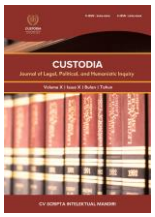

Custodia: Journal of Legal, Political, and Humanistic Inquiry
Vol 2 No 1 September 2026, Hal 364-387
ISSN: 3123-2116 (Print) ISSN: 3123-2108 (Electronic)
Open Access: https://scriptaintelektual.com/custodia

Personal Data Protection in Indonesia's Digital Public Services: Implementation and Accountability

Ade Wahyuni Azhar[1*], Hasan Ahmad[2], Diganta Hatiboruah[3]
[1] APP APIPSU Medan, Indonesia
[2] London Academy For Applied Technology, United Kingdom
[3] Majuli College, India
email: doktoradewahyuni@gmail.com[1]

Article Info :
Received:
02-09-2026
Revised:
18-09-2026
Accepted:
26-09-2026

Abstract

Indonesia's integrated digital public services create legal accountability challenges concerning the collection, exchange, and subsequent use of personal data across government institutions. This study examines whether Indonesia's personal-data protection framework establishes coherent legal responsibilities and safeguards for public-sector processing. A normative-doctrinal research design applies statutory, conceptual, and comparative legal analysis to Law No. 27 of 2022, digital-government regulations, Constitutional Court Decision No. 151/PUU-XXII/2024, and Government Regulation No. 33 of 2026. Public-sector cybersecurity incidents serve as documentary illustrations rather than empirical proof of statutory violations. The findings establish that governmental processing must satisfy recognized lawful bases, purpose-related limitations, security obligations, and identifiable controller responsibilities. However, statutory completeness does not itself demonstrate consistent institutional compliance, particularly across interconnected processing activities and supervisory arrangements. Government Regulation No. 33 of 2026, promulgated in July 2026, provides additional implementing provisions but does not enter into force until January 2027. The analysis identifies a need for documented processing responsibilities, risk assessment, verifiable audit records, and effective institutional supervision. These mechanisms constitute operational recommendations grounded in statutory and comparative analysis. The study concludes that Indonesia's principal normative challenge concerns translating established legal obligations into demonstrable, traceable, and independently reviewable accountability across digital public services.

Keywords: *Accountability, Digital Public Services, Indonesia, Personal Data Protection, Public Sector.*

©2026 Authors.. This work is licensed under a Creative Commons Attribution-Non Commercial 4.0 International License.
(https://creativecommons.org/licenses/by-nc/4.0/)

INTRODUCTION

Digital public services have altered the legal characteristics of administrative data processing by enabling information collected for specific governmental purposes to be stored, combined, exchanged, and reused across interconnected information systems. Indonesia has pursued this transformation through the Electronic-Based Government System (Sistem Pemerintahan Berbasis Elektronik, SPBE) and the subsequent integration of national digital services, expanding the role of digital infrastructure in interactions between public institutions and citizens (Abdurrahman et al., 2025). Interoperability enables administrative efficiency by reducing repetitive data collection, facilitating interagency coordination, and supporting more consistent service delivery, although these benefits depend on the institutional arrangements governing information exchange (Eom & Lee, 2022). Population administration, taxation, social protection, licensing, healthcare, and electoral administration increasingly involve the continuous processing of personal identifiers and other information across multiple organizational units. The resulting administrative arrangements extend the legal implications of data processing beyond the institution that initially collects personal information. Personal-data protection consequently concerns not only the security of electronic systems but also the legality of governmental decisions concerning data collection, access, retention, disclosure, and subsequent use.

.

The integration of digital public services raises a distinct accountability problem because public authorities exercise considerable control over personal information that individuals must disclose to obtain legally mandated administrative services. This informational power derives from the statutory authority of public institutions to collect and process information, the practical necessity of citizen participation in administrative procedures, and the asymmetry between governmental access to integrated databases and individual control over subsequent processing. Citizens may have limited opportunities to refuse processing associated with mandatory identification, taxation, or eligibility verification without affecting their access to public services. Research on e-government adoption identifies privacy, security, institutional reliability, and public trust as relevant considerations in citizens' relationships with digital government systems (Gupta et al., 2025). These considerations acquire legal significance where information initially obtained for one administrative function becomes accessible to other institutions through interoperable infrastructures. The existence of a statutory public function does not independently establish unrestricted authority to reuse personal data for additional purposes. The central legal question concerns whether public institutions can demonstrate that each processing operation remains within a recognized legal basis, serves a specified purpose, and is subject to identifiable institutional responsibility.

The constitutional foundation of personal-data protection in Indonesia is principally derived from Article 28G(1) of the 1945 Constitution, which guarantees protection of the individual, personal dignity, and security, together with Article 28D(1), which guarantees recognition, protection, and fair legal certainty. Article 28G(1) provides the substantive constitutional basis for protecting personal information against unjustified interference, while Article 28D(1) supports the requirement that governmental processing activities rest upon legally ascertainable authority and procedures. Constitutional Court Decision No. 151/PUU-XXII/2024, delivered on 30 July 2025, reinforced this relationship by recognizing personal-data protection as an integral component of the constitutional right to personal protection and clarifying the statutory conditions governing the appointment of personal-data protection officers. Law No. 27 of 2022 on Personal Data Protection (PDP Law) translates these constitutional guarantees into a statutory framework governing data-subject rights, lawful processing, controller and processor responsibilities, institutional supervision, and legal remedies (Lestari & Mujib, 2022). Articles 5–13 establish specific data-subject rights, subject to applicable statutory qualifications and exceptions, while Article 16(2) regulates the principles applicable throughout the personal-data processing lifecycle. Article 16(2)(a) requires collection to be limited, specific, lawful, and transparent, Article 16(2)(b) requires processing to correspond to its purpose, Article 16(2)(e) requires protection against unauthorized access and disclosure, and Article 16(2)(h) requires processing to be accountable and demonstrable. These provisions establish a normative relationship between constitutional protection, substantive processing requirements, and the obligation of public institutions to justify their handling of personal information.

The application of these provisions to digital public administration requires particular attention to the distinction between the legal authorization for initial collection and the authorization for subsequent processing or interagency data sharing. Article 20(1) of the PDP Law obliges personal-data controllers to possess a lawful basis for processing, while Article 20(2)(c) recognizes compliance with legal obligations and Article 20(2)(e) recognizes the performance of tasks in the public interest, public services, or the exercise of lawful governmental authority. These provisions permit public-sector processing where the relevant statutory conditions are satisfied, but they do not establish an unrestricted entitlement to process information for purposes unrelated to the original administrative function. Subsequent disclosure, data matching, or secondary use must also be assessed against the applicable lawful basis and the purpose-related limitations established by Article 16(2). Article 18(2) further requires arrangements between joint controllers to specify their respective roles, responsibilities, processing purposes, and designated contact arrangements. The distinction is particularly significant where governmental institutions and external service providers exercise different degrees of control over interconnected databases. Indonesian legal scholarship identifies tensions between administrative authority, regulatory coordination, and personal-data protection as recurring issues in the implementation of the PDP Law (Rahman, 2025). Comparative analysis of data-subject rights also indicates that formal statutory recognition does not necessarily secure effective protection where institutional procedures for exercising rights remain insufficiently operationalized (Roselin & Syailendra, 2025). The legal problem extends beyond the existence of

recognized rights to the capacity of administrative institutions to identify the lawful grounds, responsible actors, and procedural safeguards applicable to each processing activity.

Indonesia's digital-government regulations create an additional dimension of this problem by establishing administrative mechanisms for increasingly integrated information systems. Presidential Regulation No. 95 of 2018 provides the regulatory foundation for SPBE, including the coordination and organization of electronic government administration (Republik Indonesia, 2018). Presidential Regulation No. 82 of 2023 strengthens the governmental policy of accelerating digital transformation and integrating national priority digital services, increasing the practical importance of interagency data exchange (Republik Indonesia, 2023). Presidential Regulation No. 174 of 2024 defines the institutional responsibilities of the Ministry of Communication and Digital within the developing governmental structure for digital administration and related policy functions (Republik Indonesia, 2024). These instruments organize the administrative and institutional conditions for digital integration but do not independently displace the substantive requirements of Law No. 27 of 2022. Their application must be examined through a systematic interpretation that distinguishes technical interoperability, administrative competence, and lawful personal-data processing. Government Regulation No. 33 of 2026 concerning the implementation of Law No. 27 of 2022 was promulgated on 16 July 2026, with its entry into force scheduled for 16 January 2027 (Republik Indonesia, 2026a). The regulation provides more detailed provisions concerning processing procedures, data-subject rights, controller and processor obligations, impact assessments, data-protection functions, transfers, supervision, administrative sanctions, and dispute resolution. Its promulgation establishes a further regulatory framework, but the provisions scheduled to enter into force in January 2027 cannot be treated as having already produced enforceable operational consequences during the preceding period. The assessment must distinguish obligations already established under the PDP Law from the more detailed implementing requirements that remain prospective.

