

Personal Data Protection and Legal Accountability in the Digital Transformation of Public and Private Institutions

Dominicus Djoko Budi Susilo
Universitas Terbuka, Indonesia

Corresponding Author: Dominicus Djoko: ddjokobudisusilo1971@gmail.com

ARTICLE INFO

Keywords: Personal Data Protection, Legal Liability, Digital Transformation, Accountability, Institutions.

Received : 20, July

Revised : 02, August

Accepted: 20, September

©2026 Susilo (s): This is an open-access article distributed under the terms of the [Creative Commons Atribusi 4.0 Internasional](https://creativecommons.org/licenses/by/4.0/).



ABSTRACT

Digital transformation in public and private institutions increases the processing of personal data while increasing the risk of privacy violations and unclear legal liability. This research aims to analyze the protection of personal data and the construction of institutional legal accountability in the implementation of digital systems. The research uses normative legal methods with legislative, conceptual, and comparative approaches. Data in the form of primary and secondary legal materials were collected through literature studies and analyzed qualitatively-prescriptively, without involving respondents or informants. The results show that the effectiveness of data protection depends on data controller compliance, processing security, clarity of legal obligations, and effective enforcement mechanisms. The research concludes that strengthening institutional accountability, data governance, and law enforcement consistency is needed to ensure the protection of data subjects' rights in digital transformation.

INTRODUCTION

Digital transformation has transformed the way public and private institutions collect, store, use, and exchange personal data. The digitization of public services, banking, healthcare, e-commerce, and platform-based services creates efficiencies, but at the same time increases the risk of unauthorized data processing, data leakage, misuse of information, and privacy violations. In a global context, developments in data protection law indicate a shift from an approach that relies on individual consent to a model that emphasizes organizational responsibility for the entire data processing cycle. Karjalainen (2022) explained that the principle of accountability in the General Data Protection Regulation (GDPR) increases the responsibility of data controllers and supports the enforcement of data protection obligations. Labadie and Legner (2023) also show that compliance with data protection regulations requires integrated data governance capabilities at the organizational level.

This urgency is also seen in the Indonesian context. The ratification of Law Number 27 of 2022 concerning Personal Data Protection provides a more comprehensive legal framework for the processing of personal data by public bodies and corporations. However, the existence of regulations does not in itself guarantee effective protection. Widiatedja and Mishra (2023) assessed that the effectiveness of Indonesia's data protection system is greatly influenced by the independence and capacity of supervisory institutions. Meanwhile, Rahman and Mulyani (2025) show that Indonesia still faces regulatory and institutional problems in the management and transfer of cross-border data after the enactment of the Personal Data Protection Law. These conditions show that digital transformation must be followed by clarity of legal obligations, supervisory mechanisms, and institutional accountability when there is a violation of the rights of data subjects.

Theoretically, this research is based on the principle of accountability in data protection law, which requires data controllers not only to comply with legal provisions, but also to be able to prove their compliance through adequate governance, documentation, security, and oversight mechanisms. Karjalainen (2022) emphasized that accountability functions to strengthen the obligations of data controllers and facilitate law enforcement. This principle is closely related to data protection by design, which is the obligation to integrate data protection from the system design stage and processing process. Hof (2024) shows that the implementation of data protection by design and effective enforcement plays an important role in preventing data breaches. In cloud-based digital environments, Zhou et al. (2023) also point to the importance of activity documentation, auditing, and compliance verification as concrete elements of accountability.

Although research on data protection is growing rapidly, there are still gaps in the existing literature. Kurtz et al. (2022) focus on the accountability of platform providers for the data processing carried out in the digital ecosystem. Labadie and Legner (2023) emphasize more on the ability of organizational data management to comply with GDPR, while Widiatedja and Mishra (2023) focus on the need for independent data protection authorities in Indonesia. Rahman and Mulyani (2025) mainly discuss the regulation of cross-border data flows after

the enactment of the Personal Data Protection Law. These studies provide an important, but not yet integrated, analysis of the relationship between personal data protection and the legal accountability of public and private institutions in the digital transformation process, especially related to data controller obligations, processing security, supervision, and legal consequences for non-compliance. More recent Indonesian studies extend this discussion to online lending agreements and AI-based credit profiling (Susilo, 2025; Susilo et al., 2025; Susilo, 2026).

Based on these gaps, this study aims to analyze the legal construction of personal data protection and the legal accountability of public and private institutions in the implementation of digital systems. The analysis is directed at the obligations of data controllers and processors, the principle of accountability, data protection from the design stage, processing security, and enforcement mechanisms in the event of a breach. The research also assesses the extent to which Indonesia's legal framework is able to accommodate data protection standards that are developing internationally. This focus allows normative legal research not to stop at regulatory inventory, but to assess the consistency of norms, the adequacy of accountability mechanisms, and the relationship between legal obligations and the protection of data subject rights in an increasingly digitized institutional environment.

