Law. Human. Environment

Journal homepage: https://environmentalscience.com.ua/en
Law. Human. Environment, 16(3), 173-190

UDC 343.98:347.74(4+71)
DOI: 10.31548/law/3.2025.173

Administrative legal liability for data breaches: Securing the right to compensation in Indonesia and the EU

Diah Pawestri Maharani*
Master of Law
Brawijaya University
65145, 169 Jl. MT. Haryono, Malang, Indonesia
https://orcid.org/0000-0001-9734-5475

Afifah Kusumadara
Doctor of Law, Professor
Brawijaya University
65145, 169 Jl. MT. Haryono, Malang, Indonesia
https://orcid.org/0000-0001-7167-8044

Hanif Nur Widhiyanti
Doctor of Law
Brawijaya University
65145, 169 Jl. MT. Haryono, Malang, Indonesia
https://orcid.org/0009-0003-6100-382X

Reka Dewantara
Doctor of Law
Brawijaya University
65145, 169 Jl. MT. Haryono, Malang, Indonesia
https://orcid.org/0000-0002-6010-0279

Article's History:

Received: 17.05.2025
Revised: 20.08.2025
Accepted: 23.09.2025

Abstract

The protection of personal data has become a fundamental concern in both legal theory and governance due to the exponential growth of digital ecosystems. With an emphasis on the right to compensation for impacted parties,

Suggested Citation:
Maharani, D.P., Kusumadara, A., Widhiyanti, H.N., & Dewantara, R. (2025). Administrative legal liability for data breaches: Securing the right to compensation in Indonesia and the EU. *Law. Human. Environment*, 16(3), 173-190. doi: 10.31548/law/3.2025.173.

*Corresponding author

this study critically evaluated Indonesia's institutional and legal framework for handling breaches of personal data. The analysis, which employed doctrinal legal research methods, focused on the General Data Protection Regulation of the European Union, Government Regulation No. 71 of 2019, and the Personal Data Protection Law, specifically Article 82, which provides compensation for both material and non-material harm. The findings pointed to serious institutional shortcomings in Indonesia's legal system. The 2020 Tokopedia data breach, which affected over 91 million users, serves as an example of the absence of institutional oversight and procedural clarity. Citing the applicability of administrative jurisdiction under the Law on Public Administration, the Central Jakarta District Court dismissed the case on jurisdictional grounds. On June 15, 2022, the Supreme Court subsequently affirmed this decision. Although compensation was prescribed in Article 58 of the Personal Data Protection Law, the mechanisms for implementing this provision have not yet been developed. On the other hand, the General Data Protection Regulation ensures that data subjects have effective remedies by requiring both administrative oversight through independent supervisory bodies and judicial access. The study concluded that Indonesia must harmonise public-private liability structures, codify explicit procedural remedies, and establish an empowered data protection authority. Comparative observations from the General Data Protection Regulation highlight how crucial dual-track enforcement, enforceable rights, and institutional autonomy are to protecting personal information and rebuilding public confidence

Keywords: administrative dispute resolution; compensatory justice systems; institutional accountability; procedural legal mechanisms; misuse of personal data; remedies for privacy violations

Introduction

The increasing significance of digital infrastructure in modern life has made protecting personal data even more urgent. The misuse of personal information presents systemic risks that extend beyond individual harm as digital interactions increasingly shape the social, economic, and political spheres. In this regard, data protection is a fundamental issue of democratic accountability, institutional legitimacy, and public trust rather than just a technical or legal one. Contemporary research underscores the need for stronger mechanisms to ensure accountability and redress in cases of data misuse (Lynskey, 2023). Data protection is framed as a fundamental right, emphasising the significance of cohesive institutional mechanisms for cross-jurisdictional enforcement (Syrlybayeva *et al*., 2024). Institutional ambiguity is identified as a key barrier to safeguarding personal data, with legal clarity being essential in digital governance. G. Hilary *et al*. (2016) argued that negligent corporate actors who fail to implement adequate security measures effectively facilitate harm and violate privacy rights, further noting that delayed breach notifications absent exigent circumstances are ethically impermissible. Together, these perspectives highlight the need for legal systems that combine preventive safeguards with prompt, enforceable remedies.

Within the European Union, Article 82 of the General Data Protection Regulation (GDPR) (2016) guarantees the right to compensation for both material and non-material harm arising from infringements, imposing liability on controllers and processors. Judicial practice, particularly the Court of Justice of the European Union (CJEU) ruling in Case No. C-300/21 (2023), clarifies that mere breaches do not automatically entitle for compensation; claimants must

demonstrate actual damage and causation, while Member States retain flexibility in defining damage thresholds. N. Lomas (2023) observed that courts are increasingly expanding the interpretation of "non-material damage", thereby expanding victims' access to remedies. A.A. Rahman and G. Greenleaf (2023) emphasised that independent data protection authorities (DPAs) are critical to effective enforcement, particularly in emerging legal systems.

In the Indonesian context, earlier studies have examined personal data protection from various legal perspectives. One line of analysis views privacy as a constitutional right under Article 28G of the Constitution of the Republic of Indonesia (1945) but notes the absence of an adequate compensation mechanism for victims of data breaches. Research on the Tokopedia case points to overlapping jurisdictions and fragmented enforcement as major barriers to redress (Saputra, 2020), while other studies highlight how the lack of an independent data protection authority, coupled with legal uncertainty, weakens enforcement and erodes institutional trust (Widiatedja & Mishra, 2022)

A data breach is defined as unauthorised actors accessing, obtaining, or sharing private information for commercial, political, or financial reasons. Cyberattacks accounted for 80% of global data compromises in 2024. S.S. Gracy (2024) demonstrated a steep increase in the volume of exposed data worldwide during the same period. While over 660 million records were reportedly compromised in Indonesia, particularly affecting the information services sector, these national figures are drawn from industry reports rather than peer-reviewed studies (SOCRadar Your Eyes Beyond, n.d.).

