection stresses that violations of these obligations constitute serious breaches, as they directly affect public trust in the nation's legal framework and digital governance. In the context of tax data, the Directorate General of Taxes and other parties responsible for managing NPWP information may qualify as data controllers. Accordingly, when a data breach occurs, it becomes essential to examine how their legal liability is constructed—administratively, civilly, and criminally—within the framework of the PDP Law.

From the perspective of victims' rights, the PDP Law enables data subjects to seek the fulfillment of specific entitlements, including the right to obtain information about the breach, the right to update or delete data, and the right to pursue compensation for losses arising from unlawful data processing. However, as noted in several studies, the effectiveness of these remedies depends heavily on the clarity of complaint mechanisms, the capacity of the supervisory authority, and access to dispute resolution processes, including the potential for individual and class-action civil claims. In practice, barriers such as information asymmetry between data controllers and data subjects, high transaction costs associated with filing claims, and the limited number of precedent-setting court decisions often weaken the legal position of data breach victims.

The alleged 2024 Taxpayer Identification Number (NPWP) data leak provides a concrete example and an early test of the effectiveness of the PDP Law as a new legal framework for personal data protection.[9] On one hand, the incident illustrates the urgency of applying core data protection principles—such as lawful processing, data minimization, integrity and confidentiality, and accountability of data controllers—in the management of tax data. On the other hand, it raises legal questions concerning who should bear responsibility when a breach occurs—whether the primary data controller, a third-party processor, or other actors within the data processing chain—and how standards of negligence and duty of care should be assessed within modern cybersecurity and data governance contexts.[10]

[9] Intan Rakhmayanti, "6 Juta Data NPWP Bocor, Kapan Lembaga PDP Hadir?," cnbcindonesia.com, 2024.

[10] Muhammad Akbar Eka Pradana and Horadin Saragih, "Prinsip Akuntabilitas Dalam Undang-Undang Perlindungan Data Pribadi Terhadap GDPR Dan Akibat Hukumnya," *Innovative: Journal Of Social Science Research* 4, no. 4 (2024): 3412–25, https://doi.org/10.31004/innovative.v4i4.13476.

From a legal and political standpoint, the enactment of the PDP Law is viewed as a democratic response to increasing internet penetration and the growing complexity of personal data processing in Indonesia, as well as an attempt to balance individual privacy interests with state and business interests in data utilization. However, without consistent enforcement and clear accountability for violations, including in cases such as the NPWP data leak, the law's objective of protecting and guaranteeing citizens' fundamental rights regarding personal data may not be fully achieved. In light of these issues, this study evaluates the application of personal data protection provisions in the management of NPWP data and examines the forms of legal liability arising from negligence that led to the 2024 data breach. These two focal points form the foundation for assessing the extent to which the current legal framework is capable of providing adequate protection for the public.

2. RESEARCH METHODOLOGY

This study employs a normative legal research method using statutory, conceptual, and case-based approaches. The statutory approach is applied to examine the legal provisions governing personal data protection in Indonesia, particularly Law No. 27 of 2022 on Personal Data Protection, the Electronic Information and Transactions Law, the Population Administration Law, and regulations concerning the confidentiality of tax data. The conceptual approach is used to explore theories of state accountability, principles of personal data protection, the precautionary principle in cybersecurity, and doctrines relevant to data controllers in order to construct the government's legal duties to prevent data breaches. The case-based approach involves an in-depth examination of the 2024 Taxpayer Identification Number (NPWP) data leak as a case study to assess the application of legal norms and the effectiveness of the existing regulatory framework.

Legal materials were obtained through a literature review of primary, secondary, and tertiary sources. Primary materials include statutes and official government documents related to personal data protection. Secondary materials consist of legal scholarship, academic journals, institutional reports, and publications addressing data breaches and public data governance. Tertiary materials comprise legal dictionaries, encyclopedias, and other supporting references. The analysis was conducted qualitatively by interpreting and reconstructing the relationship between legal norms and the facts of the case to answer the two central issues of this study. The findings are presented descriptively and analytically to generate systematic and academically defensible legal conclusions.[11]

[11] Jonaedi Efendi and Johnny Ibrahim, *Metode Penelitian Hukum: Normatif Dan Empiris* (Depok: Prenada Media, 2016).

