Law Sinergy Conference
Volume III; Number I; Year 2026; Pages 053 – 059
Website:https://sinergilp.com
E-ISSN: 3048-3530

Liability of Personal Data Controllers for Data Breaches Tort Claims and Compensation Mechanisms under Law Number 27 of 2022 and Government Regulation Number 33 of 2026

J.E. Melky Purba

Email : jemelky_purba@dosen.pancabudi.ac.id

Universitas Pembangunan Panca Budi

Abstract

Personal data breaches have become an everyday risk in the digital society, yet civil redress for affected data subjects rarely succeeds. Law Number 27 of 2022 on Personal Data Protection grants data subjects the right to sue and receive compensation, and Government Regulation Number 33 of 2026, enacted on 16 July 2026 and effective from 16 January 2027, details the procedure for compensation claims. This study analyzes the legal basis of data controllers' civil liability, the construction of tort claims for data breaches and the related evidentiary problems, and the effectiveness of the compensation mechanism under the new implementing regulation. It employs a normative juridical method with statutory and conceptual approaches. The findings show that the security and accountability obligations of controllers under the Personal Data Protection Law can serve as the benchmark for unlawfulness under Article 1365 of the Civil Code, but victims still face difficulties in proving fault, non-material loss, and causation. The procedure for requesting compensation from controllers under Government Regulation 33/2026 represents progress, but its effectiveness is hampered by the absence of the personal data protection authority. This study recommends a presumption of fault for controllers, guidelines for assessing non-material damages, wider use of class actions, and accelerated establishment of the supervisory authority.

Keywords: *personal data protection, data breach, tort, compensation, civil liability*

INTRODUCTION

Digital transformation has made personal data both an economic asset and a new source of vulnerability. Almost every transaction, from online shopping and financial services to public services, requires the surrender of personal data to another party. When such data leak, data subjects may suffer various harms, such as fraud, identity misuse, loss of a sense of security, and financial loss. Tanjung and Adriani (2022) show that cybercrime develops faster than the law's capacity to address it, so a legal policy that prioritizes victim protection is needed.

Indonesia has Law Number 27 of 2022 on Personal Data Protection (PDP Law), which has been fully in force since October 2024. Article 12 paragraph (1) of the PDP Law affirms that data subjects have the right to sue and receive compensation for violations in the processing of their personal data. Further provisions on the procedure for imposing compensation were mandated to be set out in a government regulation. This mandate was only fulfilled through Government Regulation Number 33 of 2026 on the Implementing Regulation of Law Number 27 of 2022, which was enacted and promulgated on 16 July 2026 and takes effect on 16 January 2027 (Hukumonline, 2026).

CC Attribution-ShareAlike 4.0 License.

Although a normative framework is now available, civil redress for data breach victims still faces serious obstacles. To date, civil claims for data breaches have generally been brought under Article 1365 of the Civil Code on unlawful acts (torts), but proving a data breach violation remains difficult for victims (Hukumonline, 2019). Victims have no access to the controller's security systems, find it difficult to show a causal link between the breach and the loss, and face uncertainty about how to assess immaterial damage. Meanwhile, the personal data protection authority that should supervise controllers' compliance has not yet been established (Bisnis.com, 2026b).

Studies in civil law and the digital economy show that the liability of business actors in the digital ecosystem requires a new construction. Sitorus et al. (2025) discuss the resolution of civil disputes over crypto investment through arbitration and litigation, Tanjung et al. (2026) emphasize the principle of justice in regulating electronic commerce, while Bangun et al. (2025) show that consumers still face obstacles in obtaining redress through consumer dispute settlement mechanisms. This study complements these works by focusing on the liability of personal data controllers after the issuance of GR 33/2026. Accordingly, this study formulates three research questions:

1. What is the legal basis for the liability of personal data controllers for data breaches in Indonesian positive law?
2. How is a tort claim for a data breach constructed, and what are its evidentiary problems?
3. How effective is the compensation mechanism under GR 33/2026, and what improvements are needed?