The 2020 Tokopedia data breach is among the most well-known incidents illustrating Indonesia's legal restrictions (Rohendi & Kharisma, 2024). On dark web platforms, a hacker going by the name ShinyHunters offered to sell the data of 91 million users (Perkasa & Saly, 2022). The Indonesian Consumer Community responded by suing PT Tokopedia and the Ministry of Communication and Information Technology (Kominfo), alleging that they had violated a series of laws, including Regulation of the Minister of Communication and Informatics of the Republic of Indonesia No. 20 (2016), Government Regulation of the Republic of Indonesia No. 71 (2019), the Law of the Republic of Indonesia No. 27 (2022) (PDP Law). Uncertainties regarding public and private legal responsibilities were exposed when the Central Jakarta District Court dismissed the case on jurisdictional grounds and sent it to the State Administrative Court (Judgement of the Central Jakarta District Court in Case No. 235/PDT.G/2020/PN.JKT.PST, 2022). Although this decision was upheld in the Supreme Court's final decision on June 15, 2022, it did not address how overlapping responsibilities between private entities and regulatory bodies should be handled. This outcome reinforces concerns over Indonesia's fragmented legal system, marked by the absence of a centralised oversight body, limited liability frameworks, and practical remedies for victims of personal data breaches. In contrast, the GDPR offers a more integrated model. M. Marelli (2023) showed that effective governance relies on robust institutional mechanisms to manage overlapping jurisdictions, enabling national DPAs to coordinate and resolve conflicts consistently. These insights underscore that effective data governance demands clear legal mandates, institutional independence, and enforceable rights.

Based on these advancements, the purpose of the present study was to investigate how Indonesia developed a logical legal framework for protecting personal data that combines administrative supervision with private law tools. The key objective of the study was to examine the institutional obligations and legal foundation for

handling data breaches and providing compensation to victims. Additionally, the study assessed the shortcomings of the existing regulatory remedies, especially when administrative inaction is involved. Finally, to identify normative principles that could guide future reforms in Indonesia's data governance system, the study compared and contrasted local legal framework to the GDPR.

Materials and Methods

This study adopted a doctrinal legal methodology (also known as black-letter law research), focusing on the systematic exposition, interpretation, and critical analysis of legal provisions governing personal data protection and the right to compensation following data breaches. This approach was well-suited to the purpose of this study, as it enabled a detailed engagement with statutory texts, judicial reasoning, and secondary legal scholarship. The study was structured around four complementary approaches. The statutory approach involved interpreting key legislative instruments, particularly the Law of the Republic of Indonesia No. 27 (2022) and GDPR (2016) of the European Union. The analysis identified the scope of administrative and civil liability as well as procedural avenues available for data subjects seeking compensation. Conceptual approach explored the regulatory foundations of privacy, data subject rights, and administrative justice. By grounding the analysis in constitutional and human rights principles, such as Article 28G of the Constitution of the Republic of Indonesia (1945) and Article 8 of the Charter of Fundamental Rights of the European Union (2000), this approach clarified how liability and compensation are situated within broader frameworks of public accountability and legal redress.

The Tokopedia data breach was analysed as a representative case of data protection litigation in Indonesia. Judgement of the Central Jakarta District Court in Case No. 235/PDT.G/2020/PN.JKT.PST (2022), the Court of Appeals, and the Supreme Court (final ruling dated 15 June 2022) are critically examined to uncover the reasoning behind dismissals and to assess the structural limitations facing Indonesian courts in addressing personal data violations. A comparison with the European framework, particularly Article 82 of the GDPR (2016) and relevant judicial practice from the Court of Justice of the European Union (CJEU) served as a benchmark for evaluating Indonesia's liability regime. This comparative analysis helped to highlight divergences in enforceability, institutional capacity, and access to remedies.

Results

Personal data protection as a human right and administrative duty. Personal data protection emerged as a pivotal legal concern, intertwining the safeguarding of individual privacy rights with the administrative responsibilities of both public and private entities. It is essential to define 'personal data' to understand the scope and application of data protection law. International and regional legal instruments, including European Union Data Protection Directive (1995), the Convention for the Protection of Individuals about Automatic Processing of Personal Data (1981), and the OECD (2002) guidelines generally define personal data as any information relating to an identified or identifiable individual. Even when such information is disaggregated or anonymised, data protection authorities have affirmed that such data must still be protected if it can be retraced to a particular individual.

Indonesia adopts an analogous approach through the Law of the Republic of Indonesia No. 27 (2022), which defines personal data as "any data about an identified or identifiable individual, either directly or indirectly, through electronic or non-electronic systems" (Article 1, Item 1). Furthermore, the Regulation of the Minister of Communication and Informatics of the Republic of Indonesia No. 20 (2016) classifies

personal data as part of "specific individual data", which must be stored, maintained, and kept confidential following the regulatory standards. The regulation highlights that personal data includes any true and verifiable information that can be directly or indirectly attributed to an individual (Wibowo *et al*., 2024)

In both Indonesian and European contexts, the protection of personal data is directly linked to the broader concept of the right to privacy. Indonesia's legal system explicitly recognises this in the elucidation of the PDP Law (2022), which affirms that data protection is a manifestation of the constitutional right to dignity and security under Article 28G(1) of the Constitution of the Republic of Indonesia (1945). The Law further defines personal data protection (Article 1, Item 2) as "the entire effort to safeguard personal data during its processing to protect the constitutional rights of the data subject". The PDP Law categorises personal data into two types: specific personal data and general personal data. Specific personal data includes sensitive categories such as health records, biometric data, genetic information, criminal records, data on children, and personal financial information. General personal data encompasses identifiers such as full name, gender, nationality, religion, and marital status, including combinations of data that can lead to the identification of the individual (Cholil & Rahmi, 2024).

The framing of personal data protection as a human right has been further reinforced by Indonesia's ratification of the International Covenant on Civil and Political Rights (1966) (ICCPR). Article 17 prescribes that no individual shall be subjected to arbitrary or unlawful interference with their privacy, and that national legislation must effectively regulate the collection and processing of personal information. Analogously, in the European legal order, the right to privacy is prescribed in Article 7 of the Charter of Fundamental Rights of the European Union (2000) and Article 8 of the European Convention on Human Rights (1950) which recognise privacy and data protection as core elements of fundamental, which established minimum privacy and security standards for member states. However, with the proliferation of digital technologies and online services, the European data protection authorities acknowledged the need for a more comprehensive approach.

