International Journal of Law Analytics (IJLA)
Vol. 4, No. 3 2026: 503-522

Legal Protection of Personal Data in Indonesia's Digital Public Service Transformation: A Juridical Perspective

Suyono Musimin[1]*, Taufiq Amini[2], Khaoeirun Nissa[3]
[1]Universitas Pancasila Jakarta
[2]Universitas Muslim Indonesia
[3]Universitas Negeri Lampung
Corresponding Author: Suyono Musimin synmusimin@gmail.com

A R T I C L E I N F O

Keywords: Personal Data Protection, Digital Public Services, Legal Certainty, Accountability, Indonesia

Received : 20, April
Revised : 22, June
Accepted: 24, August

A B S T R A C T

The transformation of digital public services in Indonesia increases the processing of personal data and raises issues of legal certainty, governance, and accountability. This research aims to analyze the adequacy of legal protection of personal data in the transformation of digital public services. The research uses normative juridical methods with legislative, conceptual, and case approaches. Data is collected through the study of documents on laws and regulations, policies, rulings, and legal literature without involving respondents or informants, then analyzed qualitatively through legal interpretation and regulatory synchronization. The results show that substantive personal data protection has strengthened, but governance fragmentation, weak supervision, unequal compliance, and limited rights restoration are still obstacles. The research concludes that regulatory harmonization, independent oversight, the implementation of privacy from design, and strengthening accountability are needed to ensure legal certainty and protection of people's rights.

DOI: https://doi.org/10.59890/ijla.v4i3.301
ISSN-E: 3032-4041
https://journal.multitechpublisher.com/index.php/ijla/index

INTRODUCTION

Digital transformation has changed the pattern of relations between the state and citizens through the implementation of electronic-based public services. The use of integrated service portals, digital identities, government administration applications, cloud computing, and inter-agency data exchange allows services to be provided faster, easier, and more efficiently. However, the process also increases the collection, storage, utilization, and transfer of people's personal data by public bodies and third parties technology providers. In the global context, security and privacy are important factors that determine public acceptance of digital government services. Wirtz et al. (2021) show that the quality of digital services is not only determined by ease of access, but also by security guarantees and protection of user privacy. These findings are strengthened by a meta-analysis of 68 studies that show that perceptions of privacy and security affect people's trust and intentions in using electronic government services. Thus, the protection of personal data in digital public services is not just a technical issue, but a legal issue related to citizens' rights, government legitimacy, and public trust.

In Indonesia, the urgency of personal data protection is increasing along with the development of an Electronic-Based Government System and the integration of various public services. In this implementation, the government occupies a complex position as a policy maker, service provider, personal data controller, as well as a party that is obliged to ensure the fulfillment of data subject rights. Rahman (2021) explained that the development of electronic government must balance the interests of the state in providing services with the interests of citizens for data privacy and security. The enactment of Law Number 27 of 2022 concerning Personal Data Protection has substantively strengthened the legal basis for data protection. However, a number of studies show that its implementation still faces problems in the form of weak law enforcement, overlapping authority, uneven compliance of data controllers, limited supervision, and ineffective mechanisms for restoring people's rights. This condition is becoming increasingly crucial in public services because people often have no choice but to submit their personal data to obtain population documents, health services, education, social security, licensing, and other administrative services (Hertianto, 2021; Marwenny et al., 2024; Rinjani & Firmansyah, 2025).

Theoretically, the protection of personal data in digital public services can be analyzed through the theory of legal protection, legal certainty, and government accountability. Preventive legal protection is realized through lawful processing bases, purpose restrictions, data minimization, transparency, system security, impact assessment, and the application of privacy-by-design principles. Meanwhile, repressive protection includes a complaint mechanism, violation examination, sanctions, compensation, and restoration of data subject rights. Tsamara (2021) shows that data protection regimes in various countries are generally built on the principles of restriction of purposes, consent or lawful processing basis, security, and responsibility of data controllers. Mahardika (2021) emphasized the importance of the existence of an independent supervisory authority to ensure the effectiveness of supervision and avoid

conflicts of interest when the government acts as a data controller as well as a supervisor. On the technical-juridical aspect, Gerunov (2022) explained that privacy-by-design needs to be applied from the planning, development, and evaluation stages of the digital government system, not only used as a corrective step after data leaks or misuse.

Previous studies have provided an important basis, but still show research gaps. Rahman (2021) focuses on the legal framework for data protection in the Electronic-Based Government System before the enactment of the Personal Data Protection Law, while Tsamara (2021) focuses more on comparing Indonesia's privacy regulations with several countries. Hertianto (2021) examines the weaknesses of law enforcement against data protection failures, while Mahardika (2021) specifically discusses the institutional design of independent supervisory authorities. Marwenny et al. (2024) discuss data protection in public services in general, and Sarjito (2024) examine the challenges of data security and privacy in modern government. Rinjani and Firmansyah (2025) have identified obstacles to the implementation of the Personal Data Protection Law, but have not specifically integrated it with the legal character of digital public services. At the international level, Wirtz et al. (2021) and Gupta et al. (2025) study more user preferences, trusts, and behaviors, while Gerunov (2022) is oriented towards the methodology of implementing privacy-by-design. Therefore, there is still limited juridical research after the enactment of the Personal Data Protection Law which in an integrated analysis of regulatory harmonization, the government's position as a data controller, the independence of supervision, the accountability of technology providers, the implementation of privacy-by-design, and the effectiveness of rights restoration in the transformation of digital public services in Indonesia.

