JIHK is licensed undera Creative Commons Atribusi4.0 Internasional license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

DOI: 10.46924/jihk.v8i2.542

Civil Liability of Digital Platform Providers for User Losses Resulting from Data Breaches

Mukti Asmara Winisuda[1*], Suparwi Suparwi [2], & Yulian Dwi Nurwanti[3]

[1,2,3]Universitas Islam Batik Surakarta, Indonesia

Correspondence

Mukti Asmara Winisuda, Universitas Islam Batik Surakarta, Indonesia, Jl. Agus Salim No.10, Sondakan, Kec. Laweyan, Kota Surakarta, Jawa Tengah 57147, *e-mail:* ceoasmara@gmail.com

How to cite

Winisuda, Mukti Asmara., Suparwi, & Nurwanti, Yulian Dwi. 2027. Civil Liability of Digital Platform Providers for User Losses Resulting from Data Breaches. *Jurnal Ilmu Hukum Kyadiren* 8(2), 274-287. https://doi.org/10.46924/jihk.v8i2.542

Original Article

Abstract

The proliferation of digital platforms has increased the collection and processing of personal data while simultaneously amplifying the risk of data breaches that may result in user losses. The central issue concerns the legal framework governing the civil liability of digital platform providers and the effectiveness of mechanisms for obtaining compensation for such losses. This study examines the forms of civil liability applicable to digital platform providers acting as personal data controllers and the mechanisms for resolving compensation claims through both nonjudicial and judicial proceedings. It employs a normative legal research methodology, incorporating statutory, conceptual, and case-based approaches, together with a qualitative and prescriptive analysis of primary and secondary legal sources. Civil liability may arise from either a breach of contract (wanprestasi) or a tort (perbuatan melawan hukum), as governed by Indonesia's Personal Data Protection (PDP) Law and Civil Code. The effectiveness of compensation mechanisms depends on establishing the violation, fault, damages, and a causal relationship between the wrongful conduct and the resulting losses, including both material and nonmaterial damages. This study concludes that strengthening data controllers' accountability, ensuring transparency in evidentiary procedures, and improving access to dispute resolution mechanisms are essential to ensuring the effective protection and restoration of users' rights.

Keywords: *Civil Liability, Personal Data Breach, Digital Platform, Compensation*

Abstrak

Perkembangan platform digital meningkatkan pengumpulan dan pemrosesan data pribadi, tetapi sekaligus memperbesar risiko kebocoran yang dapat menimbulkan kerugian bagi pengguna. Permasalahan utamanya terletak pada konstruksi pertanggungjawaban perdata penyedia platform dan efektivitas mekanisme pemulihan kerugian. Penelitian ini bertujuan menganalisis bentuk pertanggungjawaban perdata penyedia platform sebagai pengendali data pribadi serta mekanisme penyelesaian tuntutan ganti rugi melalui jalur nonlitigasi dan litigasi. Penelitian menggunakan metode hukum normatif dengan pendekatan perundang-undangan, konseptual, dan kasus, serta analisis preskriptif kualitatif terhadap bahan hukum primer dan sekunder. pertanggungjawaban dapat didasarkan pada wanprestasi dan perbuatan melawan hukum dengan merujuk pada UU PDP dan KUHPerdata. Efektivitas ganti rugi bergantung pada pembuktian pelanggaran, kesalahan, kerugian, dan hubungan kausal, termasuk kerugian materiil maupun immateriil. Penelitian menyimpulkan bahwa penguatan akuntabilitas pengendali data, transparansi pembuktian, dan akses terhadap mekanisme penyelesaian sengketa diperlukan untuk menjamin pemulihan hak pengguna secara efektif.

Kata kunci: *Pertanggungjawaban Perdata, Kebocoran Data Pribadi, Platform Digital, Ganti Rugi*

1. INTRODUCTION

The development of information and communication technologies has transformed economic activities by facilitating the use of digital platforms for commercial transactions, service delivery, and information exchange. The emergence of online marketplaces, digital financial services, and various internet-based applications has accelerated transactions and improved efficiency while expanding access to broader markets.[1] This transformation has also reshaped the legal relationships between platform providers and users, particularly because the operation of digital services depends on the collection, storage, processing, and use of personal data. Information such as names, addresses, telephone numbers, email addresses, and transaction histories is not merely an operational necessity; it also constitutes an information asset with significant economic value. Accordingly, the more extensively personal data are processed, the greater the legal responsibility of platform providers to ensure data security, confidentiality, and the protection of users' rights.

The increasing reliance on personal data processing also heightens the risk of data breaches and unauthorized use of personal information. Incidents such as the 2014 eBay data breach and the alleged compromise of approximately 91 million Tokopedia accounts in 2020 demonstrate that vulnerabilities in digital security systems can have far-reaching consequences for users. Illegally accessed personal data may be sold, used for identity theft or fraud, or exploited for other purposes that result in material and nonmaterial losses.[2] The issue, therefore, extends beyond the occurrence of security incidents within electronic systems to encompass whether platform providers have fulfilled their legal obligations and whether they can be held civilly liable for the resulting damages.

