OPEN ACCESS

LAW RESEARCH
Review Quarterly

Law Research Review Quarterly is a **Journal for Law, Justice, and Crime in Indonesia and Southeast Asia**. The Journal is a peer-reviewed journal published by Faculty of Law Universitas Negeri Semarang, Indonesia. The Journal published quarterly on February, May, August, and November. ISSN 2716-3415 (Online)
Online at https://journal.unnes.ac.id/journals/snh

Legal Protection for Biznet Customers for Data Leak from the Perspective of Law Number 27 of 2022

Romadona Putri Pertiwi
Universitas Negeri Semarang, Semarang, Indonesia
romadonaputri@unnes.students.ac.id

Ratih Damayanti
Universitas Negeri Semarang, Semarang, Indonesia
ratihdamayanti@mail.unnes.ac.id

Abstract

The incident of PT Biznet Networks' data leak in March 2024 which impacted more than 380,000 customer data became the starting point of this study. This study aims to analyze two main problems: (1) legal protection and Biznet's responsibility for the leakage of customers' personal data based on Law Number 27 of 2022 concerning Personal Data Protection; and (2) critical evaluation of the Personal Data Protection Law in the case of Biznet data leak. This study applies a normative legal approach, supported by a regulatory analysis and a conceptual perspective. The findings of the study reveal that Biznet customers are positioned as Personal Data Subjects who receive layered protection from the Personal Data Protection Law, Consumer Protection Law, and Civil Code. Preventive protection is realized through a series of obligations imposed on data controllers, while repressive protection is available through three cumulative channels: administrative, civil, and criminal. Biznet is juridically positioned as the Personal Data Controller who bears the burden of reverse proof and non-delegable liability. The effectiveness of this legal framework is still constrained by the lack of independent supervisory institutions as mandated.

KEYWORDS
Legal Protection; Personal Data; **Cybercrime**

Introduction

Technological advances that are so significant have caused fundamental transformations in various aspects of modern human life. The era of digitalization has changed the pattern of human interaction in communicating, working, making transactions, and obtaining information.[1] The Internet, which serves as the main foundation of the digital revolution, has now become essentially integrated into the daily routines of Indonesians. Based on the 2024 Indonesian Internet Penetration Survey published by the Indonesian Internet Service Providers Association (APJII) on January 31, 2024, Indonesians who access the internet amount to 221,563,479 people, or an estimated 79.5% of the country's total population.[2] The increase in internet penetration shows the increasing dependence of people on digital services. This trend carries double implications, on the one hand driving the growth of the digital economy, on the other hand enlarging the surface of attacks on citizens' personal data.

In carrying out its services, Internet Service Providers (ISPs) such as PT Biznet Networks have access to their customers' personal data, ranging from full names, domiciles, Population Identification Number (NIK), Taxpayer Identification Number (NPWP), mobile phone numbers, emails, to data related to internet usage patterns. Thus, ISPs are positioned as controllers and processors of personal data, so responsibility for the security and confidentiality of such data becomes very crucial. In addition to system and technology factors, human factors such as workload and work stress can also affect the level of accuracy and compliance in data management, which

[1] Ratih Damayanti et al., "Transforming Taxation: Unlocking Efficiency and Resilience Through Digitalization," *The Indonesian Journal of International Clinical Legal Education* 6, no. 4 (2024): 453–76.
[2] APJII (Indonesian Internet Service Providers Association, "Indonesian Internet Penetration Survey 2024" (Jakarta, 2024).

ultimately has the potential to increase the risk of data leaks.[3] In fact, on March 10, 2024, the incident really happened to Biznet, resulting in approximately 380,000 customer information allegedly spread to the *dark web*, which includes names, email addresses, NIK, NPWP, phone numbers, and domiciles.[4]

It doesn't stop there. At the end of March 2024, there were again 154,091 data leaks in the accounts of Biznet Gio Cloud service users. Cybersecurity expert Teguh Aprianto validated the leaked data by randomly testing 2,000 samples and found that 99.65% of the data was declared valid and registered actively in the Biznet Gio system. The exposed data includes cloud infrastructure information, including IP addresses, usernames, and access credentials, which has the potential to cause multiple losses to corporate customers using the service.[5]

Both incidents received a response from the Ministry of Communication and Information Technology (Kemenkominfo). The Ministry of Communication and Information sent a clarification letter to Biznet and asked the company to explain the facts and scope of the leak.[6] Semuel Abrijani Pangerapan, as the Director General of Informatics Applications of the Ministry of Communication and Informatics, expressly revealed that the owner of data that has been leaked can file a civil lawsuit against companies that are proven to have been negligent in maintaining the security of their customers' personal data, based on the rules of the Personal Data Protection Law.

Throughout 2023, the State Cyber and Cryptography Agency (BSSN) recorded 403,990,813 traffic anomalies or cyberattack attempts targeting

[3] Ratih Damayanti and Erwin Dyah Nawawinetu, "Determinant Factors of Work Stress among Teaching and Non Teaching Staff in Indonesia," *Indian Journal of Public Health Research & Development* 10, no. 3 (2019): 307–11.
[4] Liputan6.com, "380 Thousand Biznet User Data Allegedly Leaked on the Dark Web, Perpetrators Called Employees," 2024, https://www.liputan6.com/tekno/read/5547088/.
[5] CNN Indonesia, "Biznet Customer Data Allegedly Leaked Again, Experts Call It Valid," 2024, https://www.cnnindonesia.com/teknologi/20240325135001-192-1078671/data-pelanggan-biznet-diduga-kembali-bocor-ahli-sebut-valid.
[6] Tirto.id, "Kominfo Asks Biznet to Clarify Customer Data Leaks," 2024, https://tirto.id/kominfo-minta-biznet-klarifikasi-soal-kebocoran-data-pelanggan-gWVv.

various electronic systems throughout Indonesia.[7] This figure reflects the escalation of cyber threats that not only target government agencies, but also penetrate the private sector, including internet service providers. The background of this dangerous situation prompted the birth of Law Number 27 of 2022 concerning Personal Data Protection, which was inaugurated starting October 17, 2022 and will be effective in October 2024. Before the regulation was fully active, existing provisions such as Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE Law) and other sectoral regulations were considered insufficient to overcome the complexity of risks to personal data in the era of digital technological advancement. This underscores that data leaks are not just a technical issue, but an urgent legal challenge that is directly related to ensuring security for data owners.