3. RESULT AND DISCUSION

3.1. The Application of Personal Data Protection Provisions under the PDP Law in the Governance and Security of NPWP Data in Indonesia

The implementation of personal data protection provisions under Law No. 27 of 2022 on Personal Data Protection (PDP Law) in the management of Taxpayer Identification Number (NPWP) data effectively designates the Directorate General of Taxes (DGT) as the Personal Data Controller, as it determines the purposes, scope, and methods of processing taxpayer information.[12] Under the PDP Law, a data controller is not merely the "system owner" but a legal entity mandated to ensure that data processing adheres to personal data protection principles and to citizens' constitutional right to personal protection as guaranteed by Article 28G paragraph (1) of the 1945 Constitution. In this role, the DGT is not only responsible for tax administrative functions but also serves as a central actor in national personal data governance, given that the NPWP functions as a key identifier in nearly all tax-related legal relations.

Although NPWP data may formally fall under the category of general personal data in the PDP Law, it is substantively sensitive because it is linked to additional identifiers such as the National Identity Number (NIK), address, telephone number, and email address, making it possible to construct a complete profile of the data subject. The Tax Administration Law, as amended and strengthened by the HPP Law, imposes strict confidentiality obligations on tax information. Article 34, for example, requires tax officials to maintain the confidentiality of taxpayer data except for specific purposes permitted by law.[13] In this regard, the tax confidentiality regime and the personal data protection regime reinforce one another: tax confidentiality safeguards fiscal interests and public trust, while the PDP Law protects individual privacy and dignity. Thus, an NPWP data leak is not merely a technical breach but a dual failure—both a failure to protect personal data and a failure to uphold tax confidentiality.

Normatively, the PDP Law establishes several core principles of personal data protection that must be observed by Data Controllers, including lawfulness, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability.[14] In the context of NPWP management, the purpose limitation principle requires that tax data be used solely for tax collection or other legally authorized purposes,

[12] Pasal 1 angka 4 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP).

[13] Hizkia Roland Prawyra Sitorus et al., "Tinjauan Hukum Dan Upaya Pencegahan Terhadap Kasus Kebocoran Data NPWP," *Aspirasi: Publikasi Hasil Pengabdian Dan Kegiatan Masyarakat* 3, no. 4 (2025): 14–18, https://doi.org/10.61132/aspirasi.v3i4.1851.

[14] Pasal 3 dan Pasal 4 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP)

and not for commercial activities or undisclosed secondary processing. The data minimization principle obliges the DGT to collect only data that is strictly necessary, while the accountability principle requires the DGT to demonstrate concrete evidence of compliance, such as records of processing activities, internal policies, and audit documentation.

The application of these principles should be reflected in the design, development, and operation of tax information systems. The PDP Law endorses a privacy-by-design and privacy-by-default approach, meaning that data protection must be embedded from the earliest stages of system development rather than added retroactively. For the DGT, this requires that every tax application—such as e-Registration, e-Filing, e-Invoice, and the NIK–NPWP integration—be designed from the outset with defined access controls, encryption mechanisms, anonymization or pseudonymization where appropriate, and logging features that enable detailed tracking of data access.[15] If these systems are developed solely with functional considerations in mind, such as usability and processing speed, without fully integrating data protection principles, then normatively the DGT cannot be considered to have fulfilled its obligations as a Data Controller.