Indonesia has established a normative framework for personal data protection through Law Number 27 of 2022 concerning Personal Data Protection (hereinafter, the PDP Law). Article 12 recognizes the right of personal data subjects to file claims and obtain compensation for violations involving the processing of their personal data. These rights correspond to the obligations imposed on personal data controllers, particularly under Articles 35, 36, and 39, concerning data security, accuracy, and the prevention of unauthorized access to personal data. However, the existence of these legal provisions does not necessarily ensure that users can effectively recover their losses. A significant challenge arises when users must establish the existence of a

---

1 Yanci Libria Fista et al., "Perlindungan Hukum Konsumen Dalam Transaksi E-Commerce Ditinjau Dari Perspektif Undang-Undang Perlindungan Konsumen," *Binamulia Hukum* 12, no. 1 (2023): 177–89, https://doi.org/10.37893/jbh.v12i1.599.

2 Limrogate Immanuel et al., "Perlindungan Hukum Perdata Terhadap Korban Kebocoran Data Pribadi Dalam Transaksi Digital Pasca Berlakunya Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi," *Indonesian Journal of Innovation Multidisipliner Research* 4, no. 3 (2026): 1580–93, https://doi.org/10.69693/ijim.v4i3.1259.

violation, fault, a causal relationship, and resulting damages, while information concerning security systems and data processing procedures remains largely under the control of platform providers. Accordingly, personal data breaches must be examined through two interrelated dimensions: the legal framework governing the civil liability of digital platform providers and the effectiveness of mechanisms through which users can seek compensation.

Research on personal data protection and the liability of digital service providers has developed alongside the increasing incidence of data breaches in electronic transactions. For example, Audiawaty et al. examine the protection of user data on the Tokopedia platform, focusing on the consistency of the regulatory framework established under the Law on Electronic Information and Transactions and the Consumer Protection Law. Their study identifies limitations in the personal data protection regulations that existed before the enactment of the PDP Law and establishes the legal basis for filing civil claims against electronic system operators.[3] Although this research provides a foundation for understanding the relationship between consumer protection and data security, it does not comprehensively examine the legal framework governing compensation claims under the current personal data protection regime.

The liability of digital service providers has also been examined by Anggraini, Diah, and Wiraguna, who analyze the liability of online lending service providers in cases involving the misuse and unlawful disclosure of consumers' personal data.[4] Their study identifies the administrative, criminal, and civil dimensions of liability, as well as the challenges associated with regulatory oversight. Meanwhile, Amelia examines the obligations of electronic system providers under the PDP Law, Government Regulation Number 71 of 2019, and other relevant regulations. The study emphasizes the importance of technical security measures, incident notification, security audits, and transparency as essential components of electronic system providers' legal obligations.[5] Although these studies broaden the understanding of the various dimensions of legal liability, neither specifically examines the mechanisms of civil redress through which users of e-commerce platforms can recover losses resulting from personal data breaches.

Research by Diah and Wiraguna examines the liability of e-commerce platforms under the Personal Data Protection (PDP) Law. Their findings indicate that the obligations of personal data controllers include establishing a lawful basis for

---

[3] Verra Sely Audiawaty et al., "Pertanggungjawaban Pelaku Usahaterhadap Data Konsumen Yang Menggunakan Aplikasi Tokopedia," *Jurnal Online Mahasiswa* 9, no. 1 (2022): 1–16.

[4] Al Satria Diah and Sidi Ahyar Wiraguna, "Tanggung Jawab Hukum Platform E-Commerce Atas Kebocoran Data Pribadi Dalam Perspektif UU No. 27 Tahun 2022," *Jurnal Kajian Hukum Dan Kebijakan Publik* 2, no. 4 (2025): 1089–96, https://doi.org/10.62379/3w415f14.

[5] Shelomita Putri Amelia, "Tanggung Jawab Hukum Penyelenggara Sistem Elektronik Terhadap Kebocoran Data Pribadi Pengguna," *Studia: Journal of Humanities and Education Studies* 1, no. 2 (2025): 132–41.

processing, ensuring transparency, and implementing adequate security measures.[6] Furthermore, Alparabi and Dikrurahman identify Article 1365 of the Indonesian Civil Code as a legal basis for characterizing data breaches as torts (perbuatan melawan hukum) and outline the legal remedies available to consumers.[7] Similarly, Taruni et al. examine the potential liability of business operators arising from either a breach of contract or a tort.[8]

The studies most closely related to the present research are those conducted by Fajrini and Rahmayani and Novianto.[9] Novianto examines the legal framework governing the civil liability of personal data controllers based on both breach of contract and tort, while identifying challenges such as information asymmetry and the difficulties associated with class-action lawsuits. Fajrini and Rahmayani highlight the relationship between the right to compensation under Article 12 of the PDP Law, the obligations of personal data controllers, and the provisions of Articles 1365 and 1366 of the Indonesian Civil Code. Nevertheless, the interaction between establishing the legal basis for civil liability, proving damages, and determining the appropriate mechanisms for resolving compensation claims by e-commerce users requires a more integrated analysis.