In response, the General Data Protection Regulation (2016) (GDPR) applies to all entities, both public and private, that process personal data of individuals within the EU, regardless of the entity's location. The regulation imposes not only legal but also administrative obligations, requiring data controllers and processors to implement technical and organisational measures, conduct impact assessments, and notify authorities and data subjects in case of breaches. From this perspective, personal data protection functions dually as a human rights safeguard and as an administrative obligation. The role of state authorities is not merely to declare the right but to establish effective institutional mechanisms, such as independent supervisory bodies, administrative procedures, and sanctioning powers, to ensure enforcement. Likewise, private entities are subject to strict administrative liability for failing to implement adequate data protection safeguards. Thus, both Indonesia and the European Union recognise personal data protection as essential to individual autonomy and democratic governance. However, the degree to which these rights are supported by administrative enforcement mechanisms continues to be a key point of divergence and an area for ongoing legal development.

Conceptualisation and classification of personal data and breaches. The protection of personal data is intrinsically tied to the constitutional mandate to safeguard individual dignity, privacy, and security (Yustina, 2022). In Indonesia, the Law of the Republic of Indonesia No. 27 (2022) was established as a legislative

response to growing concerns regarding the misuse and exposure of personal data in both public and private domains. According to its preamble and general elucidation, the Law seeks to enact Article 28G (1) of the Constitution of the Republic of Indonesia (1945), which affirms every individual's right to the protection of their person, family, honour, dignity, property, and sense of security. Personal data breaches are therefore not only violations of administrative standards but also of fundamental rights (Attidhira & Permana, 2022).

In global discourse, the term 'data breach' typically refers to any incident wherein personal data is accessed, disclosed, lost, or destroyed in an unauthorised or unlawful manner (Budiman, 2023). The GDPR (2016) of the European Union defines a data breach comprehensively as any violation of data security leading to the "accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data" that is transmitted, stored, or otherwise processed. This broad definition encompasses a variety of scenarios, including unauthorised access by both internal and external actors, intentional or negligent conduct by data controllers or processors, the transmission of personal data to unintended recipients, and the theft or loss of devices containing such data. Additionally, data breaches may involve unauthorised alteration or destruction of personal data, as well as instances where critical data systems become inaccessible or unavailable, thereby undermining data integrity and availability.

The PDP Law (2022) reflects conceptions of data governance analogous to those found in international frameworks. Article 16(1) outlines the core phases of personal data processing, which include the collection, analysis, storage, disclosure, and eventual destruction of data. Each of these phases is governed by a set of binding principles as specified in Article 16(2), which align closely with international best practices. These principles include data minimisation, requiring that data collection be limited and specific to its stated purpose; purpose limitation, mandating that processing activities correspond to clearly disclosed objectives; and the foundational standards of lawfulness, fairness, and transparency. Additionally, the PDP Law (2022) emphasises the accuracy and accountability of data, insisting that information be correct and verifiable. It also mandates the implementation of adequate security and confidentiality measures to prevent unauthorised access or disclosure. Storage limitation principles ensure that data must be erased or destroyed once its retention period has expired. Finally, the law introduces the principle of demonstrable responsibility, which obligates data controllers to maintain evidence of compliance with all applicable data protection standards.

The failure to adhere to these principles may result in what the Law categorises as a "personal data protection failure". As defined in Article 46(1) of the PDP Law (2022), this failure encompasses any breach of confidentiality, integrity, or availability of personal data, whether intentional or accidental. It includes security violations that result in the destruction, loss, modification, disclosure, or unauthorised access to personal data. At this point of failure, the rights of the data subject are directly harmed. Moreover, personal data breaches may be classified according to the source or cause of the breach. These may include:

1) internal breaches, such as employee negligence or intentional leaks for financial gain (e.g., espionage or lack of encryption);

2) external breaches, including cyberattacks, phishing, malware infections, or unauthorised third-party access.

This classification is critical in determining the degree of liability, the nature of sanctions, and the relevant administrative measures to be taken. The Indonesian legal framework, while normatively robust, still lacks clearly defined

mechanisms for accountability in cases where these principles are violated, particularly regarding the legal consequences for failure to prevent such breaches. Comparatively, under the GDPR (2016) framework, a breach not only triggers legal liability but also administrative obligations such as prompt notification to the supervisory authority and affected individuals, documentation of the breach, and immediate mitigation measures. The administrative response becomes a measure of institutional responsibility and the seriousness with which data protection principles are implemented. (Maleno & Kusumawati, 2024)

In conclusion, both Indonesian and EU legal frameworks conceptualise data breaches as critical violations that infringe on the individual's right to privacy. However, the administrative response and procedural clarity in addressing such failures, especially in terms of enforcement, remedies, and institutional oversight, are stronger and more operationalised in the EU context. For Indonesia, bridging this gap requires not only comprehensive legislation but also an enforceable administrative infrastructure to uphold the principles of personal data governance.

Tokopedia data breach and the limits of judicial and administrative redress in Indonesia. As established in the preceding sections, the processing of personal data must guarantee the rights of data subjects at every stage. Articles 5-15 of the PDP Law (2022) outline those rights, including the right to clear information regarding the identity and legal basis of the data processor, the purpose of data collection, the right to delete or terminate processing, and the right to file claims and receive compensation for the unlawful or unauthorised use of personal data. One of the earliest and most publicised legal cases involving a data breach in Indonesia is the 2020 Tokopedia data breach, where approximately 91 million user accounts were compromised. The Indonesian Consumer Community filed a lawsuit against both PT Tokopedia and the Ministry of Communication and Information (Kominfo), seeking IDR 100 billion in damages. The claim was based on allegations that Tokopedia had failed to implement adequate information security systems, leading to a massive data leak. The lawsuit was filed on 8 May 2020 under the Judgement of the Central Jakarta District Court in Case No. 235/PDT.G/2020/PN.JKT.PST (2022), categorising the case as an unlawful act (tort), due to resulting immaterial damages suffered by the users.

According to the plaintiff, the breach fell within the scope of "unforeseen loss" caused by an unlawful act, as stipulated in Article 59(2)(g) of Government Regulation of the Republic of Indonesia No. 80 (2019). In its claims, KKI requested the court to issue both provisional and final orders, including an injunction to temporarily suspend Tokopedia's electronic system operations during the trial process. Additionally, they demanded that Tokopedia notify all affected users in writing, detailing which categories of personal data had been accessed by third parties without user consent. Furthermore, they requested Kominfo to revoke Tokopedia's registration as an electronic system provider. In response, Tokopedia maintained that it had always prioritised the confidentiality and security of user data, characterising its platform as a "business of trust". The company stated that no sensitive user data, such as passwords, had been compromised despite the attack. The company asserted that "no critical information such as passwords was successfully leaked", emphasising that while a breach had occurred, sensitive data was protected.