This study aims to analyze the legal basis and construction of the liability of personal data controllers, identify the evidentiary obstacles faced by victims, and formulate recommendations so that the right to compensation under the PDP Law can be exercised effectively.

METHOD

This study is normative legal research using statutory and conceptual approaches (Tanjung, 2024). The statutory approach is used to examine the Civil Code, the PDP Law, GR 33/2026, the Electronic Information and Transactions Law, and regulations on class actions. The conceptual approach is used to examine the concepts of fault-based liability, presumed fault, and strict liability, as well as the concept of damage in the context of data breaches.

Primary legal materials consist of legislation, while secondary legal materials consist of books, journal articles, and expert opinions. The materials were analyzed qualitatively using deductive reasoning and systematic interpretation, linking the special provisions of the PDP Law and GR 33/2026 with the general doctrine of torts in civil law.

RESULTS AND DISCUSSION

1. Legal Basis for the Liability of Personal Data Controllers

The liability of personal data controllers for data breaches may derive from several legal bases. The first is Article 1365 of the Civil Code, which provides that every unlawful act causing loss to another obliges the person whose fault caused the loss to compensate it. The second is breach of contract, where there is a contractual relationship between the data subject and the controller, for example in financial services or e-commerce that include a promise to keep data confidential. The third is Article 12 of the PDP Law, which specifically grants data subjects the right to sue and to compensation. The fourth is Article 26 of the Electronic Information and Transactions Law, which grants the right to sue for the use of personal data without consent.

CC Attribution-ShareAlike 4.0 License.

These four legal bases are not mutually exclusive but complementary. The PDP Law serves as a special provision containing concrete obligations of controllers, while the Civil Code provides the general framework for the elements of liability and forms of compensation. A comparison of the four legal bases is presented in Table 1.

Table 1. Legal Bases for Compensation Claims for Personal Data Breaches

Legal Basis	Main Requirements	Notes
Article 1365 of the Civil Code	Unlawful act, fault, damage, and causal link	Burden of proof on the claimant; applies generally without a contractual relationship
Breach of contract (Article 1243 of the Civil Code)	Existence of an agreement and failure to perform obligations	Available only where there is a contractual relationship
Article 12 of the PDP Law	Violation in the processing of personal data	Procedure detailed in GR 33/2026; requires a request to the controller
Article 26 of the ITE Law	Use of personal data through electronic media without consent	Applies to data misuse, not specifically to breaches

Source: Author's formulation based on legislation.

The strength of the PDP Law lies in its clear formulation of controllers' obligations. Controllers must protect and ensure the security of the personal data they process through operational technical measures and a level of security appropriate to the nature and risks of the data. Controllers must also be accountable for the processing of personal data and demonstrate their accountability in fulfilling data protection principles. In the event of a protection failure, Article 46 paragraph (1) of the PDP Law requires controllers to submit written notification no later than 3 x 24 hours to the data subjects and the competent authority. These obligations become an important benchmark for assessing whether a controller has acted unlawfully.

Liability may also involve other parties in the data processing chain. Controllers often use data processors, such as cloud computing providers or technology partners. In civil law, Article 1367 of the Civil Code recognizes liability for the acts of persons under one's supervision. By analogy, the controller remains liable to the data subject for the processor's negligence, without removing the controller's right of recourse against the processor. This principle is in line with the idea that the management of a business entity bears administrative, criminal, and civil liability for negligence in managing the organization (Tanjung et al., 2024).

A different situation arises when a data breach occurs at a public body. In addition to GR 33/2026, which directs compensation requests against state public bodies through provisions on state administration, Supreme Court Regulation Number 2 of 2019 has established that disputes over unlawful acts by government bodies and/or officials fall under the jurisdiction of the administrative courts. As a result, victims of breaches at government institutions must take a different route from victims of breaches at private enterprises, with evidentiary characteristics and forms of redress that are not entirely the same. This difference in routes needs to be clearly explained to the public so that victims do not choose the wrong forum.

