International Journal of Economic Literature (INJOLE) https://sociohum.net/index.php/INJOLE
Vol. 4 No. 2 (2026), page., 273-287 e-ISSN: 3026-0221

LEGAL LIABILITY OF BUSINESS ENTITIES FOR VIOLATIONS OF CONSUMER PERSONAL DATA PROTECTION IN DIGITAL TRANSACTIONS IN INDONESIA: A LITERATURE REVIEW ON LEGAL CERTAINTY AND COMPENSATION MECHANISMS

Imam Jayanto *
Universitas Sam Ratulangi
imamjay_anto@unsrat.ac.id

Kamillah Firyaal Kanayah Hullah
Universitas Sam Ratulangi
hullahkanayah@gmail.com

Fikri Liputo
Universitas Sam Ratulangi
fikriliputo82@gmail.com

Abstract

The processing of personal data in digital transactions gives rise to a need for clarity regarding the liability of business operators and redress mechanisms for consumers who have suffered breaches. This study aims to analyse the legal certainty of business operators' liability for breaches of consumer personal data protection, as well as redress mechanisms in digital transactions in Indonesia. The method employed is normative legal research through a literature review using a legislative and conceptual approach. Primary and secondary legal sources were analysed qualitatively through inventory, systematic interpretation and synthesis. The findings indicate that Law No. 27 of 2022 on the Protection of Personal Data and Law No. 8 of 1999 on Consumer Protection provide a normative foundation for business operators' liability and the redress of consumer rights. Legal certainty requires clarity regarding the status of business operators as data controllers or processors, the basis for processing, security obligations, and the consequences of breaches. Redress mechanisms may be pursued through direct claims for redress, out-of-court settlements, or legal action in court in accordance with applicable jurisdiction and provisions. However, the implementation of remedies faces challenges regarding the identification of the liable party, access to evidence, proving a causal link, and the assessment of damages. This study concludes that clarity regarding liability norms must be linked to enforceable redress procedures. Strengthening consumer protection requires clarity on the forum for resolution, proportionate access to evidence, guidelines for assessing damages, and the enforcement of dispute resolution outcomes.

Keywords: legal liability; personal data protection; consumers; legal certainty; compensation.

Introduction

The development of digital transactions has expanded the scope of interaction between businesses and consumers whilst placing information management at the heart of commercial activities. Transactions are no longer merely about the delivery of goods or

the provision of services, but also involve a series of data-processing steps that enable user identification, payment processing, order fulfilment, and the provision (Yudha et al., 2025). In the Indonesian context, e-commerce activities have become the subject of official data collection covering business profiles, worker characteristics, business activities, and transaction values, as presented in the *2024 E-Commerce Statistics* publication (Central Statistics Agency [BPS], 2025). This scope demonstrates that e-commerce needs to be understood as an ecosystem of business activities, rather than merely a change in the medium of buying and selling. In line with this, the paper by Yu & Zhao (2019) emphasises that the significance of personal data in digital economic transactions is increasing in tandem with the expanding use of big data. This situation positions the protection of personal data as a fundamental issue in the legal relationship between businesses and consumers, as the quality of digital services cannot be assessed solely on the basis of the ease of transactions, but also on compliance in managing the data accompanying those transactions.

The role of personal data in digital transactions cannot be separated from an individual's right to self-protection. Law No. 27 of 2022 on the Protection of Personal Data, hereinafter referred to as the PDP Law, defines personal data as data relating to an identified or identifiable natural person, either on its own or in combination with other information, directly or indirectly, through electronic or non-electronic systems (Xiaying, 2019). This definition indicates that the scope of protection is not limited to identity information that explicitly identifies a person, but also encompasses information that can be used to recognise an individual through the combination of data. Furthermore, the preamble to the Personal Data Protection Act (PDP Act) emphasises that the protection of personal data forms part of human rights and the right to personal autonomy, which requires a legal basis to ensure data security (Republic of Indonesia, 2022, Article 1 and preamble, point a). Consequently, the provision of data by consumers to access digital services cannot be interpreted as granting unlimited authority to business operators. The use of data must still be situated within a framework of respect for the rights of data subjects, the legitimacy of the basis for processing, and the purpose limitation set out by law.

The issue of personal data protection should also not be narrowed down solely to incidents of data breaches resulting from system security breaches. The Personal Data Protection Act regulates data processing as a series of activities encompassing the acquisition and collection, processing and analysis, storage, correction and updating, display or disclosure, and finally the erasure or destruction of data. Each of these stages must be carried out in accordance with the principles of limited and specific collection, legal validity, transparency, purpose limitation, security, and accountability (Republic of Indonesia, 2022, Article 16). Consequently, an investigation into a breach must also cover the possibility of processing that is not in accordance with the purpose, collection that exceeds what is necessary, or disclosure that does not comply with the legal requirements of ‘ . In this context, consumer consent must not be regarded as the sole basis for

processing, as Article 20 of the Personal Data Protection Act recognises other bases, including the fulfilment of contractual and legal obligations. Consequently, the assessment of a business operator's actions must be carried out by identifying the legal basis for processing used and the obligations attached to that basis, rather than merely by checking for the existence of consent in the terms of service (Wiriani et al., 2025).

