

Borobudur Law and Society Journal
ISSN: 2809-9664
Vol. 5 No. 2 (2026)
pp: 1-11
DOI: https://doi.org/10.31603/15581

UNIMMA PRESS
UNIVERSITAS MUHAMMADIYAH MAGELANG

Legal Responsibility of an Internet Service Provider for a User Data Breach under the Personal Data Protection Law: The Biznet Case

Oremia Exilla Rafelina Sihombing[1*]

[1] Faculty of Law, Universitas Pembangunan Nasional "Veteran" Jakarta, Jakarta, Indonesia
[*]Corresponding author: Oremia Exilla Rafelina Sihombing

Abstract

Indonesia's Personal Data Protection Law (Law No 27 of 2022) imposes detailed duties on data controllers, yet breaches continue and the Law's enforcement structure is still incomplete. This study examines the legal responsibility of an internet service provider, Biznet, for two user-data breaches reported in March 2024: about 380,000 records of its internet customers and 154,091 records of customers of its cloud service, Biznet Gio, reportedly including identity, tax, contact and account data. It asks what the Law requires of a controller before and after a breach, how far those duties were enforceable during the Law's two-year transition period, and which forms of liability may follow. The research is normative, using statute, conceptual and case approaches; the facts are taken from press reports and the company's public statements and are treated as allegations. The Law requires a lawful basis, an impact assessment for high-risk processing, security and confidentiality measures, supervision of processors and written notice within three days of a failure. The reports raise doubts about security and notification, but do not establish a breach of duty. Administrative, civil and criminal liability are all possible; their imposition depends on the controller's documented compliance and on a functioning supervisory agency, which had still not been formed in 2026. Breach notification procedures, security audits and a compensation route for data subjects are recommended.

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License

Keywords

Breach; Controller; Liability; Notification; Privacy; Security

Introduction

Access to technology has become part of the exercise of fundamental rights in education, work, health and information. The 1945 Constitution protects the person, family, honour, dignity and property under a person's control, and the right to

security against threats.[1] Digital services have changed the way that companies collect and keep personal data, which can easily be misused for identity theft, online fraud and other harm. Law No 27 of 2022 on Personal Data Protection (the PDP Law) gives Indonesia its first comprehensive statute on the rights of data subjects, the duties of controllers and processors, and sanctions.[2] Breaches have nonetheless continued. In March 2024 two sets of data of customers of Biznet, an integrated digital-infrastructure company whose services include internet access and cloud computing, were reported to have been leaked. Because an internet service provider processes the identity, address, tax and billing data of many subscribers, the case shows how the Law's duties apply to a large-scale controller.

Earlier Indonesian studies have examined the division of roles between controllers and processors under the PDP Law,[3] and the liability of e-commerce platforms for leaked customer data.[4] A study of the Bhinneka e-commerce breach concluded that the platform, as an electronic system operator, should apologise and compensate users for material and immaterial loss, and that administrative sanctions were available, but found that no sanction or remedy had followed.[5] A study of the BPJS Kesehatan breach likewise found that the PDP Law attaches administrative, civil and criminal consequences to a controller's failures and called for stronger security and internal audits.[6] These studies concern platforms and public bodies and treat the Law as fully applicable. None examines a telecommunications and cloud provider, which may act both as controller of its customers' data and as processor of data that customers host on its infrastructure, and none asks how the Law's two-year transition period, which ran from 17 October 2022 to October 2024,[7] and the absence of the supervisory agency affect liability for breaches that occurred within it.

This article therefore asks three questions: (1) what obligations does the PDP Law impose on a personal data controller before and after a breach; (2) how far were those obligations enforceable against Biznet when the reported breaches occurred

---

[1] Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 [1945 Constitution of the Republic of Indonesia], art 28G(1).

[2] Law No 27 of 2022 on Personal Data Protection (Indonesia).

[3] Jonathan Matthew Pakpahan, "Kesadaran Urgensi Peran Pengendali dan Prosesor Data Pribadi dalam Rangka Pelindungan Data Pribadi Individu berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi" (2024) 10:1 *Jurnal Hukum To-Ra: Hukum untuk Mengatur dan Melindungi Masyarakat* 119.

[4] Sidi Ahyar Wiraguna et al, "Tanggung Jawab Hukum Platform E-Commerce atas Kebocoran Data Pribadi dalam Perspektif UU No. 27 Tahun 2022" (2025) 2:2 *Jurnal Kajian Hukum dan Kebijakan Publik* 1089.