Theoretically, the study of legal protection and legal accountability in the Indonesian legal system has been based on a number of basic concepts. Rahardjo (2000) defines the idea of legal protection as measures to guarantee basic rights that are disturbed by the actions of other parties.[8] Hadjon (2011) classifies legal protection into preventive and repressive dimensions which are the central analytical framework of this research.[9] Fuady (2002) explained the construction of legal responsibility in the *civil law system* as the basis for the accountability of data controllers.[10]

A number of previous studies have examined the protection of personal data in various contexts of electronic system operators. Wulandari and Wiraguna (2025) concluded that the PDP Law provides a basis for protection for users as data subjects, although its implementation is still constrained by weak internal security systems and the absence of

[7] BSSN (State Cyber and Cryptography Agency), "Indonesia's Cybersecurity Landscape 2023" (Jakarta, 2023).
[8] Satjipto Rahardjo, "Legal Sciences, PT," *Citra Aditya Bakti, Bandung*, 2000.
[9] Philipus M. Hadjon, *Introduction to Indonesian Administrative Law*, 1st Edition (Yogyakarta: Gadjah Mada University Press, 2011).
[10] Munir Fuady, *Unlawful Conduct: A Contemporary Approach* (Bandung: PT Citra Aditya Bakti, 2002).

notifications in accordance with the provisions.[11] Wiraguna (2025) emphasized that the implementation of data controller obligations is still faced with serious obstacles in the form of complexity in proving causality and inadequate regulatory supervision.[12] Maharani and Prakoso (2024) added that electronic system operators' non-compliance with data protection obligations carries the consequences of administrative sanctions that require continuous monitoring.[13] Yanti (2025) highlighted the urgency of harmonization between the PDP Law and the Civil Code so that the construction of civil liability due to data leaks can run effectively.[14] Hasian and Fitria (2025) show that the responsibility of telecommunication service providers for customer data leakage can be carried out through three cumulative mechanisms: administrative, civil, and criminal.[15]

Although previous studies have made significant contributions, there are some academic gaps that need to be filled. First, most of the studies focused on *the e-commerce* and mobile telecommunications sectors, not specifically examining fiber-optic ISPs in the context of actual data leak incidents. Second, there has not been a study that integrates the normative analysis of the PDP Law with concrete case studies after the effective enactment of the law in October 2024. Third, the construction of data controller liability based on the PDP Law, especially the reverse burden of proof mechanism and *non-delegable liability* in the context of ISPs, has not been extensively analyzed in depth. Fourth, the study of the interaction

[11] Devi Wulandari and Sidi Ahyar Wiraguna, "Legal Protection for Tokopedia Application Users from Personal Data Leakage from the Perspective of Law Number 27 of 2022," *Journal of Legal and Public Policy Studies| E-ISSN: 3031-8882* 2, no. 2 (2025): 1321–25.
[12] Sidi Ahyar Wiraguna, "Legal Responsibility of E-Commerce Platforms for Personal Data Leakage in the Perspective of Law No. 27 of 2022," *Journal of Legal and Public Policy Studies| E-ISSN: 3031-8882* 2, no. 2 (2025): 1089–96.
[13] Rista Maharani and Andria Luhur Prakoso, "Protection of Consumer Personal Data by Electronic System Operators in Digital Transactions," *USM Law Review Journal* 7, no. 1 (2024): 333–47.
[14] Musrika Yanti, "Analysis of Civil Liability in Data Leaks: Synchronization of the Personal Data Protection Law and the Civil Code," *Journal of Social Sciences and Humanities* 1, no. 4 (2025): 1539–49.
[15] Diah Putri Hasian and Annisa Fitria, "Telkomsel's Responsibility for the Leak of Indihome Users' Personal Data," *Journal of Social and Humanities* 5, no. 2 (2025): 1812–21.

between the PDP Law and other legal instruments such as the Civil Code and the UUPK in one integrated protection framework is still limited.

From the previous explanation, this study focuses on two main problems: (1) how to protect Biznet's legal and responsibility for the leakage of customers' personal data based on Law Number 27 of 2022 concerning Personal Data Protection; and (2) how to critically evaluate the protection of personal data in the case of Biznet data leak. The purpose of this study is to examine Biznet's legal protection and responsibility and evaluate the protection of sensitive individual data related to the event of unauthorized data disclosure. Furthermore, based on the formulation of the problem, theoretically this study is anticipated to be able to contribute significantly to the improvement of the data controller accountability doctrine in the Indonesian ISP industry. In practical terms, this study provides a systematic legal map for customers who want to demand legal accountability for the leakage of their personal data.

Methods

This study utilizes a *normative legal research* approach, which is a study that focuses on secondary sources of literature or data used to identify legal norms, legal principles, and various doctrines in the field of law that are relevant to the issues at hand (Soekanto and Mamudji, 2001; Marzuki, 2005). This method is used because this research prioritizes the examination of the current positive legal norms, the interpretation of their meaning, and their implementation in practice for concrete cases of Biznet data leaks.

The approach method used includes two main types. The initial approach is in the form *of a statute approach* or legislative analysis, which involves the study of various relevant legal rules such as Law Number 27 of 2022, the Civil Code, and Law Number 8 of 1999 concerning Consumer Protection. The next approach is to deconstruct the theory of legal protection according to Hadjon, the theory of legal responsibility in the style

of Fuady, and the idea of personal data law from a comparative perspective with the European Union's GDPR.