After extensive proceedings, the case reached the Supreme Court, which issued a final ruling on 15 June 2022, rejecting the cassation appeal by KKI (Judgement of the Central Jakarta District Court in Case No. 235/PDT.G/2020/PN.JKT.PST, 2022). The Court reasoned that the law-

suit against the Ministry of Communication and Information constituted a challenge to the administrative acts as regulated by Article 87 of Government Regulation of the Republic of Indonesia No. 30 (2014). Therefore, the claim fell under the jurisdiction of the Administrative Court (PTUN), as opposed to the General Court. However, Tokopedia, as a private sector entity, complicated the jurisdictional boundaries, raising questions about the proper legal venue for mixed public-private liability in data breach cases (Hasan, 2024).

This outcome illustrates a significant limitation in Indonesia's current legal framework for personal data protection: the absence of an effective judicial or administrative mechanism for individual compensation claims. No precedent currently exists in Indonesia where a court has upheld a compensation claim by data subjects for breach-related damages. The lack of enforcement clarity, especially regarding whether cases should be adjudicated in general courts or administrative courts, creates a regulatory vacuum, undermining the right to redress.

While the PDP Law (2022) contains general provisions on compensation (damages), it delegates the procedural specifics to future government regulations. The Draft Government Regulation of the Republic of Indonesia "Implementing Regulations of Law Number 27 of 2022 Concerning Personal Data Protection" (2023) has since been circulated and addresses compensation in Articles 115-120. It recognises both material and immaterial losses, mandating that compensation may be paid in monetary form based on the extent of the loss experienced by the data subject. To claim compensation, data subjects must submit:

1) proof of the breach;

2) evidence of material or immaterial loss;

3) evidence linking the breach to the data controller or processor;

4) documentation of which data was compromised.

According to Article 120 of the Draft Government Regulation of the Republic of Indonesia "Implementing Regulations of Law Number 27 of 2022 Concerning Personal Data Protection" (2023), if a data controller or processor rejects or fails to fulfil the compensation request, the data subject may file a dispute resolution request with the personal data protection authority. This dispute mechanism may result in a) an agreement on the form and amount of compensation; b) specific guarantees to prevent the recurrence of the data breach or harm.

Notably, the PDP Law (2022) and its accompanying draft regulations do not provide direct access to courts for compensation claims, an omission that raises crucial questions regarding the judicial accountability and access to justice. Whether such administrative dispute resolution will be effective in practice is uncertain and warrants critical examination. In the absence of a functioning data protection authority and clear administrative enforcement pathways, the Tokopedia case exposes systemic challenges in implementing the right to compensation under Indonesia's legal regime. Therefore, this case study exemplifies the urgent need for clearer administrative mechanisms, a designated enforcement authority, and better-defined jurisdictional procedures for pursuing personal data breach claims in Indonesia. Comparative insights from other jurisdictions, particularly the European Union, offer a potential model for structuring an enforceable, dual-track compensation system that includes both administrative and judicial redress.

Comparative review: the right to compensation and liability under the GDPR. The GDPR (2016) provides a comprehensive legal framework for the protection of personal data and the enforcement of data subject rights. It applies not only to all 27 EU Member States but also to countries in the European Economic Area (EEA). One of the central features of the GDPR is

its recognition of the right to compensation and the legal liability of both data controllers and processors in cases where personal data is processed in violation of the Regulation. This right is codified in Article 82 of the Regulation, titled "Right to Compensation and Liability", which states that any individual who has suffered material or non-material damage as a result of a violation of the Regulation is entitled to receive compensation from the responsible controller or processor. The provision is structured as follows:

1) any person who suffers damage, either material or non-material, due to an infringement of the GDPR is entitled to receive compensation from the controller or processor responsible for the damage;

2) controllers are liable for damage resulting from any unlawful processing activity, while processors are liable only if they failed to processor-specific obligations or acted beyond or against the controller's instructions;

3) liability may be avoided if the controller or processor proves that it is not in any way responsible for the event giving rise to the damage;

4) in joint-processing situations, each controller or processor involved may be held jointly and severally liable to ensure full and effective compensation;

5) a controller or processor that pays full compensation retains the right to seek proportional reimbursement from other parties involved, based on their share of responsibility – Article 82 of GDPR (2016).

Importantly, Article 82(6) affirms the data subject's right to bring compensation claims before the competent national court of the relevant Member State, following Article 79(2). This integration of judicial redress into the data protection regime underscores the GDPR's commitment to not only substantive but also procedural justice.

Further clarification is provided in GDPR (2016), which outlines the interpretive principles for Article 82. It confirms that "damage" should be interpreted broadly according to the case law of the Court of Justice of the European Union (CJEU). This includes recognising both pecuniary and non-pecuniary damage and ensuring that data subjects receive full and effective compensation. The Recital also reiterates that controllers or processors must compensate for any damage resulting from unlawful processing; they may be exempt from liability if they demonstrate a complete absence of responsibility; in cases involving multiple actors, joint and several liability ensures that victims are not left uncompensated due to complexities in legal attribution (Judgment of the Court of Justice (Eighth Chamber) in Case No. C507/23, 2024).

Although the GDPR (2016) mandates compensation, it does not provide specific standards for assessing the scope or amounts of damages. This discretion is left to national courts of each Member State, which are obliged to apply domestic procedural law in harmony with GDPR principles of equivalence and effectiveness. This ensures consistency in protecting fundamental rights across the EU while respecting domestic legal autonomy. To guarantee enforcement, Article 51 GDPR requires each Member State to establish at least one independent public authority, known as a data protection authority, responsible for monitoring compliance with the Regulation. DPAs are empowered not only to supervise the application of GDPR provisions but also to investigate complaints, issue warnings, and impose administrative fines. In serious breach cases, DPAs may also mandate the payment of compensation or refer matters for judicial enforcement.