The clearest obligation relating to security is set out in Article 39 of the Personal Data Protection Law, which requires Data Controllers to implement appropriate technical and organizational measures to safeguard personal data from unauthorized processing, loss, destruction, or unlawful disclosure. In information security practice, technical measures may include database encryption, the use of intrusion detection and prevention systems (IDPS), network segmentation, vulnerability management, and periodic penetration testing. Organizational measures include written security policies, incident response procedures, routine employee training, disciplinary mechanisms for access misuse, and the integration of data protection into institutional risk management frameworks. A Data Controller's inability to demonstrate adequate implementation of these technical and organizational measures may give rise to a finding of negligence in meeting the standard of care required under the Personal Data Protection Law.

The law also introduces the Data Protection Impact Assessment (DPIA) as a risk management tool for high-risk processing activities, including large-scale and systematic data processing.[16] The processing of national tax data covering hundreds of millions of individuals falls squarely into this high-risk category, making the Directorate General of

[15] Wyanda Kinanti Syauqi Ramadhani and Sidi Ahyar Wiraguna, "Implementasi Pelindungan Data Pribadi Dalam Sistem Informasi Pada Perusahaan Jasa Keuangan," *Appisi: Perspektif Administrasi Publik Dan Hukum* 2, no. 2 (2025): 158–75, https://doi.org/10.62383/perspektif.v2i2.248.

[16] Filal Khair and Sidi Ahyar Wiraguna, "Data Protection Impact Assessment (DPIA) Sebagai Instrumen Kunci Menjamin Kepatuhan UU PDP 2022 Di Indonesia," *Politika Progresif Jurnal Hukum, Politik Dan Humaniora* 2, no. 2 (2025): 246–54, https://doi.org/10.62383/progres.v2i2.1821.

Taxes (DGT) doctrinally obligated to conduct DPIAs on a regular and structured basis. The DPIA serves to identify potential risks—such as the possibility of mass data leaks—assess their impact on data subjects' rights, and develop mitigation measures before such risks materialize. Recent scholarship indicates that the DPIA plays a critical role in aligning international standards, such as the GDPR, with Indonesia's regulatory and institutional context, including within the public sector. The occurrence of an NPWP data breach on a massive scale suggests a fundamental weakness in this risk assessment process, whether due to the absence of a DPIA, deficiencies in its implementation, or inadequate follow-up of its findings.

Beyond technical considerations, the implementation of the PDP Law in the management of NPWP data also depends on institutional governance. The law requires Data Controllers to appoint personal data protection officers (DPOs) under certain conditions and to maintain records of data processing activities. For government institutions, this necessitates a dedicated structure responsible for overseeing data protection across organizational units, rather than relegating data security to IT divisions alone. Effective coordination with the Ministry of Communication and Informatics, the National Cyber and Crypto Agency (BSSN), and, prospectively, the Personal Data Protection Authority to be established by the President is essential for harmonizing cybersecurity and personal data protection standards within the government. Institutional shortcomings—such as the absence of an effective DPO or an unclear chain of command for incident response—significantly undermine the quality of PDP Law implementation in the tax sector.

With respect to the 2024 Taxpayer Identification Number (NPWP) breach, several reports indicate that approximately 6 to 6.6 million NPWP records—along with corresponding National Identification Numbers (NIK), addresses, phone numbers, and email addresses—were sold on the Breach Forums hacking platform for roughly USD 10,000.[17] The publicly circulated sample data reportedly included information belonging to the President and several high-ranking state officials. This incident shows that the system managing NPWP data permitted large-scale exfiltration, something that, under contemporary information security standards, should be difficult if data segmentation, strict access controls, and robust anomaly detection mechanisms are properly implemented. From the standpoint of PDP Law compliance, a breach of this magnitude strongly indicates that security obligations (Article 39) and risk management duties (Article 34) were not carried out in accordance with the level of risk involved.

[17] Novina Putri Bestari, "NPWP Jokowi, Gibran, Dan 6 Juta Data Pajak Warga RI Dijual Di Internet," cnbcindonesia.com, 2024.