Legal data is obtained through *library research* which includes: (1) primary legal materials in the form of laws and regulations; (2) secondary legal materials in the form of scientific literature and indexed law journals; and (3) tertiary legal materials in the form of dictionaries and legal encyclopedias. The Biznet case is used as non-legal factual material for contextualizing normative analysis. The analysis is carried out in a qualitative juridical manner through grammatical, systematic, and teleological interpretation to obtain argumentative conclusions (Fajar and Achmad, 2010). This study does not include an empirical analysis of the implementation of the PDP Law in court practice, considering the lack of court decisions that specifically apply the provisions of the PDP Law in data leak disputes.

Result and Discussion

1. Legal Protection and Responsibility of Biznet for Leakage of Customer Personal Data

1.1. Legal Protection for Biznet Customers

Based on Article 1 number 2 of the PDP Law, Biznet customers whose data is leaked automatically obtain juridical status as the subject of personal data entitled to full protection. The Biznet data leak in March 2024 allegedly included around 380 thousand customer data, including NIK, NPWP, name, address, phone number, and email address.[16] NIK and NPWP include personal information that allows direct identification of individuals in accordance with Article 4 of the PDP Law. This carries high risks, including identity fraud, fictitious account openings, and illegal access to digital financial services. This

[16] Liputan6.com, "380 thousand Biznet user data is suspected to have been leaked on the dark web, the perpetrators are called employees."

condition shows the importance of the existence of a legal protection mechanism that is able to ensure security and restoration of rights for personal data owners.[17]

Theoretically, Satjipto Rahardjo defines legal protection as an effort to protect the rights of a person who has suffered violations or losses due to the actions of other parties.[18] Philipus M. Hadjon then emphasized the concept by dividing it into two forms. Preventive protection, namely the prevention of violations through normative obligations before losses occur, and repressive protection, namely post-violation recovery through sanctions and compensation.[19] These two forms of protection should run in a balanced manner and reinforce each other in handling personal data leak cases. Legal protection efforts aim to protect the honor, self-esteem, and fundamental rights inherent in every legal subject based on laws and regulations, so as to be able to ward off arbitrary acts.

The PDP Law requires data controllers to carry out a number of proactive obligations. Article 31 requires the documentation of all processing activities in the Records of Processing Activities (ROPA). This creates a structural incentive for Biznet to build auditable data governance. In line with that, Article 40 of the PDP Law requires the implementation of adequate technical and organizational measures to ensure the security of personal data. In practice, international cybersecurity standards operationalize these obligations through, among others, data encryption, the application of *the least privilege* principle, and monitoring through *Security Information and Event Management* (SIEM). Failure to implement these measures is a strong indication of technical negligence that can be held accountable. In

[17] Fidia Wati Khairani Alawiyah Matondang, Tia Handani, Annisa Handayani, "Business Ethics in the Protection of Consumer Personal Data in the Digital Business Era: In a Literature Study," *Journal of Information Systems and Business Management Publications* 4 (2025), https://doi.org/https://doi.org/10.55606/jupsim.v4i3.5508.
[18] Rahardjo, "Legal Science, PT."
[19] Philipus M. Hadjon, *Introduction to Indonesian Administrative Law*.

addition, the implementation of *Data Protection Impact Assessment* (DPIA) is required based on Article 34 of the PDP Law for data controllers whose processing has the potential to pose a high risk to the rights of data subjects. As an internet service provider with millions of active customers, Biznet is required to run DPIA on a regular basis, the absence of DPIA is a strong indicator of systemic deficiencies in the company's compliance program.[20]

An important aspect that often goes unnoticed is the character of the data security obligation in Article 46 of the PDP Law. This provision can be interpreted as *an obligation of result* rather than an *obligation of means*. Consequently, the occurrence of data leaks has basically become evidence of the failure to fulfill these obligations prima *facie*.[21] The data controller can only be relieved of liability if it succeeds in proving the existence of force *majeure* or external factors that cannot be controlled, as known in the construction of civil liability based on Articles 1244–1245 of the Civil Code. The phrase "obliged to keep" in Article 36 grammatically and telelogically supports this interpretation. In the same framework, Article 46 of the PDP Law requires data controllers to provide written announcements to data owners and supervisory authorities no later than 3×24 hours after the incident is detected, with content that includes the identity of the controller, data that has been leaked, the time and mechanism of the incident, the possible risks that have arisen, and the handling efforts that have been made. In the case of Biznet, the company's official response only emerged after pressure from the mass media rather than through proactive notifications to customers. Reactive patterns have the potential to violate Article 47, but they also exacerbate customer losses by eliminating critical time for early mitigation measures.

[20] Mediodecci Lustarini, "Legal Certainty of Personal Data Protection After the Ratification of Law Number 27 of 2022," *Ministry of Communication and Information*, 2022, jdih.komdigi.go.id%0A.
[21] Jooyong Jun and Jeong-Yoo Kim, "Strict Liability versus Negligence in the Case of Data Breach," *International Review of Law and Economics* 79 (2024): 106218.

Article 53 of the PDP Law requires the appointment *of a Data Protection Officer* (DPO) for data controllers who meet certain criteria. This obligation is further strengthened through the Constitutional Court's Decision on the material test of Article 53 paragraph (1) which emphasizes that the obligation to appoint a DPO applies if *one of* the three criteria is met, not all three cumulatively.[22] As an ISP with millions of active customers whose activities require regular and structured data monitoring at a broad level, Biznet is juridically included in the category that is required to have a DPO. If the DPO's function is not running optimally in accordance with Article 54 of the PDP Law which includes providing compliance information and advice to the company, monitoring compliance with the PDP Law, and consulting related to the DPIA. This is a structural factor that can contribute to the occurrence of large-scale data leaks such as the one experienced by Biznet.