Thus, the GDPR offers a dual-track enforcement model: administrative enforcement through independent DPAs with investigatory and sanctioning powers and judicial enforcement through national courts, enabling individuals to assert their rights and seek damages (Oliver Yaros & Ana

Hadnes Bruder, 2023). This robust legal architecture stands in contrast to the current framework in Indonesia, where the absence of a functional data protection authority and unclear judicial mechanisms for compensation continue to hinder the exercise of data subject rights. While the Indonesian PDP Law mandates compensation in general terms, the GDPR goes further by establishing clear standards of liability, structured redress procedures, and the institutional capacity necessary to ensure compliance and accountability.

Key differences and implications: Indonesia's PDP Law vs the GDPR. The comparative review of Indonesia's PDP Law (2022) and the European Union's GDPR (2016) revealed significant structural and procedural differences in how each jurisdiction addresses the right to compensation and legal liability for data breaches. While both legal frameworks recognise the protection of personal data as a fundamental right, the implementation mechanisms for redress and enforcement diverge substantially. These differences have critical implications for the effectiveness of data protection regimes, particularly regarding administrative oversight, judicial enforcement, and the clarity of liability principles. Table 1 presents a synthesised comparison of key legal features.

Table 1. Comparison of Indonesia's PDP Law and the EU's GDPR

Aspect	PDP Law (2022)	GDPR (2016)
Right to compensation	Recognised (Article 58); procedural mechanism not yet fully operational	Recognised (Article 82); enforced through judicial mechanisms
Types of damage	Material and non-material losses acknowledged in Draft Government Regulation	Material and non-material damage explicitly protected; broad interpretation mandated by Recital 146
Enforcement body	Planned data protection authority (not yet fully established)	Independent DPAs operating in all EU Member States
Judicial access	No direct court access provided for compensation; redress through administrative dispute mechanisms only	Direct access to competent national courts guaranteed under Article 79(2) and Article 82 GDPR
Liability structure	Liability assigned to controllers/ processors; criteria under development	Controllers and processors are jointly/ severally liable; defined scope for exemption and recourse
Administrative oversight	Not yet enforced; implementation of oversight body pending	Active, independent administrative enforcement with the power to issue fines, investigate, and impose sanctions
Clarity of procedure	General provisions in the Law; detailed procedural steps deferred to implementing regulations	Full procedural clarity in GDPR and supported by CJEU case law
Public notification and breach reporting	Regulated but not systematically enforced	Mandatory breach notification to DPA and affected data subjects within 72 hours

Source: compiled by the authors of this study

These distinctions underscore several critical deficiencies in Indonesia's current data protection enforcement framework. Firstly, there is an institutional gap resulting from the absence of a fully operational data protection authority with the legal mandate to investigate personal data breaches and impose administrative sanctions. This gap limits proactive enforcement and regulatory oversight. Secondly, judicial ambiguity continues to be a persistent issue, as exemplified by the Tokopedia data breach case, where jurisdictional uncertainty arose due to the involvement of both public and private entities. The case highlighted a lack of clear procedural guidelines for handling data-related claims in Indonesian courts. Thirdly, and perhaps most significantly, the legal

architecture offers limited redress for victims of data breaches. Without direct judicial mechanisms or a robust system of remedies, individuals are unable to effectively claim compensation, a shortcoming that stands in contrast to international human rights norms guaranteeing the right to an effective remedy (Judijanto *et al*., 2024).

To bridge these enforcement and procedural gaps and bring Indonesia's data protection regime in line with global standards, several key reforms are necessary. The foremost priority is the establishment and empowerment of an independent Personal Data Protection Authority with clearly defined administrative powers, including investigatory and sanctioning functions. In parallel, the PDP Law and its implementing regulations must codify judicial redress mechanisms that allow data subjects to bring claims directly before competent courts. Furthermore, the legal framework should introduce binding procedural rules for compensation claims, addressing issues such as burden of proof, admissibility of claims, and the assessment of material and immaterial harm. Finally, a dual-access system should be instituted, ensuring that data breach victims have the option to pursue both administrative and judicial remedies. Such reforms are essential to operationalise the right to data protection and to uphold the broader constitutional commitment to individual privacy and legal accountability.

Administrative disputes in the enforcement of data protection obligations in Indonesia. The enforcement of personal data protection in Indonesia not only involves private and judicial claims but also opens a significant pathway for administrative dispute resolution, especially where violations concern procedural or compliance failures by data controllers or processors. These administrative disputes are increasingly central in a legal system transitioning toward a comprehensive data governance framework (Algamar & Ismail, 2023).

The PDP Law (2022), specifically Article 64, acknowledges that disputes arising from personal data violations may be resolved through arbitration, courts, or alternative dispute resolution mechanisms. However, the Law does not explicitly classify the nature of these disputes as civil, criminal, or administrative, nor does it delineate jurisdiction when the parties include both private and public actors. This ambiguity is partially addressed in the Draft Government Regulation of the Republic of Indonesia "Implementing Regulations of Law Number 27 of 2022 Concerning Personal Data Protection" (2023), which maps out the typologies of disputes and clarifies the role of administrative bodies in enforcement.

Administrative violations form a crucial dimension of enforcement under the PDP Law (2022), targeting procedural and regulatory failures committed by data controllers and processors. Codified in Articles 20-56, these obligations are foundational to lawful data governance. When breached, they give rise to administrative disputes that fall under the jurisdiction of the PDA – a body still awaiting operationalisation. Unlike civil or criminal violations, these infractions focus on compliance failures and procedural neglect, underscoring a regulatory rather than punitive approach. To illustrate the scope of such violations, Table 2 maps key categories of administrative breaches to their corresponding legal provisions.

