

Pertanggungjawaban Pidana Korporasi atas Kebocoran Data Pribadi Konsumen di Indonesia

Corporate Criminal Liability for Consumer Personal Data Breaches in Indonesia

Aulia Rahman Hakim Hasibuan

Universitas Pembangunan Panca Budi, Indonesia

Abstrak

Kebocoran data pribadi konsumen tidak selalu merupakan tindak pidana korporasi. Artikel ini mengkaji kapan pengungkapan, penggunaan, perolehan, atau pemalsuan data dapat diatribusikan kepada korporasi penyelenggara sistem elektronik menurut Undang-Undang Pelindungan Data Pribadi (UU PDP), Kitab Undang-Undang Hukum Pidana (KUHP), dan aturan penanganan perkara korporasi. Penelitian hukum normatif ini menggunakan pendekatan perundang-undangan, konseptual, dan perbandingan terbatas; bahan hukum ditafsirkan secara tekstual dan sistematis, sedangkan satu putusan Uni Eropa digunakan hanya untuk menilai batas analogi. Artikel ini mengusulkan pemeriksaan berurutan atas unsur delik, hubungan pelaku dengan kegiatan korporasi, dan dasar pertanggungjawaban organisasi. Kegagalan pengamanan atau notifikasi dapat memicu respons administratif dan menjadi bukti kontekstual, tetapi tidak menggantikan pembuktian kesengajaan dan sifat melawan hukum dalam Pasal 67 dan 68 UU PDP. Tanggung jawab pengendali, prosesor, dan pengurus perlu mengikuti fungsi, kewenangan, dan keputusan yang dapat dibuktikan. Penjatuhan sanksi harus membedakan denda administratif dari pidana denda, memperhitungkan penyesuaian pidana yang berlaku sejak 2026, serta menjaga pemulihan subjek data. Kerangka ini merupakan usulan doktrinal yang masih memerlukan pengujian terhadap praktik perkara.

Kata Kunci: pertanggungjawaban pidana korporasi; pelindungan data pribadi; kebocoran data; atribusi; pemulihan

Abstract

A consumer data breach does not, by itself, establish a corporation's criminal liability. This article asks when unlawful acquisition, disclosure, use, or falsification of personal data can be attributed to an electronic system operator under Indonesia's Personal Data Protection Law (PDP Law), Criminal Code, and rules on corporate criminal proceedings. It applies doctrinal legal research, combining textual and systematic interpretation with a limited functional comparison to a judgment of the Court of Justice of the European Union. The proposed sequence first tests the elements of a specific offence, then the actor's connection with the corporation, and finally the statutory grounds for corporate responsibility. A failure to secure data or notify data subjects may warrant an administrative response and provide relevant context, but it cannot replace proof of the intentional and unlawful conduct required by Articles 67 and 68 of the PDP Law. The respective roles of controllers, processors, managers, and outside attackers must be established from actual control and evidence of decisions. Sanctions require a distinction between administrative and criminal fines, attention to the criminal law adjustments effective in 2026, and remedies that remain useful to affected people. The framework is a doctrinal proposal, not an empirical finding about prosecution outcomes.

Keywords: corporate criminal liability; personal data protection; data breach; attribution; remedies

*

Introduction

Personal data breaches expose consumers to fraud, loss of control over information, and the practical burden of protecting themselves. The technical cause may be an outside intrusion, misuse of an employee's access, or a deliberate corporate decision to disclose or monetise data. Those situations call for different legal responses. The occurrence of a breach

establishes a need to investigate what happened; it does not establish that the electronic system operator committed an intentional offence. A rule that equated every security failure with criminal disclosure would obscure the elements enacted by the legislature and make the criminal process a substitute for ordinary compliance enforcement (Republic of Indonesia, 2022, arts. 35–39, 46, 57, 65–70).

The PDP Law assigns duties to personal data controllers and processors, grants data subjects a right to seek compensation, provides administrative sanctions, and defines particular offences. Articles 67 and 68 specify conduct and mental elements; Article 70 addresses offences committed by corporations. Supreme Court Regulation No. 13 of 2016 supplies rules for handling corporate criminal cases. The Criminal Code enacted in 2023 is discussed only as a prospective development because its general corporate provisions had not entered into force by the end of the study period (Republic of Indonesia, 2022, arts. 12, 67–70; Supreme Court of the Republic of Indonesia, 2016, arts. 3–4; Republic of Indonesia, 2023, arts. 45–49).