Unlike previous studies, which have tended to examine legal liability, grounds for litigation, or personal data protection as separate issues, this research integrates the framework governing the civil liability of digital platform providers with the mechanisms for resolving users' compensation claims. Its originality lies in examining the relationship between the obligations of personal data controllers, the legal grounds for civil claims—namely, breach of contract and tort—the substantiation of damages, and the available dispute resolution mechanisms under the current Indonesian legal framework.

This study has two objectives. First, it analyzes the forms of civil liability applicable to digital platform providers acting as personal data controllers under the PDP Law, the Indonesian Civil Code, and other relevant regulations, including the application of the legal doctrines of breach of contract (wanprestasi) and tort (perbuatan melawan hukum). Second, it examines the mechanisms for resolving users' compensation claims

---

6 Diah and Wiraguna, "Tanggung Jawab Hukum Platform E-Commerce Atas Kebocoran Data Pribadi Dalam Perspektif UU No. 27 Tahun 2022."

7 Aufa Aqlani Alparabi and Diky Dikrurahman, "Tinjauan Hukum Kebocoran Data Pribadi Konsumen Dalam Transaksi Elektronik Berdasarkan Perspektif Pasal 1365 KUHPERDATA," *Jurnal Hukum Lex Generalis* 7, no. 4 (2026): 1–27, https://doi.org/10.56370/jhlg.v7i4.3791.

8 Dwynhi Putri Taruni et al., "Pertanggungjawaban Perdata Pelaku Usaha E-Commerce Terhadap Kebocoran Informasi Data Pribadi Konsumen Dalam Transaksi Elektronik," *Unizar Recht Journal* 5, no. 1 (2026): 25–32, https://doi.org/10.36679/urj.v5i1.301.

9 Maulidia Fajrini and Nuzul Rahmayani, "Tanggung Jawab Perdata Platform E-Commerce Atas Kebocoran Data Pribadi Konsumen Berdasarkan Undang-Undang Perlindungan Data Pribadi," *Indonesian Journal of Innovation Multidisipliner Research* 4, no. 3 (2026): 12890–901, https://doi.org/10.69693/ijim.v4i3.2548; Mochamad Wahyu Novianto, "Tanggung Jawab Perdata Pengendali Dan Penyelenggara Sistem Elektronik Atas Kebocoran Data Pribadi Konsumen Di Indonesia," *Al-Zayn: Jurnal Ilmu Sosial & Hukum* 4, no. 4 (2026): 13827–41, https://doi.org/10.61104/alz.v4i4.10482.

through both out-of-court settlements and judicial proceedings, with particular attention to the burden of proof, causal relationships, and the recovery of both material and nonmaterial damages.

2. RESEARCH METHODOLOGY

This study employs a normative legal research methodology to examine the civil liability of digital platform providers for user losses resulting from personal data breaches and the legal mechanisms available for seeking compensation under Indonesian law. It adopts three complementary approaches. First, the statutory approach examines Law No. 27 of 2022 concerning Personal Data Protection, the Indonesian Civil Code, Law No. 8 of 1999 concerning Consumer Protection, and Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions. Second, the conceptual approach analyzes the legal doctrines governing civil liability, breach of contract (wanprestasi), tort (perbuatan melawan hukum), negligence, causation, damages, and legal remedies. Third, the case approach examines the 2020 Tokopedia data breach to contextualize the application of Indonesian legal norms to data breach-related disputes.

This study relies on secondary legal materials comprising primary legal sources, including legislation and relevant judicial decisions; secondary legal sources, such as scholarly books, journal articles, and legal commentaries; and tertiary legal sources, including legal dictionaries and encyclopedias. The materials are collected through documentary research and a review of relevant legal literature. They are analyzed qualitatively using prescriptive legal analysis and deductive reasoning. The analysis identifies the legal obligations of digital platform providers, examines the legal grounds and requirements for establishing civil liability, and evaluates the mechanisms for obtaining compensation through out-of-court settlements and judicial proceedings, with particular attention to evidentiary requirements, causal relationships, and the recovery of material and nonmaterial damages.

3. RESEARCH RESULT AND DISCUSSION

3.1. Forms of Civil Liability of Digital Platform Providers for User Losses Resulting from Personal Data Breaches

Digital platform providers that determine the purposes of and exercise control over the processing of personal data may be classified as personal data controllers. This status entails a legal obligation to ensure that personal data processing complies with the applicable principles of personal data protection. Article 47 of the Personal Data Protection (PDP) Law expressly provides that personal data controllers are responsible for the processing of personal data and must demonstrate their accountability in

fulfilling their personal data protection obligations. This provision reflects a shift in the focus of legal protection from the mere recognition of users' privacy rights to the imposition of accountability obligations on entities that control personal data processing. Accordingly, a platform provider cannot simply assert that it has obtained users' consent; it must also demonstrate that the collection, storage, use, and protection of personal data comply with applicable legal standards and obligations.