The transitional regulatory position also raises questions concerning the institutional arrangements necessary to supervise compliance. Articles 58–60 of Law No. 27 of 2022 provide for a personal-data protection institution designated by the President and assign functions concerning policy formulation, supervision, administrative enforcement, and dispute resolution. These statutory provisions establish the legal framework for supervision, while the effectiveness of oversight depends on the establishment of institutional procedures and the exercise of the relevant powers. Official information published in July 2026 indicated that the government was continuing preparations for the personal-data protection authority contemplated by the statutory framework (Kementerian Komunikasi dan Digital Republik Indonesia, 2026). This institutional position must be distinguished from the statutory responsibilities already imposed on controllers and processors, including the duty to assess high-risk processing under Article 34(1), maintain appropriate security safeguards under Article 35, and demonstrate accountability under Article 47. Article 51 further regulates processor activities undertaken on behalf of controllers, while Article 53(1), as constitutionally interpreted in Decision No. 151/PUU-XXII/2024, establishes conditions requiring the appointment of officers responsible for personal-data protection functions, including processing undertaken for public services. The relationship between these obligations and the developing supervisory structure presents a question of institutional accountability rather than merely the completeness of legislative provisions. An operationally coherent system requires legal responsibilities to correspond to identifiable decision-making authority, documented processing activities, mechanisms for compliance verification, and procedures through which supervisory powers can be exercised.

Public-sector cybersecurity incidents provide factual circumstances for examining the practical relevance of these statutory obligations without establishing legal violations in the absence of competent findings. The ransomware incident affecting the Temporary National Data Center (Pusat Data Nasional Sementara, PDNS) in June 2024 disrupted government services and demonstrated the administrative consequences of failures affecting shared digital infrastructure (Kementerian Komunikasi dan Informatika Republik Indonesia, 2024). Its occurrence during the statutory adjustment period established by Article 74 of Law No. 27 of 2022 is relevant to determining the temporal application of particular compliance obligations and prevents the retrospective application of requirements that had not yet entered into force. Separate reports concerning taxpayer and electoral information have raised questions about data access, institutional responsibility, and the handling of possible exposure, although publicly reported allegations must remain distinct from verified official

findings (Alatas & Djajaputra, 2025). Research on e-government cybersecurity identifies technological vulnerabilities, organizational arrangements, administrative procedures, and human factors as interrelated sources of digital-government risk (Distel et al., 2022). From a normative legal standpoint, these incidents provide circumstances for examining the allocation of controller and processor responsibilities, security obligations under Article 35, oversight duties under Article 37, notification requirements under Article 46 where a legally relevant personal-data protection failure is established, and the accountability requirement under Article 47. The application of each provision must account for the documented facts, the applicable temporal legal framework, and any statutory exceptions or qualifications. The analytical significance of these incidents lies in identifying which institutional records, preventive measures, decision-making responsibilities, and corrective procedures would be necessary to evaluate legal compliance, rather than presuming that an administrative or cybersecurity disruption constitutes a proven violation of the PDP Law.

The theoretical basis for examining these relationships is provided by the principle of accountability in public administration and its application to personal-data governance. Government-data scholarship recognizes that the administrative benefits associated with information accessibility and reuse must be assessed against risks of unauthorized disclosure, inferential identification, and the re-identification of individuals (Bowen, 2024). Privacy-by-design scholarship emphasizes the incorporation of protection requirements into the development and operation of governmental information systems rather than their introduction solely as corrective measures following an incident (Gerunov, 2022). Data-protection impact assessments provide an institutional mechanism for identifying processing-related risks, evaluating their implications for individual rights, and documenting appropriate mitigation measures (Riemann et al., 2023). Research on e-government service quality also identifies institutional performance and public trust as important dimensions of the relationship between governmental organizations and service users (Alsarraf et al., 2023). These perspectives provide distinct but complementary explanations of accountability: legal accountability requires compliance with identifiable statutory obligations, organizational accountability requires responsibilities and procedures capable of being verified, and public accountability requires mechanisms through which governmental actions can be explained and subjected to appropriate scrutiny. Comparative data-protection arrangements, particularly those addressing public-authority processing and supervisory independence, provide analytical references for evaluating these requirements without assuming that foreign institutional models can be directly transferred to Indonesia. The resulting conceptual framework treats accountability as a demonstrable relationship between lawful authority, institutional conduct, documented safeguards, and independent review.

Existing scholarship on Indonesian personal-data protection has examined statutory development, data-subject rights, regulatory harmonization, cybersecurity risks, and institutional implementation, but these issues are frequently analyzed as distinct regulatory or organizational concerns. The relationship between the legal basis for public-service processing, the allocation of responsibilities across interconnected systems, preventive compliance obligations, and institutional supervision requires a more integrated doctrinal assessment. In particular, the interaction between Law No. 27 of 2022, the SPBE framework, national digital-service integration policies, constitutional interpretation, and the prospective implementation of Government Regulation No. 33 of 2026 presents a legal problem that cannot be resolved solely through an examination of individual statutory provisions. The relevant research gap concerns how these instruments collectively establish an accountable processing framework and whether their normative requirements provide sufficiently identifiable responsibilities throughout the governmental data-processing lifecycle. This problem also requires separating the legal completeness of the regulatory architecture from claims concerning actual institutional compliance, which cannot be established conclusively through doctrinal analysis alone. A comprehensive normative assessment can nevertheless identify legal relationships, inconsistencies, areas requiring administrative implementation, and the institutional conditions necessary for demonstrating compliance. The distinction provides a more precise basis for evaluating personal-data protection within Indonesia's integrated digital public services.

This study examines the implementation and accountability of personal-data protection in Indonesia's digital public services by addressing three interrelated legal questions: how the PDP Law and digital-government regulations establish lawful grounds and limitations for public-sector data processing; how the rights and obligations of data subjects, controllers, and processors are distributed

across integrated governmental information systems; and how the existing and prospective regulatory arrangements structure institutional responsibility, incident response, and supervisory accountability. The research applies a normative-doctrinal design incorporating statutory, conceptual, and comparative legal approaches, supported by publicly documented incidents used as contextual materials for examining the implications of the applicable legal framework. Statutory interpretation is directed toward the relationship between specific legal provisions, their regulatory purposes, and the allocation of obligations throughout the personal-data processing lifecycle. The analysis distinguishes presently applicable legal requirements from provisions awaiting commencement and separates established legal duties from institutional improvements proposed through normative assessment. Its theoretical contribution consists of an accountability-centered legal framework linking constitutional protection, statutory processing principles, and demonstrable institutional responsibility. Its methodological contribution lies in integrating legislative interpretation, constitutional jurisprudence, institutional regulations, comparative legal materials, and documented public-sector incidents within a common analytical structure. The study evaluates whether Indonesia's developing personal-data protection regime provides a legally coherent basis for processing activities that are authorized, traceable, verifiable, and subject to effective supervisory review.