Based on these gaps, this study aims to analyze the adequacy and consistency of the legal framework for personal data protection in the transformation of digital public services in Indonesia. The analysis focused on the relationship between personal data protection provisions, the implementation of government electronic systems, public services, and the responsibilities of public bodies as data controllers. The research also aims to identify forms of regulatory and institutional fragmentation, assess the adequacy of security obligations and accountability of public bodies and technology providers, and analyze the effectiveness of supervision, law enforcement, and restoration of data subject rights. To achieve this goal, the research uses normative juridical methods with legislative, conceptual, and case approaches. Legal materials are collected through the study of documents on laws and regulations, government policies, relevant decisions or cases, as well as national and international legal literature, then analyzed qualitatively through legal interpretation, regulatory synchronization, and concept comparison.

Theoretically, this research is expected to enrich the development of state administrative law and technology law through the integration of legal protection theory, legal certainty, public accountability, and privacy-by-design principles in the framework of rights-based digital governance. This research also offers the perspective that data protection in public services should be placed as an inherent state legal obligation from the system design stage, not just as a responsibility after a breach occurs. Practically, the results of the research are expected to be the basis for governments and policymakers to harmonize regulations, clarify the division of responsibilities between agencies, strengthen independent supervision, and establish a complaint and recovery mechanism that is easily accessible to the public. In addition, this research encourages the implementation of data protection impact assessments, minimization of data collection, access control, security audits, and enforceable accountability to public bodies and third parties. This step is needed so that the transformation of digital public services not only results in administrative efficiency, but also ensures legal certainty, protection of personal rights, and public trust in digital government.

THEORETICAL REVIEW

Personal Data as a Constitutional Right

Personal data is part of the right to privacy, security, and personal protection. Fauzy and Shandy (2023) explained that Law Number 27 of 2022 concerning Personal Data Protection is a legal policy that is responsive to the increase in data processing through digital technology. In public services, personal data cannot be treated only as an administrative necessity because its use is directly related to the dignity and autonomy of citizens. The protection is also related to Article 28G paragraph (1) of the 1945 Constitution which guarantees personal protection and a sense of security.

Legal protection of personal data includes preventive and repressive measures. Preventive protection is carried out through destination restrictions, lawful processing grounds, data minimization, system security, and transparency. Meanwhile, repressive protection is implemented through complaints, termination of processing, sanctions, compensation, and restoration of rights. Aruan (2024) emphasized that the existence of norms is not enough if it is not accompanied by the ability of institutions to prevent and handle violations effectively.

Legal Framework for Digital Public Services

Data protection in digital public services is mainly based on Law Number 27 of 2022 concerning Personal Data Protection and Law Number 25 of 2009 concerning Public Services. The implementation of electronic systems also refers to Government Regulation Number 71 of 2019, while digital governance is regulated through Presidential Regulation Number 95 of 2018 concerning Electronic-Based Government Systems. The regulation places public bodies as parties that are obliged to provide services safely, responsibly, and respect the rights of the community.

The SPBE framework was then strengthened through Presidential Regulation Number 132 of 2022 concerning the National SPBE Architecture and Presidential Regulation Number 82 of 2023 concerning the Acceleration of Digital Transformation and Integration of National Digital Services. Presidential Decree Number 83 of 2025 also establishes the Government's Digital Transformation Acceleration Committee to strengthen the coordination of the government's digital agenda. The integration of such services improves efficiency, but also expands the exchange of data and the risk of ambiguity of interagency liability.

Country as a Personal Data Controller

The government has a complex position as a policymaker, service provider, and controller of personal data. Suhardi (2025) introduced the concept of the state as a constitutional data controller. The concept emphasizes that the government's responsibility does not stop at technical compliance, but also includes the protection of privacy, dignity, equality, legal certainty, and citizens' access to public services. Data processing by the government has a different character than commercial processing. Citizens often have to submit data to obtain health, population, education, licensing, and social assistance services. Therefore, processing cannot always rely on consent. Its validity must be assessed based on legal authority, needs, suitability of objectives, and proportionality. This provision is important so that government authority does not lead to excessive data collection or use.

Validity, Purpose Limitations, and Transparency

Any processing of personal data must have a clear purpose and a legitimate legal basis. Data collected for one service may not be used automatically for other purposes. The risk of use outside of the original purpose is greater when government databases are integrated and exchanged between agencies. Therefore, limiting the purpose and minimizing data is an important measure in assessing the validity of digital public services.

Pakpahan (2024) emphasized that controllers and processors are obliged to understand their responsibilities in maintaining confidentiality, accuracy, security, and the use of data. Public bodies must explain the type of data collected, the purposes of the processing, the storage period, who can access it, and the procedures for correction and complaints. This openness is needed so that the public can understand how their data is managed.

Agozie and Kaya (2021) show that information regarding data collection and use affects the perception of transparency in e-government services. Lengthy and technical privacy notices can lead to user fatigue and cynicism. Therefore, transparency needs to be conveyed concisely, clearly, specifically, and at the time of processing.

Third-Party Accountability and Involvement

Digital public services often involve application developers, data center providers, cloud computing services, and cybersecurity companies. The involvement of third parties does not remove the liability of a public body. The government is still obliged to determine the purpose of processing, set security standards, supervise vendors, and ensure that data is returned or deleted after the employment relationship ends.

Priliasari (2023) shows that parties who control the system and neglect to maintain security can be held accountable for data leaks. Although his study focuses on electronic commerce, the principle is relevant to public services. Public bodies should have data processing agreements, compliance audits, access restrictions, and clear sharing of responsibilities with technology providers.

Accountability also demands the ability to prove compliance. Agencies need to document the basis of processing, data flow, access rights, retention periods, vendor evaluations, security incidents, and complaint resolution. Thus, accountability is not only the obligation to comply with the law, but also the obligation to show evidence that protections have been applied.