Civil liability arising from tort (perbuatan melawan hukum) is primarily grounded in Article 1365 of the Indonesian Civil Code, read in conjunction with Article 1366, which addresses liability for losses resulting from fault or negligence. This legal framework requires the establishment of four elements: an unlawful act, fault, damages, and a causal relationship. An unlawful act may consist of either an act or an omission by a platform provider in fulfilling its personal data protection obligations, such as failing to implement adequate security measures, allowing unauthorized access, or disregarding system vulnerabilities that could and should have been anticipated. The element of fault involves either intentional misconduct or negligence, while the resulting damages may be material, such as financial losses arising from identity theft, or nonmaterial, such as violations of users' privacy, sense of security, or reputation. Causation requires a demonstrable connection between the platform provider's conduct or omission and the damages claimed. Consequently, the occurrence of a data breach does not automatically establish an unlawful act. Rather, it provides a basis for assessing whether the personal data controller has fulfilled its obligations of due care and data security.

In addition to tort liability, breach of contract (wanprestasi) may also serve as a basis for civil liability when a contractual relationship exists between the user and the platform provider.[10] Such a relationship is generally established when users accept the platform's terms and conditions upon creating an account or accessing a digital service.[11] The provider's contractual obligations extend beyond delivering the agreed-upon services to include compliance with data protection commitments stipulated in the agreement and required under applicable laws and regulations. Article 1238 of the Indonesian Civil Code addresses a debtor's default in fulfilling an obligation, while Article 1243 provides the legal basis for claims seeking reimbursement of costs, damages, and interest arising from nonperformance. A platform provider's failure to fulfill its relevant contractual obligations may therefore give rise to liability for breach of contract, provided that the breach is established and its connection to the user's losses is demonstrated. However, not every data breach automatically constitutes a breach of

---

[10] Markus Suryoutomo et al., "Tanggung Jawab Perdata Dalam Kasus Wanprestasi Dan Perbuatan Melawan Hukum," *Jurnal Kolaboratif Sains* 8, no. 4 (2025): 2018–23, https://doi.org/10.56338/jks.v8i4.7261.

[11] Nursahada Maharani et al., "Analisis Yuridis Keabsahan Kontrak Elektronik Di E-Commerce Menurut Pasal 1320 KUHPerdata (Studi Putusan Nomor 629/Pdt.G/2020/PN Jkt.Sel): Penelitian," *Jurnal Pustaka Cendekia Hukum Dan Ilmu Sosial* 4, no. 2 (2026): 3555–62, https://doi.org/10.70292/pchukumsosial.v4i2.507.

contract. The determination requires an examination of the contractual terms, the nature of the obligation violated, the circumstances surrounding the alleged nonperformance, and the causal relationship between the breach and the resulting damages.

The PDP Law does not displace the civil liability framework established under the Indonesian Civil Code. Rather, it supplements that framework by establishing specific rights for personal data subjects and corresponding obligations for personal data controllers. Article 12(1) of the PDP Law grants personal data subjects the right to file claims and obtain compensation for violations involving the processing of their personal data, in accordance with applicable laws and regulations. This provision must be read in conjunction with Articles 35, 39, and 47 of the PDP Law, which address data security obligations, the prevention of unauthorized access, and the accountability of personal data controllers. Accordingly, a normative relationship exists between the specific obligations established under the PDP Law and the civil remedies available under the Indonesian Civil Code. Article 12 establishes the statutory basis for the right to seek compensation, while the relevant civil law provisions provide the legal grounds and elements necessary to establish liability.

This perspective is further supported by Constitutional Court Decision No. 284/PUU-XXIII/2025, which examined the constitutionality of Article 20(2)(a) of the Personal Data Protection (PDP) Law concerning valid consent for personal data processing. In that case, the petitioner emphasized the difficulties faced by victims of personal data misuse in pursuing legal remedies, as well as the imbalance of power between personal data subjects and controllers. It is important to clarify, however, that these arguments represented the petitioner's position and should not be construed as the Court's legal findings. On March 2, 2026, the Constitutional Court dismissed the petition in its entirety, affirming that valid consent must be given on the basis of adequate information concerning the purposes and activities of personal data processing. Although this decision does not directly address the burden of proof in compensation claims, it reinforces the obligation of personal data controllers to ensure that consent is validly obtained.