2. The Construction of Tort Claims and Evidentiary Problems

Since the Lindenbaum-Cohen judgment of 1919, unlawful acts have been understood broadly, not only as violations of statutes but also as violations of the subjective rights of others, violations of the actor's legal duties, and violations of morality and propriety in social life (Agustina, 2003). In the context of data breaches, unlawfulness can be proven through violations of the security and accountability obligations under the PDP Law, violations of the data subject's right to confidentiality, and violations of the standard of care reasonably expected of those managing large volumes of data.

CC Attribution-ShareAlike 4.0 License.

The main difficulty lies in the element of fault. Victims have no access to the controller's security systems and procedures, so it is almost impossible to prove that the breach resulted from negligence. Fuady (2002) explains that civil law recognizes three models of liability, namely fault-based liability, presumed fault, and strict liability. This study argues that the controller's obligation to demonstrate accountability under the PDP Law can be interpreted as a basis for applying presumed fault. This means that if a breach is proven, the controller is deemed negligent unless it can prove that it applied adequate security measures. This construction shifts the burden of proof to the party that best controls the information.

The element of damage is also problematic. Material damage, such as funds lost through fraud using leaked data, is relatively easy to calculate. However, many data breach victims have not yet suffered direct financial loss but instead face an increased risk of misuse and anxiety. Solove and Citron (2018) argue that risk and anxiety resulting from data breaches are real harms that should be recognized by law, because victims are forced to spend time, money, and effort to prevent misuse of their data. In Indonesian judicial practice, immaterial damages can indeed be awarded, but their assessment depends heavily on the judge's consideration. Mubarak and Zarzani (2024) show how the Supreme Court assesses compensation for professional negligence, which can serve as an analogical reference for assessing damage arising from negligent data management.

The experience of the European Union can serve as a comparison. Article 82 of the General Data Protection Regulation (GDPR) grants anyone who suffers material or non-material damage as a result of an infringement the right to receive compensation from the controller or processor, and exempts the controller or processor from liability only if it proves that it is not in any way responsible for the event giving rise to the damage (European Union, 2016). This construction is essentially a presumption of fault. The Court of Justice of the European Union in Österreichische Post (C-300/21) also affirmed that a mere infringement does not automatically give rise to a right to compensation, but non-material damage need not reach a certain threshold of seriousness (Court of Justice of the European Union, 2023). Both principles are relevant for developing the interpretation of Article 12 of the PDP Law.

The element of causation is the next challenge. A person's personal data may be held by many controllers, making it difficult to establish that the fraud suffered by the victim originated from a breach at a particular controller. In such situations, courts need to accept proof based on reasonable probability, such as the similarity between the type of data misused and the data leaked and the temporal proximity between the breach and the misuse. This approach is important so that the right to sue under Article 12 of the PDP Law does not become an unenforceable right.

Because data breaches usually affect thousands or even millions of people with relatively small individual losses, class actions are the most suitable instrument. Class actions allow victims to combine similar claims so that litigation costs are more efficient and their bargaining position against the controller is stronger. Experience in consumer dispute settlement shows that individual victims are often unable to fight for their rights alone (Bangun et al., 2025).

Besides the courts, victims who are consumers may also use the consumer dispute settlement mechanism under Law Number 8 of 1999 on Consumer Protection, since failure to maintain data security can be regarded as a violation of the consumer's right to safety in using services. However, Bangun et al. (2025) show that consumer complaints through the Consumer Dispute Settlement Agency are not always accepted and resolved effectively. Therefore, this route needs to be strengthened with specific guidelines on personal data disputes so that it can become a fast and inexpensive alternative.