Privacy Since System Design and Security

The principle of privacy-by-design requires that data protection be implemented from the system planning stage. Its implementation includes data minimization, privacy settings as the initial standard, access restrictions based on tasks, encryption, activity logging, and data deletion according to the retention period. Such an approach is more effective than simply fixing the system after a leak has occurred.

Simanjuntak (2025) assesses that the Personal Data Protection Law has adopted principles that are in line with international standards. However, its effectiveness still depends on institutional readiness, supervision, and technical implementation. Therefore, normative compliance needs to be realized through security audits, employee training, vulnerability assessments, and incident response procedures.

Ribeiro et al. (2025) found that many public service platforms in the world still use outdated protocols, poorly configured certificates, and systems that have not been updated. The findings show that security is part of the legal obligations of data controllers. Failure to update the system can increase the risk of attack and harm the community.

Identification and Management of Privacy Risks

Privacy risks in public services do not only come from technology. Li et al. (2024) identified five risk dimensions, namely data, institutional, technical, structural, and behavioral risks. The multidimensional approach suggests that leaks can occur due to poor system design, poor coordination, employee error, or inadequate access policies. A data protection impact assessment is required before a public body undertakes high-risk processing. Such assessments are especially important for health data, biometrics, children, financial data, large-scale database matching, and automated decisions. The results of the assessment

should be used to restrict data, improve security, and determine whether processing is worth continuing.

Independent Oversight

Oversight is necessary to ensure data protection norms are applied consistently. Problems arise when the government acts as a data controller while supervising its own actions. Such structures have the potential to create conflicts of interest, especially when violations involve strategic public bodies. Ayiliani and Farida (2024) recommend the establishment of independent regulatory agencies based on the concept of independent regulatory agencies. The institution needs to have the authority to receive complaints, conduct examinations, request documents, audit the system, provide corrective actions, and impose sanctions. Independence is needed so that supervision is not easily influenced by the institution being examined. Supervision also requires coordination with cybersecurity agencies, ministries in charge of digital governance, and sectoral supervisors. Unclear division of authority can lead to overlapping examinations or unhandled complaints. Therefore, institutional harmonization must include prevention, technical audits, legal investigations, sanctions, and restoration of services.

Law Enforcement and Rights Restoration

Data protection should provide an easy, fast, and affordable recovery mechanism. The public needs to have access to know the processing, obtain copies of the data, correct inaccurate data, raise objections, and demand compensation. In public services, data errors can also affect administrative decisions and access to social rights. Recovery is not enough through the provision of sanctions to agencies. Public bodies must also fix data, stop illegal access, notify incidents, restore services, and review decisions made based on erroneous data. The approach reflects legal protection that is oriented towards the restoration of rights, not just the punishment of the violator.

Literature Synthesis and Research Position

The literature shows that public data protection involves the relationship between legal norms, institutions, system design, security, and organizational behavior. The Indonesian study deals more with privacy rights, controlling obligations, and supervision separately. Meanwhile, international studies emphasize transparency, multidimensional risks, and technical security of digital services. This research fills this gap by analyzing data protection as an integrated legal system. The analysis includes regulatory harmonization, the government's position as a data controller, third-party liability, privacy-by-design, independent oversight, and rights restoration. The framework corresponds to abstracts and introductions that highlight governance fragmentation, weak oversight, uneven compliance, and limitations of recovery.

METHODOLOGY

Types of Research

This research is a normative or doctrinal juridical law research with a descriptive-analytical and prescriptive design. The approaches used include a legislative approach to analyze consistency between regulations, a conceptual approach to examine the theory of legal protection, legal certainty, accountability, and privacy since design, and a case approach to analyze the application of norms through relevant decisions. The research is directed to assess the adequacy of the legal framework for personal data protection in the transformation of digital public services in Indonesia (Disemadi, 2022; Country, 2023; Conaghan, 2023).

Legal Materials and Document Selection Techniques

This study did not use populations, sample of respondents, or human participants. The object of the research is in the form of legal materials that are purposively selected based on relevance, authority, validity status, and their relevance to the research problem. The primary legal materials include ten main instruments, namely the 1945 Constitution, Law Number 25 of 2009 concerning Public Services, Law Number 27 of 2022 concerning Personal Data Protection, Law Number 1 of 2024 concerning the Second Amendment to the Law on Information and Electronic Transactions, Government Regulation Number 71 of 2019, Presidential Regulation Number 95 of 2018, Presidential Regulation Number 132 of 2022, Presidential Regulation Number 82 of 2023, Presidential Regulation Number 83 of 2025, and Constitutional Court Decision Number 151/PUU-XXII/2024. Secondary legal materials consist of journal articles and scientific literature in 2021–2025.

Research Instruments

The main instrument of the research is the researcher with the help of a matrix of legal material analysis and document coding sheets. The matrix contains the hierarchy and regulatory status, the basis for data processing, the rights of the data subject, the obligations of controllers and processors, system security, supervision, sanctions, and rights recovery mechanisms. Since the study did not use questionnaires or measurement scales, testing of construct validity and statistical reliability was not required. The validity of the analysis is maintained through checking the authenticity of the source, triangulating legal materials, using consistent analysis categories, and recording the interpretation process (Mitchell, 2023; Byrne & Olsen, 2024).

Data Collection Procedure

The collection of legal materials begins with the formulation of legal issues regarding regulatory fragmentation, the position of public bodies as data controllers, accountability of technology providers, supervision, privacy since design, and restoration of rights. Regulations and rulings are searched through official databases of government and judicial institutions, while scientific literature is searched through journal databases. Documents are selected based on relevance, validity status, issuing authority, accessibility, and verifiability. The selected documents are then classified and included in a matrix based on the research theme (Tan, 2021; Sukmawan & Damayanti, 2025).