Theoretically, this research is expected to strengthen the development of data protection legal studies by integrating the principles of accountability, data protection by design, and institutional legal accountability into one analytical framework. This approach is important because responsibility for personal data cannot be placed solely on the security aspect of technology, but must be constructed as a legal obligation that can be monitored and enforced. Practically, the results of the research are expected to provide a basis for governments, public bodies, companies, data controllers, and policymakers to strengthen data governance, compliance mechanisms, internal supervision, risk mitigation, and accountability mechanisms when violations occur. Thus, digital transformation can develop in line with the protection of privacy rights, legal certainty, and increased trust in public and private digital services.

THEORETICAL FRAMEWORK

Personal Data Protection as a Rights-Based and Risk-Based Legal Framework

The protection of personal data in the digital transformation is not only related to the confidentiality of information, but also to the protection of the rights of individuals from risks arising from data processing. Yeung and Bygrave (2022) explain that modern data protection regimes combine fundamental rights-based approaches with risk-based regulation. Consequently, legal compliance is not only judged by the existence of consent or the legal basis of processing, but also by the institution's ability to identify risks, apply proportionate safeguards, and prove compliance. This perspective is relevant for both public and private institutions because the intensity of data processing in digital services has increased the potential for misuse, unauthorized access, and use of data beyond the original purpose.

Data Controller and Attribution of Legal Accountability

Determining responsible parties becomes increasingly complex when data processing involves institutions, *cloud providers*, technology vendors, digital platforms, and third parties. Wong (2021) shows that data controller-based accountability models face difficulties when multiple entities are involved in a single set of data processing. Finck (2021) even criticized the expansion of the *concept of controller* because imposing responsibility on too many parties can obscure parties who actually have control over the purpose and means of processing. The literature suggests that legal accountability needs to be linked to a party's level of real control, decision-making capacity, and influence on processing. In this study, the concept is important to analyze the distribution of legal obligations in public and private institutions that use interconnected digital infrastructure.

Institutional Accountability, Compliance, and Privacy Risk Management

Legal accountability also has a preventive dimension. Institutions should not wait for violations to occur before taking protection. Georgiadis and Poels (2022) place *privacy impact assessment* as an important mechanism for recognizing and controlling data protection risks in complex data analytics environments. Meanwhile, Zaguir et al. (2024) found that compliance with data protection regulations requires integration between *information governance*, organizational architecture, processing procedures, and oversight mechanisms. The findings reinforce the view that accountability does not only take the form of sanctions after a violation, but includes the obligation to establish governance, documentation, risk evaluation, security, and compliance systems that run on an ongoing basis.

Personal Data Protection in Public Institutions

The transformation of public services results in large-scale data processing and often involves sensitive information. Li et al. (2024) identified five risk groups in government data management, namely data, institutional, technological, structural, and behavioral risks. The findings suggest that privacy risks stem not only from the weaknesses of technological systems, but also from organizational structures and data management practices. Daud (2025) further shows that there is a legal tension between the need for data sharing in public services and the obligation to maintain data privacy and security. Therefore, the public interest cannot be used as an excuse to eliminate the principles of purpose limitation, processing security, supervision, and accountability of public bodies.

Data Governance and Accountability in Private Institutions

In private institutions, digital transformation is driving the use of data for analytics, automation, service personalization, decision-making, and cross-border commercial activities. Coche et al. (2024) show that differences in data protection regimes between countries create regulatory complexity for organizations that carry out digital activities across jurisdictions. These conditions require companies to integrate legal obligations into data governance and business strategies, rather than treating data protection as a mere administrative requirement. In the perspective of this study, the responsibilities of private institutions include the lawfulness of processing, data security, third-

party control, transparency, fulfillment of data subject rights, and the ability to account for these processes when a breach occurs.

Enforcement and the Effectiveness of Legal Accountability

The effectiveness of data protection ultimately depends on the ability of the legal system to oversee and enforce those obligations. Buckley et al. (2024) found that there is a discrepancy between the broad objectives of data protection regulators and the indicators used to assess enforcement effectiveness. An overly fined assessment can overlook aspects of compliance, organizational behavior change, transparency, and violation prevention. Thus, it is not enough to build legal accountability only through the threat of sanctions. An effective system requires supervisory bodies that have capacity, clear enforcement procedures, transparency of decisions, complaint mechanisms, and measures that can assess whether the rights of data subjects are truly protected.