[5] Brandon Christoper Kantong & Jeane Neltje Saly, "Tanggung Jawab Hukum E-Commerce Bhineka terhadap Kebocoran Data Pribadi Pengguna" (2023) 7:2 *Jurnal Kewarganegaraan*, DOI: <10.31316/jk.v7i2.5761>.

[6] Ridho Rivantoro & Dyah Permata Budi Asri, "Tanggung Jawab Hukum Korporasi atas Kebocoran Data Peserta BPJS Kesehatan berdasarkan UU No. 27 Tahun 2022" (2026) 4:3 *Jurnal Pengabdian Masyarakat dan Riset Pendidikan* 16034, DOI: <10.31004/jerkin.v4i3.4575>.

[7] Law No 27 of 2022, *supra* note 2, art 74.

in 2024; and (3) what forms of administrative, civil and criminal liability may follow if the obligations were not met, and what must be proved to establish them? Its purpose is to set out, for a large-scale service provider, the standard of conduct the Law requires and the conditions under which liability can be imposed, without prejudging whether this company breached its duties.

Research Method

This is normative (doctrinal) legal research using statute, conceptual and case approaches; no interviews or fieldwork were conducted. The primary legal materials are the 1945 Constitution, the PDP Law, the Electronic Information and Transactions Law as amended, Government Regulation No 71 of 2019 on electronic systems, Government Regulation No 33 of 2026 implementing the PDP Law and the Civil Code; the EU General Data Protection Regulation (GDPR), on which much of the Indonesian Law is modelled, is used for comparison. The secondary materials are a commentary on the PDP Law and journal articles on controller liability. The facts of the case are not legal materials: they are taken from press reports in CNN Indonesia, Gizmologi, Selular.ID and Inilah.com, which quote the company's spokespeople, the then Ministry of Communication and Informatics and an independent researcher who checked a sample of the leaked records. No decision of a court or of a supervisory authority on the incidents was found. The facts are therefore treated as reported allegations, reports were cross-checked against one another, and the company's own statements are reported as such. Each statutory duty was set against the reported facts to identify what is known, what is unknown and what would have to be proved; the analysis is qualitative and prescriptive.

Results and Discussion

Obligations of a Personal Data Controller under the PDP Law

A personal data controller is any person, public body or international organisation that, alone or jointly, determines the purposes and controls the processing of personal data.[8] A company acting as controller must have a lawful basis for processing, such as the data subject's explicit consent, the performance of an agreement with the data subject or a legal obligation.[9] It must carry out a data protection impact assessment where processing is likely to pose a high risk to data

[8] *Ibid*, art 1(4).
[9] *Ibid*, art 20(2).

subjects;[10] protect and ensure the security of the data by technical and operational measures with a level of security suited to the nature and risk of the data;[11] keep the data confidential;[12] supervise every party involved in processing under its control;[13] protect the data from unlawful processing;[14] and prevent unauthorised access, using a reliable, secure and accountable electronic system.[15] When protection fails, it must give written notice to the data subjects and to the supervisory agency within three days (3 × 24 hours), stating at least the data disclosed, when and how they were disclosed, and the efforts to handle and recover from the failure.[16] Above all, the controller is responsible for its processing and must demonstrate its accountability in meeting the principles of data protection.[17] The commentary on the Law reads these duties as a risk-based standard: the greater the volume and sensitivity of the data, the higher the security expected.[18] Where a controller appoints a processor, the processor must act on the controller's instructions, and the security and confidentiality duties apply to the processor as well.[19]

Timing matters for the case. The PDP Law came into force on its promulgation on 17 October 2022,[20] but controllers and processors were given two years to bring their processing into line with it.[21] The reported breaches of March 2024 thus fell within the transition period. The better reading is that the transition clause postponed the expectation of full compliance and the imposition of administrative sanctions for non-compliance, not the existence of the duties or the rights of data subjects. Existing regulations remained in force as long as they did not conflict with the Law.[22] A provider of internet and cloud services was therefore already bound, as an electronic system operator, to operate its electronic systems reliably and securely and to be responsible for their proper operation,[23] and to notify the owners of personal data in writing of any failure to protect the data it manages.[24] Two further gaps remain. The supervisory agency that is to receive breach notices, examine