From a consumer protection perspective, the management of personal data is linked to the rights to security, accurate information, the submission of complaints, dispute resolution and compensation for losses. Law No. 8 of 1999 on Consumer Protection, hereinafter referred to as the UUPK, recognises consumers' rights to comfort, security and safety when using goods or services, as well as the right to compensation, damages or replacement if the goods or services received do not comply with the agreement or are not as they ought to be. On the other hand, business operators are obliged to act in good faith, provide accurate and clear information, and pay compensation under the circumstances specified by law (Republic of Indonesia, 1999, Articles 4 and 7). These provisions provide a basis for examining the relationship between the security of digital services and the protection of consumer interests. However, the application of the Consumer Protection Act (UUPK) to personal data breaches must be analysed based on the legal relationship, the nature of the service, and the form of loss in question; it should not be assumed to apply automatically to every incident. Therefore, the relationship between the Consumer Protection Act and the Personal Data Protection Act (UU PDP) must be examined so that consumers' rights as service users and as data subjects can be understood holistically without obscuring the differences in the scope of the two Acts.

Legal certainty is a key dimension in determining the liability of business operators for breaches of personal data protection. The Personal Data Protection Act explicitly establishes legal certainty and accountability as the principles underpinning the administration of personal data protection. The explanatory notes on the principle of legal certainty emphasise that data processing must be carried out on a legal basis so as to be recognised both in and out of court (Republic of Indonesia, 2022, Article 3 and its explanatory notes). In digital transactions, the application of this principle requires clarity regarding the party that determines the purpose and controls the processing, the party that carries out the processing on behalf of another party, and the allocation of obligations amongst them. The distinction between the controller and the processor is relevant because the Personal Data Protection Act defines both based on their roles in the processing, not merely on their title or the nature of their business activities. Indeed, processing by two or more controllers requires arrangements regarding their roles, responsibilities and relationships (Republic of Indonesia, 2022, Article 1 and Article 18). Consequently, legal certainty in this article is understood not only as the existence of written rules, but also as the fundamental clarity in determining the responsible party and the obligations that serve as the benchmark for assessing their actions (Waruwu & Siswoyo, 2024).

In addition to clarity regarding responsibilities, the effectiveness of consumer protection needs to be assessed through redress mechanisms that can be utilised in the event of a breach. Article 12(1) of the Personal Data Protection Act grants data subjects the right to bring a claim and receive compensation for breaches relating to the processing of their personal data, whilst paragraph (2) mandates that further provisions regarding processing breaches and the procedures for awarding compensation be laid down by government regulation (Republic of Indonesia, 2022). Meanwhile, Article 19 of the Consumer Protection Act (UUPK) sets out the liability of business operators to provide compensation for losses suffered by consumers as a result of the use of goods or services produced or traded by them. The UUPK also provides for the option of dispute resolution through the courts and out-of-court, and stipulates that out-of-court settlement is intended to reach an agreement on the form and amount of compensation as well as specific measures to prevent recurring losses (Republic of Indonesia, 1999, Article 19, Article 45, and Article 47). This convergence of regulations gives rise to the need for an analysis of the basis of claims, the appropriateness of the forum, the form of redress, and the scope of application of each provision. The recognition of the right to compensation must therefore be linked to the means of its enforcement so that the discussion does not stop at the mere statement that consumers have the right to claim (Vila Seoane, 2021).

The issue of proof serves as a crucial link between the regulation of liability and the exercise of the right to compensation. The Personal Data Protection Act (UU PDP) requires data controllers to maintain records of all processing activities and to grant data subjects access to their data and the processing records in accordance with applicable provisions. These obligations are relevant to examine in relation to the investigation of data breaches and the identification of the parties involved (Republic of Indonesia, 2022, Articles 31–32). On the other hand, Article 28 of the UUPK places the burden of proof regarding the presence or absence of an element of fault in the claim for compensation to which it refers upon the business operator (Republic of Indonesia, 1999). However, the provision concerning the element of fault cannot, in itself, be equated with the transfer of the entire burden of proof for every element of the claim.

In previous research, Versaci, (2018) examined the obligations of electronic system operators from the perspective of legal certainty, with a focus on privacy policies, compliance, administrative sanctions and efforts to prevent infringements. Building on this focus, this article adopts a more specific research approach centred on the relationship between the determination of liability, the proof of infringements and damages, and redress mechanisms for consumers, without claiming that this relationship has never been studied before.