Synthesis of Literature and Research Position

Previous literature provides a solid foundation, but most of it addresses data protection issues separately. Wong (2021) and Finck (2021) focus on controller responsibility attribution, Georgiadis and Poels (2022) and Zaguir et al. (2024) emphasize risk management and organizational compliance, Li et al. (2024) and David (2025) discuss risk in the public sector, while Coche et al. (2024) examine the complexities of data governance across jurisdictions. Meanwhile, Buckley et al. (2024) place the effectiveness of regulators as a separate issue. This research unites these dimensions through normative legal analysis of personal **data protection and legal accountability of public and private institutions in digital transformation**. The analysis focused on the obligations of data controllers and processors, processing security, governance and risk prevention, attribution of responsibilities, and the effectiveness of enforcement mechanisms. This framework allows data protection to be understood as an institutional accountability system that takes place from the design stage of processing to the resolution of breaches.

METHODS

Types of Research

This study uses normative legal research with legislative, conceptual, and comparative approaches. This approach is used to analyze personal data protection norms, the obligations of data controllers and processors, and the legal liability of public and private institutions. Normative legal research places regulations, legal principles, and doctrines as the main objects of analysis (Nyathi, 2023; Byrne & Olsen, 2024). Indonesia's legal framework is analyzed based on Law Number 27 of 2022 concerning the Protection of Personal Data, Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions, and Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions. GDPR is used as an international benchmark.

Population and Sample

This study did not use human populations, respondents, or informants because it was normative. The unit of analysis is in the form of primary and

secondary legal materials that are selected *purposively* based on the relevance and authority of the source. Primary legal materials include applicable data protection regulations and electronic systems, while secondary materials consist of peer-reviewed international journal articles, books, and academic studies related to data protection, accountability, data governance, and legal accountability.

Research Instruments

The research instruments are in the form of legal documents and legal analysis matrices. Legal materials are classified based on the rights of the data subject, the obligations of controllers and processors, processing security, institutional accountability, supervision, and forms of legal liability. The statistical validity and reliability of the instruments were not used because the study did not use questionnaires. The validity of the analysis is maintained through the use of official sources, checking the status of the applicability of regulations, and consistency of legal interpretation (van Gestel, 2023).

Data Collection Procedure

Data was collected through literature studies and documentation. The research stage includes identification of legal issues, search for regulations through official legal databases, literature collection through Google Scholar and journal databases, classification of legal materials, and critical reading of norms related to data protection and institutional accountability. Secondary literature is prioritized in 2021–2025 publications.

Data Analysis Techniques

Legal materials are analyzed qualitatively-prescriptively through interpretation, systematization, and legal comparison. The analysis is focused on the obligations of data controllers and processors, processing security, accountability, data subject rights, and law enforcement mechanisms. The results of the comparison are used to assess the adequacy of the Indonesian legal framework and formulate recommendations to strengthen the accountability of public and private institutions.

RESULTS AND DISCUSSION

Personal Data Protection as an Institutional Legal Obligation in Digital Transformation

The results of the study show that digital transformation has changed the position of personal data protection from a technical issue to an institutional legal obligation. Law Number 27 of 2022 concerning Personal Data Protection places data protection as part of the protection of personal rights and establishes obligations for data controllers and processors. Article 19 expressly covers every person, public body and international organization in the category of data controller or processor. Furthermore, Article 20 requires each controller to have a lawful processing basis, such as explicit consent, execution of agreements, legal obligations, vital interests, public interest or public services, and other legitimate interests (Susilo, 2025; Susilo et al., 2025). Consequently, public and private institutions cannot base data collection and use solely on the operational needs of the organization. Each processing activity must have a legal basis, an

explainable purpose and a relationship proportionate to the rights of the data subject.

The findings show a shift from a consent-centered approach to accountability-centered protection. Consent remains important, but it is not the only measure of the validity of processing. Institutions must be able to prove the reasons for processing, limit the use of data for the purpose, maintain accuracy, determine retention periods, and ensure the fulfillment of the rights of data subjects. This position has become increasingly important because the two-year adjustment period provided by Article 74 of the PDP Law has expired since October 17, 2024. Thus, in the context of this research, these obligations are no longer appropriately seen as a transition agenda, but as legal standards that should have been integrated into institutional governance.

These findings support Coche et al. (2024), who point out that digitalization requires data governance that not only governs the use of data, but also the storage, transfer, and flow of data. However, this study expands this perspective by showing that in the Indonesian context, data governance must be understood as a mechanism of legal accountability, not just an organizational strategy. Thus, the *research gap* that emerges is that there are still limited studies that directly link digital transformation with the construction of legal obligations that apply in parallel to public and private institutions.