Data Analysis Techniques

Legal materials are analyzed qualitatively through legal content analysis and doctrinal reasoning. Grammatical, systematic, and teleological interpretations are used to understand the meaning and purpose of norms. Vertical synchronization is performed to assess the compliance of lower regulations with legislation, while horizontal synchronization is used to identify overlaps, ambiguities, or gaps between data protection regulations, public services, and SPBEs. The results of the analysis were compiled deductively and prescriptively to formulate the strengthening of legal protection. NVivo 14 for theme coding, Microsoft Excel for regulatory matrices, and Mendeley for reference management (State, 2023; Conaghan, 2023; Byrne & Olsen, 2024).

RESEARCH RESULTS

Scope of Legal Materials Analyzed

This research analyzes ten primary legal materials consisting of the 1945 Constitution, Law Number 25 of 2009 concerning Public Services, Law Number 27 of 2022 concerning Personal Data Protection, Law Number 1 of 2024 concerning the Second Amendment to the Law on Information and Electronic Transactions, Government Regulation Number 71 of 2019, Presidential Regulation Number 95 of 2018, Presidential Regulation Number 132 of 2022, Presidential Regulation Number 82 of 2023, Presidential Regulation Number 83 of 2025, and Constitutional Court Decision Number 151/PUU-XXII/2024. The analysis is also supported by government policies and the scientific literature for 2021–2025.

The study did not involve respondents or informants. Therefore, the findings presented are the result of normative analysis of the clarity of norms, inter-regulatory relationships, division of responsibilities, institutional supervision, processing security, and rights restoration mechanisms. The results of the coding of legal materials produce seven main aspects as presented in Table 1.

Table 1. Results of Analysis of the Adequacy of Legal Protection of Personal Data in Digital Public Services in Indonesia

Aspects analyzed	Key findings	Normative adequacy
Constitutional basis	Personal data is placed as part of personal personal protection and security	Strong
Data subject rights	The right of access, correction, deletion, objection, termination of processing, and redress has been set up	Substantively strong
Obligations of public bodies	The basis for processing, security, accuracy, transparency, and accountability has been determined	Enough
Integration with SPBE	Integration and interoperability have been arranged, but the division of data protection responsibilities has not been detailed	Partial
Privacy from design	There is a basis for security obligations and risk assessments, but the standards of implementation are not yet uniform	Partial
Supervision	The supervisory functions have been regulated, but are spread across several institutional structures	Not optimal yet
Restoration of rights	Grievance, sanction, dispute, and redress channels are available, but they are within several legal regimes	Fragmented

Strengthening Substantive Legal Protection

The results of the analysis show that Law Number 27 of 2022 has strengthened the legal basis for personal data protection in Indonesia. The law regulates the categories of personal data, the rights of the data subject, the basis for processing, the obligations of controllers and processors, data transfers, the appointment of data protection officials or officers, dispute resolution, administrative sanctions, and criminal provisions.

The rights of the identified data subjects include the right to obtain information, access data, correct inaccurate data, terminate certain processing, delete data, withdraw consent, file objections, and demand compensation. On the data controller side, it is found the obligation to ensure the lawfulness of the processing, maintain accuracy, ensure security, restrict access, record processing activities, and be responsible for the processing carried out. These results show that preventive and repressive protection has gained a clearer legal basis. Preventive protection is reflected in security obligations, purpose limitations, accuracy, and access control. Repressive protection is reflected in the termination of processing, deletion of data, administrative sanctions, dispute resolution, compensation demands, and criminal provisions.

Fragmentation between Data Protection and SPBE Governance

The results of horizontal synchronization show that personal data protection regulations and Electronic-Based Government System regulations have different regulatory focuses. The Personal Data Protection Law focuses on the rights of data subjects, lawfulness of processing, restriction of purposes, security, and controller accountability. Meanwhile, Presidential Regulation Number 95 of 2018 and Presidential Regulation Number 132 of 2022 focus more on business processes, data, applications, infrastructure, security, architecture, and SPBE integration. Presidential Regulation Number 82 of 2023 regulates the acceleration of the integration of national digital services and the use of priority SPBE applications. However, the analysis did not find detailed arrangements regarding the division of positions as data controllers, shared controllers, or processors when data is exchanged by multiple agencies in a single integrated service.

Term differences are also found between the SPBE regime and the personal data protection regime. The SPBE Regulation uses the terms information security, interoperability, data architecture, and service integration, while the Personal Data Protection Law uses the terms controller, processor, data subject, processing purpose, and data subject rights. The operational relationship between the two concept groups has not been uniformly formulated. This condition creates an unclear division of responsibility when one agency collects data, another agency utilizes data, and a third party manages its system or infrastructure. The SPBE structure can show the technical flow of data management, but it does not necessarily show the party responsible for fulfilling the rights of the data subject and handling the violation.

Position of Public Bodies and Technology Providers

The results of the analysis show that the public body that determines the main purpose and means of processing is positioned as the controller of personal data. That position remains inherent even if the storage, system maintenance, application development, or technical processing is performed by the technology provider. In public services, the basis for data processing is not always in the form of the consent of the data subject. Processing may be based on a legal obligation, the performance of a task in the public interest, or the exercise of authority based on laws and regulations. This is found in population services, health, education, taxation, social security, social assistance, and licensing.