The government's initial response—stating that the Directorate General of Taxes (DGT) was conducting a "technical investigation" into the alleged breach—may be understood as part of incident management, but is insufficient from the perspective of the PDP Law. Article 46 requires Data Controllers to notify affected data subjects of any personal data breach within 3 × 24 hours of its discovery, providing at minimum a description of the affected data and the steps taken in response. In the NPWP case, there is no strong indication that millions of affected taxpayers received adequate individual notification, nor is there evidence of a systematic public communication effort outlining the risks and recommended mitigation steps. This lack of structured notification may be interpreted as an indication that the reporting and transparency obligations mandated under the PDP Law have not been fully observed.

Compared with EU practice under the GDPR—which requires breach notifications to supervisory authorities and, in many cases, to data subjects within 72 hours—the Indonesian government's response in this case remains minimal and defensive.[18] In numerous jurisdictions, breach notification is regarded as an element of accountability and remediation rather than a mere administrative formality. When the government opts to issue only general statements without providing meaningful information to affected individuals, the PDP Law's role as a mechanism for enforcing data subjects' rights is substantially weakened. In effect, although Indonesia's data protection framework has moved closer to international standards, its implementation in the NPWP case reveals a considerable gap between the legal framework and administrative practice.

3.2. Legal Accountability for Negligent Actors in the 2024 NPWP Data Breach Incident

Legal liability for negligent actors in the 2024 NPWP data breach must be assessed based on the liability framework established under the PDP Law, which encompasses administrative, civil, and criminal dimensions. Within data protection law, negligence refers not only to overtly unlawful conduct but also to a failure to meet the duty of care in safeguarding personal data. As emphasized by Sinta Dewi, negligence by data controllers constitutes a serious violation because personal data should not be regarded merely as administrative information but as an object of human rights protection.[19] Accordingly, any negligence in the governance of NPWP data security carries clear legal implications. From

[18] Ilman Maulana Kholis, "Perlindungan Data Pribadi Dan Keamanan Siber Di Sektor Perbankan: Studi Kritis Atas Penerapan UU PDP Dan UU ITE Di Indonesia," *Staatsrecht Jurnal Hukum Kenegaraan Dan Politik Islam* 4, no. 2 (2024): 275–300, https://doi.org/10.14421/t5sfe747.

[19] Severius Waruwu and Amelia Anggriany Siswoyo, "Data Pribadi Sebagai Aset Bisnis: Sinergi Hukum Rahasia Dagang Dan Perlindungan Data," *Lex Lectio Law Journal* 3, no. 2 (2024): 118–29, https://doi.org/10.61715/jll.v3i2.118.

the perspective of administrative liability, the PDP Law authorizes supervisory authorities to impose sanctions such as written warnings, temporary suspension of data processing activities, and administrative fines. These sanctions are generally applied in cases involving violations of data security obligations, failures to provide breach notifications, or inadequate implementation of core data protection principles. In the context of state administrative law, administrative liability functions as a mechanism to discipline public institutions and ensure compliance with applicable legal standards.[20] If the Directorate General of Taxes (DGT) or a third party is found negligent in implementing required technical and organizational security measures, they may be subject to administrative sanctions within the authority of the data protection regulator.

Civil liability, meanwhile, allows data subjects to pursue compensation when they suffer harm as a result of a data breach. Such harm may include material or immaterial losses, including identity theft, fraud facilitated by stolen data, or diminished personal security. Civil liability for data breaches often requires the application of strict liability principles or, at minimum, a shifted burden of proof, given the difficulty victims face in demonstrating causation due to significant information asymmetries. In the NPWP case, the potential for class action litigation is particularly relevant due to the large number of affected individuals. Where the DGT or its contracted vendors have failed to protect data adequately, they may incur civil liability under Article 39 of the PDP Law.[21]

Within the criminal liability regime, the PDP Law provides sanctions for two categories of offenders: individuals who unlawfully access, obtain, or disclose personal data, and data controllers or processors whose negligence results in large-scale data breaches. This dual approach aligns with Bruce Schneier's view that unlawful acts involving personal data constitute violations of individual security rather than mere technical errors.[22]

If the NPWP breach stems from a hacking incident, the perpetrators may be prosecuted for unauthorized access. However, when the breach arises from institutional negligence in implementing adequate security measures, criminal liability may also extend to the data controller. Corporate criminal liability may likewise apply when vendors or third

[20] Silawati Dayang G, Sandra Putri Olivia Lase, and Anandya Kyara Putri K, "Urgensi Pembentukan Lembaga Pengawas Dalam Pembaharuan Hukum Perlindungan Data Pribadi Menurut Undang-Undang PDP," *Locus Journal of Academic Literature Review* 4, no. 2 (2025): 106–13, https://doi.org/10.56128/ljoalr.v4i2.433.