Based on this overview, research into the legal liability of businesses for breaches of consumer personal data protection must be directed towards the interconnection between legal certainty and the exercise of the right to redress. The existence of the principle of legal certainty, the obligations of data controllers and processors, and the right

to sue and receive compensation provide a normative basis for systematically examining this relationship.

Research Methodology

This study employs a normative legal research method using a statutory and conceptual approach through a literature review to analyse the legal liability of business operators for breaches of consumer personal data protection in digital transactions in Indonesia (Zed, 2008). The primary legal materials examined include Law No. 27 of 2022 on the Protection of Personal Data, Law No. 8 of 1999 on Consumer Protection, the Civil Code, and regulations relating to transactions and the operation of electronic systems, whilst secondary legal materials include books, scientific journal articles, and other relevant research findings. The collection of legal materials was carried out through a search of regulatory documentation and academic publications, with sources selected based on their relevance to the research question, the clarity of the publication's identity, and the verifiability of the source. The collected legal materials were analysed qualitatively through inventory, classification, systematic interpretation and synthesis to examine the relationships between provisions as well as academic perspectives on legal certainty regarding liability and compensation mechanisms. The analysis focused on determining the liable party, the basis for imposing liability, the proof of infringement and loss, and the choice of dispute resolution; conclusions were then drawn deductively to address both research questions (Eliyah & Aslan, 2025) .

Results and Discussion

Legal Certainty Regarding the Liability of Business Operators for Breaches of Consumer Personal Data Protection in Digital Transactions

Legal certainty regarding the liability of business operators in the protection of consumers' personal data rests on the clarity of the norms governing the subject, obligations, prohibited acts, and the consequences of their violation. In this context, accountability serves as the link between a business operator's authority to process data and its obligation to be held accountable for such processing (Versaci, 2018). Law No. 27 of 2022 on Personal Data Protection, hereinafter referred to as the PDP Law, explicitly establishes legal certainty and accountability as the principles of personal data protection. The Explanatory Notes to Article 3(b) emphasise that all data processing must be carried out on a legal basis so that its implementation is recognised by law both in and out of court (Republic of Indonesia, 2022). This provision indicates that legal certainty cannot be interpreted merely as the availability of a privacy policy or terms of service, but rather encompasses the compliance of business operators' actions with the obligations set out in the law. In the study Ventura & Coeli, (2018) legal certainty also serves as a perspective for assessing the obligations of electronic system operators in protecting consumer data. However, from an analytical standpoint, the existence of policy documents must be

distinguished from the fulfilment of those obligations, as the inclusion of data protection commitments does not in itself prove that all processing activities have been carried out lawfully, securely and responsibly (Truli, 2018). Therefore, the measure of legal certainty in digital transactions must encompass both the clarity of the rules and the traceability of compliance with obligations by the party in control of data processing.

Determining the responsible party is a preliminary issue that must be resolved before assessing whether a breach has occurred. The Personal Data Protection Act (PDP Act) distinguishes between the personal data controller—the party that determines the purposes and exercises control over the processing—and the personal data processor—the party that processes data on behalf of the controller. Meanwhile, Law No. 8 of 1999 on Consumer Protection, hereinafter referred to as the Consumer Protection Act (UUPK), defines business operators based on the business activities they carry out, whether as individuals or through business entities (Republic of Indonesia, 1999, Article 1; Republic of Indonesia, 2022, Article 1). This fundamental difference in definition implies that the status of a business operator does not automatically determine its position as a controller or processor in every data processing activity. In the context of transactions via a marketplace, the roles of the platform operator, the trader, the payment provider and the support service provider must be analysed based on who sets the purposes, controls the use of the data, or acts on the instructions of another party (Taylor, 2020). Where processing is carried out by two or more controllers, Article 18 of the PDP Act requires an agreement regarding the roles, responsibilities and relationships between controllers, the jointly determined purposes and means of processing, and a joint point of contact (Republic of Indonesia, 2022). Consequently, clarity regarding liability requires a factual mapping of each party's activities, rather than the uniform allocation of liability to all parties involved in the transaction.