An analysis of the relationship between public bodies and technology providers shows that procurement contracts have an important function in the division of responsibilities. However, the analyzed regulations have not uniformly regulated the purpose of processing, the prohibition of the use of data for other purposes, access limits, storage locations, incident reporting, audit rights, data returns, and data deletion after the contract expires. These results show that the handover of technical processing to a third party does not transfer all legal responsibilities of public entities. Public bodies still have an obligation to supervise processing and ensure that technology providers process data for the purposes that have been determined.

Unevenness of Compliance and Accountability Instruments

The results of the document study show that there are differences in the completeness of compliance instruments in the implementation of digital public services. These differences can be seen in privacy policies, internal responsibility sharing, security standards, documentation of processing activities, audit mechanisms, evaluation of technology providers, and complaint procedures. The Personal Data Protection Law has established the liability obligations of data controllers. However, the results of the analysis did not find a single national format that was applied comprehensively for recording processing activities, mapping data flows, processing bases, retention periods, technology provider assessments, incident handling, and fulfillment of data subject rights.

Inequality is also found in the implementation of the functions of officials or personal data protection officers. The differences are in organizational structure, competencies, human resources, functional independence, and work procedures. These conditions affect the implementation of internal audits, the provision of compliance advice, risk monitoring, and the service of data subject requests. The findings on compliance inequality do not indicate the level of compliance in the form of numbers or agency rankings. The findings are limited to the variety of governance instruments and documentation obtained through the analysis of documents, cases, and literature.

Privacy from Design and Risk Management

The results of the analysis show that personal data protection needs to be applied to the entire system implementation cycle, from planning, development, testing, integration, operation, storage, to data deletion. The privacy elements since the design identified include data minimization, restriction of access rights, authentication, encryption, activity logging, data separation, determination of retention periods, and deletion of data. The Personal Data Protection Law and Government Regulation Number 71 of 2019 have contained security obligations and accountability in the implementation of electronic systems. However, the results of the analysis show that the operational standards for its application are not uniform in all public bodies.

The integration of digital services also increases the need for data protection impact assessments. Processing identified as having higher risks includes health data, biometric data, child data, financial data, large-scale database matching, systematic monitoring, and automated decision-making. In the legal materials analyzed, there has not been a single uniform public mechanism to demonstrate that each public body has conducted, documented, and followed up on impact assessments before using high-risk systems.

Findings of the Constitutional Court Decision on Data Protection Officials

The Constitutional Court Decision Number 151/PUU-XXII/2024 provides changes to the meaning of Article 53 paragraph (1) of the Personal Data Protection Law. The word "and" in the provision is interpreted as "and/or", so that the requirements for the appointment of officials or data protection officers no longer have to be met cumulatively. The results of the analysis of the decision show that data processing for the benefit of public services can be a separate basis for the obligation to appoint officials or personal data protection officers. Public bodies do not have to simultaneously carry out large-scale systematic monitoring and large-scale processing of specific data to be subject to these obligations. Although the obligation of appointment has become broader, the results of the document study have not shown uniformity regarding the organizational position, competence, independence, authority, and work procedures of officials or data protection officers in all public bodies.

Institutional Oversight and Fragmentation

The Personal Data Protection Law has regulated the functions of policy formulation, supervision, administrative law enforcement, and dispute resolution facilitation. However, the results of the analysis show that functions related to digital public services are also carried out by several other institutions. These institutions include digital transformation support agencies, cybersecurity institutions, public service providers, sectoral supervisors, ombudsmen, law enforcement officials, and courts. Presidential Regulation Number 83 of 2025 also establishes the Government's Digital Transformation Acceleration Committee which functions in coordinating and synchronizing digital service transformation.

The results of the analysis show that the mandate of the Government's Digital Transformation Acceleration Committee is different from the mandate of the data protection supervisory agency. The committee focuses on accelerating and coordinating digital transformation, while the data protection oversight function includes compliance checks, complaint handling, corrective actions, and sanctioning. There has not been a single institutional flow that integrates compliance supervision, technical audits, incident handling, violation investigations, sanctions, and restoration of rights in digital public services.

Limitations of Rights Recovery Mechanism

The results of the analysis show that the data subject already has a legal basis to gain access, make corrections, lodge objections, request the cessation or deletion of certain processing, and demand compensation. In addition, there are administrative sanctions, dispute resolution, and criminal provisions. However, the recovery mechanism in digital public services is still spread across several legal regimes. Complaints regarding public services can be submitted to the organizer or the Ombudsman. Data processing breaches follow personal data protection regimes, while attacks on electronic systems may involve provisions regarding electronic systems, cybersecurity, and electronic information.

Losses arising from administrative decisions based on inaccurate data may also require an administrative objection mechanism or state administrative court. The results of the analysis did not find a single unified procedure that automatically links corrections of personal data with corrections of administrative decisions that have been generated based on the data. The remedial components found include unlawful access termination, data remediation, notification to data subjects, account security remediation, service remediation, administrative decision review, and compensation. These components have not been placed in a single integrated complaint and recovery pathway.

Summary of Key Findings

The results of the study show that the substantive legal framework for personal data protection has strengthened after the enactment of Law Number 27 of 2022. The strengthening can be seen in the regulation of data subject rights, controllers and processors' obligations, processing security, sanctions, dispute resolution, and compensation. However, four main obstacles were found. First, personal data protection regulations and SPBE governance have not been operationally integrated. Second, the division of responsibilities between public agencies, data user agencies, and technology providers has not been uniformly formulated. Third, compliance instruments, privacy since design, and the functions of the data protection office have not been applied evenly. Fourth, the supervisory function and mechanism for restoring rights are still spread across several institutions and legal regimes.