3. The Compensation Mechanism under GR 33/2026 and Institutional Challenges

GR 33/2026 consists of 225 articles in 12 chapters and details the compensation mechanism in Articles 105 to 110 (Justisio, 2026). A request for compensation for violations in the processing of personal data is submitted by the data subject to the controller, stating the identity, data, information,

CC Attribution-ShareAlike 4.0 License.

or documents used as evidence, as well as the legal relationship between the data subject and the controller. Controllers must have mechanisms and policies for handling, assessing, and responding to compensation requests. If the controller refuses or no agreement is reached, the data subject may file a lawsuit in accordance with the law. For state public bodies, compensation requests are handled under the provisions on state administration (Bisnis.com, 2026a).

This mechanism has a positive side because it opens a faster and cheaper out-of-court settlement route. Controllers are also encouraged to build documented complaint-handling systems. However, there are three important notes. First, the obligation to submit a request to the controller first may become an obstacle if the controller does not respond within a reasonable time, so certainty on response deadlines is needed. Second, the provision that compensation requests against state public bodies follow the state administration regime may shift disputes to the administrative courts, with a different character of redress. Third, further provisions on handling and settling compensation are still left to regulations of the personal data protection authority.

The third note is the most fundamental problem. As of September 2026, the personal data protection authority had not been fully established, and experts consider that without it, the PDP Law and GR 33/2026 risk applying only on paper (Bisnis.com, 2026b). The authority is needed to draft technical guidelines, receive complaints, impose administrative sanctions of up to two percent of annual revenue, and facilitate dispute settlement. Without a supervisory authority, data breach victims can only rely on civil lawsuits with all their evidentiary limitations.

Based on this analysis, this study formulates four recommendations. First, the Supreme Court needs to issue guidelines for judges on applying presumed fault to controllers and assessing immaterial damage in data breach cases. Second, regulations of the personal data protection authority need to set deadlines for controllers' responses to compensation requests, minimum compensation standards, and an obligation to provide remedial services for victims. Third, class actions need to be optimized with the support of civil society organizations and legal aid institutions. Fourth, the government needs to accelerate the establishment of an independent personal data protection authority with full powers, in line with the long-advocated legal policy direction of protecting victims of cybercrime (Tanjung and Adriani, 2022).

These recommendations are also relevant to cases of the dissemination of personal data and information on social media, which often touch on both criminal and civil domains. Hasibuan et al. (2024) show that reviews and posts on social media can give rise to complex legal disputes. Clarity in the civil liability regime will help victims choose the most appropriate route of redress without always having to resort to criminal proceedings.

CONCLUSION

The liability of personal data controllers for data breaches has multiple legal bases, namely Article 1365 of the Civil Code, breach of contract, Article 12 of the PDP Law, and Article 26 of the ITE Law. The security and accountability obligations of controllers under the PDP Law can serve as a benchmark for unlawfulness, but victims still face difficulties in proving fault, immaterial damage, and causation. GR 33/2026 introduces a mechanism for requesting compensation from the controller before litigation, which is an important advance, but its effectiveness is still hampered by the absence of a personal data protection authority.

This study recommends applying presumed fault to controllers through Supreme Court guidelines, regulating response deadlines and compensation standards in the authority's regulations, optimizing class actions, and accelerating the establishment of an independent personal data protection authority. Further research should examine court decisions after GR 33/2026 takes effect to assess the consistency of the application of the right to compensation.

CC Attribution-ShareAlike 4.0 License.

BIBLIOGRAPHY

Agustina, R. *Perbuatan Melawan Hukum*. Jakarta: Postgraduate Program, Faculty of Law, Universitas Indonesia, 2003.

Bangun, K. D., J.E. Melky Purba, and H. J. Bintang. "Analisis Yuridis Penolakan Pengaduan Konsumen Melalui BPSK dalam Pembayaran Angsuran Mobil." *Kultura: Jurnal Ilmu Hukum, Sosial, dan Humaniora*, vol. 3, no. 3, pp. 404-413, 2025.

Bisnis.com. "Masyarakat Dapat Gugat dan Terima Ganti Rugi atas Pelanggaran Data Pribadi." *Bisnis.com*, 2 September 2026a.

Bisnis.com. "Pembentukan Badan PDP Dipercepat, Implementasi UU PDP Dinilai Belum Efektif." *Bisnis.com*, 13 September 2026b.