Clarity regarding the legal basis for processing is the next factor that determines whether a business operator's actions can be justified in law. Section 20 of the PDP Act requires the controller to have a legal basis for processing, which may take the form of explicit valid consent, the fulfilment of contractual obligations, compliance with a legal obligation, the protection of vital interests, the performance of a task carried out in the public interest or in the exercise of official authority, as well as other legitimate interests, whilst taking into account the balance of the rights and interests of the parties (Republic of Indonesia, 2022). This provision makes it clear that consent is not the only available legal basis, but the existence of other legal bases does not exempt the controller from the obligation to limit the purposes and scope of processing. Analytically, data required to fulfil an order must be distinguished from data intended for additional purposes, so that the legal basis for one activity is not automatically deemed to cover all subsequent uses (Takaryanto & Lany, 2025). When a business operator relies on consent as a legal basis, Articles 21–24 of the PDP Act set out obligations regarding the provision of information, the form of consent, the validity of clauses, and the controller's duty to prove consent. Consequently, a mere statement that a consumer has consented to the terms of use is

insufficient justification without an assessment of the clarity of the purpose, the information provided, and compliance with the requirements for consent. Legal certainty is established precisely when each processing purpose can be linked to an appropriate legal basis and evidence of compliance can be demonstrated.

The scope of a business operator's liability must also be understood to encompass the entire processing cycle, not merely the obligation to react after a data breach has occurred. Article 16 of the Personal Data Protection Act covers the activities of acquisition and collection, processing and analysis, storage, correction and updating, disclosure or transfer, and erasure or destruction of data. All these activities are subject to the principles of data minimisation, transparency, purpose limitation, security, respect for the rights of data subjects, and demonstrable accountability (Republic of Indonesia, 2022). These provisions are elaborated upon through the obligations regarding limited and specific processing in Article 27, purpose limitation in Article 28, the recording of activities in Article 31, and data protection impact assessments for processing operations posing a high risk in Article 34. Furthermore, Articles 35–39 regulate technical and operational measures, the safeguarding of confidentiality, the supervision of involved parties, and the prevention of unauthorised access and processing. Supeno et al., (2025), also emphasise the importance of enhancing security systems and preventive measures in reducing the risk of breaches. Based on the relationship between these provisions, the liability of business operators has a preventative dimension that can be assessed through the adequacy of security measures in relation to the nature and risks of the data. Consequently, a legal assessment must not merely consider whether an attack has occurred, but must also examine the security measures, supervision, and documentation required of the data controller.

The relationship between the Personal Data Protection Act (UU PDP) and the Consumer Protection Act (UUPK) broadens the basis for analysing liability without eliminating the differences in their respective regulatory scope. The Personal Data Protection Act focuses on the protection of individuals in data processing activities, whilst the Consumer Protection Act regulates the relationship between businesses and consumers in the use of goods or services. Section 4 of the Consumer Protection Act grants rights to safety, accurate information, the submission of complaints, dispute resolution and compensation, whilst Section 7 requires businesses to act in good faith and to provide information and redress in accordance with the provisions (Republic of Indonesia, 1999). In digital transactions, these provisions can be interpreted systematically in relation to the rights of data subjects and processing obligations under the Personal Data Protection Act (UU PDP), provided that the relationship between the parties indeed meets the characteristics of a consumer-business relationship. This interpretation is particularly important in relation to standard terms that seek to unilaterally transfer liability. Article 18(1)(a) of the Consumer Protection Act prohibits standard terms that provide for the transfer of liability by the business operator, whilst paragraph (3) states that any clause contravening this prohibition is null and void (Republic of Indonesia, 1999). Consequently, a consumer's acceptance of terms of service cannot be regarded as

automatic justification for the removal of legal obligations. Nevertheless, each clause must still be examined on the basis of its wording, context and legal consequences; not every allocation of obligations in a contract can be directly equated with a prohibited transfer of liability.

In determining the consequences of a breach, legal certainty requires a distinction to be made between obligations of protection, sanctions for non-compliance, and liability to pay compensation. Section 12 of the Personal Data Protection Act (PDP Act) recognises the right of data subjects to bring a claim and receive compensation for breaches involving the processing of their personal data, whilst Section 19 of the Consumer Protection Act (UUPK) governs the liability of businesses for consumer losses arising from the use of goods or services produced or traded (Republic of Indonesia, 1999, 2022). On the other hand, the PDP Act sets out administrative sanctions in Article 57, as well as prohibitions and criminal provisions in Articles 65–70. This distinction indicates that the occurrence of an incident should not automatically be equated with the fulfilment of all elements of civil liability or criminal liability. As a normative example, Article 67 requires the elements of intent and unlawfulness for certain acts; consequently, a failure to ensure security is not automatically equivalent to a criminal offence as defined in that article. Similarly, the imposition of administrative sanctions does not in itself address the basis and extent of claims for consumer losses. Analytically, legal certainty demands that every consequence be linked to the appropriate legal norm and elements, so that business operators are not burdened with liability without grounds, but nor can they evade their obligations merely because their breach does not yet fulfil the elements of a criminal offence (Sun et al., 2024).