RESEARCH METHODS

This study employed a non-empirical normative-doctrinal legal research design incorporating statutory, conceptual, and comparative approaches, supported by documentary examination of selected public-sector cybersecurity incidents. The research examined the legal relationship between personal-data protection, governmental authority, and institutional accountability within Indonesia's integrated digital public services. Primary legal materials comprised Articles 28D(1) and 28G(1) of the 1945 Constitution of the Republic of Indonesia, Law No. 27 of 2022 on Personal Data Protection, Presidential Regulation No. 95 of 2018 concerning the Electronic-Based Government System, Presidential Regulation No. 82 of 2023 concerning the Acceleration of Digital Transformation and Integration of National Digital Services, and Presidential Regulation No. 174 of 2024 concerning the Ministry of Communication and Digital. The analysis also incorporated Constitutional Court Decision No. 151/PUU-XXII/2024 and Government Regulation No. 33 of 2026 concerning the implementation of the PDP Law. The temporal scope of the legal assessment was established as July 2026, distinguishing legal provisions already in force from prospective implementing requirements. Government Regulation No. 33 of 2026, promulgated on 16 July 2026 and scheduled to enter into force on 16 January 2027, was examined as a promulgated regulatory instrument whose detailed operational provisions had not yet entered into force at the research cut-off date (Republik Indonesia, 2026a). Secondary legal materials included peer-reviewed publications addressing Indonesian personal-data protection, digital administration, cybersecurity, information governance, institutional responsibility, and regulatory implementation, primarily published between 2022 and 2026 (Syailendra et al., 2024).

Legal materials were obtained through structured identification and purposive selection of legislation, constitutional jurisprudence, official government publications, and relevant academic literature. Primary materials were selected according to their legal authority, direct applicability to governmental personal-data processing, and relevance to the relationship between public-service integration and statutory accountability obligations. Judicial materials were included where constitutional interpretation affected the legal meaning or application of the PDP Law, particularly the appointment requirements for personal-data protection officers under Article 53(1). Academic publications were selected on the basis of substantive relevance, identifiable scholarly provenance, and their contribution to legal interpretation or the conceptual explanation of institutional accountability. Earlier authoritative legal and theoretical materials were retained where necessary to establish the applicable constitutional framework or foundational regulatory principles. European Union data-protection law, particularly Regulation (EU) 2016/679, was examined as a comparative reference concerning lawful public-authority processing, organizational accountability, data-protection impact assessments, data-protection officers, and supervisory independence (European Union, 2016). Comparative materials were used to identify differences in regulatory design and institutional safeguards rather than to assume the direct applicability of European legal obligations to Indonesian public institutions. The selection procedure constituted structured doctrinal source

identification and analysis rather than a systematic literature review or statistical assessment of regulatory implementation.

The legal analysis applied grammatical, systematic, and purposive interpretation to determine the scope and relationship of statutory obligations governing public-sector personal-data processing. Grammatical interpretation was applied to Article 20(2) of Law No. 27 of 2022 to identify the recognized grounds for lawful processing, including the performance of tasks in the public interest, public services, and the exercise of governmental authority established by law. Read independently, this provision recognizes governmental functions as a possible lawful basis for processing personal data, subject to the conditions specified by the statute. Systematic interpretation subsequently examined Article 20(2) in conjunction with Article 16(2), particularly the requirements of limited and specific collection, purpose-related processing, security, and demonstrable accountability. This combined interpretation established that the existence of governmental authority does not independently authorize unrestricted secondary use or interagency disclosure of personal data. Purposive interpretation evaluated these provisions against the constitutional protection established under Article 28G(1) and the regulatory objective of protecting individuals throughout the processing lifecycle. The same interpretative procedure was applied to Article 34 concerning high-risk processing assessments, Article 35 concerning security safeguards, Article 46 concerning notification of personal-data protection failures, and Article 53 concerning the appointment of personal-data protection officers. Constitutional Court Decision No. 151/PUU-XXII/2024 was incorporated to determine the binding interpretation of Article 53(1), particularly the alternative application of the statutory criteria for appointing personal-data protection officers. These interpretative results were assessed alongside the SPBE and national digital-service regulations to distinguish administrative authority to integrate information systems from legal authorization to undertake particular personal-data processing activities.

The analytical framework organized statutory requirements according to the personal-data processing lifecycle, including collection, lawful-basis determination, subsequent use, interagency disclosure, storage, security, impact assessment, processor involvement, incident response, data-subject rights, supervision, and disposal. Each processing stage was examined through three connected questions: which legal provisions established the relevant obligation, which institutional actor was responsible for compliance, and which documentary or procedural mechanisms could demonstrate fulfillment of that obligation. The conceptual approach distinguished legal accountability, organizational accountability, and supervisory accountability to assess whether statutory responsibilities corresponded to identifiable institutions and verifiable administrative procedures. The comparative approach examined selected European data-protection mechanisms as analytical benchmarks for assessing the coherence of Indonesian regulatory arrangements, without treating differences between legal systems as evidence of statutory non-compliance (Taufiq & Kenyo, 2025). Publicly documented incidents, including the June 2024 disruption of the Temporary National Data Center and reported controversies concerning taxpayer and electoral information, were used as contextual documentary illustrations of accountability questions arising within government information systems. These materials were not treated as independent empirical case studies or conclusive evidence of violations of the PDP Law. The analysis distinguished officially documented circumstances from allegations and unresolved public reports, and examined only the legal obligations potentially relevant to the documented facts and applicable regulatory period (Alatas & Djajaputra, 2025). Interpretative consistency was assessed through cross-examination of statutory provisions, judicial decisions, official institutional materials, and relevant scholarly explanations. The resulting findings were organized into four dimensions corresponding to the substantive analysis: normative architecture and lawful processing, data-subject rights and controller obligations, institutional accountability and public-sector incidents, and regulatory gaps associated with the transition toward full implementation of Indonesia's personal-data protection framework.

RESULTS AND DISCUSSION

Normative Architecture and Lawful Processing in Digital Public Services

Indonesia’s legal framework for personal-data protection in digital public services is constructed through the interaction of constitutional principles, statutory provisions, presidential regulations, implementing regulations, and judicial interpretation. The principal statutory foundation

.

is Law No. 27 of 2022 on Personal Data Protection (PDP Law), which establishes personal-data principles, data-subject rights, lawful bases, controller and processor obligations, cross-border transfers, sanctions, and institutional arrangements. Its horizontal character means that public institutions processing personal data remain subject to statutory limitations even when processing is undertaken for the fulfillment of governmental functions. Rahman (2025) emphasizes that public-sector processing requires particular legal scrutiny because the exercise of governmental authority can involve extensive collection and use of citizens' personal information. The constitutional dimension is reinforced by the recognition of privacy and personal dignity within Indonesia's constitutional framework, while the PDP Law translates these general guarantees into more operational statutory duties. Syailendra et al. (2024) identify the enactment of the PDP Law as a major development in Indonesia's personal-data protection regime while also highlighting continuing challenges concerning institutional capacity and implementation. The legal architecture therefore cannot be understood merely as a collection of separate regulations, but as a hierarchical and functionally connected system governing how public authority may process personal data.

The relationship between the PDP Law and the digital-government framework is particularly important because Presidential Regulation No. 95 of 2018 concerning the Electronic-Based Government System (SPBE) and Presidential Regulation No. 82 of 2023 concerning the Acceleration of Digital Transformation and Integration of National Digital Services promote increasingly interconnected government systems. Presidential Regulation No. 95 of 2018 provides the administrative and technological architecture for electronic government, while Presidential Regulation No. 82 of 2023 strengthens integration and interoperability among national digital services. These regulations facilitate data exchange as an administrative instrument, but they do not constitute an autonomous exemption from the requirements of Law No. 27 of 2022. A systematic interpretation consequently requires interoperability to operate within the boundaries of lawful purpose, necessity, proportionality, access control, and security. Rukanova et al. (2023) demonstrate that digital infrastructure can facilitate public-value creation through information sharing, but such value depends on institutional arrangements governing how information is exchanged and used. Abdurrahman et al. (2025) similarly position digital-government transformation as a governance process in which technological integration must be connected with institutional and administrative arrangements.

The interaction between these instruments is further illustrated by the regulatory architecture presented in Table 1, which separates substantive data-protection rules from the regulations governing digital-government organization and institutional authority. This distinction is legally significant because a regulation establishing a governmental system cannot automatically expand the substantive authority to process personal data beyond the limits established by the PDP Law. Presidential Regulation No. 174 of 2024 concerning the Ministry of Communication and Digital is relevant to this institutional configuration because it defines the ministry's governmental mandate during the continuing development of Indonesia's digital-governance structure. Constitutional Court Decision No. 151/PUU-XXII/2024 also demonstrates that the statutory framework remains subject to constitutional interpretation and judicial refinement. Government Regulation No. 33 of 2026 adds another layer by detailing implementation of the PDP Law, including matters concerning DPIA, DPO, data-subject rights, transfers, supervision, and sanctions. Its promulgation on 16 July 2026 must, however, be distinguished from its commencement on 16 January 2027, so that prospective implementing obligations are not treated as already effective legal duties. The resulting framework is therefore characterized by normative continuity between existing rules and prospective implementation rather than by a single regulatory instrument governing every aspect of public-sector processing (Republik Indonesia, 2026a).