Furthermore, the accountability of personal data controllers encompasses the obligation to respond to personal data protection breaches. Article 46(1) of the PDP Law requires personal data controllers to provide written notification to both affected data subjects and the relevant authority within 72 hours (3 × 24 hours) of a personal data protection breach. At a minimum, the notification must identify the personal data affected, specify the time and manner in which the breach occurred, and describe the measures taken to address and mitigate its consequences. This obligation is consistent with the accountability principle established under Article 47 of the PDP Law, as it enables data subjects to become aware of incidents affecting their personal information and assess the corrective measures undertaken by the data controller. This requirement

is also consistent with Article 14 of Government Regulation No. 71 of 2019, which requires electronic system operators to implement personal data protection principles, including safeguards against loss, misuse, unauthorized access, and unauthorized disclosure. In comparison with previous studies, this analysis extends Novianto's perspective, which conceptualizes civil liability through the doctrines of breach of contract (wanprestasi) and tort (perbuatan melawan hukum), while also recognizing evidentiary challenges arising from information asymmetry.[12] Similarly, Fajrini and Rahmayani emphasize the relationship between Article 12 of the PDP Law and Articles 1365 and 1366 of the Indonesian Civil Code.[13] Meanwhile, Alparabi and Dikrurahman focus on characterizing data breaches as torts and examining the legal remedies available to consumers.[14] In contrast to these approaches, the present analysis argues that civil liability should be examined through an integrated framework that encompasses both the obligation to provide notification following a personal data protection breach and the accountability of personal data controllers. Such an integrated approach is essential because the assessment of liability involves not only the occurrence of harm but also the extent to which platform providers have fulfilled their preventive and corrective obligations.

The civil liability of digital platform providers may be established on two complementary legal grounds: tort and breach of contract.[15] The applicability of either ground depends on the nature of the legal relationship, the specific obligation breached, the existence of fault, the resulting damages, and the causal relationship between the wrongful conduct and the harm suffered. The PDP Law establishes a specific framework for protecting the rights of personal data subjects, while the Indonesian Civil Code provides the foundational legal framework for establishing liability and awarding compensation. A data breach resulting from a third-party cyberattack does not automatically exempt a platform provider from liability, nor does it necessarily establish the provider's fault.[16] The determining factor is whether the personal data controller can demonstrate that it has fulfilled its legal obligations concerning data security, due care, and accountability. Accordingly, personal data protection should be understood as a continuing legal obligation rather than merely an administrative or technical requirement. This understanding provides a stronger legal foundation for enabling users

---

12 Novianto, "Tanggung Jawab Perdata Pengendali Dan Penyelenggara Sistem Elektronik Atas Kebocoran Data Pribadi Konsumen Di Indonesia."

13 Fajrini and Rahmayani, "Tanggung Jawab Perdata Platform E-Commerce Atas Kebocoran Data Pribadi Konsumen Berdasarkan Undang-Undang Perlindungan Data Pribadi."

14 Alparabi and Dikrurahman, "Tinjauan Hukum Kebocoran Data Pribadi Konsumen Dalam Transaksi Elektronik Berdasarkan Perspektif Pasal 1365 KUHPERDATA."

15 Agung Prabowo Widyasaputro et al., "Pertanggungjawaban Hukum Platform Marketplace Atas Penjualan Barang Palsu Dan Dampaknya Terhadap Perlindungan Konsumen," *Jurnal Hukum Lex Generalis* 7, no. 4 (2026), https://doi.org/10.56370/jhlg.v7i4.3244.

16 Mangaraja Gideon Silaen and Men Wih Widiatno, "Tanggung Jawab Mutlak Pengendali Data Akibat Kebocoran Data Pribadi Di Aplikasi Mypertamina," *Jurnal Impresi Indonesia* 5, no. 3 (2026): 1259–74, https://doi.org/10.58344/jii.v5i3.7569.

to pursue civil remedies and obtain compensation for losses resulting from personal data breaches.

3.2. Mechanisms for Resolving Compensation Claims by Users Affected by Personal Data Breaches

The effectiveness of the right to compensation depends not only on the availability of a legal basis for filing a claim but also on users' ability to establish violations and obtain appropriate remedies. Personal data subjects have the right to file claims and receive compensation for violations involving the processing of their personal data in accordance with applicable laws and regulations. This provision establishes a statutory basis for users to seek redress when their rights to personal data protection have been violated.

This right should not be interpreted as guaranteeing automatic compensation whenever a data breach occurs. Users must still identify the nature of the violation, the applicable legal basis for liability, the type of damages suffered, and the causal relationship between the violation and the resulting harm. Article 12 of the PDP Law must be interpreted systematically in conjunction with the relevant provisions of the Indonesian Civil Code, particularly Articles 1238 and 1243 for claims based on breach of contract, and Articles 1365 and 1366 for claims based on tort and negligence.

Out-of-court dispute resolution constitutes an initial mechanism that allows users and platform providers to resolve disputes more efficiently and proportionately.[17] Users may submit complaints to platform providers by presenting preliminary evidence of the alleged data breach and the resulting losses. Such complaints should be followed by an internal investigation, an explanation of the incident, identification of the affected personal data, and disclosure of the measures undertaken to address the breach and mitigate its consequences. This process is closely related to the obligation to notify personal data protection breaches under Article 46 of the PDP Law, which requires personal data controllers to provide written notification to affected data subjects and the relevant authorities within 72 hours (3 × 24 hours). If the investigation establishes a breach of legal obligations that has resulted in user losses, the parties may negotiate appropriate forms of compensation, including reimbursement for economic losses and other relevant remedial measures. Accordingly, nonjudicial dispute resolution serves not only as a means of resolving disputes but also as an instrument for enforcing the accountability of platform providers in their capacity as personal data controllers.