Legal Accountability of Data Controllers and Processors

The second finding shows that the accountability of data controllers is central to Indonesia's personal data protection system. Article 47 of the PDP Law explicitly requires the controller to be responsible for the processing of personal data and to be able to demonstrate accountability in fulfilling the principle of data protection. The norm has two dimensions. First, institutions are obliged to comply with the law substantively. Second, institutions must be able to prove that compliance is actually implemented. Thus, accountability is not enough to be realized through a privacy policy or formal documents, but requires records of processing, division of responsibility, internal procedures, supervision, risk control, and evidence of data protection implementation.

The analysis also found that the use of a third party did not remove the controller's liability. Article 51 of the PDP Law specifies that when a processor performs processing based on the controller's order, the activity remains within the controller's responsibility. The processor bears only direct responsibility when processing outside of the predetermined order or purpose. In addition, the use of other processors requires written consent from the controller. This norm is particularly relevant for digital transformation as institutions increasingly rely on *cloud providers*, technology companies, application vendors, payment providers, analytics companies, and digital infrastructure providers (Susilo, 2026).

These results are in line with Wong (2021), who found that controller-based accountability models become complex when a processing activity involves multiple organizations. Finck (2021) also shows that the attribution of responsibility becomes less simple when control over data is spread among multiple actors. This study found that the PDP Law tries to address these

problems through a command-based approach, processing objectives, and control of the process. This means that responsibility should be determined based on who determines the purpose, gives the order, and has the substantive capacity to control the processing.

This is where this research differs from Wong (2021) and Finck (2021). Both mainly discuss the conceptual problem of *controllers* in EU law. This study places these problems in the relationship between public institutions, private institutions, processors, and digital service providers in Indonesia. The results show that the contract with the vendor is not enough to divert legal risks. Institutions must still conduct *due diligence*, determine processing limits, supervise processors, and provide audit mechanisms. As such, digital transformation requires a *chain of accountability* that follows data even when processing is carried out outside of the main organizational structure.

Data Security, Risk Prevention, and Privacy by Design

The results of the study further show that data security is a preventive legal obligation, not just an information technology security issue. Article 35 of the PDP Law requires controllers to protect and ensure data security through the preparation and implementation of operational technical measures. Article 39 further requires controllers to prevent unauthorized access and to use reliable, secure, and responsible electronic systems. This norm is related to Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions which has been in force until now. The Government Regulation also places reliability, security, and accountability as the obligations of Electronic System Operators.

Normatively, the findings show that the occurrence of data leaks does not automatically prove a violation of the law. The legal issue lies in whether the controller has implemented reasonable and appropriate protection measures before the incident occurred. Therefore, accountability testing needs to consider the quality of the security system, risk assessment, access control, documentation, internal oversight, system updates, and mitigation after vulnerability is discovered. This perspective shifts the assessment from simply "whether the data was leaked" to "whether the institution has carried out an accountable preventive obligation".

The empirical-secondary findings of Alatas and Djajaputra (2025) strengthen this analysis. In a study of the leakage of more than six million NPWP data, they found weaknesses in access control, *Data Protection Impact Assessment*, *privacy by design*, and leak notification procedures. These findings are important for this study because they show the possible distance between the already clear protection norms and the institutional capacity to translate them into operational controls.

Thus, the results of this study confirm that privacy by design must be read as a concrete form of legal accountability. Protection should not be added after the digital system has been created. Institutions must incorporate the principles of data minimization, access restriction, retention, security, and risk mitigation from the design of digital services. At this point the research expands on previous studies. While previous research has mostly discussed security or privacy as

technical and compliance issues, this study shows that design failures can have legal consequences if they show that the controller's obligations are not met.

Accountability of Public Institutions in Personal Data Processing

An analysis of public institutions yielded an important finding that the interests of public services do not remove the obligation to protect personal data. Article 20 of the PDP Law does recognize the implementation of duties for the public interest, public services, or the exercise of authority based on laws and regulations as the basis for processing. However, the existence of the basis does not give unlimited authority to public bodies. Processing must still be subject to the principles of clear purpose, proportionality, security, accuracy and accountability.

The position of public bodies even has clearer institutional standards. Article 53 of the PDP Law requires the appointment of officials or officers who carry out the function of Personal Data Protection when processing is carried out for the benefit of public services. The official must have professionalism, knowledge of data protection laws and practices, as well as the ability to carry out data protection duties. This provision shows that the accountability of public bodies is not only at the institutional level in the abstract, but needs to be realized through the division of internal functions and responsibilities that can be identified.