Table 2. Categories of administrative violations under Indonesia's PDP Law (2022)

Administrative violation	Description	Legal basis
Unlawful data processing	Data processed without legal justification	Article 20
Lack of processing transparency	Failure to inform data subjects clearly and promptly	Article 21
Consent management failures	Inability to demonstrate valid consent from users	Articles 24-26

Table 2. Continued

Administrative violation	Description	Legal basis
Data integrity neglect	Errors in data accuracy or absence of impact assessments	Articles 29-34
Security and breach notification failures	Missing safeguards or delay in breach disclosures	Articles 35-46
Non-compliance with subject rights	Denial of rights such as access, correction, and erasure	Articles 32-44
Oversight disobedience	Failure to appoint Data Protection Officers or follow DPA instructions	Articles 51-53
Unauthorised cross-border transfers	Transferring personal data abroad without safeguards	Articles 55-56

Source: compiled by the authors of this study

Each of these violations constitutes an administrative breach rather than a mere civil wrongdoing. Article 57 of the PDP Law (2022) grants enforcement powers to the Data Protection Authority, authorising sanctions that range from written warnings to severe financial penalties. Specifically, the Law prescribes written warnings as a first response to non-compliance, temporary suspension of data processing operations, mandatory erasure or destruction of unlawfully obtained data, administrative fines of up to 2% of the violator's annual revenue. These penalties are distinctively non-judicial; they are to be imposed administratively rather than through the courts. The mechanisms for assessing these violations, determining sanctions, and handling appeals are expected to be fully elaborated in a forthcoming Government Regulation. This structure closely mirrors global best practices, particularly the GDPR (2016) framework, where DPAs play a central role in monitoring and enforcing data governance through independent administrative power.

Yet, several challenges persist. The current lack of a functioning DPA severely limits the enforceability of these administrative provisions. Moreover, procedural ambiguities, such as unclear jurisdiction and undefined appeal pathways-complicate the legal landscape. The Tokopedia case, for instance, highlighted the overlap between administrative and civil remedies, revealing the urgent need for clearer legal classifications and institutional coordination. To fully act on the PDP Law's (2022) promise of effective data protection, Indonesia must not only operationalise its supervisory authority but also establish a transparent, accessible administrative dispute mechanism. This should include clear procedural rules, enforcement pathways, and a well-publicised framework for handling violations. Only through such reforms can the balance between individual rights and institutional responsibility be meaningfully maintained.

The findings of this study revealed substantial institutional and procedural gaps in Indonesia's current data protection regime. Based on these findings, and compared to the GDPR (2016) framework, several policy-oriented recommendations can be made. Firstly, the establishment of an independent and fully empowered DPA is imperative. As observed in EU jurisdictions, a structurally autonomous DPA with investigatory and sanctioning powers ensures both preventive and corrective enforcement. The absence of such an institution in Indonesia continues to be a major institutional gap. Secondly, the lack of judicial redress mechanisms for data breaches must be addressed. Unlike the GDPR (2016), which guarantees direct access to courts under Article 79(2) and 82, the Indonesian PDP Law (2022) still relies on future implementing regulations to operationalise compensation. Judicial procedures for claiming damages, particularly standards of proof, jurisdiction, and admissibility, must be clearly codified. Thirdly, to reinforce regulatory compliance, detailed procedures for administrative sanctions and appeals should be developed. The

GDPR (2016) offers a model where penalties are governed by transparent guidelines, including the right to appeal and proportionality in sanctioning. Indonesia's legal framework should emulate this clarity. Fourthly, mandatory breach notification standards must be clearly enforced. Prompt and transparent reporting of data breaches is not yet systematically practiced in Indonesia. GDPR Article 33 and 34 mandate prompt notification to authorities and data subjects, standards that should be reflected in Indonesian regulations to ensure accountability. Fifthly, the legal relationship between administrative and civil liability should be clarified. The Tokopedia case illustrates how overlapping jurisdictions can lead to procedural confusion and delays in enforcement. Legal reforms must establish when a claim should be resolved through administrative mechanisms or the courts, avoiding jurisdictional fragmentation. Sixthly, capacity building in digital forensics and cyber investigation should be prioritised. Regulatory staff, judges, and law enforcement officials require specialised training to interpret and apply data protection norms effectively. This includes developing technological competencies for breach investigation and evidence evaluation. Lastly, Indonesia should promote regional cooperation and harmonisation through ASEAN. Aligning cross-border data protection standards, enabling joint investigations, and coordinating enforcement with regional partners will enhance cybersecurity and regulatory effectiveness. These recommendations are designed not only to bridge the current legal and institutional gaps but also to transform data protection into a truly enforceable right in Indonesia. An integrated approach that merges regulatory, judicial, and regional strategies is essential for building a trustworthy digital environment.

This findings of this study affirm that personal data protection in Indonesia currently lacks cohesive enforcement mechanisms, especially concerning compensation for victims of data breaches. These findings resonate with those of A. Saputra (2020) and F.N. Heriani (2020) who analogously concluded that overlapping jurisdictions and fragmented enforcement limit legal redress. However, the present analysis offers a more precise breakdown of institutional gaps, particularly the absence of an operational Data Protection Authority and the lack of binding procedural remedies, adding depth to their conclusions.

Conversely, Article 82 of the GDPR (2016) guarantees the right to compensation for both material and non-material harm arising from infringements, imposing liability on controllers and processors. Jurisprudence, especially the CJEU's ruling in Judgment of the Court of Justice in Case No. C-300/21 (2023), clarifies that mere breaches do not automatically entitle compensation; data subjects must demonstrate factual damage and causation, while national law retains flexibility in setting damage thresholds. The present findings reinforced these principles by showing that both controllers and processors are more likely to adopt preventive measures when legal obligations and enforcement structures are clearly defined. However, in contrast to the EU framework, the present study emphasised Indonesia's intricate jurisdictional relationships, arguing that both judicial access and administrative clarity are necessary for successful reform.

N. Lomas (2023) emphasised the judicial interpretation of "non-material damage" as expanding the scope of victims' rights. The judicial outcomes in the Tokopedia case do not align with this trend. The dismissal by the Central Jakarta District Court and the Supreme Court's refusal to address dual liability illustrate a contrasting reality where judicial recourse is still tenuous. The divergence likely stems from differences in institutional maturity and normative frameworks between EU and Indonesian courts. Analogously, A.A. Rahman and G. Greenleaf (2023) emphasised that the establishment of independent data

protection authorities significantly improves the enforcement of privacy rights, particularly in emerging legal systems. The present study supported the researchers' observation by showing that without an operational authority, Indonesian enforcement continues to be largely aspirational and lacks accountability mechanisms.

These comparative insights also resonate with F. Syrlybayeva *et al*. (2024), who identified institutional ambiguity as a barrier to data protection in Kazakhstan. Admittedly, the findings of the present study suggest that analogous institutional ambiguity in Indonesia likewise obstructs data governance clarity. Both studies converge on the conclusion that legal certainty and robust institutions are indispensable. Lastly, O. Lynskey's (2023) call for harmonised legal standards across jurisdictions gains greater relevance in light of the findings presented herein. The divergence between Indonesian enforcement and international norms underscores the imperative for legal alignment and cross-jurisdictional consistency.