Court of Justice of the European Union. Judgment of 4 May 2023, UI v Österreichische Post AG, Case C-300/21, ECLI:EU:C:2023:370.

European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation).

Fuady, M. *Perbuatan Melawan Hukum: Pendekatan Kontemporer*. Bandung: Citra Aditya Bakti, 2002.

Hasibuan, Aulia Rahman Hakim, Indra Utama Tanjung, and K. P. Q. C. Br. Panjaitan. "The Rule of Law for Criminal Defamation of Product Reviews on Social Media." *International Journal of Synergy in Law, Criminal, and Justice*, vol. 1, no. 2, 2024, doi:10.70321/ijslcj.v1i2.37.

Hukumonline. "Data Pribadi Bocor, Bagaimana Mekanisme Penyelesaiannya?" *Hukumonline.com*, 2019.

Hukumonline. "Memandang PDP sebagai Investasi Korporasi." *Hukumonline.com*, 2026.

Justisio. "PP PDP Disahkan, Jangan Sampai Kena Sanksi." *Justisio.com*, 2026.

Mubarak, R. H., and T. Riza Zarzani. "Legal Analysis of Compensation to Doctors and Hospitals due to Doctors' Negligence (Study of Supreme Court Decision Number 2921K/Pdt/2018)." *International Journal of Synergy in Law, Criminal, and Justice*, vol. 1, no. 2, 2024, doi:10.70321/ijslcj.v1i2.34.

Republic of Indonesia. Civil Code (Burgerlijk Wetboek).

Republic of Indonesia. Government Regulation Number 33 of 2026 on the Implementation of Law Number 27 of 2022 on Personal Data Protection.

Republic of Indonesia. Law Number 8 of 1999 on Consumer Protection.

Republic of Indonesia. Law Number 27 of 2022 on Personal Data Protection.

Sitorus, H. K., A. D. A. Harahap, A. Latif, A. Syawalia, and Indra Utama Tanjung. "Civil Law Aspects of Crypto Investment Dispute Resolution Through Arbitration and Litigation." *ISNU Nine-Star Multidisciplinary Journal*, vol. 2, no. 3, 2025, doi:10.70826/ins9mj.v2i3.937.

Solove, D. J., and D. K. Citron. "Risk and Anxiety: A Theory of Data-Breach Harms." *Texas Law Review*, vol. 96, no. 4, pp. 737-786, 2018.

Supreme Court of the Republic of Indonesia. Supreme Court Regulation Number 2 of 2019 on Guidelines for Resolving Disputes over Government Actions and Jurisdiction over Unlawful Acts by Government Bodies and/or Officials (Onrechtmatige Overheidsdaad).

Tanjung, Indra Utama. *Dasar-Dasar Metode Penelitian Hukum*. Karanganyar: CV Pustaka Dikara, 2024.

Tanjung, Indra Utama, and E. N. Adriani. "Politik Hukum terhadap Penanggulangan Kejahatan Dunia Maya." *Judge: Jurnal Hukum*, vol. 3, no. 1, 2022, doi:10.54209/judge.v3i01.371.

CC Attribution-ShareAlike 4.0 License.

Tanjung, Indra Utama, R. M. P. Siregar, and A. Y. Anshori. "Reforming the Value-Added Tax Regulation on Electronic Commerce in Indonesia: Advancing Fairness in Digital Taxation." *Jurnal Cendikia ISNU SU*, vol. 3, no. 2, 2026, doi:10.70826/jcisnu.v3i2.1955.

Tanjung, Indra Utama, V. A. Chandra, K. A. Salsabila, R. F. Rangkuti, and A. M. S. Al Ghiffary. "The Role and Legal Responsibilities of Directors and Commissioners in Facing Administrative, Criminal and Civil Risks." *Jurnal Cendikia ISNU SU*, 2024, doi:10.70826/jcisnu.v2i2.844.

CC Attribution-ShareAlike 4.0 License.