Table 1. Regulatory Architecture for Personal Data in Indonesian Digital Public Services

Instrument	Legal function	Relevance to digital public services
Law No. 27/2022 (PDP Law)	General rights, principles, lawful bases, controller/processor duties, transfers, sanctions and	Applies horizontally to personal-data processing, including by public bodies

	institutional framework	
Presidential Regulation No. 95/2018	SPBE governance and electronic government architecture	Provides the administrative framework for digitized government functions and systems
Presidential Regulation No. 82/2023	Acceleration and integration of priority national digital services	Increases interoperability and data-sharing pressure across services
Presidential Regulation No. 174/2024	Institutional mandate of the Ministry of Communication and Digital	Locates policy and supervisory functions relating to digital systems and personal-data protection during transition
Government Regulation No. 33/2026	Detailed implementation of the PDP Law, including DPIA, DPO, rights procedures, transfers, supervision and sanctions	Provides the next operational layer for controllers and processors
Constitutional Court Decision No. 151/PUU-XXII/2024	Constitutional review affecting interpretation of the PDP Law	Shows continuing judicial refinement of statutory duties and institutional design

Lawful processing constitutes the central normative control over the expansion of governmental data practices because the existence of a public function does not itself establish an unlimited legal entitlement to collect or use personal information. Law No. 27 of 2022 requires controllers to identify an appropriate legal basis for processing, with the applicable basis depending on the circumstances and statutory purpose of the processing operation. A grammatical interpretation of the PDP Law requires the legal basis to correspond to the actual processing activity rather than merely to the terminology used in a government privacy notice. A systematic interpretation further requires the lawful basis to be read together with principles concerning purpose limitation, data minimization, accuracy, security, and accountability. Huang and Huang (2023) show that privacy calculus in digital-government environments is influenced by citizens' perceptions of benefits and privacy risks, demonstrating why formal governmental authority does not eliminate the relevance of individual privacy interests. Comparative analysis also indicates that contemporary data-protection regimes distinguish between processing grounded in consent and processing necessary for legal obligations or public authority, as reflected in Article 6(1) of Regulation (EU) 2016/679 (European Union, 2016). The Indonesian framework consequently requires public institutions to connect each processing operation with a legally recognizable basis and a demonstrable governmental purpose rather than treating public-service delivery as a blanket justification for personal-data processing.

Table 2. Lawful-Basis Decision Matrix for Digital Public-Service Processing

Digital Public-Service Processing Situation	Potential Lawful Basis Under The PDP Law	Core Legal Consideration	Accountability Requirement
Processing required to perform a statutory governmental function	Fulfillment of legal obligations or exercise of authority under applicable law	The statutory mandate must specifically support the processing activity	Identify the legal provision, purpose, data categories, and responsible controller
Processing necessary to provide a public service requested by the data subject	Contractual or service-related necessity, where legally applicable	Processing must be objectively necessary for the relevant service	Document necessity and communicate the processing purpose
Processing based on the data subject's consent	Consent	Consent must satisfy statutory requirements and must not be treated	Maintain evidence of consent and provide withdrawal

		as automatic where another legal basis governs	mechanisms where applicable
Processing involving high-risk or sensitive personal data	Applicable statutory basis together with heightened safeguards	Necessity, proportionality, security, and risk must receive additional scrutiny	Conduct appropriate risk assessment and apply enhanced safeguards
Data sharing between public institutions	Applicable legal basis for the original and subsequent processing	Interoperability does not independently establish authorization for secondary use	Document recipient, purpose, authority, access controls, and data-sharing arrangements
Cross-border transfer of personal data	Transfer mechanism recognized under the PDP Law	The controller must satisfy statutory conditions for international transfer	Document destination, legal mechanism, safeguards, and compliance assessment

The lawful-basis requirement becomes particularly important under Presidential Regulation No. 82 of 2023 because integration can transform data that were initially collected for one administrative purpose into information accessible through multiple interconnected services. Such integration must therefore be distinguished from unrestricted secondary processing, since technical interoperability answers the question of whether systems can exchange data whereas data-protection law addresses whether they are legally permitted to do so. Li et al. (2024) demonstrate that privacy risks in government-data environments may emerge from the combination and reuse of datasets even when individual data operations appear administratively legitimate. Gray (2023) likewise emphasizes that public data infrastructures are not neutral technical devices because decisions concerning what data become accessible and how they are presented have governance implications. The same principle applies to SPBE systems, where administrative efficiency cannot displace statutory requirements concerning purpose, necessity, authorization, and accountability. Figueroa et al. (2025) further identify cybersecurity as a multidimensional component of e-government governance, reinforcing the proposition that lawful processing must be accompanied by organizational and technical safeguards. The legal consequence is that every significant data flow within an integrated public-service architecture should be traceable to an identifiable processing purpose, legal basis, authorized recipient, and accountability mechanism.

The temporal position of Government Regulation No. 33 of 2026 introduces an additional issue of legal certainty into the implementation of lawful-processing requirements. Because the regulation was promulgated before its scheduled effective date of 16 January 2027, its provisions should be treated as prospective implementing standards rather than as retroactively enforceable obligations during the period preceding commencement (Republik Indonesia, 2026a). This distinction does not suspend the existing duties established by Law No. 27 of 2022, Presidential Regulation No. 95 of 2018, Presidential Regulation No. 82 of 2023, or other applicable regulations. Instead, it creates a transitional period in which public institutions must distinguish between currently enforceable statutory requirements and more detailed procedures that will become operational under the implementing regulation. Razi et al. (2024) identify implementation challenges as a significant dimension of Indonesia's PDP regime, making the transition between statutory enactment and detailed administrative implementation legally consequential. Gerunov (2022) further demonstrates the importance of embedding privacy considerations into e-government design rather than treating data protection as a remedial measure after systems have been deployed. The combined normative reading therefore establishes that digital public-service integration must remain legally grounded at every stage, while the forthcoming implementation of Government Regulation No. 33 of 2026 strengthens the procedural infrastructure through which those statutory principles can be operationalized.

.

Data-Subject Rights, Security, and Controller Duties

The protection of data-subject rights under Law No. 27 of 2022 represents a substantive limitation on the administrative power to collect and process personal information through digital public services. The PDP Law recognizes rights relating to information, access, correction, deletion, withdrawal of consent, objection to certain processing, and other forms of control over personal data, thereby positioning the individual as a rights-bearing participant rather than merely a source of administrative information. These rights must be interpreted together with the obligations imposed on controllers because the effectiveness of a right depends on whether the responsible institution has procedures capable of receiving, verifying, processing, and documenting individual requests. Roselin and Syailendra (2025) demonstrate that Indonesian data-subject rights can be understood more clearly when compared with the UK framework, particularly regarding access, correction, deletion, and institutional responsibilities. The public-service context creates an additional legal complexity because citizens may have limited practical alternatives when a government service requires personal-data processing. Rahman (2025) therefore emphasizes the importance of ensuring that public-sector data processing remains subject to enforceable safeguards despite the governmental character of the service. The normative position is that administrative necessity cannot eliminate the legal status of individuals as data subjects protected by the PDP Law.

The scope of these rights becomes particularly significant when public institutions operate integrated digital services involving large and interconnected datasets. A citizen may interact with one government service while personal information is technically processed by several systems, agencies, or processors, creating a potential separation between the institution that delivers the service and the institution or entity that technically manages the data. Law No. 27 of 2022 addresses this structural problem through the distinction between the personal-data controller and personal-data processor, assigning different responsibilities according to their respective roles in determining or carrying out processing. This distinction is legally important because accountability should follow actual decision-making authority and processing functions rather than merely the institutional label attached to a digital service. Tan et al. (2025) show that public-service personal-data protection requires attention to institutional responsibilities and governance mechanisms when comparing Indonesian and Malaysian systems. Distel et al. (2022) likewise identify organizational roles, third-party relationships, and governance weaknesses as important sources of risk in e-government environments. The controller–processor relationship must therefore be formalized through clear allocation of responsibilities, documented instructions, access restrictions, and mechanisms for monitoring compliance.