In summary, this comparative engagement illustrates critical gaps between Indonesian and EU data protection frameworks. Differences in judicial interpretation, enforcement institutions, and procedural clarity highlight systemic challenges. These divergences may be attributed to Indonesia's evolving institutional design and legislative infancy. The study demonstrates that without a functioning supervisory authority and streamlined jurisdictional frameworks, the protection of data subjects' rights continues to be compromised.

Conclusions

The present study examined the legal administrative liability frameworks for personal data breaches in Indonesia and the European Union, with a particular emphasis on the right to compensation. The findings revealed that although Indonesia's Personal Data Protection Law recognises the significance of safeguarding personal data and the rights of data subjects, its enforcement mechanisms, both judicial and administrative, are still underdeveloped. The case study of the Tokopedia data breach exemplifies how the absence of procedural clarity, institutional capacity, and legal precedent has rendered data subjects unable to access effective remedies for immaterial harm.

In contrast, the European Union's General Data Protection Regulation offers a structured and enforceable model. It provides a comprehensive basis for assigning liability to data controllers and processors and guarantees the right to compensation through both judicial proceedings and administrative oversight. The GDPR also empowers independent Data Protection Authorities to impose sanctions, investigate breaches, and implement dispute mechanisms that are notably lacking or inactive in the Indonesian context. These differences underscore the urgent need for Indonesia to strengthen its legal and institutional infrastructure. A functional and independent data protection authority must be established, procedural norms for compensation claims must be codified, and judicial access for data subjects should be ensured. Administrative law must play a more prominent role in supporting personal data protection, especially in regulating the conduct of both private and public entities engaged in data processing activities.

Prospects for further research include a comparative study of data breach litigation trends in ASEAN countries, the role of digital forensics in administrative investigations, and the integration of artificial intelligence accountability within data protection regimes. As personal data continues to shape global digital ecosystems, the development of a coherent and enforceable administrative legal liability system will be essential to protect individual rights and ensure public trust.

Acknowledgements

None.

Funding

The study was not funded.

Conflict of Interest

None.

References

[1] Algamar, M.D., & Ismail, N. (2023). Data subject access request: What Indonesia can learn and operationalise in 2024? *Journal of Central Banking Law and Institutions*, 2(3), 481-512. doi: 10.21098/jcli.v2i3.171.

[2] Attidhira, S.W., & Permana, Y.S. (2022). Review of personal data protection legal regulation in Indonesia. *Awang Long Law Review*, 5(1), 280-294. doi: 10.56301/awl.v5i1.562.

[3] Budiman, R. (2023). The development of Personal Data Protection Law in Indonesia: Challenges and prospects for the implementation of Law No. 27 of 2022. *Jurnal Smart Hukum (JSH)*, 2(1), 24-36. doi: 10.55299/jsh.v2i1.1352.

[4] Charter of Fundamental Rights of the European Union. (2000, December). Retrieved from https://www.europarl.europa.eu/charter/pdf/text_en.pdf.

[5] Cholil, A., & Rahmi. (2024). Law requirements on personal data protection and its impact in records management. *ANUVA*, 8(4), 523-536.

[6] Constitution of Indonesia. (1945, August). Retrieved from https://natlex.ilo.org/dyn/natlex2/r/natlex/fe/details?p3_isn=50148.

[7] Convention for the Protection of Individuals about Automatic Processing of Personal Data. (1981, January). Retrieved from https://rm.coe.int/1680078b37.

[8] Draft Government Regulation of the Republic of Indonesia "Implementing Regulations of Law Number 27 of 2022 Concerning Personal Data Protection". (2023, August). Retrieved from https://surl.li/pvauul.

[9] European Union Data Protection Directive. (1995, October). Retrieved from https://eur-lex.europa.eu/eli/dir/1995/46/oj/eng.

[10] General Data Protection Regulation. (2016, April). Retrieved from https://gdpr-info.eu/.

[11] Government Regulation of the Republic of Indonesia No. 71 "On the Operation of Electronic Systems and Transactions". (2019, October). Retrieved from https://peraturan.bpk.go.id/Details/122030/pp-no-71-tahun-2019.

[12] Government Regulation of the Republic of Indonesia No. 80 "On Trade through Electronic Systems". (2019, November). Retrieved from https://peraturan.bpk.go.id/Details/126143/pp-no-80-tahun-2019.

[13] Gracy, S.S. (2024). A global analysis of data breaches from 2004 to 2024. *arXiv*. doi: 10.48550/arXiv.2502.05205.

[14] Hasan, F. (2024). Liability of business actors for the protection of consumer personal data. *Mulawarman Law Review*, 9(1), 12-28. doi: 10.30872/mulrev.v9i1.1305.

[15] Heriani, F.N. (2020). *The Tokopedia consumer data leak case ends up in court*. Retrieved from https://surl.lu/teyknr.

[16] Hilary, G., Buttrick, J.D., & McGowan, R.J. (2016). The skeleton of a data breach: The ethical and legal concerns. *Richmond Journal of Law & Technology*, 23(1), article number 2.

[17] International Covenant on Civil and Political Rights. (1966, December). Retrieved from https://surl.li/qgkssk.

[18] Judgement of the Central Jakarta District Court in Case No. 235/PDT.G/2020/PN.JKT.PST. (2022, June). Retrieved from https://jdih.komdigi.go.id/perkara/view/21.

[19] Judgment of the Court of Justice (Eighth Chamber) in Case No. C507/23. (2024, October). Retrieved from https://surl.li/eohdql.

[20] Judgment of the Court of Justice in Case No. C-300/21. (2023, May). Retrieved from https://surl.li/muoxgk.

[21] Judijanto, L., Solapari, N., & Putra, I. (2024). An analysis of the gap between data protection regulations and privacy rights implementation in Indonesia. *The Easta Journal Law and Human Rights*, 3(1), 20-29. doi: 10.58812/eslhr.v3i01.351.

[22] Lomas, N. (2023). *Europe's top court clarifies GDPR compensation and data access rights*. Retrieved from https://techcrunch.com/2023/05/04/cjeu-gdpr-damages-access-rights/.