[21] Muhammad Ilham Mahrudin Zamzam, Rofanda Mina Arsyada, and Nadya Eka Amalia Al'Azza, "Keabsahan Hubungan Kontraktual Secara Elektronik Dalam E-Commerce Dan Pertanggungjawaban Hukum Atas Kebocoran Data Pribadi Pengguna," *Jurnal Suara Hukum* 5, no. 2 (2023): 130–48, https://doi.org/10.26740/jsh.v5n2.p130-148.

[22] Iskandar et al., *Cyber Smart Campus: Cakap Digital & Aman Siber* (Jambi: PT. Sonpedia Publishing Indonesia, 2025), hal. 178.

parties involved in NPWP processing fail to meet the security requirements stipulated in data processing agreements, potentially resulting in shared liability.[23]

Beyond the doctrinal aspects, legal liability in NPWP data breach cases carries political and ethical implications. The state, as the holder of constitutional obligations, must ensure the protection of its citizens' personal data, and failure to do so weakens institutional legitimacy and public trust. This reflects the principle of the rechterstaat, which requires the government not only to comply with the law but also to actively safeguard individual rights. Because NPWP data collection is mandatory and citizens cannot opt out, the state bears an even greater responsibility to ensure its protection. Legal accountability, therefore, must operate as a means of restoring public trust rather than a procedural formality.

In light of the accountability framework described above, it can be concluded that negligent actors involved in the 2024 NPWP data breach may be held liable through administrative, civil, and criminal mechanisms. These forms of liability are not mutually exclusive but operate cumulatively. Their effectiveness, however, depends largely on the performance of supervisory authorities, the good faith of government institutions, and the willingness to enforce the law even when state entities are implicated. Without consistent enforcement, data breaches will persist, and the PDP Law risks functioning merely as a declaratory norm that offers no substantive protection to the public.

4. CONCLUSION

Based on the analysis of the application of personal data protection provisions in the management of Taxpayer Identification Numbers (NPWP), it can be concluded that the Directorate General of Taxes (DGT) has not yet fully implemented the Personal Data Protection Law (PDP Law). Although the PDP Law establishes a comprehensive framework encompassing personal data protection principles, risk management, technical security, institutional governance, and breach notification obligations, its practical implementation remains incomplete. The 2024 NPWP data breach revealed deficiencies in several key areas, including insufficient access oversight, ineffective deployment of the Data Protection Impact Assessment (DPIA), and limited incorporation of privacy-by-design principles in the development of tax systems. In addition, the notification obligation to data subjects under Article 46 of the PDP Law was not effectively carried out, preventing the public from obtaining essential information needed for mitigation. These issues reflect

[23] Andrew Ardiyanto Dachlan et al., "Pertanggungjawaban Hukum Pemerintah Dalam Kebocoran Data Pribadi Pada Penyelenggaraan Pusat Data Nasional," *Jurnal Hukum Samudra Keadilan* 20, no. 1 (2025): 109–24, https://doi.org/10.33059/jhsk.v20i1.11279.

a substantial gap between the legal framework and its actual implementation within the DGT.