These findings are becoming increasingly relevant with the acceleration of digital government system integration. In 2026, the government will continue to encourage the integration of social, population, education, health, employment, housing, and social assistance data in national digital services. Integration can improve service efficiency, but it also increases the scale of impact when access errors, non-targeted processing, or security breaches occur. Therefore, the more integrated government data is, the higher the accountability standards needed.

The results of Alatas and Djajaputra's (2025) research on NPWP data leakage support this problem. They found that the government's obligations as data controllers have not been fully implemented in terms of risk mitigation. Aura et al. (2025) also concluded that Indonesia already has a normative basis for protecting the right to privacy, but effective protection for leak victims still faces implementation challenges. The difference is that this study does not only focus on government accountability after leaks. This study found that the accountability of public bodies must be built in three stages, namely before processing through prevention, during processing through supervision, and after incidents through recovery and accountability.

Accountability of Private Institutions, Third Parties, and Cross-Border Data Processing

In the private sector, the results show that digital transformation creates more complex processing structures as data is used in e-commerce, financial services, *cloud computing*, analytics, digital marketing, automation, and cross-jurisdictional cooperation. Therefore, the company's liability is not only related to the collection of data from consumers, but includes the entire processing chain and the third parties who gain access to the data.

This complexity can be seen in data transfer. Article 55 of the PDP Law requires that protection remains in place when data is transferred to other controllers in Indonesian territory. For international transfers, Article 56 establishes a tiered protection structure. The controller must first ensure that the recipient country has an equal or higher level of protection. If these conditions are not met, the controller must ensure adequate and binding protection. Data subject consent becomes an alternative when both previous conditions cannot be met. Thus, data transfer should not be understood as a transfer of legal responsibility from the originating institution to the recipient.

These results are in line with Coche et al. (2024), who show that regulatory differences regarding the use, storage, transfer, and flow of data create significant complexity for companies running cross-border operations. However, this study shows an additional aspect. Cross-border compliance is not only a matter of regulatory harmonization, but also a matter of accountability attribution. Companies must know who receives the data, for what purpose the data is used, the applicable protection standards, and the mechanisms available in the event of a breach.

The findings answer another part of the *research gap*. Previous literature has often separated the issue of international transfers from the accountability of controllers. This research shows that the two are a series. The longer the processing chain, the more important the processing contract, access restrictions, security verification, audits, incident reporting mechanisms, and documentation of transfer decisions.

Data Breach Notification, Remedies, and Legal Sanctions

The results of the study found that the PDP Law not only regulates preventive protection, but also establishes a corrective mechanism when protection fails. Article 46 requires controllers to provide written notice no later than 3×24 hours to data subjects and institutions in the event of a data protection failure. The notification should at least explain the data revealed, when and how the data was revealed, and the handling and recovery steps. Under certain circumstances, the controller is also obliged to notify the public.

These obligations have a broader function than just transparency. Notifications allow data subjects to take preventive measures against further abuse, such as identity theft, financial fraud, or account takeover. Therefore, delays in reporting can increase losses and become a liability issue in itself. These findings show that legal accountability should include incident response, not prevention.

The PDP Law also provides a fairly strong administrative mechanism. Article 57 allows for the provision of written warnings, temporary suspension of processing, deletion or destruction of data, and administrative fines of up to a maximum of 2% of annual revenue or revenue based on the variables of the violation. This structure shows that sanctions are directed not only to punish, but also to stop the processing of violators and restore data protection conditions.

Aura et al. (2025) found that despite the legal framework in place, victims of data breaches still face challenges in obtaining effective protection. The findings of this study support these results, but place the problem on a broader

structure. The effectiveness of remediation does not only depend on the existence of rights and sanctions, but also on the ability to detect violations, the obligation to report, the existence of authorities capable of examining cases, and the ability to execute sanctions.

Enforcement and the Institutional Gap in Indonesia

The most critical findings of this study are in the aspect of law enforcement. Substantively, the PDP Law has provided quite broad supervisory and enforcement authority. Article 58 specifies that the implementation of Personal Data Protection is carried out by an institution determined by the President. Article 59 provides functions in the form of policy formulation, supervision, administrative law enforcement, and dispute resolution facilitation. Article 60 further provides a number of supervisory and inspection authorities.

The problem lies in the relationship between norms and institutional readiness. Until July 22, 2026, the government still stated that it was finalizing the establishment of a personal data protection authority and presidential regulations that are the basis of its institutions. This condition results in an important gap because Article 57 paragraph (4) specifies that the imposition of administrative sanctions is carried out by the institution. Thus, there is a tension between substantive obligations that are already fully in force and the enforcement infrastructure that is still being developed.