Clarity regarding liability further depends on the ability to trace and prove processing activities. The PDP Act provides a crucial foundation through the obligation to record all processing activities under Article 31, the provision of access to data and processing records under Article 32, and the obligation to provide evidence of consent under Article 24. This framework can be understood as an effort to ensure that compliance is not merely declared, but can also be verified through relevant documentation (Republic of Indonesia, 2022). In the event of a data breach, Article 46 requires written notification to be provided to data subjects and the relevant authority within 3 × 24 hours at the latest, containing information regarding the data that has been disclosed, the time and manner of the disclosure, as well as the measures taken for handling and recovery. Such notification is important for assessing compliance, but does not in itself constitute proof of all elements of a claim for damages. Within the scope of a claim referred to in Article 28 of the Personal Data Protection Act, the burden of proving the existence or absence of the element of fault lies with the business operator (Republic of Indonesia, 1999). This provision should not be interpreted as an automatic transfer of the entire burden of proof regarding every element of the case. Consequently, legal certainty requires a clear distinction between the obligation to document compliance, the obligation to provide information on incidents, and the rules of evidence applicable to the basis of a specific claim (Siregar & Astuti, 2025).

Based on this relationship between legal norms, legal certainty regarding the liability of business operators can be assessed through four interrelated aspects, namely the clarity of the parties' positions, the legitimacy of the basis and purpose of processing, the measurability of protection obligations, and the appropriateness of the consequences for breaches. The Personal Data Protection Act (UU PDP) has provided a framework for identifying data controllers and processors, assessing the legality of processing, and evaluating security obligations and accountability; whilst the Consumer Protection Act (UUPK) provides a basis for protection in consumer relations, including restrictions on standard clauses and provisions regarding business operators' liability (Republic of Indonesia, 1999, 2022). However, from a literature review perspective, the existence of these normative frameworks is not sufficient to conclude that their application is always uniform or that consumer redress is guaranteed to be effective. Research by Putri & Putra, (2024) emphasises the need for continuous monitoring of data protection practices, as policies and the provision of digital services are dynamic in nature. Therefore, the assessment of business operators must be based on concrete processing activities and evidence of compliance with their obligations, rather than merely on the business's reputation or declarations of compliance. This synthesis emphasises that legal certainty does not mean imposing absolute liability for every incident, but rather ensuring there is a clear, testable and consistent basis for determining who is liable, for which breaches, and with what legal consequences.

Compensation Mechanisms for Consumers in the Event of Personal Data Protection Breaches in Digital Transactions

Compensation mechanisms are remedial instruments that link the recognition of rights over personal data to the liability of business operators when breaches occur. The primary normative basis is found in Article 12(1) of Law No. 27 of 2022 on the Protection of Personal Data, hereinafter referred to as the PDP Law, which grants data subjects the right to bring a claim and receive compensation for breaches relating to the processing of their personal data in accordance with the provisions of legislation. Article 12(2) further mandates that further regulations concerning data processing infringements and the procedures for awarding compensation be laid down by government regulation (Republic of Indonesia, 2022). In the context of the relationship between consumers and business operators, this provision must be read in conjunction with Article 4(h) and Article 19 of Law No. 8 of 1999 on Consumer Protection, hereinafter referred to as the UUPK, which governs the right to compensation and the liability of business operators for losses arising from the use of goods or services (Republic of Indonesia, 1999). The interplay between these two laws provides a framework for assessing consumer claims, but this does not mean that every breach automatically results in payment of a specific amount. The determination of compensation still requires the identification of the liable party, the basis of the claim, the losses claimed, and the link between the breach and those losses (Salijeni et al., 2018). Therefore, the redress mechanism must be understood as a legal process requiring an

assessment of the specific circumstances, rather than merely an administrative consequence of a data security incident.

From an operational perspective, complaints and requests for redress made directly to the business operator can serve as an initial step to explain the issue, obtain a response, and seek a resolution without protracted disputes. This step is in line with consumers' right to have their views and complaints heard under Article 4(d) of the Consumer Protection Act, as well as data subjects' right to obtain information regarding the identity, legal basis, purpose of data use, and accountability of the party processing the data under Article 5 of the Personal Data Protection Act (Republic of Indonesia, 1999, 2022). For documentation purposes, a complaint may be drafted to include a chronology of events, the service used, the alleged breach, supporting evidence, and the form of redress sought. However, the submission of a complaint must not be equated with the fulfilment of all the requirements for a legal action, nor should it be regarded as a universal prerequisite for any dispute resolution channel. Article 23 of the Consumer Protection Act specifically provides the basis for bringing a claim against a business operator who refuses, fails to respond to, or fails to fulfil a claim for compensation as referred to in that provision (Republic of Indonesia, 1999). In the context of data breaches, a business operator's response must also be distinguished between an explanation of the incident, security measures, and consent to the payment of compensation. This distinction is important because the restoration of account access or system repairs, whilst relevant to halting the impact of the breach, do not necessarily resolve claims for losses already suffered by consumers (Rotimi, 2025).