From a legal accountability standpoint, the PDP Law provides three mechanisms for holding negligent actors responsible: administrative, civil, and criminal. These avenues may be applied cumulatively to data controllers, data processors, and external actors such as hackers. Administrative liability is necessary to enforce compliance within public institutions; civil liability grants victims the opportunity to seek compensation for material and immaterial harm; and criminal liability underscores that violations of personal data protection constitute offenses that jeopardize individual and public security. However, the effectiveness of these mechanisms depends on institutional preparedness, including the operationalization of the Personal Data Protection Agency as an independent oversight body. Without consistent enforcement and firm accountability, personal data protection efforts in Indonesia risk remaining largely symbolic and failing to provide meaningful protection for citizens.

REFERENCES

Journals

Ali, Muhammad, Ni Putu Yundari, dan Ahnaf Tsaqif. "Analisis Risiko Keamanan Siber dalam Transformasi Digital Pelayanan Publik di Indonesia." *Cosmos: Jurnal Ilmu Pendidikan, Ekonomi, dan Teknologi* 6, no. 2 (2025): 1–12. https://doi.org/10.7454/jkskn.v6i2.10082.

Arrasuli, Beni Kharisma, dan Khairul Fahmi. "Perlindungan Hukum Positif Terhadap Kejahatan Penyalahgunaan Data Pribadi." *Unes Journal of Swara Justisia* 7, no. 2 (2023): 369–92. https://doi.org/10.31933/ujsj.v7i2.351.

Dachlan, Andrew Ardiyanto, Alya Nabila, Nabilatul Alimah Putri, dan Nabilah Nurmasitha. "Pertanggungjawaban Hukum Pemerintah Dalam Kebocoran Data Pribadi Pada Penyelenggaraan Pusat Data Nasional." *Jurnal Hukum Samudra Keadilan* 20, no. 1 (2025): 109–24. https://doi.org/10.33059/jhsk.v20i1.11279.

G, Silawati Dayang, Sandra Putri Olivia Lase, dan Anandya Kyara Putri K. "Urgensi Pembentukan Lembaga Pengawas dalam Pembaharuan Hukum Perlindungan Data Pribadi Menurut Undang-Undang PDP." *Locus Journal of Academic Literature Review* 4, no. 2 (2025): 106–13. https://doi.org/10.56128/ljoalr.v4i2.433.

Junaedi, Asep Mahbub. "Urgensi Perlindungan Data Pribadi Dalam Era Digital:

Analisis Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi." *Knowledge Jurnal Inovasi Hasil Penelitian dan Pengambangan* 5, no. 2 (2025): 247–57. https://doi.org/10.51878/knowledge.v5i2.5269.

Khair, Filal, dan Sidi Ahyar Wiraguna. "Data Protection Impact Assessment (DPIA) sebagai Instrumen Kunci Menjamin Kepatuhan UU PDP 2022 di Indonesia." *Politika Progresif Jurnal Hukum, Politik dan Humaniora* 2, no. 2 (2025): 246–54. https://doi.org/10.62383/progres.v2i2.1821.

Kholis, Ilman Maulana. "Perlindungan Data Pribadi dan Keamanan Siber di Sektor Perbankan: Studi Kritis atas Penerapan UU PDP dan UU ITE di Indonesia." *Staatsrecht Jurnal Hukum Kenegaraan dan Politik Islam* 4, no. 2 (2024): 275–300. https://doi.org/10.14421/t5sfe747.

Maduwu, Benyamin, Nancy Nopeline, dan Martin Luter Purba. "Analisis Pengaruh Pengguna Internet dan Transaksi E-Commerce Terhadap Pertumbuhan Ekonomi Indonesia Tahun 2011-2023." *Jurnal Eknomi dan Bisnis Islam* 4, no. 3 (2025): 389–405. https://doi.org/10.62668/attariiz.v4i03.1712.

Matheus, Juan, and Ariawan Gunadi. "Pembentukan Lembaga Pengawas Perlindungan Data Pribadi Di Era Ekonomi Digital: Kajian Perbandingan Dengan KPPU." *JUSTISI* 10, no. 1 (2024): 20–35. https://doi.org/https://doi.org/10.33506/jurnaljustisi.v10i1.2757.