DISCUSSION

Strengthening Substantive Protection and Shifting Legal Issues

The results of the study show that Law Number 27 of 2022 concerning Personal Data Protection has strengthened substantive protection through the regulation of data subject rights, processing basis, controllers and processors' obligations, sanctions, and compensation. These findings are in line with the theory of legal protection because the norm includes both preventive and repressive protection. Fauzy and Shandy (2023) place data protection as a responsive legal policy and related to the constitutional right to privacy. Aruan (2024) also emphasized that the effectiveness of protection does not sufficiently depend on norms, but requires institutions and procedures that are able to prevent and remedy violations. Thus, legal issues after the enactment of the Personal Data Protection Law have shifted from the absence of a legal umbrella to implementation effectiveness, regulatory harmonization, and institutional accountability.

The findings support the initial proposition that the existence of specific laws has not automatically resulted in effective protection. This is different from research before the passage of the Personal Data Protection Law which emphasized the lack of regulation. This difference can be explained by changes in the legal context: Indonesia now has a substantive framework, but still faces the unpreparedness of legal systems, institutions, and enforcement mechanisms. This condition is in line with Rinjani and Firmansyah (2025), who found that overlapping authority and low accountability are the main obstacles to the implementation of the Personal Data Protection Law.

Fragmentation of Digital Public Service Governance

The lack of integration of the data protection regime with the governance of the Electronic-Based Government System shows that there is a gap between the orientation of rights and the orientation of administrative efficiency. The SPBE regulation emphasizes interoperability, application integration, data architecture, and information exchange, while the Personal Data Protection Law emphasizes purpose restrictions, data minimization, data subject rights, and controller accountability. If the two orientations are not aligned, service integration can expand data processing without a clear division of responsibilities.

These findings strengthen the concept of the state as a constitutional data controller. The government is not only responsible for ensuring that the system works, but also obliged to maintain the privacy, dignity, legal certainty, and rights of citizens. Suhardi (2025) assesses that the state's responsibility in SPBE must cover the entire data processing cycle. Therefore, the division of positions as controllers, joint controllers, and processors needs to be established before data is exchanged between institutions. The contribution of this research lies in the merging of the perspectives of administrative law and technology law: the success of digital integration is measured not only by the connectedness of the system, but also by the clarity of legal accountability.

Accountability of Public Bodies and Third Parties

The involvement of data center providers, cloud computing, application developers, and security companies does not remove the responsibility of public bodies as data controllers. Pakpahan (2024) emphasized that the controller determines the processing purpose, while the processor performs the processing on behalf of the controller. Therefore, the failure of vendors does not necessarily exempt government agencies from the obligation to select, supervise, audit, and restrict access.

These findings are in line with Priliasari's (2023) study that parties who control processing activities can be held accountable when their negligence causes data leaks. Although Priliasari's research is in the context of electronic commerce, the principle of responsibility is relevant for government technology contracts. Consequently, digital procurement contracts need to contain processing purposes, prohibitions of secondary use, storage locations, incident reporting obligations, audit rights, data returns, and data deletion after the contract expires. Accountability should thus be understood as an obligation to comply as well as prove compliance through verifiable documentation.

Supervision and Law Enforcement

The findings of weak supervision do not mean that there is no supervision arrangement, but that there is no fully independent and integrated mechanism. The problem arises because public bodies are in the same government environment as the supervisory structure formed by the executive. This situation can cause a conflict of interest when violations are committed by ministries or strategic institutions. Ayiliani and Farida (2024) propose a supervisory authority based on the concept of an independent regulatory agency so that inspections and law enforcement are not easily influenced by the supervised parties. Independent oversight is important because preventive protection requires audits, guidelines, impact assessments, and corrective actions, while repressive protection requires complaint review and sanctioning. The findings of this study expand the study by showing that the supervision of personal data also needs to be linked to the supervision of public services, cybersecurity, and administrative decisions.

Privacy-by-Design, Security, and Public Trust

The inconsistency in the implementation of privacy-by-design shows that legal compliance is still often placed as an administrative measure after the system is completed. In fact, Gerunov (2022) places privacy protection as part of all stages of digital government service development. In the Indonesian context, these principles need to be applied through data minimization, access restrictions, encryption, activity logging, retention periods, security testing, and data protection impact assessments before high-risk systems are used. The implementation has wider consequences for the sustainability of digital public services. Gupta et al. (2025) found that perceptions of risk, privacy, and security affect public trust in electronic government services. Ribeiro et al. (2025), through an analysis of 3,068 public service platforms, also found gaps in the form of old protocols, improper certificates, and unpatched vulnerabilities. The international findings support the findings of the study that technical security should be positioned as part of a legal obligation, not just a technology management option.

Restoration of Research Rights and Contributions

The remedy mechanisms that are scattered in the data protection regime, public service, government administration, ITE, and the judiciary can make it difficult for society when a single breach results in multiple losses at once. Data corrections don't always automatically correct administrative decisions that have been made based on incorrect data. Therefore, remediation needs to include data correction, illegal access termination, incident notification, service recovery, decision review, and compensation.

The theoretical contribution of this research is the development of a public data protection model as an integrated legal system consisting of six components: processing lawfulness, system design, division of responsibility, supervision, law enforcement, and administrative remediation. Practically, the results of the study point to the need for harmonization between the SPBE policy and the Personal Data Protection Law, national standards for compliance documentation, strengthening the functions of data protection officials, data protection clauses in technology contracts, and a single complaint channel that can coordinate data correction and service recovery.