The PDP Law also establishes a legal basis for resolving personal data protection disputes through Article 64, which provides for dispute resolution through arbitration, courts, or alternative dispute resolution institutions in accordance with applicable laws

[17] Muhammad Marzuki, "Online Dispute Resolution Dalam Rangka Penyelesaian Sengketa Di Bidang Transaksi Elektronik," *Jurnal Pancasila Law Review* 2, no. 2 (2025): 72–88.

and regulations. This provision demonstrates that compensation claims do not necessarily have to begin with judicial proceedings. Negotiation, mediation, and other alternative dispute resolution mechanisms may be pursued, subject to the agreement of the parties and the applicable legal framework. The effectiveness of out-of-court dispute resolution depends on transparency, good faith, and the willingness of platform providers to assume responsibility for the processing of personal data under their control.[18] In the absence of such transparency, users may be placed at a disadvantage because they lack access to the technical information necessary to determine the causes of a data breach and quantify the resulting losses.

If out-of-court proceedings fail to produce an agreement, users may pursue litigation by filing a civil lawsuit. The legal basis of the claim must be determined according to the nature of the legal relationship between the parties. Where losses result from the nonperformance of obligations arising from a platform's terms of service or user agreement, the claim may be based on breach of contract, with reference to Articles 1238 and 1243 of the Indonesian Civil Code. Conversely, where losses arise from acts or omissions attributable to a platform provider that violate its legal obligations to protect personal data, the claim may be based on tort under Articles 1365 and 1366 of the Indonesian Civil Code. This distinction has significant implications for the evidentiary requirements applicable to each claim. A breach-of-contract claim requires proof of the contractual relationship and the nonperformance of contractual obligations, whereas a tort claim requires proof of the elements of an unlawful act, fault, damages, and causation. Accordingly, identifying the appropriate legal basis for a lawsuit is a critical step in ensuring the clarity of legal arguments and strengthening users' positions when seeking compensation.

Establishing proof constitutes one of the primary obstacles to obtaining compensation for losses resulting from personal data breaches. Under the principles of civil evidence, as reflected in Article 1865 of the Indonesian Civil Code and Article 163 of the *Herziene Inlandsch Reglement* (HIR), a party asserting a right or alleging an event to establish that right generally bears the burden of proving its claim. Accordingly, users must present evidence establishing their status as personal data subjects, the occurrence of data processing or disclosure alleged to be unlawful, the damages suffered, and the causal relationship between the data breach and those damages. Relevant evidence may include official breach notifications, electronic communications with platform providers, transaction records, evidence of identity theft or misuse, documentation of financial losses, and other pertinent electronic information. The admissibility and evidentiary value of electronic evidence must also be assessed in accordance with Article 5 of the Law on Electronic Information and Transactions, as subsequently amended.

---

[18] Ahmad Ubaidillah et al., "Mediasi Sebagai Alternatif Penyelesaian Sengketa," *Primer: Jurnal Ilmiah Multidisiplin* 3, no. 4 (2025): 339–52, https://doi.org/10.55681/primer.v3i4.412.

The evidentiary challenge is further compounded by the asymmetry of information between users and platform providers. Information concerning security architecture, access logs, data processing histories, and system control mechanisms generally remains under the control of platform providers. Consequently, users may encounter considerable difficulties in establishing the technical causes of a breach or demonstrating specific instances of negligence on the part of a personal data controller. In this context, the accountability principle established under Article 47 of the PDP Law is particularly relevant. Personal data controllers are not only required to comply with personal data protection principles but must also demonstrate accountability for their data processing activities. Nevertheless, this provision does not automatically reverse the burden of proof in civil proceedings. A balanced evidentiary process therefore requires a careful assessment of the available evidence, the relevance of technical information held by platform providers, and the applicable rules of civil procedure.

Causation is another critical factor in determining the validity and extent of compensation claims. Not all losses suffered by users following a data breach can automatically be attributed to the platform provider. For example, when a user's identity information is exposed and subsequently used to commit fraud, it is necessary to establish whether a sufficient causal relationship exists between the data breach and the resulting financial losses. Such an assessment must also consider potential third-party conduct, the use of personal data obtained from other sources, and other contributing circumstances. Accordingly, the liability of a platform provider must be determined by examining the relationship between the personal data protection obligation that was allegedly breached, the circumstances surrounding the incident, and the specific losses that are legally attributable to the breach.