The operational implications of data-subject rights and institutional responsibilities can be organized through the mechanisms presented in Table 3, which connects individual rights under the PDP Law with the administrative procedures required to make those rights practically exercisable. The table also demonstrates that rights protection cannot be reduced to the publication of a privacy policy because each right requires an identifiable institutional process and evidentiary record. A controller receiving an access request, for example, must possess sufficient data-management capabilities to authenticate the requester, locate relevant information, determine applicable limitations, and provide an appropriate response. Similar procedural requirements arise for correction and deletion requests, particularly where data are replicated across interconnected government systems. Spinelli and Terzidou (2022) illustrate the broader institutional importance of assigning responsibility for data protection within public authorities, including contexts in which institutional independence and oversight affect the practical protection of data rights. The Indonesian framework consequently requires public-sector organizations to translate statutory rights into operational procedures rather than treating rights as purely declaratory legal entitlements.

Table 3. Data-Subject Rights and Required Public-Sector Operational Mechanisms

Data-Subject Right	Legal Significance Under The PDP Law	Required Public-Sector Operational Mechanism	Accountability Evidence
Right to Information	Enables the data subject to understand how personal data are	Clear privacy information concerning purpose, legal basis,	Privacy notices, records of information provided,

	processed	categories of data, recipients, and retention	and communication logs
Right of Access	Enables individuals to obtain information concerning their personal data and processing	Authenticated request and retrieval procedure across relevant systems	Request records, identity verification, response records, and disclosure logs
Right to Correction	Supports accuracy of personal data	Procedure for verifying and correcting inaccurate or incomplete information	Correction requests, verification records, and amended-data logs
Right to Deletion	Enables removal of personal data where statutory conditions are satisfied	Assessment procedure identifying whether deletion is legally required or subject to an exception	Deletion requests, legal assessment, deletion records, and system logs
Right to Withdraw Consent	Prevents continued reliance on consent after valid withdrawal	Accessible withdrawal mechanism and reassessment of alternative lawful basis	Consent records, withdrawal records, and subsequent processing assessment
Right to Object or Restrict Certain Processing	Provides protection against processing in circumstances recognized by law	Case-by-case assessment of the objection or restriction request	Request documentation, legal assessment, and decision records
Right to Compensation	Provides a remedial mechanism for losses resulting from unlawful processing	Complaint, investigation, and compensation procedure	Incident records, investigation findings, and remedial documentation

Security constitutes a parallel obligation because the recognition of data-subject rights has limited practical value when personal information remains exposed to unauthorized access, alteration, disclosure, or destruction. Law No. 27 of 2022 places security and confidentiality within the responsibilities of controllers and processors, requiring organizational and technical measures appropriate to the risks associated with processing. For digital public services, these obligations become more demanding because government systems may aggregate identity, financial, health, social, electoral, or other sensitive information within interconnected infrastructures. Figueroa et al. (2025) conceptualize cybersecurity in e-government as a holistic governance problem involving technical, organizational, and procedural dimensions rather than an isolated information-technology function. Gerunov (2022) similarly argues for privacy-by-design approaches in e-government, whereby protection is incorporated into system development rather than introduced only after vulnerabilities become apparent. The legal implication is that security should be assessed across the complete data lifecycle, including collection, storage, transmission, access, modification, disclosure, retention, and disposal. A controller that delegates technical processing to another entity therefore cannot treat outsourcing as a transfer of legal responsibility, because the statutory accountability framework continues to attach duties to the controller's role.

The controller's accountability can be mapped across the processing lifecycle through Table 4, which demonstrates how legal duties extend beyond the initial collection of information. The lifecycle approach is important because a lawful collection decision may still produce unlawful consequences if subsequent access, retention, disclosure, or disposal is inadequately controlled. The controller must therefore establish governance arrangements capable of identifying processing purposes, determining appropriate legal bases, limiting access, supervising processors, conducting risk assessments, responding to incidents, and maintaining records that permit later verification.

Riemann et al. (2023) demonstrate the practical relevance of structured data-protection impact assessments for identifying and documenting privacy risks before processing activities are implemented. Gupta et al. (2025) further identify the interrelationship among trust, risk, privacy, and security in e-government use, indicating that security safeguards operate not only as technical controls but also as conditions affecting citizens' relationships with government services. The accountability framework consequently requires public institutions to demonstrate not merely that safeguards exist, but that those safeguards correspond to identifiable processing risks and can be verified through documentation and institutional oversight.

Table 4. Controller Accountability Across the Public-Service Data Lifecycle

Data-Processing Stage	Core Controller Duty	Principal Legal Issue	Required Accountability Mechanism
Collection	Establish lawful basis, defined purpose, and necessity	Whether collection is legally justified and proportionate to the public-service purpose	Processing records, legal-basis documentation, and privacy information
Storage	Protect confidentiality, integrity, and availability	Whether safeguards correspond to processing risks	Security controls, access policies, and security monitoring
Use and Access	Restrict processing to authorized purposes and personnel	Whether internal use remains compatible with the original purpose	Role-based access, authorization records, and audit logs
Sharing and Disclosure	Verify legal authority and recipient legitimacy	Whether disclosure or interoperability has an appropriate legal basis	Data-sharing agreements, recipient verification, and disclosure logs
Processor Management	Supervise processors and establish binding processing instructions	Whether outsourced processing remains subject to controller oversight	Contracts, instructions, audits, and processor monitoring
Risk Assessment	Identify and mitigate privacy and security risks	Whether processing requires enhanced assessment or DPIA	DPIA or equivalent assessment, mitigation plan, and review records
Incident Response	Detect, assess, document, and respond to personal-data incidents	Whether statutory notification and remedial obligations are triggered	Incident register, investigation records, notifications, and corrective actions
Retention and Disposal	Retain data only as legally and operationally justified and securely dispose of them	Whether continued retention remains necessary and lawful	Retention schedule, deletion controls, and disposal records

The security and accountability framework also becomes relevant to the allocation of responsibility when public institutions rely on external processors or interconnected government infrastructure. A processor may perform hosting, cloud, analytics, authentication, or other technical functions without becoming the institution that determines the purpose and essential means of processing. The controller must consequently retain sufficient supervisory capacity to establish instructions, monitor compliance, identify security weaknesses, and respond to violations involving delegated processing. Distel et al. (2022) identify trust relationships and third-party dependencies as recurring risk dimensions within e-government systems, while Kanaan et al. (2023) connect perceived quality, security, and privacy with trust and intention to use e-government services. The legal

relationship between controller and processor therefore has both compliance and governance consequences because inadequate contractual or technical supervision may obscure responsibility when an incident occurs. Government Regulation No. 33 of 2026 is particularly relevant to this operational layer because its implementing framework is intended to provide greater detail concerning institutional duties, risk management, data protection officers, and supervisory mechanisms once its provisions become effective. Until that commencement date, however, the immediate legal assessment remains anchored in the obligations already established by Law No. 27 of 2022 and other applicable regulations.

The combined interpretation of data-subject rights, security obligations, and controller duties establishes accountability as a continuous legal obligation rather than a single compliance event. Public institutions must be capable of demonstrating why data are collected, how they are processed, who can access them, which processors participate in the operation, what safeguards are applied, and how individuals can exercise their statutory rights. Bowen (2024) emphasizes that government data practices must address citizen privacy concerns because the public character of the information does not remove the individual interests attached to personal data. Gupta et al. (2025) similarly show that privacy and security considerations are structurally connected with trust in e-government, reinforcing the practical importance of enforceable institutional safeguards. The Indonesian framework therefore places the controller at the center of a chain of legal responsibility extending from lawful collection to secure disposal and remedial action. This construction also provides the legal foundation for examining concrete public-sector incidents, because the relevant question is not merely whether a security failure occurred but which statutory duty, institutional responsibility, or governance mechanism was implicated. The next analytical dimension consequently concerns the institutional allocation of accountability and the manner in which public-sector data incidents expose weaknesses or strengths within Indonesia's developing enforcement framework.