These findings support Aisy et al. (2025), who through comparisons with Ireland, Australia, and Singapore found that the weakness of administrative sanctions enforcement in Indonesia is related to the lack of effective special institutions. Badriah et al. (2024) also found that strengthening accountability requires a centralized authority that is able to link data protection in the government and private sectors.

However, the results of this study provide a broader interpretation. The establishment of authority should not be seen as a single solution. Buckley et al. (2024) show through a study of GDPR regulators that the effectiveness of regulators cannot be assessed solely on the amount of fines. The regulator's goals are much broader, including improving compliance, changing organizational behavior, preventing breaches, and creating trust in data protection systems. Thus, the establishment of the Indonesian PDP institution must be accompanied by operational independence, human resources, technical capacity, complaint procedures, transparency of decisions, investigation mechanisms, and clear performance measures.

Comparative Findings and the Position of Indonesian Data Protection Law

The results of the comparison with the GDPR show that Indonesia's PDP Law has adopted many of the core elements of the modern data protection regime. Similarities can be seen in the determination of the basis for processing, *controller responsibilities*, security obligations, risk assessment, data protection officer functions, breach notifications, international transfers, and administrative sanctions. This shows that there is normative convergence between Indonesia and the development of international data protection standards.

However, the results of the analysis show that the similarity of norms has not resulted in equality at the implementation level. The GDPR system already

has a supervisory authority structure that runs investigations, surveillance, and enforcement. In the Indonesian context, the institutional design is still in the completion stage in 2026. Therefore, Indonesia's main problem today is no longer the absence of a general law on personal data, but the implementation and enforcement gap.

This makes it clear that the quality of a data protection system cannot be judged solely on how close the text of the law is to the GDPR. The effectiveness of the law depends on the relationship between norms, organizational capacity, technology, oversight, access to remedies, and enforcement. This is one of the important contributions of research because it places data protection as a legal accountability ecosystem.

Research Gap and Main Contribution of the Study

The synthesis of the results shows that previous research tends to discuss data protection elements separately. Wong (2021) and Finck (2021) focus on the issue of controller attribution. Coche et al. (2024) focus on the complexity of cross-jurisdictional governance data. Badriah et al. (2024) and 'Aisy et al. (2025) emphasize the need for data protection institutions and enforcement effectiveness. Alatas and Djajaputra (2025) focus on government accountability in the case of certain data leaks, while Buckley et al. (2024) discuss measuring the effectiveness of regulators.

This research fills this gap by placing all these elements in one construction of institutional legal accountability in digital transformation. The findings of the study show that the effectiveness of data protection is shaped by three interconnected layers. The first layer is preventive accountability, which includes the basis of processing, purpose limitation, risk management, security, and *privacy by design*. The second layer is operational and corrective accountability, which includes processor monitoring, documentation, data protection officers, incident response, and breach notifications. The third layer is enforcement accountability, namely external supervision, dispute resolution, sanctioning, and restoration of data subject rights.

Thus, the main finding of this study is that the existence of the PDP Law cannot be treated as an end point for personal data protection in Indonesia. Effective protection requires the interconnectedness between legal norms, internal governance of institutions, technological security, distribution of responsibilities, recovery mechanisms, and effective enforcement authorities. For public institutions, the implication is that any acceleration of the integration of government services and data must be accompanied by an increase in accountability standards. For private institutions, digital transformation must place compliance and data protection as part of corporate governance and risk management, including against vendors and cross-border transfers. Therefore, the theoretical contribution of the research lies in the development of the concept of integrated institutional legal accountability, while its practical contribution lies in the need to build a compliance system that works preventively, correctively, and repressively in a continuous series.

CONCLUSIONS AND RECOMMENDATIONS

This study concludes that digital transformation in public and private institutions has transformed the protection of personal data from administrative and technical issues into a sustainable institutional legal obligation. Law Number 27 of 2022 concerning Personal Data Protection has provided a relatively comprehensive normative basis through the basic regulation of processing, data subject rights, controllers and processors' obligations, processing security, risk assessment, notification of data protection failures, data transfers, and administrative sanctions. However, the effectiveness of protection is not only determined by the completeness of the norm. The results of the study show that effective protection requires a relationship between preventive accountability, which includes the legality of processing, restriction of purposes, security, risk mitigation, and privacy by design; operational and corrective accountability, which includes documentation, processor supervision, data protection officer functions, incident response, and restoration of data subject rights; and enforcement accountability, which ensures supervision, dispute resolution, and the application of sanctions. Thus, the main contribution of this research lies in the concept of integrated institutional legal accountability, which places data protection as a series of legal responsibilities from the digital system design stage to handling and enforcing after a breach occurs.