If a data leak has occurred, the PDP Law provides three repressive protection paths that can be taken cumulatively. First, the administrative route based on Article 57 of the PDP Law, authorizes supervisory institutions to provide sanctions such as written reprimands, temporary suspension of processing processes, data deletion orders, and the imposition of fines with a maximum limit of 2% of total annual revenue. This pathway primarily serves as *a general deterrence* instrument, although it does not directly compensate the victim. However, it should be noted that in the context of the Biznet incident in March 2024, this administrative sanction cannot be fully implemented considering that the Personal Data Protection Institution required by Article 58 of the PDP Law has not yet been established.[23]

[22] Constitutional Court of the Republic of Indonesia, "Constitutional Court Decision Number 151/PUU-XXII/2024" (n.d.).
[23] David Christian, S.H, "PDP Law: Legal Basis for Personal Data Protection," in *The Law Online.Com*, 2022, https://www.hukumonline.com/klinik/a/uu-pdp--landasan-hukum-pelindungan-data-pribadi-lt5d588c1cc649e/.

Second, the civil route based on Article 64 of the PDP Law, which gives the right to claim compensation for losses based on unlawful acts (PMH) in accordance with Articles 1365-1367 of the Civil Code. In the construction of *the obligation of result* implied by Article 46 of the PDP Law, the occurrence of data leakage prima *facie* has proven the non-fulfillment of the data controller's obligations, so that the customer can reasonably show that the data is leaked and causes losses; It is Biznet that must prove that its system has met the applicable legal standards.

Third, the criminal route based on Article 67 of the PDP Law, which regulates criminal threats differs according to the type of violation: the collection and use of personal data in an unlawful manner can be punished with imprisonment for a maximum of 5 years and/or a fine of up to IDR 5 billion (Article 67 paragraphs 1 and 3), while unlawful disclosure of personal data is punishable by imprisonment of up to 4 years and/or a maximum fine of IDR 4 billion (Article 67 paragraph 2). In this context, the principle *of ultimum remedium* is an important principle that emphasizes that the application of criminal sanctions should be used as a last resort after administrative sanctions are not effective in resolving violations.[24] Article 70 regulates corporate criminal liability with fines of up to 10 times, while imprisonment can only be imposed on individual administrators or control holders. In addition to these three lines, the protection for Biznet customers is also strengthened by Law No. 8 of 1999 concerning Consumer Protection: Article 4 letter a guarantees customers' right to service security which indirectly includes the security of personal data, while Article 7 letter f requires business actors to provide compensation for services distributed that are not in accordance with standards. Ipa, Pesulima, and Sopamena (2023) concluded that the UUPK and the PDP Law can

[24] Eka Ayu Safitri, Ratih Damayanti, and Tri Sulistiyono, "Limitations and Mechanisms for the Implementation of Tax Criminal Sanctions in Indonesia in the Perspective of the Principle of Ultimum Remedium," *Journal of Statutory Law* 4, no. 3 (2025): 144–58.

be applied cumulatively to provide more comprehensive protection for victims of data leaks.[25]

Table 1. Summary of Legal Protection Instruments for Biznet Customers

Legal Instruments	Forms of Protection	Enforcement Pathway
Law No. 27 of 2022 (PDP Law)	Data subject rights (Ps. 5–13), controller obligations, 3×24-hour incident notification	Administrative, Civil, Criminal
Civil Code Ps. 1365–1367	PMH lawsuit, material and immaterial damages, liability for subordinates	District Courts
Law No. 8 of 1999 (UUPK)	The right to safety of services, compensation for losses due to the use of services	District Courts

Source: Author, 2026 (processed)

Legal protection for Biznet customers can be obtained through several legal instruments. The PDP Law authorizes data subjects and requires data controllers to protect personal data and report leak incidents within 3×24 hours. Meanwhile, Civil Code Articles 1365–1367 provide a basis for customers to file lawsuits for unlawful acts as well as request compensation through the District Court. In addition, the UUPK guarantees consumers' rights to service security and compensation if services do not meet standards, by resolving disputes through the District Court.

1.2. Biznet's Legal Responsibility for Data Leaks

The PDP Law distinguishes two fundamental positions in the data processing ecosystem. The Data Controller, based on Article 1 number 4, refers to the party that sets the target and supervises the

[25] Indah Ipa, Theresia Louize Pesulima, and Ronald Fadly Sopamena, "Consumer Protection of Indihome Customers Against Personal Data Leakage," *PATTIMURA Law Study Review* 1, no. 2 (2023): 445–51.

processing of personal data. The Personal Data Processor (*data processor*) based on Article 1 number 5 is the party that carries out the processing of personal data on behalf of the controller.[26] This distinction directly determines the amount of responsibility in a data leak incident. Although technology companies often claim the *position of the processor* to transfer responsibility to the vendor, such a construction is difficult to maintain juridically in the case of Biznet, given that the *status of the controller* is objective and must be determined based on facts, not on contractual clauses. Biznet actively determines the purpose of collecting customer data, selects storage infrastructure, establishes security procedures, and makes decisions regarding data retention, all of these elements are doctrinally characteristic of the controller, not just the *processor*.[27] Consequently, the alleged leak of 380 thousand customer data on March 10, 2024 indicates that Biznet's *obligation of result* has not been met. And technical arguments about the sophistication of cyber attacks cannot waive this responsibility unless Biznet succeeds in proving the existence of actual force majeure based on Articles 1244–1245 of the Civil Code.

Although the PDP Law does not explicitly use the phrase "reverse burden of proof," the system of liability it functionally constructs produces similar effects. Based on the character *of the obligation of result* in Article 46 jo. the obligation of comprehensive documentation in Article 31 of the PDP Law, Biznet is required to be able to show proof of its compliance through ROPA documentation, DPIA results, system logs, and track record of handling incidents if sued in a data leak dispute. However, the effectiveness of this mechanism rests on three

[26] Mochamad Januar Rizki, "Analysis of the PDP Law: The Difference Between Controllers vs Processors of Personal Data," in *The Law Online.Com*, 2022, https://www.hukumonline.com/berita/a/bedah-uu-pdp--perbedaan-pengendali-vs-prosesor-data-pribadi-lt6346065855ob0/.