[23] Lynskey, O. (2023). Complete and effective data protection. *Current Legal Problems*, 76(1), 297-344. doi: 10.1093/clp/cuad009.

[24] Maleno, M., & Kusumawati, A. (2024). Comparative analysis of Indonesia's Personal Data Protection Law with the European Union and California regulations to identify best practices in protecting public privacy rights. *Indonesia Law Collage Association Law Journal (ILCA Law Journal)*, 181(2), 91-98.

[25] Marelli, M. (2023). The law and practice of international organisations' interactions with personal data protection domestic regulation: At the crossroads between the international and domestic legal orders. *Computer Law & Security Review*, 50, article number 105849. doi: 10.1016/j.clsr.2023.105849.

[26] OECD. (2002). *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Paris: OECD Publications Service.

[27] Perkasa, J., & Saly, J.N. (2022). Legal liability of marketplace companies against leaking of user data due to third party breaking according to Law Number 8 of 1999 Concerning Consumer Protection (Case Example: Tokopedia User Data Leaking in 2020). In *Proceedings of the 2021 international conference on education, language and art (ICELA 2021)* (pp. 771-776). Paris: Atlantis Press SARL. doi: 10.2991/assehr.k.220404.096.

[28] Rahman, A.A., & Greenleaf, G. (2023). Indonesia enacts Personal Data Protection Act, with a DPA. *SSRN Electronic Journal*. doi: 10.2139/ssrn.4343593.

[29] Rohendi, A., & Kharisma, D.B. (2024). Personal data protection in fintech: A case study from Indonesia. *Journal of Infrastructure, Policy and Development*, 8(7), article number 4158. doi: 10.24294/jipd.v8i7.4158.

[30] Saputra, A. (2020). *Consumer personal data breached, Tokopedia sued for IDR 100 billion*. Retrieved from https://surl.li/zkzjzv.

[31] SOCRadar Your Eyes Beyond. (n.d.). *Indonesia Threat Landscape Report*. Retrieved from https://surl.li/vojmpz.

[32] Syrlybayeva, F., Kassymova, X., Omarova, E., Zhussipova, B., & Nurgalieva, E. (2024). Protection of information about employee's personal data in the Republic of Kazakhstan. *Social and Legal Studios*, 7(4), 90-102. doi: 10.32518/sals4.2024.90.

[33] Wibowo, A., Alawiyah, W., & Azriadi. (2024). The importance of personal data protection in Indonesia's economic development. *Cogent Social Sciences*, 10(1). doi: 10.1080/23311886.2024.2306751.

[34] Widiatedja, P., & Mishra, N. (2022). Establishing an independent data protection authority in Indonesia: A future-forward perspective. *International Review of Law, Computer & Technology*, 50, article number 105849.

[35] Yaros, O., & Bruder, A.H. (2023). *Compensation under Art. 82 GDPR: A mere violation is not enough*. Retrieved from https://surl.lt/nrierx.

[36] Yustina, E.W. (2022). Legal aspect of health data and information protection after the promulgation of Law No. 27 of 2022 about protection of personal data. In *Digital healthcare transformation: Electronic medical record and personal data protection* (pp. 312-323). Semarang: UNIKA Soegijapranata.

Адміністративна та юридична відповідальність за порушення захисту даних: забезпечення права на компенсацію в Індонезії та ЄС

Діа Павестрі Махарані
Магістр права
Університет Бравіджая
65145, 169 Jl. MT. Харьоно, Маланг, Індонезія
https://orcid.org/0000-0001-9734-5475

Афіфа Кусумадара
Доктор права, професор
Університет Бравіджая
65145, 169 Jl. MT. Харьоно, Маланг, Індонезія
https://orcid.org/0000-0001-7167-8044

Ханіф Нур Відхіянті
Доктор юридичних наук
Університет Бравіджая
65145, 169 Jl. MT. Харьоно, Маланг, Індонезія
https://orcid.org/0009-0003-6100-382X

Река Девантара
Доктор юридичних наук
Університет Бравіджая
65145, 169 Jl. MT. Харьоно, Маланг, Індонезія
https://orcid.org/0000-0002-6010-0279

Анотація

Захист персональних даних став фундаментальною проблемою як у правовій теорії, так і в управлінні через експоненціальне зростання цифрових екосистем. З акцентом на праві на компенсацію для постраждалих сторін, у цьому дослідженні критично оцінено інституційну та правову базу Індонезії, щодо вирішення питань порушення персональних даних. Аналіз, в якому

використано доктринальні методи юридичних досліджень, було зосереджено на Загальному регламенті про захист даних Європейського Союзу, Постанові уряду Індонезії № 71 від 2019 року та Законі про захист персональних даних, зокрема статті 82, яка передбачає компенсацію як матеріальної, так і нематеріальної шкоди. Результати дослідження вказали на серйозні інституційні недоліки в правовій системі Індонезії. Порушення безпеки даних Tokopedia у 2020 році, яке торкнулося понад 91 мільйона користувачів, є прикладом відсутності інституційного нагляду та процедурної ясності. Посилаючись на застосовність адміністративної юрисдикції відповідно до Закону про державне управління, Центральний районний суд Джакарти відхилив справу на підставі юрисдикції. 15 червня 2022 року Верховний суд підтвердив це рішення. Хоча компенсація передбачена статтею 58 Закону про захист персональних даних, механізми реалізації цього положення ще не розроблені. З іншого боку, Загальний регламент про захист даних гарантує суб'єктам даних ефективні засоби правового захисту, вимагаючи як адміністративного нагляду через незалежні наглядові органи, так і доступу до судової системи. У дослідженні зроблено висновок, що Індонезія повинна гармонізувати структури відповідальності державного та приватного секторів, кодифікувати чіткі процедурні засоби правового захисту та створити уповноважений орган з захисту даних. Аналіз Загального регламенту про захист даних підкреслив, наскільки важливими для захисту персональних даних та відновлення довіри громадськості є подвійний підхід до забезпечення дотримання законодавства, права, що підлягають примусовому виконанню, та інституційна автономія

Ключові слова: адміністративне вирішення спорів; системи компенсаційної справедливості; інституційна підзвітність; процедурні правові механізми; зловживання персональними даними; засоби правового захисту у разі порушення права на приватність