Based on these findings, strengthening data protection in Indonesia must be directed at consistent implementation, not just formal compliance with the PDP Law. Public institutions need to integrate data protection into every service digitization process, especially in systems that involve the integration and exchange of data between institutions. Private institutions need to make data protection part of corporate governance and risk management, including through impact assessments, vendor and processor monitoring, cross-border data transfer safeguards, processing documentation, and measurable incident response mechanisms. At the regulatory level, the government needs to ensure the readiness of the implementing apparatus and the effectiveness of supervision institutions so that the obligations and sanctions in the PDP Law can be applied consistently. The strengthening also needs to maintain alignment with Law Number 1 of 2024 concerning amendments to both the ITE Law and Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions. Thus, the success of data protection is measured not only by the existence of regulations, but by the ability of institutions to prove compliance, prevent risks, restore data subject rights, and account for every processing activity in the digital ecosystem.

FURTHER STUDY

Further research can develop these normative findings through socio-legal or empirical approaches to test the level of implementation of the PDP Law in public and private institutions. The study can focus on the effectiveness of the functions of data protection officers, the implementation of privacy by design and Data Protection Impact Assessment, third-party management, data leak handling mechanisms, and the effectiveness of supervision and enforcement

institutions after all PDP Law implementation devices are operational. Comparative studies with jurisdictions that have more mature data protection authorities can also be used to develop institutional data protection accountability indicators that are in accordance with the Indonesian legal context.

ACKNOWLEDGMENT

The author expresses his appreciation to all parties and institutions that support the completion of this research, especially through the provision of access to legal materials, scientific literature, and academic sources used in the analysis process. The author also appreciates the academic contributions of previous researchers which are the basis for the development of studies on personal data protection, digital transformation, and institutional legal accountability.

REFERENCES

- 'Aisy, F. R., Maskur, M. A., & Amiruddin, A. M. A. (2025). Establishing Indonesia's personal data protection agency: Comparative administration sanctions enforcement from Ireland, Australia, and Singapore. *Journal of Indonesian Legal Studies*, 10(1), 431–482. <https://doi.org/10.15294/jils.v10i1.13755>
- Alatas, H. H. R. A., & Djajaputra, G. (2025). Examining Indonesian government accountability and mitigation measures in the 2024 taxpayer identification number data breach. *Jurnal Ilmu Hukum Kyadiren*, 7(2), 1234–1248. <https://doi.org/10.46924/jihk.v7i2.385>
- Aura, A., Priowirjanto, E. S., & Dewi, C. T. I. (2025). Privacy protection guarantee for data hacking victims according to Indonesian law. *Padjadjaran Journal of International Law*, 9(1), 1–15. <https://doi.org/10.23920/pjil.v8i2.1823>
- Badriah, L., Indiahono, D., & Sukarso. (2024). Akuntabilitas dalam kebijakan perlindungan data pribadi di Indonesia: Belajar dari Korea Selatan dan Singapura. *Matra Pembaruan: Jurnal Inovasi Kebijakan*, 8(2), 89–102. <https://doi.org/10.21787/mp.8.2.2024.89-102>
- Buckley, G., Caulfield, T., & Becker, I. (2024). GDPR and the indefinable effectiveness of privacy regulators: Can performance assessment be improved? *Journal of Cybersecurity*, 10(1), tyae017. <https://doi.org/10.1093/cybsec/tyae017>
- Byrne, W. H., & Olsen, H. P. (2024). Doctrinal legal science: A science of its own? *Canadian Journal of Law & Jurisprudence*, 37(2), 343–367. <https://doi.org/10.1017/cjlj.2024.16>
- Coche, E., Kolk, A., & Ocelík, V. (2024). Unravelling cross-country regulatory intricacies of data governance: The relevance of legal insights for digitalization and international business. *Journal of International Business Policy*, 7, 112–127. <https://doi.org/10.1057/s42214-023-00172-1>
- Daud, M. (2025). A legal framework for public sector data sharing in Malaysia: The clash between data protection, privacy and public interest. *IIUM Law Journal*, 33(2), 279–320. <https://doi.org/10.31436/iiumlj.v33i2.1072>
- Finck, M. (2021). Cobwebs of control: The two imaginations of the data controller in EU law. *International Data Privacy Law*, 11(4), 333–347. <https://doi.org/10.1093/idpl/ipab017>
- Georgiadis, G., & Poels, G. (2022). Towards a privacy impact assessment methodology to support the requirements of the General Data Protection Regulation in a big data analytics context: A systematic literature review. *Computer Law & Security Review*,