[27] OECD, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data." (2020), https://www.oecd.org/en/publications/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en.html.

prerequisites that are not yet fully available in Indonesia.[28] First, judges with adequate technical literacy to evaluate digital evidence; second, a discovery mechanism that allows customers to access Biznet's *system logs* and internal security audit reports; and third, the jurisprudence that has been established regarding the security standards of large-scale internet service providers.[29] As far as can be identified, there has been no Indonesian court decision that specifically applies the provisions of the PDP Law in data leak disputes, so the standard of proof needed is still not defined jurisprudentially. Without these three prerequisites, the accountability system that emphasizes compliance in the PDP Law has the potential to turn into a progressive rule that loses its enforcement power in the midst of actual legal disputes.

Article 51 paragraph (3) of the PDP Law affirms the principle *of non-delegable liability* where Biznet's liability is not lost even though the technical processing is delegated to the vendor, unless it is proven that the vendor is processing in excess of the instructions and targets determined by Biznet as the controller. However, there are practical loopholes that deserve attention. The PDP Law does not regulate the mechanism of proving the locus of negligence between Biznet and the vendor, thus opening up space for a defensive strategy where Biznet recognizes its status as a *legal controller*, but directs all technical responsibility to the vendor through contractual clauses.[30] The gap in the norm regarding the obligation to recover directly to the customer before reclaiming to the vendor that is not explicitly regulated in the PDP Law needs to be filled immediately through jurisprudence or implementing regulations.

[28] Edmon Makarim, *Legal Responsibilities of Electronic System Operators* (Rajajawali Pers, 2010).
[29] Ismaidar Ismaidar and Rifqi Fairuz Ula, "Corporate Criminal Liability for Consumer Personal Data Leakage in the Perspective of Cybercriminal Law in Indonesia," *Innovative Law: Journal of Social Law and Humanities* 2, no. 3 (2025): 44–51.
[30] OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

Normatively robust liability constructions include *controller status*, *obligation of result*, compliance-based proof construction, and *non-delegable liability* face serious institutional barriers in practice. Article 57 administrative sanctions require the existence of an independent supervisory institution that has not yet been formed as mandated by Article 58 of the PDP Law. Instead, the protection mechanism still depends on Perkominfo Number 20 of 2016 which relies on the role of Komdigi instead of an independent institution required by the PDP Law.[31] Meanwhile, criminal sanctions under Articles 67–70 are hampered by the complexity of proving *corporate mens rea* in the context of cyber incidents. Article 64 civil lawsuits also face causality problems that are not easy to overcome. The most basic structural problem is the fragmentation of supervisory authority: the PDP institution mandated by Article 58 has not yet been formed, Komdigi as the communication and digital regulator is not authorized to impose sanctions under the PDP Law, and BSSN as the cybersecurity authority does not cover the realm of personal data protection.[32] This condition is a systemic risk from the institutional transition design of the PDP Law which does not ensure the formation of supervisory authorities before or at the same time as the enactment of obligations for data controllers. As a result, Biznet's accountability for the March 2024 leak is realistically very difficult to realize in Indonesia's current legal ecosystem not because of the weakness of norms, but because of the fragility of the enforcement ecosystem.

[31] Salsa Nabila Hardafi, "The Absence of PDP Institutions: Legal Loopholes in Personal Data Protection," Law Online.com, 2025, https://www.hukumonline.com/berita/a/ketiadaan-lembaga-pdp--celah-hukum-dalam-pelindungan-data-pribadi-lt686d4f5817d73/.
[32] Institute for Community Studies and Advocacy (ELSAM), "Personal Data Protection Institutions, Key to Enforcement of PDP Law Compliance," 2024, https://www.elsam.or.id/siaran-pers/lembaga-pelindungan-data-pribadi--kunci-penegakan-kepatuhan-uu-pdp.

Table 2. Summary of Biznet's Legal Liability and Sanctions

Form of Responsibility	Legal Basis	Maximum Sanctions
Administrative	Article 57 of the PDP Law	A fine of 2% of annual revenue per violation
Civil (PMH)	Ps. 1365–1367 of the Civil Code	Material and immaterial damages
Corporate Crime	Article 70 of the PDP Law	Fine 10× individual fine (IDR 40–50 billion depending on the type of violation)
Consumers	Ps. 7 letter f UUPK	Consumer Compensation/Compensation

Source: Author, 2026 (processed)

Showing that Biznet can be held legally liable through several mechanisms. Administratively, the PDP Law regulates fines of up to 2% of total annual income based on Article 57; However, in the context of the Biznet incident, this sanction cannot be applied considering that the independent supervisory institution mandated by Article 58 of the PDP Law has not yet been formed. From the civil side, referring to Articles 1365-1367 of the Civil Code, customers can claim material and immaterial damages through a lawsuit for unlawful acts. In the framework of corporate crime, Article 70 of the PDP Law allows the imposition of fines of up to ten times the individual fine ranging from Rp40 to Rp50 billion depending on the type of violation with the note that sanctions for corporations are only in the form of fines, not imprisonment. Meanwhile, based on Article 7 letter f jo. Article 19 of Law No. 8 of 1999 concerning Consumer Protection, business actors are obliged to bear the losses experienced by consumers through the provision of compensation.

2. Critical Evaluation of Personal Data Protection in the Case of Biznet Data Leak

Legislative progress marked by the birth of the PDP Law has not been balanced by institutional readiness in law enforcement. In the case of Biznet's data leak, the gap between *das sollen* and *das sein* can be identified through three structural weaknesses that are interrelated and inter-influencing each other. The most fundamental weakness lies in the non-existence of a personal data protection supervisory institution as stipulated in Article 58 of the PDP Law. The absence of this institution results in real consequences where the Ministry of Communication and Information (now Komdigi) as *an ad interim* authority is only able to send a clarification letter to Biznet, without the authority to impose sanctions, open a formal investigation, or order binding corrective actions within the framework of the PDP Law.[33] Comparisons with other countries emphasize the urgency of this problem. The UK's Information Commissioner's Office (ICO) has been in operation since 1984 and over four decades has gradually built strong supervisory capacity including the fine-laying authority gained since 2010 and significantly strengthened through the 2018 GDPR.[34] The absence of similar institutions in Indonesia makes all sanctions provisions in the PDP Law at risk of becoming *toothless norms*, norms without enforcement. The paradox that has been created is ironic: Indonesia has relatively comprehensive data protection regulations, but compliance with them is essentially voluntary, and uncommitted data controllers can ignore their obligations without facing real legal consequences.