Prior scholarship addresses organisational fault, the design of a data protection authority, and breach notification, but it rarely connects each of these topics to the precise offence and attribution provisions governing an Indonesian corporate defendant. Bedecarratz Scholz (2020) cautions against confusing organisational duties with a free-standing rule of criminal attribution; Amiati et al. (2024) examine corporate culture in the wider context of the new Criminal Code. Widiatedja and Mishra (2023) focus on institutional independence, and Situmeang et al. (2025) compare notification systems. Aulia Rahman Hakim Hasibuan and coauthors examine consumers' ability to express concerns through online product reviews (Hasibuan et al., 2024). Their subject is distinct from data offences, but the analysis supports attention to accessible channels for affected consumers. This article brings those inquiries together around a narrower question: what must be proved before a breach can support a corporate criminal charge?

It argues for a sequential inquiry into the predicate offence, the actor's organisational connection, and the grounds for corporate responsibility under the instruments applicable within the study period. The analysis then considers evidence, allocation between controllers and processors, and proportionate sanctions.

Method

This is normative or doctrinal legal research using statutory, conceptual, and limited functional comparative approaches. The primary materials are Law No. 27 of 2022 on Personal Data Protection and Supreme Court Regulation No. 13 of 2016 on corporate criminal cases. Law No. 1 of 2023 on the Criminal Code is considered solely to identify a prospective statutory approach, not as an operative basis for liability in the period examined. The judgment in Case C-340/21 is considered for the limited question of how a third-party attack bears on the assessment of security measures. Secondary materials were selected for direct relevance to corporate attribution, organisational fault, breach notification, institutional oversight, or consumer remedies; their cited publication details were checked against publisher, court, or official legal sources.

The analysis first identifies the conduct and mental elements of the PDP Law offences, then reads the corporate case rules alongside the special PDP Law provision, and finally tests the proposed evidentiary sequence against hypothetical scenarios. The European judgment concerns GDPR civil liability and does not supply an Indonesian criminal presumption or shift the prosecution's burden. No case-file sample, interviews, or systematic review of Indonesian prosecutions was undertaken. The framework and its expected uses are interpretive proposals rather than measured effects.

Results and Discussion

The Boundary Between a Security Failure and a Criminal Offence

Article 67(1) of the PDP Law penalises intentional and unlawful acquisition or collection of another person's personal data with a purpose of benefiting oneself or another and a capacity to cause loss to the data subject. Article 67(2) covers intentional and unlawful disclosure, whereas Article 67(3) addresses intentional and unlawful use. Article 68 addresses intentional creation or falsification of personal data with the stated purpose and potential for loss. The purpose and potential-loss wording in Articles 67(1) and 68 should not be mechanically imported into Articles 67(2) and 67(3); each charge must follow its own text and the related prohibitions in Articles 65 and 66 (Republic of Indonesia, 2022, arts. 65–68).

Consider, as an analytical example, a company instruction to sell a customer database without lawful basis. Communications authorising the sale, payment records, and the data transfer may together support an inference of intentional disclosure. An external attack exploiting a previously unknown software weakness presents a different question. Even if the controller failed to meet a security duty, the attacker's access is not automatically the company's intentional acquisition, use, or disclosure. Deliberately accepting a security risk may establish poor governance; whether it proves intent regarding the charged act depends on what the relevant decision makers knew, authorised, and allowed to continue.

Articles 67 and 68 of the PDP Law expressly require intentional conduct. Security, confidentiality, supervision, and notification duties cannot be converted by analogy into a negligent version of Article 67. A breach of those duties may lead to administrative consequences under Article 57 and may bear on an existing offence, but it cannot satisfy a missing element of that offence. This interpretation respects the specificity of the criminal text and the legality principle; it does not foreclose another properly charged offence whose elements are independently established (Republic of Indonesia, 2022, arts. 35–39, 46, 57, 67–68).

Organisational fault has a defined but limited role. Rules on supervision and technical security identify feasible precautions and the structure of decision making. They do not make every deficit an intentional criminal act. The distinction between an organisational duty of conduct and a legal rule of attribution is central to Bedecarratz Scholz's (2020) critique and protects the specificity of the Indonesian statutory offences.