Compensation may encompass both material and nonmaterial damages, provided that an adequate legal basis exists and the damages can be legally attributed to the wrongful conduct. Material damages may include financial losses resulting from identity theft or misuse, account recovery expenses, costs incurred to secure a user's digital identity, and other economic losses causally connected to the breach. Nonmaterial damages, by contrast, may include violations of privacy, the loss of a sense of security, psychological distress, and reputational harm. For claims based on breach of contract, compensation may be sought under Article 1243 of the Indonesian Civil Code, which provides for the recovery of costs, damages, and interest, subject to the applicable legal requirements. In cases involving tort (perbuatan melawan hukum), Article 1365 of the Indonesian Civil Code provides the legal basis for seeking compensation for damages arising from conduct that satisfies the applicable elements of civil liability. Nevertheless, nonmaterial damages are not automatically recoverable merely because a user alleges subjective harm. Such claims require adequate legal substantiation and judicial assessment of the existence, relevance, and reasonableness of the damages claimed.

The findings of this study are consistent with those of Novianto, who identifies information asymmetry and evidentiary difficulties as major obstacles to enforcing the rights of personal data subjects to pursue legal remedies.[19] Fajrini and Rahmayani similarly argue that the right to compensation under Article 12 of the PDP Law must be interpreted in conjunction with the civil liability framework established under the Indonesian Civil Code.[20] Meanwhile, Alparabi and Dikrurahman emphasize the availability of civil litigation and consumer protection mechanisms as avenues for obtaining redress following personal data breaches.[21] Extending these previous studies, the present research integrates nonjudicial and judicial dispute resolution mechanisms with an examination of evidentiary requirements, causation, and the categories of compensable damages. This integrated analysis demonstrates that the statutory recognition of the right to file a claim does not, by itself, guarantee effective redress. Effective compensation requires proportionate evidentiary mechanisms, transparency in the disclosure of relevant information, and meaningful access to evidence held by platform providers.

The resolution of compensation claims arising from personal data breaches in Indonesia may be pursued through two complementary avenues: out-of-court dispute resolution and judicial proceedings. The effectiveness of these mechanisms depends on the clarity of the legal basis for the claim, the availability of relevant evidence, the establishment of a causal relationship, and the ability to substantiate both material and nonmaterial damages. Protecting the rights of personal data subjects requires more than merely recognizing their right to file claims under Article 12 of the Personal Data Protection (PDP) Law. It also requires effective remedial mechanisms capable of addressing the information asymmetry between users and platform providers. Accordingly, dispute resolution should seek to balance legal certainty, justice for affected individuals, and the accountability of personal data controllers. Compensation serves not only as a means of redressing losses already incurred but also as an instrument for enforcing legal accountability within the digital economy.

4. CONCLUSION

Digital platform providers acting as personal data controllers may incur civil liability under the PDP Law and the Indonesian Civil Code through either breach of contract or tort, depending on the nature of the legal relationship, the obligations violated, the existence of fault, and the damages established. Articles 12, 46, and 47 of the PDP Law

---

[19] Novianto, "Tanggung Jawab Perdata Pengendali Dan Penyelenggara Sistem Elektronik Atas Kebocoran Data Pribadi Konsumen Di Indonesia."

[20] Fajrini and Rahmayani, "Tanggung Jawab Perdata Platform E-Commerce Atas Kebocoran Data Pribadi Konsumen Berdasarkan Undang-Undang Perlindungan Data Pribadi."

[21] Alparabi and Dikrurahman, "Tinjauan Hukum Kebocoran Data Pribadi Konsumen Dalam Transaksi Elektronik Berdasarkan Perspektif Pasal 1365 KUHPERDATA."

reinforce the right to compensation, the obligation to notify affected parties of personal data protection breaches, and the accountability of personal data controllers, respectively. Compensation claims may be resolved through either out-of-court mechanisms or judicial proceedings, with the burden of proof and the establishment of causation serving as critical factors in determining the recoverability of material and nonmaterial damages.

The effectiveness of personal data protection requires a balance between the accountability of personal data controllers and users' access to justice. From a theoretical perspective, this study contributes to the development of the civil liability framework within the digital economy. From a practical perspective, its findings provide a legal reference for users seeking remedies and for platform providers seeking to fulfill their personal data protection obligations. Nevertheless, this study is limited by its normative legal approach, which does not include empirical examination of the implementation of the relevant legal provisions. Accordingly, strengthening regulatory oversight, ensuring transparency in evidentiary procedures, and developing effective mechanisms for collective redress remain essential. Future research should examine judicial practices, the implementation of the PDP Law, and comparative legal frameworks across different jurisdictions.

REFERENCES

Journals

Alparabi, Aufa Aqlani, and Diky Dikrurahman. "Tinjauan Hukum Kebocoran Data Pribadi Konsumen Dalam Transaksi Elektronik Berdasarkan Perspektif Pasal 1365 KUHPERDATA." *Jurnal Hukum Lex Generalis* 7, no. 4 (2026): 1–27. https://doi.org/10.56370/jhlg.v7i4.3791.

Amelia, Shelomita Putri. "Tanggung Jawab Hukum Penyelenggara Sistem Elektronik Terhadap Kebocoran Data Pribadi Pengguna." *Studia: Journal of Humanities and Education Studies* 1, no. 2 (2025): 132–41.