Although the construction *of the obligation of result* in Article 47 of the PDP Law functionally eases the burden on customers, the specific causality challenge remains a serious obstacle. The plaintiff not only needs

[33] Mediana, "The Personal Data Protection Supervisory Institution Has Not Yet Been Formed," *Kompas.Id*, 2024, https://www.kompas.id/artikel/en-lembaga-pengawas-perlindungan-data-pribadi-belum-kunjung-terbentuk.
[34] Ece Inan, "Information Commissioner, United Kingdom," in *Encyclopedia of Big Data* (Springer, 2022), 564–66.

to prove that the leak has occurred and he is affected, but also must show a causal relationship between Biznet's negligence and the concrete losses suffered. This complexity stems from the technical characteristics of data leaks: leaked data is commonly traded and aggregated on the *dark web* alongside *datasets* from other sources, making it difficult to identify the origins of losses. In addition, the time lag between the leak and the manifestation of losses, such as credit card fraud that only appears months after the incident, further complicates the proof of temporal causality.[35] As far as can be identified, Indonesian jurisprudence on the standard of proof of causality in data leak disputes has not developed consistently, further complicating repressive protection. Even in a more mature legal system, the CJEU in case C-300/21 (2023) emphasized that not every violation of the GDPR automatically gives rise to the right to compensation, three cumulative conditions must be met: the existence of the infringement, the existence of material or immaterial losses, and the existence of a causal relationship between the two. It is important to note that this ruling at the same time confirms that there is no threshold of seriousness for immaterial damages, but the plaintiff is still obliged to prove that they are experiencing real negative consequences that are not just a matter of worry.[36] Therefore, the development of national jurisprudence that provides clear guidance on the minimum standards of causality proof, the recognition of immaterial losses without the threshold of seriousness, and the role of digital *forensic* evidence is an urgent need so that repressive protection through civil channels does not stop at a purely theoretical level.

Article 46 of the PDP Law requires data controllers to submit notifications to data owners and supervisory institutions no later than 3×24 hours after the incident is known. However, in the absence of an independent supervisory body that can supervise and enforce these

[35] David W Opderbeck, "Cybersecurity and Data Breach Harms: Theory and Reality," *Md. L. Rev.* 82 (2022): 1001.
[36] Court of Justice of the European Union., "UI v Österreichische Post AG (Case C-300/21)" (2023).

obligations, the provision is reduced to an administrative formality with no real consequences for violators. The Biznet case is a clear illustration of the leak that was first known to the public through a hacker forum in March 2024 was not immediately followed by proactive notifications to affected customers. Biznet's official response only came after pressure from the mass media, in the form of public statements that are general rather than personalized individual notifications as they should be. The GDPR experience shows a striking contrast. Before the GDPR came into effect in 2018, notification compliance in EU member states was generally low because the previous applicable Directive 95/46/EC did not contain specific notification obligations for all controllers. After the implementation of the GDPR with active oversight from *the Data Protection Authority* (DPA) of each country, DLA Piper recorded more than 160,000 notifications since the GDPR came into effect from May 2018 to January 2020 about the first 20 months of the implementation of the rule.[37] This dramatic increase reflects a change in corporate behavior driven by the threat of credible sanctions, rather than a mere increase in the number of incidents. The implication is clear: without a credible supervisory mechanism, the notification obligation in Article 46 of the PDP Law will lose its deterrent function, and companies will continue to be inclined to opt for *a wait-and-see* strategy.

Indonesia's data protection legal system is currently in a state of normative progress but institutionally premature. The PDP Law together with the Civil Code and the UUPK have provided a fairly comprehensive normative foundation, but its effectiveness depends on three prerequisites that have not been met at the same time. First, the immediate establishment of an independent supervisory institution as stipulated in Article 58 of the PDP Law not only for the purpose of sanctions enforcement, but also to provide technical guidance, develop sectoral security standards, facilitate

[37] DLA Piper, "GDPR Data Breach Survey 2020," 2020, https://www.dlapiper.com/en/insights/publications/2020/01/gdpr-data-breach-survey-2020.

pre-litigation dispute mediation, and build public awareness. Second, the harmonization of sectoral regulations, which are currently still fragmented, Law No. 1 of 2024 concerning ITE, Law No. 36 of 1999 concerning Telecommunications, Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, and Permenkominfo No. 20 of 2016 which now functions as technical rules to support the PDP Law in order to coherently support the objectives of the PDP Law and eliminate legal uncertainty for data controllers and law enforcement officials. [38] Third, the transformation of *compliance culture* among data controllers, which requires a combination of positive incentives, industry education, and compliance certification mechanisms to encourage technology companies to view data protection not as a cost burden, but as a long-term investment in trust.

The Biznet data leak case not only reflects technical security issues at the corporate level, but also reveals a much more fundamental challenge in the construction of a data protection legal system in Indonesia, the pace of legislation production far exceeds institutional readiness. The PDP Law was enacted starting October 17, 2022, with a compliance transition period ending in October 2024, but its enforcement still depends on supervisory authorities who have not yet been present a structural inequality that has become an urgent homework for policymakers.

Table 3. Evaluation Matrix: Das Sollen vs. Das Sein in the Biznet Case

Protection Aspects	Norma UU PDP (The Should)	The Reality of the Biznet Case (Das Sein)
Leak Notifications	Mandatory within 3×24 hours to data owners and supervisory agencies (Article 46)	The notification only appears after mass media exposure; No report to the regulator

[38] M. Faiz Aziz, "Personal Data: Scrutinizing the Personal Data Protection Framework in Indonesia," PSHK (Indonesian Center for Legal and Policy Studies), 2020, https://pshk.or.id/blog-id/data-pribadi-meneropong-kerangka-perlindungan-data-pribadi-di-indonesia/.