[10] *Ibid*, art 34(1).
[11] *Ibid*, art 35.
[12] *Ibid*, art 36.
[13] *Ibid*, art 37.
[14] *Ibid*, art 38.
[15] *Ibid*, art 39.
[16] *Ibid*, art 46.
[17] *Ibid*, art 47.
[18] Sinta Dewi Rosadi, *Pembahasan UU Pelindungan Data Pribadi (UU RI No. 27 Tahun 2022)* (Jakarta: Sinar Grafika, 2023).
[19] Law No 27 of 2022, *supra* note 2, arts 51(1), 52.
[20] *Ibid*, art 76.
[21] *Ibid*, art 74.
[22] *Ibid*, art 75.
[23] Law No 11 of 2008 on Electronic Information and Transactions, as amended by Law No 19 of 2016 and Law No 1 of 2024 (Indonesia), art 15(1).
[24] Government Regulation No 71 of 2019 on the Operation of Electronic Systems and Transactions (Indonesia), art 14(5).

controllers and impose sanctions is to be established by the President,[25] but in July 2026 the presidential regulation forming it was still being finalised.[26] The implementing Government Regulation was issued only in July 2026 and takes effect on 16 January 2027,[27] so that procedures for impact assessments, notification and administrative fines were not yet regulated in detail when the incidents occurred. In 2024 supervision was in practice exercised by the Ministry of Communication and Informatics, which asked the company for clarification.

The Reported Breaches Measured against the Controller's Duties

According to press reports, on 10 March 2024 an actor using the name 'Blucifer' published about 380,000 records of Biznet internet customers, said to include names, emails, identity and tax numbers, telephone numbers and addresses; the company stated that it was investigating the claim with the authorities.[28] On 24 and 25 March 2024 the same actor reportedly published 154,091 records of customers of Biznet Gio, the company's business cloud service, said to include full names, emails, account balances, password hashes, addresses, tax numbers and telephone numbers. The actor claimed to be acting in protest against the Fair Usage Policy applied to customers using more than 1 TB a month, and threatened further leaks of virtual-machine credentials unless the policy was withdrawn by 7 April 2024.[29] An independent researcher checked 2,000 randomly selected records and reported that 99.65 per cent corresponded to registered Biznet Gio accounts.[30] Biznet Gio stated that it had received the report on 25 March 2024, had begun a full investigation, was working with the National Police, offered a dedicated hotline to customers and already used two-factor authentication.[31] The Ministry said that Biznet had not reported the first incident; the company replied that it had answered the Ministry's request for clarification by letter.[32] In October 2024 the 380,000-record case resurfaced, and the company said it had opened an internal investigation with

---

[25] Law No 27 of 2022, *supra* note 2, art 58.

[26] Agus Tri Haryanto, "'Wasit' Perlindungan Data Pribadi Segera Dibentuk Secara Independen", *detikInet* (23 July 2026), online: <https://inet.detik.com/law-and-policy/d-8587033/wasit-perlindungan-data-pribadi-segera-dibentuk-secara-independen>.

[27] Government Regulation No 33 of 2026 on the Implementing Regulations of Law No 27 of 2022 on Personal Data Protection (Indonesia).

[28] Zihan Fajrin, "Tanggapan Biznet Soal Kasus Kebocoran Data Pelanggannya", *Gizmologi* (10 March 2024), online: <https://gizmologi.id/news/tanggapan-biznet-soal-kasus-kebocoran-data/>.

[29] Zihan Fajrin, "Tak Dihiraukan, Pelaku Kebocoran Data Biznet Sebar 154 Ribu Data Biznet Gio!", *Gizmologi* (25 March 2024), online: <https://gizmologi.id/news/pelaku-kebocoran-data-biznet-154-ribu-biznet-gio/>.

[30] "Data Pelanggan Biznet Diduga Kembali Bocor, Ahli Sebut Valid", *CNN Indonesia* (25 March 2024), online: <https://www.cnnindonesia.com/teknologi/20240325135001-192-1078671/data-pelanggan-biznet-diduga-kembali-bocor-ahli-sebut-valid>.

[31] Zihan Fajrin, "Biznet Gio Buka Suara Terkait Bocornya Data Pengguna Ulah Blucifer", *Gizmologi* (26 March 2024), online: <https://gizmologi.id/news/biznet-gio-buka-suara-bocornya-data-pengguna/>.