Institutional Accountability and Public-Sector Incidents

Institutional accountability is a central component of personal-data protection because the effectiveness of statutory rights depends on whether identifiable public authorities possess sufficient powers, procedures, and resources to enforce them. Law No. 27 of 2022 establishes an institutional framework for supervision and enforcement, while Presidential Regulation No. 174 of 2024 determines the governmental position and functions of the Ministry of Communication and Digital within the broader digital-governance structure. The institutional question is particularly important because personal-data processing in public services is distributed across ministries, agencies, local governments, public enterprises, and technical service providers. Widiatedja and Mishra (2023) argue that the establishment of an independent data-protection authority is important for developing an institutional structure capable of exercising credible supervisory functions. The issue is also connected with the principle of accountability because supervisory independence affects the capacity to examine government institutions whose processing activities may generate risks for citizens. As of July 2026, the Ministry of Communication and Digital stated that the government was finalizing the establishment of an independent Personal Data Protection Authority, with the proposed authority projected to operate independently while reporting to the President through the ministry. The institutional transition therefore remains an important element in assessing how the PDP Law is translated from statutory standards into enforceable public-sector accountability.

The allocation of institutional responsibility can be mapped through Table 5, which distinguishes policy, supervisory, operational, investigative, and judicial functions within the Indonesian data-protection environment. Such differentiation is necessary because regulatory effectiveness depends not only on the existence of legal obligations but also on the capacity of particular institutions to detect non-compliance, require corrective action, and impose or facilitate appropriate remedies. The Ministry of Communication and Digital occupies an important position within the current administrative structure, while sector-specific institutions retain responsibilities arising from their respective statutory mandates. The Constitutional Court also performs a distinct function because its decisions can affect the constitutional interpretation of statutory provisions and institutional arrangements, as illustrated by Decision No. 151/PUU-XXII/2024. Spinelli and Terzidou (2022) demonstrate comparatively that data-protection accountability within public institutions requires careful consideration of oversight structures and institutional independence. The Indonesian

framework therefore requires coordination among administrative, supervisory, sectoral, investigative, and judicial actors rather than reliance on a single institutional mechanism.

Table 5. Institutional Accountability Map for Public-Sector Personal Data

Institution / Actor	Principal Accountability Function	Relevant Legal or Institutional Basis	Accountability Issue
Ministry of Communication and Digital	Digital-policy administration, regulatory coordination, and functions related to personal-data protection during institutional transition	Presidential Regulation No. 174/2024 and applicable PDP framework	Separation and coordination between policy, administrative, and supervisory functions
Proposed independent Personal Data Protection Authority	Independent supervision, enforcement, and protection of data-subject rights	Law No. 27/2022 and forthcoming implementing institutional arrangements	Institutional independence, authority, resources, and enforcement capacity
Public-sector data controller	Determines purposes and means of personal-data processing and ensures compliance	Law No. 27/2022	Lawful basis, purpose limitation, security, rights, records, and incident response
Personal-data processor	Performs processing on behalf of the controller according to authorized instructions	Law No. 27/2022 and contractual arrangements	Compliance with instructions, security, confidentiality, and cooperation
BSSN / cybersecurity authorities	Cybersecurity coordination, technical response, and incident investigation within their mandates	Applicable cybersecurity and electronic-system regulations	Technical attribution, evidence preservation, mitigation, and institutional coordination
Sectoral public institutions	Apply data-protection obligations within specialized statutory functions	Sector-specific legislation and PDP Law	Harmonization between sectoral mandates and general data-protection duties
Police / investigative authorities	Investigation of conduct potentially constituting an offense	Applicable criminal and procedural law	Evidence, attribution, and coordination with affected institutions
Constitutional Court / courts	Judicial interpretation and adjudication within respective jurisdictions	Constitution and applicable procedural statutes	Constitutional review, legal remedies, and interpretation of statutory duties

Public-sector incidents provide concrete material for testing whether this institutional architecture operates effectively, but an incident should not automatically be treated as conclusive proof of a legal violation. The June 2024 ransomware attack on the Temporary National Data Center (PDNS) illustrates this distinction because the official government account identified ransomware as the cause of disruption and reported impacts on several public services, including immigration services. BSSN and the Ministry of Communication and Informatics reported that the investigation involved multiple institutions and that forensic evidence was constrained because some evidence had been encrypted during the attack. From a legal perspective, the relevant questions extend beyond the existence of malicious activity to whether the responsible controller and other actors had implemented appropriate security measures, maintained effective access controls, preserved operational resilience,

and fulfilled applicable incident-response obligations. Figueroa et al. (2025) characterize cybersecurity in e-government as a holistic governance problem, supporting an assessment that technical security cannot be separated from institutional accountability. Distel et al. (2022) likewise identify organizational dependencies and governance arrangements as important dimensions of e-government risk. The PDNS incident therefore functions analytically as an implementation probe for examining how technical failures, institutional responsibilities, evidence preservation, and public-service continuity intersect under the Indonesian legal framework.

The same accountability questions arise in incidents involving databases containing particularly extensive populations of personal information. The KPU publicly reported in November 2023 that it had received information concerning the alleged sale of data purportedly originating from its voter-information system, after which it notified BSSN, the Criminal Investigation Agency of the Indonesian National Police, and other relevant institutions and conducted technical examinations of the affected system. The incident is legally significant because electoral data are processed pursuant to statutory public functions, meaning that the legal basis for processing does not remove the obligation to protect the information against unauthorized access or disclosure. Syifa et al. (2025) specifically examine the legal responsibility of the General Elections Commission in relation to the 2024 election data-leak context and connect the issue with the integration of personal-data protection principles into election administration. KPU's subsequent privacy-management documentation also identifies data-protection purposes, security controls, access management, logging, DPO oversight, and procedures for correcting voter information, illustrating the operational mechanisms expected within a public-sector controller environment. The incident consequently demonstrates why accountability analysis must examine both the legal authority for collecting electoral information and the organizational safeguards governing its subsequent storage and access. It also shows that public transparency and personal-data protection must be reconciled through legally defined limits rather than by assuming that information associated with a public function is automatically open for unrestricted disclosure.

Taxpayer information provides another illustration of the legal tension between data integration and institutional accountability because Indonesia has progressively integrated the Population Identification Number (NIK) with taxpayer administration. The Directorate General of Taxes explains that the NIK–NPWP integration was designed to support administrative efficiency and a standardized identification framework, while also being connected to the implementation of the PDP Law. Alatas and Djajaputra (2025) examine government accountability and mitigation measures in relation to the 2024 taxpayer-identification-number data-breach context, demonstrating how the legal analysis extends from the existence of an integrated database to questions concerning institutional safeguards and remedial measures. The integration of identity and taxation records increases the importance of purpose limitation because the same identifier can facilitate linkage among datasets originally created for different administrative functions. Bowen (2024) emphasizes that government data systems must account for citizen privacy concerns when information is collected and reused for public administration. Li et al. (2024) similarly show that privacy risks can arise from the identification and combination of information across open-government data environments. The legal issue is therefore not whether data integration is inherently impermissible, but whether each subsequent processing operation remains supported by an appropriate legal basis, a defined public purpose, adequate safeguards, and traceable institutional responsibility.

The incidents considered above can be organized through Table 6 by distinguishing the documented event from the legal accountability questions that require separate examination. This distinction prevents the analytical error of equating a cyberattack or alleged data disclosure with automatic proof that a particular institution violated the PDP Law. The appropriate legal inquiry is instead whether the controller and other responsible actors complied with applicable duties before, during, and after the incident, including security, monitoring, documentation, notification, investigation, and remediation requirements. Rukanova et al. (2023) emphasize that public-value creation through government information sharing depends on institutional arrangements that make information exchange accountable and governable. Alsarraf et al. (2023) similarly link e-government service quality with institutional trust, indicating that accountability mechanisms have implications for the relationship between public institutions and service users. The incident-based approach therefore provides evidence for identifying implementation questions without converting individual events into generalized conclusions about the legality of the entire Indonesian digital-government

system. The resulting framework also clarifies why the forthcoming independent supervisory authority and the detailed implementation regime under Government Regulation No. 33 of 2026 are important for strengthening the institutional mechanisms through which such questions can be investigated and resolved.