Independent Oversight	Independent institutions (Article 58)	Not yet formed; only a clarification letter from the Ministry of Communication and Information
Administrative Sanctions	Fine of 2% of annual income (Article 57)	Not yet applicable; Supervisory authority does not yet exist
Compliance-Based Accountability	Operators are required to show proof of compliance — ROPA, DPIA, log system (Article 31 jo. Article 46)	Untested; Data Leak Jurisprudence Not Yet
Victims' Compensation	Right to file a lawsuit (Article 64)	No civil lawsuit has been successfully filed by the victim
Technical Security	Mandatory encryption and mitigation (Article 40)	Biznet's security system is inadequate when a leak occurs

Source: Author, 2026 (processed)

There is a gap between the ideal principles or normative provisions in the PDP Law and the reality on the ground in the case of Biznet. Normatively, the PDP Law requires notification of data leaks within 3×24 hours to data owners and supervisory agencies, the existence of independent supervisory agencies, the application of administrative sanctions, the accountability of data controllers, the victim's right to sue, and the obligation to implement adequate security technical measures. However, in practice, some of these provisions have not run optimally, such as notifications that appear after media reports, supervisory agencies have not been formed, administrative sanctions have not been implemented, and no civil lawsuits have been successfully filed.

Conclusion

Biznet customers who experience data leaks have the status of Personal Data Subjects who have the authority for layered legal guarantees based on Law Number 27 of 2022 concerning Personal Data Protection (UU PDP), the Civil Code (Civil Code), and Law Number 8 of 1999 concerning

Consumer Protection (UUPK). In the preventive aspect, the PDP Law instructs Biznet as the Personal Data Controller to act in anticipation, including the implementation of adequate technical and organizational measures (Article 40), the implementation of DPIA (Article 34), the appointment of a Data Protection Officer (Article 53), and the documentation of data processing activities through ROPA (Article 31). The data security obligation in the PDP Law, especially Article 46, reflects the character of the obligation of result, so that the occurrence of a data leak prima facie indicates the non-fulfillment of the obligation, unless it can be proven that there is a force majeure. In the repressive dimension, customers can take three enforcement paths cumulatively: (1) administrative route in the form of fines of up to 2% of annual revenue by supervisory agencies (Article 57); (2) civil proceedings by filing a compensation lawsuit based on unlawful acts. based on Article 64 of the PDP Law jo. Articles 1365–1367 of the Civil Code, with a reverse evidentiary mechanism that requires Biznet to prove its compliance (Article 35); and (3) criminal proceedings with the threat of corporate fines of up to 10 times the individual fine based on Article 70 of the PDP Law. Juridically, Biznet is positioned as the Personal Data Controller which bears the burden of reverse proof and non-delegable liability that cannot be transferred to third-party vendors based on Article 52 paragraph (3) of the PDP Law.

Critically, the relatively comprehensive normative framework of the PDP Law has not been balanced by adequate institutional readiness, so that Indonesia's data protection system is currently in a normatively advanced but premature condition institutionally. The effectiveness of personal data protection in Biznet's data leak case reflects the striking difference between ideal (*das sollen*) and practice (*das sein*). The main weakness lies in the lack of the establishment of an independent supervisory authority as required by Article 58 of the PDP Law, resulting in the entire administrative sanction mechanism in Article 57 becoming toothless norms, as reflected in the inability of the Ministry of Communication and Information to impose

sanctions and only being able to send clarification letters. In addition, the constraints of proving causality in civil lawsuits, the lack of development of jurisprudence related to data leaks, and weak compliance with incident notification obligations weaken repressive protection for victims. The fragmentation of authority between institutions also exacerbates this condition, so that law enforcement is not optimal. Thus, although the normative framework of the PDP Law has been relatively comprehensive, its implementation still faces serious institutional obstacles. Therefore, it is necessary to immediately establish an independent supervisory authority, strengthen law enforcement and proof mechanisms, and transform the compliance culture among data controllers so that personal data protection can run optimally and provide legal certainty for the public.

References

APJII (Indonesian Internet Service Providers Association. "Indonesian Internet Penetration Survey 2024." Jakarta, 2024.

Aziz, M. Faiz. "Personal Data: Examining the Personal Data Protection Framework in Indonesia." PSHK (Indonesian Center for Law and Policy Studies), 2020. https://pshk.or.id/blog-id/data-pribadi-meneropong-kerangka-perlindungan-data-pribadi-di-indonesia/.

CNN Indonesia. "Biznet's Customer Data Allegedly Leaked Again, Experts Call It Valid," 2024. https://www.cnnindonesia.com/teknologi/20240325135001-192-1078671/data-pelanggan-biznet-diduga-kembali-bocor-ahli-sebut-valid.

Damayanti, Ratih, Muhammad Azil Masykur, Feiruz Rachmita Alamsyah, Ali Masyhar Mursyid, and Dani Muhtada. “Transforming Taxation: Unlocking Efficiency and Resilience Through Digitalization.” *The Indonesian Journal of International Clinical Legal Education* 6, no. 4 (2024): 453–76.

Damayanti, Ratih, and Erwin Dyah Nawawinetu. “Determinant Factors of Work Stress among Teaching and Non Teaching Staff in Indonesia.” *Indian Journal of Public Health Research & Development* 10, no. 3 (2019): 307–11.

David Christian, S.H. "PDP Law: Legal Basis for Personal Data Protection." In *Law Online.Com*, 2022. https://www.hukumonline.com/klinik/a/uu-pdp--landasan-hukum-pelindungan-data-pribadi-lt5d588c1cc649e/.

FOR Piper. "GDPR Data Breach Survey 2020," 2020.

https://www.dlapiper.com/en/insights/publications/2020/01/gdpr-data-breach-survey-2020.