[32] Suharno, "Biznet Klaim Telah Respon Kominfo Terkait Kebocoran Data Pelanggan", *Selular.ID* (22 March 2024), online: <https://selular.id/2024/03/biznet-klaim-telah-respon-kominfo-terkait-kebocoran-data-pelanggan/>.

external security consultants.[33] None of these reports states how the data were obtained, and no finding by an authority has been published.

Measured against the Law, the reported facts raise questions rather than answer them. The processing of the identity, tax, address and billing data of hundreds of thousands of subscribers is large-scale processing that is likely to pose a high risk, so an impact assessment and risk-based security measures were required.[34] Whether they were in place is not known from public sources. The storage of passwords as hashes and the use of two-factor authentication on the cloud service are measures that point towards some security; the exposure of the records and the claim that the actor was an insider point towards possible weaknesses in access control and in the supervision of personnel, which the Law requires.[35] The fact that two datasets were leaked within a month does not by itself show that the systems were unreliable: the incidents may have shared a cause, such as a persistent weakness or a compromised internal account, or may have had different causes, such as stolen credentials or access through a third party. What the repetition does show is that, after the first incident, the second dataset was still exposed, which makes the adequacy of the response to the first incident a central question for any investigation.

The notification duty is the clearest test. The Law requires written notice to data subjects and to the agency within three days of the failure.[36] The public statements describe investigation, cooperation with the police and a hotline, but none of the reports examined mentions a written notice to affected customers stating what data were disclosed and what they should do; whether such notices were sent cannot be determined from public sources and would have to be established in an investigation. The dispute between the Ministry and the company over reporting shows why the procedure needs to be defined: the Law names an agency that did not yet exist as the recipient of the notice. The cloud service raises a further point. For the account data of its own customers, such as names, balances and password hashes, Biznet Gio acts as controller. For data that its business customers store on its virtual machines, it would normally act as processor, bound by those customers' instructions and by the security and confidentiality duties that extend to

[33] Ibnu Naufal, "Kebocoran Data 380 Ribu Pengguna Biznet Kembali Diangkat, Investigasi Berlanjut", *Inilah.com* (30 October 2024), online: <https://www.inilah.com/kebocoran-data-380-ribu-pengguna-biznet-kembali-diangkat-investigasi-berlanjut>.
[34] Law No 27 of 2022, *supra* note 2, arts 34(1), 35.
[35] *Ibid*, arts 37, 39.
[36] *Ibid*, art 46.

processors,[37] while the customers remain controllers with their own duties of notification. Table 1 summarises the position.

Table 1. The controller's duties and the reported facts

Duty (PDP Law)	What the public reports show	What would have to be established
Impact assessment for high-risk processing (art 34)	Nothing reported	Whether an assessment was made and acted on
Security, confidentiality, protection against unlawful access (arts 35–39)	Password hashes and two-factor authentication on the cloud service; data nevertheless exposed; actor claimed to be an insider	How the data were obtained and whether measures matched the risk
Supervision of personnel and processors (art 37)	Insider claim unverified	Access rights and supervision of staff and contractors
Written notice within three days (art 46)	Investigation, police involvement and hotline announced; no written notice to customers reported	Whether and when notices were sent and what they said
Accountability (art 47)	Internal investigation and external consultants announced in October 2024	Documented compliance that the controller can show

Source: compiled from the PDP Law and the press reports cited above.

Forms of Liability and What Must Be Proved

Three forms of liability may follow from a controller's failure. Administrative liability attaches to breaches of the duties described above, including those on security, confidentiality, supervision, notification and accountability; the sanctions are a written warning, temporary suspension of processing, deletion or destruction of data and an administrative fine of up to two per cent of annual revenue or receipts in respect of the violation.[38] These sanctions are imposed by the supervisory agency, and the implementing regulation now sets the factors for calculating fines;[39] because the agency had not been formed, no such sanction could be imposed for the 2024 incidents under the PDP Law, although sanctions for electronic system operators under the existing regulation remained available. Civil liability is independent of the agency: a data subject may sue for and receive compensation for a breach of processing concerning his or her data,[40] and a person whose personal data are used without consent in an electronic system may also sue for the loss caused,[41] while the general rule on unlawful acts requires the person at fault to compensate the loss.[42] Criminal liability attaches chiefly to the person who unlawfully obtains, discloses or uses another's personal data,[43] which on the reports would be the actor who published the records, and corporations may be fined for