Corporate Attribution Under the PDP Law and Corporate Case Rules

An electronic system operator is not necessarily the controller of all data carried on its system. Under the PDP Law, a controller determines the purposes of and exercises control over processing; a processor processes data on the controller's behalf. The practical function performed in the relevant transaction, rather than the label in a contract, determines which duty applies. Article 70 permits the corporation and specified controlling or directing persons to be sanctioned where an Article 67 or 68 offence is committed by a corporation (Republic of Indonesia, 2022, arts. 1, 51, 70).

Supreme Court Regulation No. 13 of 2016 provides the relevant framework for examining conduct by a person acting through an employment or other relationship for and on behalf of a corporation. Article 4 permits a court to assess whether the corporation benefited, tolerated the offence, or failed to take necessary preventive and compliance steps. These indicators must be connected to a charged offence and the conduct of an identifiable actor. A weak security programme alone does not establish intentional disclosure (Supreme Court of the Republic of Indonesia, 2016, arts. 3–4).

Article 70 of the PDP Law identifies managers, persons exercising control, order givers, beneficial owners, and the corporation as possible subjects of punishment when an Article 67 or 68 offence is committed by a corporation. It does not make an individual's title, beneficial ownership entry, or receipt of an incident report conclusive evidence of criminal participation. A charge should identify each person's conduct, authority, and knowledge, with separate reasons for pursuing the legal person and any individual (Republic of Indonesia, 2022, art. 70).

The Criminal Code enacted in 2023 provides a more detailed prospective framework in Articles 45–49, addressing organisational relationships, benefit, policy, failure to prevent, and tolerance. Those provisions can illuminate a doctrinal debate but must not be applied as law already in force during this article's study period. T. Riza Zarzani and coauthors examine the range of sanctions for corporate offenders and the difficulty of treating a legal person like an individual offender (Zarzani et al., 2024). Their general account frames the sanctioning question, while Bedecarratz Scholz (2020) and Amiati et al. (2024) distinguish organisational duties from attribution and corporate culture. None substitutes for proof under the PDP Law and the applicable corporate case rules (Republic of Indonesia, 2023, arts. 45–49).

A Sequential Test and the Evidence Needed to Apply It

The first step identifies the specific prohibited act, the personal data at issue, the absence of lawful authority, and every mental or purpose element in the charged paragraph. The second traces the actor's employment, mandate, instruction, or other relationship with the corporation under the corporate case rule. The third tests whether the evidence supports benefit, tolerance, or failure to prevent the established offence. This sequence prevents an evidentiary shortcut from consumer harm directly to corporate guilt. The factors in Supreme Court Regulation No. 13 of 2016 are aids to assessment, not a general presumption of fault (Republic of Indonesia, 2022, arts. 67–70; Supreme Court of the Republic of Indonesia, 2016, arts. 3–4).

Different records answer different questions. Access logs, transfer records, and permissions may identify when data moved and through which account; they do not by themselves establish the lawfulness or purpose of the transfer. Processing agreements, job descriptions, authorisation chains, and internal messages may show who instructed it. Audit reports, incident tickets, budget decisions, and documented warnings can show what risks decision makers knew and when they could intervene. Investigators should record provenance, collection time, integrity, and any transformations of digital material, then compare technical records with witness and governance evidence. Article 47 of the PDP Law requires a controller to demonstrate accountability for processing, but that duty must not be recast as an automatic reversal of the criminal burden of proof (Republic of Indonesia, 2022, art. 47).

For an omission to support attribution, analysis should specify the control that was reasonably required at the time, the person able to implement it, and the connection between its absence and the charged act. Article 35 ties security measures to the nature and risk of the data; Article 37 requires supervision of parties under the controller's control. A vulnerability discovered only after an attack is different from a warning repeatedly escalated before a continuing unlawful transfer. Combining fragments of several employees' knowledge into corporate intent without tracing communication and authority would conceal the actual decision process (Republic of Indonesia, 2022, arts. 35, 37).

A compliance certificate is neither a defence in itself nor proof of adequate practice. Conversely, documented access controls, supervision, prompt containment, and a meaningful response may weaken an allegation of tolerance or failure to prevent the particular offence. The inquiry concerns controls actually operating in the relevant period, with due regard to the size, function, data, and known risks of the organisation. The duty to designate a data-protection officer under Article 53 is conditional; the absence of that officer cannot be treated as universal non-compliance (Republic of Indonesia, 2022, art. 53).