Hasian, Diah Putri, and Annisa Fitria. "Telkomsel's Responsibility for the Leak of Confidential Personal Data of Indihome Users." *Journal of Social and Humanities* 5, no. 2 (2025): 1812–21.

Inan, Ece. "Information Commissioner, United Kingdom." In *Encyclopedia of Big Data*, 564–66. Springer, 2022.

Ipa, Indah, Theresia Louize Pesulima, and Ronald Fadly Sopamena. "Indihome Customer Consumer Protection Against Personal Data Leakage." *PATTIMURA Law Study Review* 1, no. 2 (2023): 445–51.

Ismaidar, Ismaidar, and Rifqi Fairuz Ula. "Corporate Criminal Liability for Consumer Personal Data Leakage in the Perspective of Cybercriminal Law in Indonesia." *Innovative Law: Journal of Social Law and Humanities* 2, no. 3 (2025): 44–51.

Jun, Jooyong, and Jeong-Yoo Kim. "Strict Liability versus Negligence in the Case of Data Breach." *International Review of Law and Economics* 79 (2024): 106218.

Khairani Alawiyah Matondang, Tia Handani, Annisa Handayani, Fidia Wati. "Business ethics in the protection of consumers' personal data in the digital business era: in a literature study." *Journal of Information Systems and Business Management Publication* 4 (2025). https://doi.org/https://doi.org/10.55606/jupsim.v4i3.5508.

Institute for Community Studies and Advocacy (ELSAM). "Personal Data Protection Institution, Key to Enforcement of PDP Law Compliance," 2024. https://www.elsam.or.id/siaran-pers/lembaga-pelindungan-data-pribadi--kunci-penegakan-kepatuhan-uu-pdp.

Liputan6.com. "380 thousand Biznet user data allegedly leaked on the dark web, the perpetrators are called employees," 2024. https://www.liputan6.com/tekno/read/5547088/.

Lustarini, Mediodecci. "Legal Certainty of Personal Data Protection After the Ratification of Law Number 27 of 2022." *Ministry of Communication and Informatics*, 2022. jdih.komdigi.go.id%0A.

Maharani, Rista, and Andria Luhur Prakoso. "Protection of Consumer Personal Data by Electronic System Operators in Digital Transactions." *Journal of USM Law Review* 7, no. 1 (2024): 333–47.

Constitutional Court of the Republic of Indonesia. Constitutional Court Decision Number 151/PUU-XXII/2024 (n.d.).

"Please, Edmon. *Legal Responsibility of Electronic System Operators*. Rajajawali Press, 2010.

Medium. "The Personal Data Protection Supervisory Agency has not yet been formed." *Kompas.Id*, 2024. https://www.kompas.id/artikel/en-lembaga-pengawas-perlindungan-data-pribadi-belum-kunjung-terbentuk.

Mochamad Januar Rizki. "A Critique of the PDP Law: The Difference Between Controllers vs Processors of Personal Data." In *Law Online.Com*, 2022. https://www.hukumonline.com/berita/a/bedah-uu-pdp--perbedaan-pengendali-vs-prosesor-data-pribadi-

lt63460658550b0/.
Munir Fuady. *Unlawful Conduct: A Contemporary Approach*. Bandung: PT Citra Aditya Bakti, 2002.
State), BSSN (Cyber and Cryptography Agency. "Indonesia's Cybersecurity Landscape 2023." Jakarta, 2023.
OECD. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. (2020). https://www.oecd.org/en/publications/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en.html.
Opderbeck, David W. "Cybersecurity and Data Breach Harms: Theory and Reality." *Md. L. Rev.* 82 (2022): 1001.
Philipus M. Hadjon. *Introduction to Indonesian Administrative Law*. 1st edition. Yogyakarta: Gadjah Mada University Press, 2011.
Rahardjo, Satjipto. "Science, PT." *Citra Aditya Bakti, Bandung*, 2000.
Republic of Indonesia. (1847). Civil Code (Civil Code)
Republic of Indonesia. (1999). Law No. 8 of 1999 concerning Consumer Protection
Republic of Indonesia. (2008). Law Number 11 of 2008 concerning Information and Electronic Transactions
Republic of Indonesia. (2022). Law Number 27 of 2022 concerning Personal Data Protection
Safitri, Eka Ayu, Ratih Damayanti, and Tri Sulistiyono. "Limitations and Mechanisms for the Implementation of Tax Criminal Sanctions in Indonesia in the Perspective of the Principle of Ultimum Remedium." *Journal of Statutory* Law 4, no. 3 (2025): 144–58.
Salsa Nabila Hardafi. "The Absence of PDP Institutions: Legal Loopholes in Personal Data Protection." Law Online.com, 2025. https://www.hukumonline.com/berita/a/ketiadaan-lembaga-pdp--celah-hukum-dalam-pelindungan-data-pribadi-lt686d4f5817d73/.
Tirto.id. "Kominfo Asks Biznet to Clarify Customer Data Leak," 2024. https://tirto.id/kominfo-minta-biznet-klarifikasi-soal-kebocoran-data-pelanggan-gWVv.
Union., Court of Justice of the European. UI v Österreichische Post AG (Case C-300/21) (2023).
Hero, Sidi Ahyar. "Legal Responsibility of E-Commerce Platforms for Personal Data Leakage in the Perspective of Law No. 27 of 2022." *Journal of Legal and Public Policy Studies| E-ISSN: 3031-8882* 2, no. 2 (2025): 1089–96.
Wulandari, Devi, and Sidi Ahyar Wiraguna. "Legal Protection for Tokopedia Application Users from Personal Data Leakage from the Perspective of Law Number 27 of 2022." *Journal of Legal and Public Policy Studies| E-ISSN: 3031-8882* 2, no. 2 (2025): 1321–25.
Yes, Musrika. "Analysis of Civil Liability in Data Leaks: Synchronization of the Personal Data Protection Law and the Civil Code." *Journal of Social Sciences and Humanities* 1, no. 4 (2025): 1539–49.