Table 6. Public-Sector Incident Evidence and Accountability Questions

Public-Sector Incident / Context	Documented Institutional Response or Context	Principal Legal Accountability Questions	Analytical Significance
PDNS ransomware attack, June 2024	BSSN, Kominfo, Polri, and technical entities coordinated investigation and recovery; several public services were disrupted	Whether security measures, access controls, monitoring, incident response, and continuity arrangements were adequate	Tests cybersecurity and controller accountability within shared government infrastructure
KPU voter-data incident, November 2023	KPU reported alleged sale of voter data, notified BSSN and Polri, disabled relevant accounts, and conducted technical analysis	Whether access controls, monitoring, data security, disclosure controls, and incident response complied with applicable obligations	Tests accountability for large-scale electoral personal-data processing
Taxpayer identification-data breach context, 2024	Government administration increasingly integrated NIK and NPWP systems while accountability and mitigation issues arose around taxpayer data	Whether data integration, access, security, purpose limitation, and remedial mechanisms were adequately governed	Tests accountability where a single identifier facilitates cross-system data linkage
Integrated public-service databases	Multiple public institutions exchange or interconnect personal-data systems under digital-government architecture	Whether each transfer or secondary use has a legal basis, defined purpose, authorized recipient, and adequate safeguards	Tests the relationship between interoperability and personal-data protection
Institutional transition toward an independent data-protection authority	Government reported in July 2026 that an independent authority was being prepared	Whether the future institution will possess sufficient independence, authority, resources, and enforcement mechanisms	Tests the structural capacity of the PDP framework to provide independent oversight

Institutional accountability ultimately depends on whether legal responsibility can be traced from the processing activity to an identifiable decision-maker and then connected to enforceable duties. Public-sector data incidents demonstrate that this traceability may become difficult when data infrastructure involves multiple controllers, processors, ministries, cybersecurity institutions, and external technology providers. Jansen et al. (2023) show that governmental digital sovereignty involves institutional control over digital infrastructures and dependencies, a concern that becomes directly relevant when public services depend on shared or externally supported systems. The accountability model under Law No. 27 of 2022 therefore needs to operate alongside cybersecurity governance, sector-specific legislation, and administrative controls rather than being isolated within a single privacy instrument. Widiatedja and Mishra (2023) identify institutional independence as an important consideration in establishing Indonesia's future data-protection authority, while the government's July 2026 announcement confirms that institutional development remained underway at that point. The incidents examined in this section consequently reveal a recurring legal requirement: public institutions must be able to demonstrate not only that digital services are legally authorized, but

also that personal-data risks are actively governed, incidents are investigated through identifiable procedures, and affected rights are connected to meaningful accountability mechanisms. This institutional dimension provides the basis for assessing the remaining regulatory gaps and the transition toward fuller implementation under Government Regulation No. 33 of 2026.

Regulatory Gaps and the Path to Full Implementation

Indonesia's personal-data protection framework has developed substantially through Law No. 27 of 2022, yet the existence of a comprehensive statute does not automatically establish complete institutional and operational protection. The PDP Law provides the principal legal basis for personal-data rights, processing principles, controller and processor obligations, sanctions, and institutional arrangements, while Presidential Regulation No. 95 of 2018 and Presidential Regulation No. 82 of 2023 establish the digital-government architecture within which many public-sector processing activities occur. Government Regulation No. 33 of 2026 subsequently provides more detailed implementation rules concerning data protection impact assessments (DPIA), data protection officers (DPO), data-subject rights, international transfers, supervision, and sanctions (Republik Indonesia, 2026a). Its promulgation on 16 July 2026 and scheduled effectiveness on 16 January 2027 create a legally significant transition between the existing statutory framework and its more detailed operational regime. Razi et al. (2024) identify implementation challenges as a continuing issue following enactment of the PDP Law, particularly where statutory requirements must be translated into institutional procedures and technical safeguards. The central regulatory issue is therefore not simply whether Indonesia possesses legal rules for personal-data protection, but whether those rules are supported by institutional authority, procedural clarity, technical capacity, and mechanisms capable of demonstrating compliance. This distinction between normative completeness and implementation capacity is essential for evaluating the remaining gaps in Indonesia's digital public-service governance.

The first major institutional gap concerns the establishment and operationalization of an independent supervisory authority responsible for personal-data protection. Law No. 27 of 2022 provides the statutory basis for such an institutional function, while Presidential Regulation No. 174 of 2024 situates digital governance and related governmental functions within the Ministry of Communication and Digital. As of July 2026, the Ministry of Communication and Digital reported that the government was preparing an independent Personal Data Protection Authority and the regulatory framework necessary for its establishment. Widiatedja and Mishra (2023) argue that an independent data-protection authority is important for ensuring credible supervision because institutional independence affects the ability to oversee both private and public-sector data controllers. The issue extends beyond formal institutional creation because the authority requires clearly defined powers, adequate resources, investigative capacity, sanctioning authority, and mechanisms for protecting data-subject interests. Spinelli and Terzidou (2022) similarly demonstrate through the European context that data-protection supervision within public institutions requires institutional arrangements capable of maintaining effective oversight. The Indonesian transition therefore requires attention to the substantive independence and practical capacity of the supervisory institution rather than treating institutional formation as sufficient evidence of completed implementation.

A second regulatory gap concerns the operationalization of accountability obligations inside public institutions that function as personal-data controllers. Law No. 27 of 2022 establishes general duties, but Government Regulation No. 33 of 2026 provides a more detailed framework for mechanisms such as DPIA and DPO functions that can translate statutory principles into repeatable administrative procedures (Republik Indonesia, 2026a). Gerunov (2022) demonstrates the relevance of privacy-by-design for e-government because protection is more effective when privacy requirements are incorporated into system development, data architecture, and organizational procedures from the beginning. Riemann et al. (2023) similarly show that structured DPIA methodologies can support systematic identification and mitigation of privacy risks before high-risk processing is implemented. This requirement is particularly relevant to public services governed by Presidential Regulation No. 82 of 2023 because integration and interoperability can increase the number of systems and institutions involved in a single data flow. Figueroa et al. (2025) further emphasize that cybersecurity in e-government requires an integrated framework combining technical, organizational, and governance dimensions rather than relying on isolated technical controls. The

implementation gap consequently lies in converting broad legal obligations into auditable institutional practices covering data mapping, risk assessment, access control, processor supervision, incident response, retention, and secure disposal.

Table 7. Comparative Accountability Features: Indonesia and the European GDPR Model

Accountability Feature	Indonesian Framework	European GDPR Model	Principal Implementation Implication For Indonesia
General accountability principle	Accountability obligations established through Law No. 27/2022 and implementing regulations	Article 5(2) expressly establishes responsibility and the ability to demonstrate compliance	Public controllers need documented evidence demonstrating compliance
Lawful basis	Law No. 27/2022 provides statutory lawful bases for processing	Article 6 provides an enumerated set of lawful bases	Each public-sector processing activity should be mapped to a specific legal basis
Data-subject rights	Rights established under Law No. 27/2022 and detailed through implementing rules	Articles 12–22 provide extensive procedural rights	Public institutions require accessible and auditable rights-request procedures
Data Protection Officer / privacy function	DPO-related requirements developed through the PDP Law and Government Regulation No. 33/2026	Articles 37–39 establish DPO requirements and functions	Institutions need defined privacy responsibilities, expertise, and reporting lines
Data Protection Impact Assessment	Detailed implementation provided through Government Regulation No. 33/2026	Article 35 establishes DPIA for high-risk processing	High-risk public-sector processing requires systematic risk identification and mitigation
Security of processing	Security obligations established under the PDP Law and implementing framework	Article 32 requires appropriate technical and organizational measures	Security controls must correspond to processing risks and be periodically evaluated
Breach / incident accountability	PDP Law and implementing rules establish incident-related duties	Articles 33–34 establish breach notification and controller responsibilities	Institutions require documented detection, assessment, notification, and remediation procedures
Independent supervision	Independent authority being developed under the Indonesian framework	Independent supervisory authorities required under Articles 51–59	Indonesia requires operational independence, sufficient authority, and institutional capacity
International transfers	Transfer requirements established by the PDP Law and further detailed by implementing regulations	Chapter V establishes adequacy and safeguard mechanisms	Transfer procedures should provide predictable safeguards without unnecessarily obstructing legitimate data flows

.