If direct settlement does not result in an agreement, out-of-court dispute resolution may be utilised, taking into account the parties' preferences and the jurisdiction of the relevant body. Article 45(2) of the Consumer Protection Act (UUPK) stipulates that the resolution of disputes, whether through the courts or out of court, is based on the voluntary choice of the parties. Article 47, meanwhile, directs out-of-court settlement to reach an agreement on the form and amount of compensation and/or specific measures to prevent the recurrence of losses (Republic of Indonesia, 1999). Within this framework, an out-of-court settlement may be designed not only to cover payment but also relevant corrective measures that are enforceable under the law, such as the rectification of data or the cessation of the disputed processing. The Consumer Dispute Resolution Body (BPSK) is one forum that should be considered, as Article 52 of the Consumer Protection Act (UUPK) sets out its authority to handle disputes through mediation, arbitration or conciliation. Nevertheless, the BPSK's jurisdiction over a personal data case cannot be assumed merely because the complainant identifies themselves as a consumer; the relationship between the parties, the subject matter of the dispute and the basis of the claim must still be examined. Furthermore, Article 45(4) stipulates that where out-of-court settlement has been chosen, legal action may be taken if such efforts are deemed unsuccessful by one or both parties. Consequently, the choice of forum requires

procedural consistency to avoid creating new issues regarding the resolution pathway being pursued.

The court route provides consumers with the opportunity to seek a binding ruling on the infringement, the liable party, and the redress to be granted. Article 45(1) of the Consumer Protection Act grants aggrieved consumers the right to bring a claim through a consumer dispute resolution body or the courts within the general judicial system, whilst Article 48 directs court-based resolution in accordance with the provisions of the general judicial system, taking into account Article 45 (Republic of Indonesia, 1999). When drafting a claim, the statement of claim must explain the consumer's status as a data subject, the actions or omissions in question, the role of each defendant in the processing, as well as the damages and remedies sought. The identification of defendants is crucial because involvement in a single transactional ecosystem does not necessarily imply identical roles or legal liabilities. For infringements affecting multiple consumers, Article 46(1)(b) of the Consumer Protection Act recognises the possibility of a claim by a group of consumers with a common interest, to be brought before the general courts as provided for in paragraph (2) (Republic of Indonesia, 1999). However, the fact that consumers share the same platform or have experienced the same incident does not in itself prove that all victims have identical circumstances and losses. Therefore, the use of class actions must take into account the applicable procedural requirements as well as differences in the impact on individual consumers, so that collective claims do not obscure the need for proof and assessment of the losses of each group represented.

The burden of proof is a central issue, as the right to claim damages must be translated into a verifiable account of the infringement and its consequences. The Personal Data Protection Act (PDP Act) requires data controllers to record all processing activities under Article 31 and to grant data subjects access to their data and the processing audit trail under Article 32, in accordance with applicable provisions (Republic of Indonesia, 2022). These provisions are relevant for supporting the tracing of data usage, although they cannot be equated with an unlimited right to obtain all technical information held by business operators. Transaction evidence, correspondence regarding complaints, the privacy policy in force at the time of the incident, incident notifications, and records of losses may be gathered to support the statement of claim, whilst still assessing their validity and relevance in accordance with the rules of civil procedure (Rinjani & Firmansyah, 2025). Within the scope of claims referred to in Article 28 of the Consumer Protection Act, the burden of proving the existence or absence of fault lies with the business operator (Republic of Indonesia, 1999). However, this provision should not be interpreted as an automatic shift of the entire burden of proof regarding the victim's identity, the existence of loss, and the causal link. Zamani et al., (2023), also identify the difficulties in proving fault, causation and loss as issues in civil liability for data breaches. Therefore, strengthening remedies must be directed towards ensuring accessible evidence and the appropriate application of the allocation of the burden of proof, rather than merely increasing the options for dispute resolution forums.

The determination of the form and amount of compensation must distinguish between losses that can be quantified economically and non-economic impacts that require further argumentation and assessment. Material losses may be quantified, for example, as financial losses or relevant recovery costs, provided that their existence, reasonableness and connection to the breach can be demonstrated. Meanwhile, non-material losses may be claimed by explaining the impact on personal interests, but their award must not be assumed automatically merely on the basis of a statement that data has been leaked. Yudha et al., (2025) highlight that proving non-material losses is one of the obstacles in establishing civil liability for data breaches. In the UUPK, Article 19(2) specifies forms of compensation in the form of a refund, replacement of goods or services of a similar nature or equivalent value, healthcare, and/or compensation in accordance with legal provisions (Republic of Indonesia, 1999). The suitability of these forms of compensation must be assessed in light of the nature of the data breach, as the reimbursement of service costs does not necessarily reflect the full extent of the losses proven by the consumer. Similarly, the seven-day period following the transaction date in Article 19(3) must not be automatically interpreted as seven days from the date the breach was discovered or regarded as a universal deadline for all claims under the Personal Data Protection Act (PDP Act). Differences in the timing of transactions, processing, and the occurrence of losses actually highlight the need for a careful interpretation of the basis for the claims being made.