Controllers, Processors, Outsiders, and the Limits of Comparison

The use of a vendor does not automatically transfer the controller's responsibility. Article 51 of the PDP Law places processing under the controller's instructions within its responsibility, while processing by a processor outside those instructions and purposes becomes the processor's responsibility. Those rules allocate data-processing responsibilities; they do not establish the criminal guilt of both companies. Each proposed corporate defendant still requires a predicate offence, a relevant organisational connection, and an applicable ground of responsibility (Republic of Indonesia, 2022, art. 51). Muhammad Juang Rambe and coauthors examine data protection risks in the digital issuance of land deeds as part of a wider allocation of institutional responsibility (Ginting et al., 2025). That sectoral setting does

not resolve criminal attribution here, but illustrates why control over the relevant system and processing decision must be identified before responsibility is assigned.

If a vendor employee sells data for a private benefit in violation of effective instructions, the employee's conduct and the processor's possible responsibility must be assessed separately from the controller's instructions, oversight, and knowledge. If management ordered the sale or knowingly kept an access channel open for it, the documentary trail may justify a different conclusion. Cost savings from lower security expenditure should not simply be equated with profit derived from the intentional offence. Equally, later reputational loss does not erase earlier unlawful benefit. The inference should follow transactions and decisions, not a presumed outcome.

In Case C-340/21, the Court of Justice of the European Union held, in a GDPR civil compensation setting, that unauthorised access by a third party does not alone show that security measures were inappropriate, and a third-party act does not automatically exclude controller liability. The judgment supports a concrete assessment of precautions and causation. Its civil-law rules on proof and compensation cannot be imported as a presumption of corporate criminal guilt in Indonesia (Court of Justice of the European Union, 2023). This is a functional comparison, not an assertion that the two systems impose identical obligations.

Sanctions, Enforcement Choices, and Consumer Redress

The PDP Law's administrative fine of up to two per cent of annual income or receipts under Article 57(3) is distinct from a criminal fine. Article 70(2) makes a fine the principal corporate penalty, Article 70(3) permits up to ten times the maximum fine for the underlying offence, and Article 70(4) lists additional penalties, including forfeiture, performance of neglected duties, compensation, restrictions, licence revocation, and dissolution. Under the statutory text in the study period, the maximum individual fines in Articles 67(1), 67(2), 67(3), and 68 are respectively IDR 5 billion, IDR 4 billion, IDR 5 billion, and IDR 6 billion. The corporate multiplier is tied to the relevant charge; the two per cent administrative ceiling cannot be used as the criminal ceiling (Republic of Indonesia, 2022, arts. 57, 67–68, 70).

Administrative supervision and criminal investigation address different conduct and purposes. A regulator's response to deficient security or late notice should not, without more, be treated as proof of intentional unlawful disclosure. Equally, the presence of administrative sanctions does not erase the criminal offences expressly enacted in Articles 67 and 68. Enforcement authorities should document the factual basis for each route, preserve relevant evidence, and coordinate victim notification and containment. This is a proposed practice of reasoned enforcement rather than a categorical statutory requirement to exhaust administrative measures first (Republic of Indonesia, 2022, arts. 46, 57, 67–70).

Affected people need timely information even if fault is contested. Article 46 of the PDP Law requires written notice within 3×24 hours to data subjects and the designated institution, including the exposed data, when and how exposure occurred, and response and recovery measures. Notification can enable protective action, but the message should avoid exposing further personal data. Schwartz and Janger (2007) explain the value of coordinated breach notification. Romanosky et al. (2014) find associations between breach characteristics, mitigation, and litigation in United States federal cases; those findings do not establish what compensation or monitoring will achieve in Indonesia (Republic of Indonesia, 2022, art. 46).

A remedy should be tied to demonstrable effects and lawful powers: secure the compromised access, notify affected subjects, provide a workable claims channel, and verify completion of the order. A court should consider whether dissolution would impede compensation and protection of data still held by the company. Preservation of evidence must be coordinated with legal duties to end unlawful processing and delete data when required. The PDP Law's listed additional penalties permit a reasoned account of culpability, prevention, and redress without inventing a new sanction through guidance (Republic of Indonesia, 2022, arts. 43–44, 70).

Effective administration also depends on a clear path between compliance supervision, criminal investigation, and victim support. Scholarship on authority design and comparative

notification practice supplies reasons to specify responsibilities and protect access to victims' records, but it cannot establish the current staffing or operational status of any Indonesian agency without separate evidence (Widiatedja & Mishra, 2023; Situmeang et al., 2025).