Audiawaty, Verra Sely, Firdaus Firdaus, and Ulfia Hasanah. "Pertanggungjawaban Pelaku Usahaterhadap Data Konsumen Yang Menggunakan Aplikasi Tokopedia." *Jurnal Online Mahasiswa* 9, no. 1 (2022): 1–16.

Diah, Al Satria, and Sidi Ahyar Wiraguna. "Tanggung Jawab Hukum Platform E-Commerce Atas Kebocoran Data Pribadi Dalam Perspektif UU No. 27 Tahun 2022." *Jurnal Kajian Hukum Dan Kebijakan Publik* 2, no. 4 (2025): 1089–96. https://doi.org/10.62379/3w415f14.

Fajrini, Maulidia, and Nuzul Rahmayani. "Tanggung Jawab Perdata Platform E-Commerce Atas Kebocoran Data Pribadi Konsumen Berdasarkan Undang-Undang Perlindungan Data Pribadi." *Indonesian Journal of Innovation Multidisipliner Research* 4, no. 3 (2026): 12890–901. https://doi.org/10.69693/ijim.v4i3.2548.

Fista, Yanci Libria, Aris Machmud, and Suartini Suartini. "Perlindungan Hukum Konsumen Dalam Transaksi E-Commerce Ditinjau Dari Perspektif Undang-Undang Perlindungan Konsumen." *Binamulia Hukum* 12, no. 1 (2023): 177–89. https://doi.org/10.37893/jbh.v12i1.599.

Immanuel, Limrogate, Mhd. Raihan Rizqullah, and Sabda Abdillah Lubis. "Perlindungan Hukum Perdata Terhadap Korban Kebocoran Data Pribadi Dalam Transaksi Digital Pasca Berlakunya Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi." *Indonesian Journal of Innovation Multidisipliner Research* 4, no. 3 (2026): 1580–93. https://doi.org/10.69693/ijim.v4i3.1259.

Maharani, Nursahada, Naufal Ilham Ramadhan, and Yudi Rijali Muslim. "Analisis Yuridis Keabsahan Kontrak Elektronik Di E-Commerce Menurut Pasal 1320 KUHPerdata (Studi Putusan Nomor 629/Pdt.G/2020/PN Jkt.Sel): Penelitian." *Jurnal Pustaka Cendekia Hukum Dan Ilmu Sosial* 4, no. 2 (2026): 3555–62. https://doi.org/10.70292/pchukumsosial.v4i2.507.

Marzuki, Muhammad. "Online Dispute Resolution Dalam Rangka Penyelesaian Sengketa Di Bidang Transaksi Elektronik." *Jurnal Pancasila Law Review* 2, no. 2 (2025): 72–88.

Novianto, Mochamad Wahyu. "Tanggung Jawab Perdata Pengendali Dan Penyelenggara Sistem Elektronik Atas Kebocoran Data Pribadi Konsumen Di Indonesia." *Al-Zayn: Jurnal Ilmu Sosial & Hukum* 4, no. 4 (2026): 13827–41. https://doi.org/10.61104/alz.v4i4.10482.

Silaen, Mangaraja Gideon, and Men Wih Widiatno. "Tanggung Jawab Mutlak Pengendali Data Akibat Kebocoran Data Pribadi Di Aplikasi Mypertamina." *Jurnal Impresi Indonesia* 5, no. 3 (2026): 1259–74. https://doi.org/10.58344/jii.v5i3.7569.

Suryoutomo, Markus, Mohammad Solekhan, Sri Murni, Hamdani Hamdani, and Saryana Saryana. "Tanggung Jawab Perdata Dalam Kasus Wanprestasi Dan Perbuatan Melawan Hukum." *Jurnal Kolaboratif Sains* 8, no. 4 (2025): 2018–23. https://doi.org/10.56338/jks.v8i4.7261.

Taruni, Dwynhi Putri, Haerani Haerani, and I. Gusti Ayu Ratih Damayanti. "Pertanggungjawaban Perdata Pelaku Usaha E-Commerce Terhadap Kebocoran Informasi Data Pribadi Konsumen Dalam Transaksi Elektronik." *Unizar Recht Journal* 5, no. 1 (2026): 25–32. https://doi.org/10.36679/urj.v5i1.301.

Ubaidillah, Ahmad, Hesti Nurkolistiana, Dewi Iriani, and Abid Rohmanu. "Mediasi Sebagai Alternatif Penyelesaian Sengketa." *Primer: Jurnal Ilmiah Multidisiplin* 3, no. 4 (2025): 339–52. https://doi.org/10.55681/primer.v3i4.412.

Widyasaputro, Agung Prabowo, Dewi Iryani, and Gradios Nyoman Tio Rae. "Pertanggungjawaban Hukum Platform Marketplace Atas Penjualan Barang Palsu Dan Dampaknya Terhadap Perlindungan Konsumen." *Jurnal Hukum Lex Generalis* 7, no. 4 (2026). https://doi.org/10.56370/jhlg.v7i4.3244.