The effectiveness of the compensation mechanism is ultimately determined by the implementation of the settlement outcome, not merely by the success in reaching an agreement or obtaining a ruling. In the BPSK procedure, the UUPK sets out the obligation to implement decisions in Article 56(1), the possibility of lodging an objection with the district court in Article 56(2), and the application for an enforcement order in Article 57. Therefore, the reference to BPSK rulings as final and binding in Article 54(3) must be read in conjunction with these provisions on objections, rather than being interpreted as the absence of any review mechanism whatsoever (Republic of Indonesia, 1999). In settlement by agreement, clarity regarding the party liable, the amount payable, the deadline for implementation, and corrective measures are essential elements to ensure that the outcome of the settlement can be evaluated. Based on a synthesis of regulations and the literature, the strengthening of redress mechanisms should focus on documented complaint procedures, clarity regarding the forum's jurisdiction, proportionate access to evidence, and accountable guidelines for assessing damages. These recommendations are in line with the concerns raised by Zamani et al., (2023) regarding the need for more detailed regulations on compensation mechanisms and standards of proof. Thus, the fulfilment of consumer rights cannot be measured solely by the availability of legal recourse, but by the real possibility of proving a breach, obtaining redress commensurate with the loss, and ensuring that the obligations of business operators are effectively enforced.

Conclusion

The legal liability of businesses for breaches of consumer personal data protection in digital transactions in Indonesia has a normative basis in Law No. 27 of 2022 on Personal Data Protection and Law No. 8 of 1999 on Consumer Protection. Based on the analysis outlined above, legal certainty lies in the clarity of the business operator's status as a data controller or processor, the validity of the basis for processing, the measurability of security obligations, and the appropriateness of the consequences for breaches. The determination of liability must be based on the role, actions, or negligence of each party; thus, involvement in a digital transaction does not automatically give rise to the same liability. Privacy policies and consumer consent cannot be used as grounds for setting aside legal obligations. Consequently, the assessment of liability must distinguish between breaches of processing obligations, the grounds for civil claims, administrative sanctions, and the elements of criminal offences, so that the application of the law remains proportionate and justifiable.

Mechanisms for consumer redress may be pursued through a claim for redress against the business operator, out-of-court settlement, or legal action in court, depending on the nature of the dispute and the applicable provisions. However, the recognition of the right to sue does not in itself guarantee redress, as consumers still face the need to identify the liable party, demonstrate the loss suffered, and explain the link between the breach and that loss. The burden of proof must be allocated in accordance with the basis of the claim, whilst the determination of compensation must take into account the evidence and the concrete impact, without assuming that every breach results in the same compensation. Therefore, the strengthening of consumer protection must be directed towards clarity in complaint procedures, the jurisdiction of dispute resolution forums, access to relevant evidence, guidelines for assessing losses, and the enforcement of dispute resolution outcomes. The balance between clarity of liability and the enforceability of remedies is fundamental to ensuring that personal data protection does not stop at the normative recognition of rights.

References

Eliyah, E., & Aslan, A. (2025). STAKE'S EVALUATION MODEL: METODE PENELITIAN. *Prosiding Seminar Nasional Indonesia*, *3*(2), Article 2.

Putri, T. S., & Putra, M. R. S. (2024). Implementasi Undang-Undang Pelindungan Data Pribadi: Peran Manajemen Risiko Hukum bagi Prosesor Data Pribadi. *Jurnal Hukum Lex Generalis*, *5*(4). https://ojs.rewangrencang.com/index.php/JHLG/article/view/730

Rinjani, M. A., & Firmansyah, R. (2025). Hambatan Implementasi UU 27/2022 dan Strategi Penguatan Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, *8*(1), 70–83. https://doi.org/10.38043/jah.v8i1.6793

Rotimi, O. (2025). *Digital Sovereignty and the Politics of Data Localization* (SSRN Scholarly Paper No. 5921642). Social Science Research Network. https://doi.org/10.2139/ssrn.5921642

Salijeni, G., Samsonova-Taddei, A., & Turley, S. (2018). *Big Data and Changes in Audit Technology: Contemplating a Research Agenda* (SSRN Scholarly Paper No. 3148904). Social Science Research Network. https://papers.ssrn.com/abstract=3148904

Siregar, R. A., & Astuti, N. K. (2025). Assessing legal and institutional readiness for patient data protection in the age of big health data: An empirical study of health facilities in Indonesia. *International Journal of Law, Policy and Social Review*, *7*(3), 15–21.