Conclusion

Corporate criminal responsibility for a consumer data breach requires proof of an offence under Article 67 or 68 of the PDP Law, a legally relevant connection between the actor and the corporation, and a statutory basis for attributing responsibility to that corporation. Failures in security, supervision, or notification can require administrative action and furnish contextual evidence. They do not substitute for the intentional and unlawful conduct specified by the offence. Controllers, processors, and individuals should be assessed according to their actual role, authority, decisions, and evidence, rather than their titles or the fact that an incident occurred.

The proposed sequence connects technical records to instructions, policy, known risks, and the capacity to intervene. Enforcement should keep administrative compliance, criminal proof, notification, and consumer redress distinct while coordinating their practical responses. The Code enacted in 2023 remains a prospective point of comparison for this study period. Future research on charges, judgments, and incident records is needed to assess how consistently the framework works in practice.

References

- Amiati, M., Adhryansah, & Prihandono, I. (2024). Human rights violations and corporate criminal liability: An analysis of the new Indonesian criminal law. *Sriwijaya Law Review*, 8(2), 230–248. <https://doi.org/10.28946/slrev.Vol8.Iss2.3687.pp230-248>
- Bedecarratz Scholz, F. J. (2020). Defecto de organización y reglas de comportamiento en la imputación de las personas jurídicas. *Política Criminal*, 15(30), 694–728. <https://doi.org/10.4067/S0718-33992020000200694>
- Court of Justice of the European Union. (2023). *Natsionalna agentsia za prihodite* (Case C-340/21), judgment of 14 December 2023, ECLI:EU:C:2023:986. <https://curia.europa.eu/juris/liste.jsf?num=C-340/21>
- Ginting, G. G. P., Aspan, H., & Rambe, M. J. (2025). Electronic land deed issuance by land deed officials in Indonesia: Regulation, data protection, and legal certainty. *International Journal of Educational Review, Law and Social Sciences*, 5(4), 1081–1093. <https://doi.org/10.54443/ijerlas.v5i4.805>
- Hasibuan, A. R. H., Tanjung, I. U., & Panjaitan, K. P. Q. C. B. (2024). Legal protection for consumers from defamation crimes due to product reviews on social media. *Law Sinergy Conference*, 1(1), 337–344. <https://conference.sinergilp.com/index.php/lsc/article/view/47>
- Republic of Indonesia. (2022). Law No. 27 of 2022 on Personal Data Protection (Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi). <https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022>
- Republic of Indonesia. (2023). Law No. 1 of 2023 on the Criminal Code (Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana). <https://peraturan.bpk.go.id/Details/234935/uu-no-1-tahun-2023>
- Romanosky, S., Hoffman, D., & Acquisti, A. (2014). Empirical analysis of data breach litigation. *Journal of Empirical Legal Studies*, 11(1), 74–104. <https://doi.org/10.1111/jels.12035>
- Schwartz, P. M., & Janger, E. J. (2007). Notification of data security breaches. *Michigan Law Review*, 105(5), 913–984. <https://repository.law.umich.edu/mlr/vol105/iss5/2/>
- Situmeang, A., Park, J., Sudirman, L., Silviani, N. Z., & Agustini, S. (2025). Evaluating data breach notification protocols: Comparative analysis of Indonesia and South Korea. *Lentera Hukum*, 12(1), 42–61. <https://doi.org/10.19184/ejhl.v12i1.47621>

- Supreme Court of the Republic of Indonesia. (2016). Supreme Court Regulation No. 13 of 2016 on Procedures for Handling Criminal Cases by Corporations (Peraturan Mahkamah Agung Nomor 13 Tahun 2016). <https://peraturan.bpk.go.id/Details/209693/perma-no-13-tahun-2016>
- Widiatedja, I. G. N. P., & Mishra, N. (2023). Establishing an independent data protection authority in Indonesia: A future-forward perspective. *International Review of Law, Computers & Technology*, 37(3), 252–273. <https://doi.org/10.1080/13600869.2022.2155793>
- Zarzani, T. R., Ismaidar, & Barus, J. N. Br. (2024). Pemidanaan korporasi. *Juris Sinergi Journal*, 1(1), 9–12. <https://doi.org/10.70321/jsj.v1i1.12>