- 44, 105640. <https://doi.org/10.1016/j.clsr.2021.105640>
- Hof, J. P. (2024). Enforcement of data breaches in the Dutch and British healthcare sector: A contribution to clarifying requirements of data protection by design? *International Review of Law, Computers & Technology*, 38(3), 327–345. <https://doi.org/10.1080/13600869.2024.2324544>
- Karjalainen, T. (2022). All talk, no action? The effect of the GDPR accountability principle on the EU data protection paradigm. *European Data Protection Law Review*, 8(1), 19–30. <https://doi.org/10.21552/edpl/2022/1/6>
- Kurtz, C., Wittner, F., Semmann, M., Schulz, W., & Böhmman, T. (2022). Accountability of platform providers for unlawful personal data processing in their ecosystems: A socio-techno-legal analysis of Facebook and Apple's iOS according to GDPR. *Journal of Responsible Technology*, 9, 100018. <https://doi.org/10.1016/j.jrt.2021.100018>
- Labadie, C., & Legner, C. (2023). Building data management capabilities to address data protection regulations: Learnings from EU-GDPR. *Journal of Information Technology*, 38(1), 16–44. <https://doi.org/10.1177/02683962221141456>
- Li, Y., Yang, R., & Lu, Y. (2024). A privacy risk identification framework of open government data: A mixed-method study in China. *Government Information Quarterly*, 41(1), 101916. <https://doi.org/10.1016/j.giq.2024.101916>
- Nyathi, M. (2023). Re-asserting the doctrinal legal research methodology in the South African academy: Navigating the maze. *South African Law Journal*, 140(2), 365–386. <https://doi.org/10.47348/SALJ/v140/i2a5>
- Rahman, F., & Mulyani, C. K. (2025). Minimising unnecessary restrictions on cross-border data flows? Indonesia's position and challenges post personal data protection act enactment. *International Review of Law, Computers & Technology*, 39(2), 281–300. <https://doi.org/10.1080/13600869.2024.2359901>
- Susilo, D. D. B. (2025). *Pelindungan hukum data pribadi terhadap data peminjam online dalam perspektif hukum perjanjian* [Master's thesis, Program Studi Magister Hukum, Universitas Mahasaraswati, Denpasar].
- Susilo, D. D. B., Perbawa, I. K. S. L. P., & Wedha, Y. Y. (2025). Legal aspects of agreement in the protection of personal data on the withdrawal of online loan borrower information. *FireNav: Financial Resilience and National Values Journal*, 1(1), 60-73.
- Susilo, D. D. B. (2026). Tanggung jawab hukum BPR atas profiling skor kredit berbasis AI berdasarkan UU PDP. *JPGI (Jurnal Penelitian Guru Indonesia)*, 11(2), 1314-1325. <https://doi.org/10.29210/027185jpgi0005>
- van Gestel, R. (2023). Quality, methodology, and politics in doctrinal legal scholarship. *Law and Method*, 2023, 1–24. <https://doi.org/10.5553/REM/000070>
- Widiatedja, I. G. N. P., & Mishra, N. (2023). Establishing an independent data protection authority in Indonesia: A future-forward perspective. *International Review of Law, Computers & Technology*, 37(3), 252–273. <https://doi.org/10.1080/13600869.2022.2155793>
- Wong, B. (2021). Problems with controller-based responsibility in EU data protection law. *International Data Privacy Law*, 11(4), 375–387. <https://doi.org/10.1093/idpl/ipab014>
- Yeung, K., & Bygrave, L. A. (2022). Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship. *Regulation & Governance*, 16(1), 137–155. <https://doi.org/10.1111/rego.12401>
- Zaguir, N. A., Magalhães, G. H. de, & Spínola, M. (2024). Challenges and enablers for

- GDPR compliance: Systematic literature review and future research directions. *IEEE Access*, 12, 81608–81630. <https://doi.org/10.1109/ACCESS.2024.3406724>
- Zhou, C., Barati, M., & Shafiq, O. (2023). A compliance-based architecture for supporting GDPR accountability in cloud computing. *Future Generation Computer Systems*, 145, 104–120. <https://doi.org/10.1016/j.future.2023.03.021>

Peraturan Perundang-undangan dan Instrumen Hukum

- European Parliament & Council of the European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation)*.
- Indonesia. (2019). *Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik*.
- Indonesia. (2022). *Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*.
- Indonesia. (2024). *Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.