Differences with Previous Research

The findings of this study show a change in the focus of the problem compared to research before the enactment of Law Number 27 of 2022. Previous research has mostly placed the absence of special laws as the main weakness, while this study shows that problems have shifted towards governance fragmentation, unequal compliance, suboptimal supervision, and limited rights restoration. The study also expands on previous studies by linking the protection of personal data with the SPBE architecture, the division of responsibilities between institutions, the position of technology providers, and the correction of administrative decisions that use inaccurate data.

Limitations and Recommendations for Advanced Research

The main limitation of the research lies in the normative juridical design that does not measure the compliance of each agency empirically. Findings on compliance inequality are based on an analysis of documents, cases, and literature, so they cannot be used to make quantitative rankings of ministries, institutions, or local governments. The research is also limited by the development of the implementing policies of the Personal Data Protection Law, which is still dynamic. Follow-up research is recommended using an empirical juridical approach or mixed method with audits of several public services, interviews of data protection officials, analysis of public complaints, and evaluation of technology provider contracts. Comparisons between population, health, education, and social assistance services are also needed to determine the difference in risk and effectiveness of recovery in each sector.

CONCLUSIONS AND RECOMMENDATIONS

This study concludes that the legal protection of personal data in the transformation of digital public services in Indonesia has experienced substantive strengthening after the enactment of Law Number 27 of 2022. Data subject rights, processing basis, controller and processor obligations, data security, sanctions, and compensation have obtained a clearer legal basis. However, its effectiveness is still limited by the lack of integration of data protection governance with SPBE, the unclear division of responsibilities in inter-agency data exchange, the unevenness of compliance instruments, supervision that is not yet fully independent, and rights restoration mechanisms that are still scattered in several legal regimes.

The government needs to align the SPBE policy with the Personal Data Protection Law through a clear division of the roles of controllers, joint controllers, and processors. Public bodies need to implement privacy from design, data protection impact assessment, data minimization, access restrictions, security audits, compliance documentation, and data protection clauses in technology contracts. Oversight needs to be strengthened through independent institutional functions, while complaints mechanisms should link data correction, service recovery, review of administrative decisions, and compensation.

ADVANCED RESEARCH

Follow-up research needs to use an empirical juridical approach or mixed methods to test the implementation of data protection in population, health, education, licensing, and social assistance services. Research can be conducted through compliance audits, interviews with data protection officials, analysis of public complaints, and evaluation of contracts between public bodies and technology providers.

ACKNOWLEDGMENT

The author expresses his gratitude to those who have supported access to legal sources and scientific literature used in this study. All analysis, opinions, and responsibility for the content of the article rests entirely with the author.

REFERENCES

Agozie, D. Q., & Kaya, T. (2021). Discerning the effect of privacy information transparency on privacy fatigue in e-government. Government Information Quarterly, 38(4), Article 101601. https://doi.org/10.1016/j.giq.2021.101601.

Aruan, J. E. S. (2024). Perlindungan data pribadi ditinjau dari teori perlindungan hukum dan teori perlindungan hak atas privasi. Jurnal Globalisasi Hukum, 1(1), 1–22. https://doi.org/10.25105/jgh.v1i1.19499.

Ayiliani, F. M., & Farida, E. (2024). Urgensi pembentukan lembaga pengawas data pribadi sebagai upaya pelindungan hukum terhadap transfer data pribadi lintas negara. Jurnal Pembangunan Hukum Indonesia, 6(3), 431–455. https://doi.org/10.14710/jphi.v6i3.431-455.

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.

Conaghan, J. (2023). Legal research and the public good: The current landscape. Legal Studies, 43(4), 569–582. https://doi.org/10.1017/lst.2023.37.

Disemadi, H. S. (2022). Lenses of legal research: A descriptive essay on legal research methodologies. Journal of Judicial Review, 24(2), 289–304. https://doi.org/10.37253/jjr.v24i2.7280.

Fauzy, E., & Shandy, N. A. R. (2023). Hak atas privasi dan politik hukum Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Lex Renaissance, 7(3), 445–461. https://doi.org/10.20885/JLR.vol7.iss3.art1.

Gerunov, A. A. (2022). A privacy-by-design implementation methodology for e-government. International Journal of Electronic Government Research, 18(1), 1–20. https://doi.org/10.4018/IJEGR.288067.

Gupta, P., Hooda, A., Jeyaraj, A., Seddon, J. J. M., & Dwivedi, Y. K. (2025). Trust, risk, privacy and security in e-government use: Insights from a MASEM analysis. Information Systems Frontiers, 27(3), 1089–1105. https://doi.org/10.1007/s10796-024-10497-8.

Hertianto, M. R. (2021). Sistem penegakan hukum terhadap kegagalan dalam perlindungan data pribadi di Indonesia. Kertha Patrika, 43(1), 93–109. https://doi.org/10.24843/KP.2021.v43.i01.p07.

Indonesia. (1945). Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 dan perubahannya. https://peraturan.bpk.go.id/Details/101646.

Indonesia. (2009). Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik. https://peraturan.bpk.go.id/Details/38748/uu-no-25-tahun-2009.

Indonesia. (2018). Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik. https://peraturan.bpk.go.id/Details/96913/perpres-no-95-tahun-2018.

Indonesia. (2019). Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. https://peraturan.bpk.go.id/Details/122030/pp-no-71-tahun-2019.

Indonesia. (2022a). Peraturan Presiden Nomor 132 Tahun 2022 tentang Arsitektur Sistem Pemerintahan Berbasis Elektronik Nasional. https://peraturan.bpk.go.id/Details/233483/perpres-no-132-tahun-2022.

Indonesia. (2022b). Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022.

Indonesia. (2023). Peraturan Presiden Nomor 82 Tahun 2023 tentang Percepatan Transformasi Digital dan Keterpaduan Layanan Digital Nasional. https://peraturan.bpk.go.id/Details/273981/perpres-no-82-tahun-2023.