Pradana, Muhammad Akbar Eka, dan Horadin Saragih. "Prinsip Akuntabilitas dalam Undang-Undang Perlindungan Data Pribadi Terhadap GDPR dan Akibat Hukumnya." *Innovative: Journal Of Social Science Research* 4, no. 4 (2024): 3412–25. https://doi.org/10.31004/innovative.v4i4.13476.

Ramadhani, Wyanda Kinanti Syauqi, dan Sidi Ahyar Wiraguna. "Implementasi Pelindungan Data Pribadi dalam Sistem Informasi pada Perusahaan Jasa Keuangan." *Appisi: Perspektif Administrasi Publik dan Hukum* 2, no. 2 (2025): 158–75. https://doi.org/10.62383/perspektif.v2i2.248.

Salsabila, Shafa, dan Sidi Ahyar Wiraguna. "Pertanggungjawaban Hukum atas Pelanggaran Data Pribadi dalam Perspektif Undang-Undang Pelindungan Data Pribadi Indonesia." *Konsensus: Jurnal Ilmu Pertahanan, Hukum dan Ilmu Komunikasi* 2, no. 2 (2025): 145–57. https://doi.org/10.62383/konsensus.v2i2.736.

Sitorus, Hizkia Roland Prawyra, Dewi Pika Lumbanbatu, Daniel David Sidebang, Dules Ery Pratama, dan Risky Sakti Lumban Gaol. "Tinjauan Hukum dan Upaya

Pencegahan terhadap Kasus Kebocoran Data NPWP." *Aspirasi: Publikasi Hasil Pengabdian dan Kegiatan Masyarakat* 3, no. 4 (2025): 14–18. https://doi.org/10.61132/aspirasi.v3i4.1851.

Waruwu, Severius, dan Amelia Anggriany Siswoyo. "Data Pribadi Sebagai Aset Bisnis: Sinergi Hukum Rahasia Dagang dan Perlindungan Data." *Lex Lectio Law Journal* 3, no. 2 (2024): 118–29. https://doi.org/10.61715/jll.v3i2.118.

Zamzam, Muhammad Ilham Mahrudin, Rofanda Mina Arsyada, dan Nadya Eka Amalia Al'Azza. "Keabsahan Hubungan Kontraktual Secara Elektronik Dalam E-Commerce Dan Pertanggungjawaban Hukum Atas Kebocoran Data Pribadi Pengguna." *Jurnal Suara Hukum* 5, no. 2 (2023): 130–48. https://doi.org/10.26740/jsh.v5n2.p130-148.

Books

Efendi, Jonaedi, dan Johnny Ibrahim. *Metode Penelitian Hukum : Normatif dan Empiris*. 1 ed. Jakarta: Prenadamedia Group, 2016.

Iskandar, Dedy Dwi Putra, Alifa Irna Yasin, dan Khairan. *Cyber Smart Campus: Cakap Digital & Aman Siber*. Jambi: PT. Sonpedia Publishing Indonesia, 2025.

Regulations

DPR RI. Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi, Pub. L. No. 27, 1 (2022). https://jdih.setkab.go.id/PUUdoc/176837/Salinan_UU_Nomor_27_Tahun_2022.pdf.

Pemerintah Republik Indonesia. "Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 Pasal 27 Ayat (2)." Jakarta: Pemerintah Republik Indonesia, n.d.

Webpages

Bestari, Novina Putri. "NPWP Jokowi, Gibran, dan 6 Juta Data Pajak Warga RI Dijual di Internet." cnbcindonesia.com, 2024. https://www.cnbcindonesia.com/tech/20240918175353-37-572797/npwp-jokowi-gibran-dan-6-juta-data-pajak-warga-ri-dijual-di-internet.

Rakhmayanti, Intan. "6 Juta Data NPWP Bocor, Kapan Lembaga PDP Hadir?" cnbcindonesia.com, 2024. https://www.cnbcindonesia.com/tech/20241001183527-37-576176/6-juta-data-npwp-bocor-kapan-lembaga-pdp-hadir.