[37] *Ibid*, arts 51(1), 52.
[38] *Ibid*, art 57.
[39] Government Regulation No 33 of 2026, *supra* note 27.
[40] Law No 27 of 2022, *supra* note 2, art 12(1).
[41] Law No 11 of 2008, *supra* note 23, art 26(2).
[42] Kitab Undang-Undang Hukum Perdata [Civil Code] (Indonesia), art 1365.
[43] Law No 27 of 2022, *supra* note 2, arts 65, 67.

such offences where they are committed for them; a controller that is itself the victim of an intrusion does not commit these offences merely by having been breached.

The conclusion that the company is responsible 'if proven' thus requires precision about proof. For administrative liability, the accountability principle places the burden of showing compliance on the controller: it must be able to demonstrate its impact assessment, its security measures and its notices,[44] and the agency would assess these against the risk of the data. For civil liability, the claimant must prove the unlawful act, fault, loss and causation, but a controller that cannot show reasonable security will find it hard to rebut an inference of fault from the breach itself. The GDPR, from which the Indonesian provisions draw, takes the same structure: it requires security appropriate to the risk, notice to the supervisory authority within 72 hours and to data subjects where the risk to them is high,[45] and a right to compensation from which a controller is exempt only if it proves that it is not in any way responsible for the event giving rise to the damage,[46] while fines for breaches of these duties reach two per cent of worldwide annual turnover.[47] The Indonesian Law has no equivalent express reversal of the burden in civil claims, which leaves data subjects in a weaker position than the comparable European rule.

Comparison with Earlier Research

The findings agree with earlier studies that a controller's failure engages administrative, civil and criminal consequences under the PDP Law,[48] and that leaked customer data ground claims for compensation against the platform.[49] They also confirm the Bhinneka study's observation that liability in principle has rarely produced sanctions or remedies in practice.[50] The study adds three points. First, liability for breaches during the transition period rests mainly on the electronic-systems regime and on civil law, because the PDP Law's administrative sanctions depend on an agency that did not exist. Second, a cloud provider must be analysed in two roles, as controller of its customers' account data and as processor of hosted data, which the controller–processor literature describes in general terms but does not apply to infrastructure providers.[51] Third, the decisive evidence is the

[44] *Ibid*, art 47.
[45] EC, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), [2016] OJ L 119/1, arts 32–34.
[46] *Ibid*, art 82(3).
[47] *Ibid*, art 83(4).
[48] Rivantoro & Asri, *supra* note 6.
[49] Wiraguna et al, *supra* note 4.
[50] Kantong & Saly, *supra* note 5.
[51] Pakpahan, *supra* note 3.

controller's own documentation, so that responsibility cannot be inferred from the fact or repetition of a breach alone.

Conclusion

The PDP Law requires a controller to process data on a lawful basis, to assess the impact of high-risk processing, to secure the data and keep them confidential, to supervise those who process them, to notify data subjects and the agency in writing within three days of a failure and to demonstrate its compliance. When the Biznet breaches were reported in March 2024, these duties existed but were still within the two-year transition period, and the agency that should receive notices and impose sanctions had not been formed; the company was nonetheless bound by the duties of electronic system operators to operate secure systems and notify data owners. The reported facts raise doubts about the security of the data and about written notice to customers, but they do not establish that the company failed in its duties, and no authority has found that it did. Administrative, civil and criminal liability are all possible, the last chiefly for the person who obtained and published the data; each depends on evidence of the company's impact assessment, security measures and notices. The government should form the supervisory agency without further delay and, through it, issue a standard breach notification procedure; large-scale processors such as internet and cloud providers should be subject to periodic independent security audits; and data subjects should have a simple compensation route with a burden on the controller to show reasonable security. The study relies on press accounts and company statements, has no information on the company's internal response or on any notices sent, and analyses a statute whose enforcement structure is still being set up.

Ethics and Data Availability

This normative legal research did not involve human participants or personal data, so ethical approval was not required. The leaked data discussed were not accessed or used; all legal materials and press reports used are publicly available.

Use of Generative AI

Generative AI was used only to improve the language of this article (grammar, clarity and style). The authors reviewed the output and are responsible for the content of the article.