Indonesia. (2024). Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. https://peraturan.bpk.go.id/Details/274494/uu-no-1-tahun-2024.

Indonesia. (2025). Peraturan Presiden Nomor 83 Tahun 2025 tentang Komite Percepatan Transformasi Digital Pemerintah. https://peraturan.bpk.go.id/Details/329002/perpres-no-83-tahun-2025.

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), Article 101916. https://doi.org/10.1016/j.giq.2024.101916.

Mahardika, A. M. (2021). Desain ideal pembentukan otoritas independen perlindungan data pribadi dalam sistem ketatanegaraan Indonesia. Jurnal Hukum, 37(2), 213–230. https://doi.org/10.26532/jh.v37i2.16994.

Mahkamah Konstitusi Republik Indonesia. (2025). Putusan Nomor 151/PUU-XXII/2024 mengenai pengujian Pasal 53 ayat (1) Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. https://www.mkri.id/berita/mk%3A-data-pribadi-warga-wajib-dilindungi-negara-secara-maksimal-23553.

Marwenny, E., Syafwar, R., & Yani, P. (2024). Personal data protection in public services. Jurnal Ilmiah Ekotrans & Erudisi, 4(2), 74–85. https://doi.org/10.69989/yjew5p90.

Mitchell, M. (2023). Analyzing the law qualitatively. Qualitative Research Journal, 23(1), 102–113. https://doi.org/10.1108/QRJ-04-2022-0061.

Negara, T. A. S. (2023). Normative legal research in Indonesia: Its originis and approaches. Audito Comparative Law Journal, 4(1), 1–9. https://doi.org/10.22219/aclj.v4i1.24855.

Pakpahan, J. M. (2024). Kesadaran urgensi peran pengendali dan prosesor data pribadi dalam rangka pelindungan data pribadi individu berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Jurnal Hukum to-Ra: Hukum untuk Mengatur dan Melindungi Masyarakat, 10(1), 119–137. https://doi.org/10.55809/tora.v10i1.331.

Peraturan Perundang-undangan dan Putusan

Priliasari, E. (2023). Perlindungan data pribadi konsumen dalam transaksi e-commerce. Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional, 12(2), 261–279. https://doi.org/10.33331/rechtsvinding.v12i2.1285.

Rahman, F. (2021). Kerangka hukum perlindungan data pribadi dalam penerapan sistem pemerintahan berbasis elektronik di Indonesia. Jurnal Legislasi Indonesia, 18(1), 81–102. https://doi.org/10.54629/jli.v18i1.736.

Ribeiro, D., Fonte, V., Ramos, L. F., & Silva, J. M. (2025). Assessing the information security posture of online public services worldwide: Technical insights, trends, and policy implications. Government Information Quarterly, 42(2), Article 102031. https://doi.org/10.1016/j.giq.2025.102031.

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.

Rosidi, A., Zainuddin, M., & Arifiana, I. (2024). Metode dalam penelitian hukum normatif dan sosiologis (field research). Journal Law and Government, 2(1), 46–58. https://doi.org/10.31764/jlag.v2i1.21606.

Sarjito, A. (2024). Data security and privacy in the digital era: Challenges for modern government. JIAN (Jurnal Ilmiah Administrasi Negara), 8(2), 1–13. https://doi.org/10.56071/jian.v8i3.933.

Simanjuntak, P. H. (2025). Perlindungan hukum terhadap data pribadi pada era digital di Indonesia: Studi Undang-Undang Pelindungan Data Pribadi dan General Data Protection Regulation (GDPR). Esensi Hukum, 6(2), 105–124. https://doi.org/10.35586/esensihukum.v6i2.412.

Suhardi, M. (2025). State responsibility in personal data protection within the electronic-based government system. Jurnal Kecerdasan Buatan dan Teknologi Informasi, 4(3), 292–302. https://doi.org/10.69916/jkbti.v4i3.458.

Sukmawan, Y. A., & Damayanti, D. (2025). Metode penelitian hukum normatif dan empiris sebagai strategi penguatan perspektif kajian ilmu hukum. Notary Law Journal, 4(3), 114–128. https://doi.org/10.32801/nolaj.v4i3.116.

Tan, D. (2021). Metode penelitian hukum: Mengupas dan mengulas metodologi dalam menyelenggarakan penelitian hukum. NUSANTARA: Jurnal Ilmu Pengetahuan Sosial, 8(8), 2463–2478. https://doi.org/10.31604/jips.v8i8.2021.2463-2478.

Tsamara, N. (2021). Perbandingan aturan perlindungan privasi atas data pribadi antara Indonesia dengan beberapa negara. Jurnal Suara Hukum, 3(1), 53–84. https://doi.org/10.26740/jsh.v3n1.p53-84.

Wiraguna, S. A. (2025). Eksplorasi metode penelitian dengan pendekatan normatif dan empiris dalam penelitian hukum di Indonesia. Lex Jurnalica, 22(1), 66–72. https://doi.org/10.47007/lj.v22i1.8801.

Wirtz, B. W., Müller, W. M., & Schmidt, F. W. (2021). Digital public services in smart cities—An empirical analysis of lead user preferences. Public Organization Review, 21, 299–315. https://doi.org/10.1007/s11115-020-00492-3.

Yanova, M. H., Komarudin, P., & Hadi, H. (2023). Metode penelitian hukum: Analisis problematika hukum dengan metode penelitian normatif dan empiris. Badamai Law Journal, 8(2), 394–408. https://doi.org/10.32801/damai.v8i2.17423.