Sun, Y., Li, J., Lu, M., & Guo, Z. (2024, Maret 11). *Study of the Impact of the Big Data Era on Accounting and Auditing*. arXiv.Org. https://arxiv.org/abs/2403.07180v1

Supeno, S., Rosmidah, R., & Iqbal, S. M. U. (2025). Personal Data Protection in Review of Legal Theories and Principles. *Journal of Law and Legal Reform*, *6*(3), 1349–1376. https://doi.org/10.15294/jllr.v6i3.10252

Takaryanto, D., & Lany, A. (2025). Legal Protection of Personal Data in the Exchange of Electronic Medical Record in Healthcare Services. *Research Horizon*, *5*(6), 2817–2830. https://doi.org/10.54518/rh.5.6.2025.897

Taylor, R. D. (2020). "Data localization": The internet in the balance. *Telecommunications Policy*, *44*(8), 102003. https://doi.org/10.1016/j.telpol.2020.102003

Truli, E. (2018). The General Data Protection Regulation and Civil Liability. Dalam M. Bakhoum, B. Conde Gallego, M.-O. Mackenrodt, & G. Surblytė-Namavičienė (Ed.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?* (hlm. 303–329). Springer. https://doi.org/10.1007/978-3-662-57646-5_12

Ventura, M., & Coeli, C. M. (2018). Beyond privacy: The right to health information, personal data protection, and governance. *Cadernos de Saúde Pública*, *34*, e00106818. https://doi.org/https://doi.org/10.1590/0102-311X00106818

Versaci, G. (2018). Personal Data and Contract Law: Challenges and Concerns about the Economic Exploitation of the Right to Data Protection. *European Review of Contract Law*, *14*(4), 374–392. https://doi.org/10.1515/ercl-2018-1022

Vila Seoane, M. F. (2021). Data securitisation: The challenges of data sovereignty in India. *Third World Quarterly*, *42*(8), 1733–1750. https://doi.org/10.1080/01436597.2021.1915122

Waruwu, S., & Siswoyo, A. A. (2024). DATA PRIBADI SEBAGAI ASET BISNIS: SINERGI HUKUM RAHASIA DAGANG DAN PERLINDUNGAN DATA. *Lex Lectio Law Journal*, *3*(2), 118–129. https://doi.org/10.61715/jll.v3i2.118

Wiriani, E., Maknuni, J., Puspita, E. A., & Masitah, M. (2025). Peran Artificial Intelligence dalam Mitigasi Risiko Transaksi Mobile Banking: Tinjauan Governansi dan Etika Data. *Journal of Trends Economics and Accounting Research*, *6*(1), 103–111. https://doi.org/10.47065/jtear.v6i1.2223

Wooldridge, J. M. (2010). *Econometric Analysis of Cross Section and Panel Data, second edition*. MIT Press.

Xiaying, M. (2019). The Legal Attributes of Electronic Data and the Positioning of Data in Civil Law*. *Social Sciences in China*, *40*(1), 82–99. https://doi.org/10.1080/02529203.2018.1519208

Yu, X., & Zhao, Y. (2019). Dualism in data protection: Balancing the right to personal data and the data property right. *Computer Law & Security Review*, *35*(5), 105318. https://doi.org/10.1016/j.clsr.2019.04.001

Yudha, Sahril, I., & Atmadja3, D. A. R. W. (2025). Perlindungan Data Pribadi Konsumen, Dokumen dan Tanda Tangan Elektronik yang Dipergunakan oleh Pihak Ketiga dalam Transaksi E-Commerce. *CENDEKIA : Jurnal Penelitian Dan Pengkajian Ilmiah*, *2*(2), 173–189. https://doi.org/10.62335/cendekia.v2i2.897

Zamani, E. D., Smyth, C., Gupta, S., & Dennehy, D. (2023). Artificial intelligence and big data analytics for supply chain resilience: A systematic literature review. *Annals of Operations Research*, *327*(2), 605–632. https://doi.org/10.1007/s10479-022-04983-y

Zed, M. (2008). *Metode Penelitian Kepustakaan*. Yayasan Pustaka Obor Indonesia.

Republik Indonesia. (1999). *Undang-Undang Republik Indonesia Nomor 8 Tahun 1999 tentang Perlindungan Konsumen*. Lembaran Negara Republik Indonesia Tahun 1999 Nomor 42, Tambahan Lembaran Negara Republik Indonesia Nomor 3821.

Republik Indonesia. (2022). *Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820.

UU PDP: *(Republik Indonesia, 2022)*, dengan nomor pasal bila diperlukan.

UUPK: *(Republik Indonesia, 1999)*, dengan nomor pasal bila merujuk ketentuan tertentu.