Funding and Conflicts of Interest

The authors declare no conflict of interest. This research received no external funding.

References

Kitab Undang-Undang Hukum Perdata [Civil Code] (Indonesia).

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 [1945 Constitution of the Republic of Indonesia].

Law No 11 of 2008 on Electronic Information and Transactions, as amended by Law No 19 of 2016 and Law No 1 of 2024 (Indonesia).

Law No 27 of 2022 on Personal Data Protection (Indonesia).

Government Regulation No 71 of 2019 on the Operation of Electronic Systems and Transactions (Indonesia).

Government Regulation No 33 of 2026 on the Implementing Regulations of Law No 27 of 2022 on Personal Data Protection (Indonesia).

EC, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), [2016] OJ L 119/1.

"Data Pelanggan Biznet Diduga Kembali Bocor, Ahli Sebut Valid". *CNN Indonesia* (25 March 2024), online: <https://www.cnnindonesia.com/teknologi/20240325135001-192-1078671/data-pelanggan-biznet-diduga-kembali-bocor-ahli-sebut-valid>.

Zihan Fajrin. "Biznet Gio Buka Suara Terkait Bocornya Data Pengguna Ulah Blucifer". *Gizmologi* (26 March 2024), online: <https://gizmologi.id/news/biznet-gio-buka-suara-bocornya-data-pengguna/>.

Zihan Fajrin. "Tak Dihiraukan, Pelaku Kebocoran Data Biznet Sebar 154 Ribu Data Biznet Gio!". *Gizmologi* (25 March 2024), online: <https://gizmologi.id/news/pelaku-kebocoran-data-biznet-154-ribu-biznet-gio/>.

Zihan Fajrin. "Tanggapan Biznet Soal Kasus Kebocoran Data Pelanggannya". *Gizmologi* (10 March 2024), online: <https://gizmologi.id/news/tanggapan-biznet-soal-kasus-kebocoran-data/>.

Agus Tri Haryanto. "'Wasit' Perlindungan Data Pribadi Segera Dibentuk Secara Independen". *detikInet* (23 July 2026), online: <https://inet.detik.com/law-and-policy/d-8587033/wasit-perlindungan-data-pribadi-segera-dibentuk-secara-independen>.

Kantong, Brandon Christoper & Jeane Neltje Saly. "Tanggung Jawab Hukum E-

Commerce Bhineka terhadap Kebocoran Data Pribadi Pengguna" (2023) 7:2 *Jurnal Kewarganegaraan*, DOI: <10.31316/jk.v7i2.5761>.

Ibnu Naufal. "Kebocoran Data 380 Ribu Pengguna Biznet Kembali Diangkat, Investigasi Berlanjut". *Inilah.com* (30 October 2024), online: <https://www.inilah.com/kebocoran-data-380-ribu-pengguna-biznet-kembali-diangkat-investigasi-berlanjut>.

Pakpahan, Jonathan Matthew. "Kesadaran Urgensi Peran Pengendali dan Prosesor Data Pribadi dalam Rangka Pelindungan Data Pribadi Individu berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi" (2024) 10:1 *Jurnal Hukum To-Ra: Hukum untuk Mengatur dan Melindungi Masyarakat* 119.

Rivantoro, Ridho & Dyah Permata Budi Asri. "Tanggung Jawab Hukum Korporasi atas Kebocoran Data Peserta BPJS Kesehatan berdasarkan UU No. 27 Tahun 2022" (2026) 4:3 *Jurnal Pengabdian Masyarakat dan Riset Pendidikan* 16034, DOI: <10.31004/jerkin.v4i3.4575>.

Rosadi, Sinta Dewi. *Pembahasan UU Pelindungan Data Pribadi (UU RI No. 27 Tahun 2022)*. Jakarta: Sinar Grafika, 2023.

Suharno. "Biznet Klaim Telah Respon Kominfo Terkait Kebocoran Data Pelanggan". *Selular.ID* (22 March 2024), online: <https://selular.id/2024/03/biznet-klaim-telah-respon-kominfo-terkait-kebocoran-data-pelanggan/>.

Wiraguna, Sidi Ahyar et al. "Tanggung Jawab Hukum Platform E-Commerce atas Kebocoran Data Pribadi dalam Perspektif UU No. 27 Tahun 2022" (2025) 2:2 *Jurnal Kajian Hukum dan Kebijakan Publik* 1089.