The cross-border dimension constitutes another area requiring regulatory clarification because digital public services increasingly depend on cloud infrastructure, international technology providers, and transnational information exchange. Law No. 27 of 2022 establishes requirements for international transfers, while Government Regulation No. 33 of 2026 provides additional implementing provisions that become relevant upon its effective date. Rahman and Mulyani (2025) identify the challenge of minimizing unnecessary restrictions on cross-border data flows while maintaining adequate personal-data protection under Indonesia's post-PDP Law framework. Safitri and Mahfud (2023) similarly examine Indonesia's relationship with the ASEAN cross-border personal-data-transfer instrument and highlight the importance of compatibility between domestic rules and regional data-governance arrangements. Regulation (EU) 2016/679 provides a comparative model through Chapter V, which links international data transfers with safeguards intended to maintain an appropriate level of protection. Regulation (EU) 2016/679 (GDPR) Taufiq and Kenyo (2025) identify the GDPR as a useful comparative reference for evaluating Indonesian personal-data protection, although its provisions cannot be treated as directly applicable Indonesian law. The Indonesian implementation challenge is therefore to develop predictable transfer procedures that reconcile data-subject protection, administrative necessity, technological dependence, and legitimate international data exchange.

The principal regulatory gaps and corresponding implementation priorities can be synthesized in Table 8, which connects existing legal foundations with institutional and operational measures required during the 2026–2027 transition. The table emphasizes that implementation requires simultaneous development of supervision, internal compliance, risk assessment, rights procedures, processor governance, incident response, and cross-border transfer mechanisms rather than sequential reform of isolated components. Gupta et al. (2025) demonstrate that privacy, security, perceived risk, and trust are interconnected dimensions of e-government use, making institutional accountability relevant to both legal compliance and public confidence in digital services. Jansen et al. (2023) further demonstrate that governmental digital sovereignty depends partly on institutional control over digital infrastructures and dependencies, which is particularly significant when public services rely on shared platforms or external technology providers. Rukanova et al. (2023) similarly show that public value generated through information sharing depends on institutional arrangements that make data exchange governable and accountable. The implementation of Government Regulation No. 33 of 2026 should consequently be accompanied by standardized compliance documentation, interoperable audit mechanisms, clear allocation of controller and processor responsibilities, and institutional procedures for monitoring high-risk processing. Full implementation should be assessed through demonstrable legal and organizational capabilities rather than merely through the formal existence of statutes, regulations, or institutional mandates.

Table 8. Priority Implementation Gaps and Reform Actions for 2026–2027

Regulatory / institutional gap	Existing legal foundation	Priority implementation action	Expected accountability outcome
Independent supervisory authority not yet fully operational	Law No. 27/2022; Presidential Regulation No. 174/2024; institutional preparation in 2026	Finalize institutional regulation, authority, organizational structure, resources, and reporting mechanisms	Independent and credible supervision
General statutory principles require detailed operational procedures	Law No. 27/2022; Government Regulation No. 33/2026	Develop standardized compliance procedures, templates, and sector-specific guidance	Consistent application of statutory obligations
DPIA implementation	Law No. 27/2022; Government Regulation	Establish risk-screening criteria,	Earlier identification and mitigation of high-risk

.

requires institutionalization	No. 33/2026	DPIA methodology, review procedures, and documentation requirements	processing
DPO / privacy functions require organizational integration	Law No. 27/2022; Government Regulation No. 33/2026	Designate qualified personnel, define independence and reporting lines, and establish monitoring functions	Clear internal responsibility for data protection
Data-subject rights require interoperable administrative procedures	Law No. 27/2022; Government Regulation No. 33/2026	Establish authentication, request handling, response, escalation, and audit procedures	Rights become practically exercisable and traceable
Processor and third-party governance remains complex	Law No. 27/2022 and applicable electronic-system regulations	Standardize processing agreements, instructions, security requirements, audits, and termination controls	Greater traceability of delegated processing
Public-sector incident response requires stronger coordination	PDP Law; cybersecurity regulations; sectoral rules	Integrate detection, evidence preservation, notification, investigation, recovery, and remediation	Faster and more accountable incident management
Cross-border transfer mechanisms require predictable implementation	Law No. 27/2022; Government Regulation No. 33/2026	Establish assessment criteria, safeguards, documentation, and transfer monitoring	Balance data protection with legitimate international data flows
Interoperability creates continuing purpose-limitation risks	Presidential Regulation No. 82/2023; PDP Law	Map data flows, purposes, recipients, access rights, and secondary uses across integrated systems	Lawful and auditable data sharing

The transition toward full implementation also requires harmonization between personal-data protection and the architecture of integrated digital public services. Presidential Regulation No. 95 of 2018 and Presidential Regulation No. 82 of 2023 promote interoperable government systems, while Law No. 27 of 2022 requires personal-data processing to remain lawful, proportionate, secure, and accountable. A fragmented compliance model in which individual agencies develop incompatible standards could weaken both data protection and the interoperability objectives of SPBE. Li et al. (2024) demonstrate that privacy risks may emerge when government datasets are combined or reused across institutional contexts, making data mapping and purpose limitation important safeguards within integrated infrastructures. Gray (2023) similarly shows that government data infrastructures involve governance choices concerning accessibility, disclosure, and the public presentation of information. The implementation of Government Regulation No. 33 of 2026 should therefore support standardized procedures that can operate across interconnected public institutions while preserving institution-specific legal responsibilities. Zhao et al. (2022) reinforce this governance perspective by showing that government-data performance depends on institutional arrangements surrounding data production, access, and use. The resulting regulatory pathway requires digital integration to be accompanied by interoperable accountability mechanisms so that efficiency does not become detached from the legal protection of data subjects.

.

The legal trajectory from Law No. 27 of 2022 toward the full implementation of Government Regulation No. 33 of 2026 consequently reflects a transition from foundational regulation toward institutionalized accountability. The remaining gaps concern the operational independence of supervision, internal compliance structures, DPIA and DPO implementation, data-subject rights procedures, processor governance, cybersecurity coordination, and cross-border transfer mechanisms. Yusliwidaka et al. (2024) emphasize that Indonesia's responsibility for personal-data protection must be understood through domestic and international legal dimensions, particularly as digital information increasingly moves across institutional and territorial boundaries. Tan et al. (2025) likewise demonstrate the importance of institutional and regulatory arrangements for protecting personal data within public-service delivery. The GDPR comparison indicates that mature data-protection systems generally connect lawful processing, individual rights, organizational accountability, risk assessment, security, supervisory independence, and transfer safeguards as interdependent components rather than isolated requirements. Government Regulation No. 33 of 2026 provides Indonesia with a more detailed legal foundation for this transition, but its effectiveness will depend on how public institutions and supervisory bodies operationalize those requirements after its commencement on 16 January 2027 (Republik Indonesia, 2026a). The resulting legal framework can therefore be assessed through the extent to which statutory rights and obligations become measurable, documented, enforceable, and consistently integrated into the governance of digital public services.

CONCLUSION

The normative analysis establishes that Indonesia possesses a substantial legal foundation for protecting personal data within integrated digital public services, but the coherence of institutional accountability cannot be inferred solely from the existence of statutory obligations. Law No. 27 of 2022 provides lawful grounds and substantive limitations for governmental processing, while the SPBE and national digital-service regulations establish the administrative architecture for interagency information integration. The legal authorization for public-service processing does not independently permit unrestricted data collection, secondary use, or interagency disclosure, since processing remains subject to the principles and obligations established by the PDP Law. Data-subject rights are supported by corresponding controller and processor responsibilities concerning security, risk assessment, incident notification, and organizational accountability. Nevertheless, the legal allocation of these obligations does not establish that compliance procedures have been implemented consistently across public institutions. Documentary examination of public-sector incidents identifies relevant questions concerning preventive safeguards, institutional responsibility, and corrective procedures without establishing violations in the absence of competent findings. Government Regulation No. 33 of 2026 introduces additional operational provisions but remains prospective until its scheduled commencement on 16 January 2027. The principal normative finding is that Indonesia's legal challenge concerns the operationalization of mechanisms capable of making governmental personal-data processing demonstrable, traceable, and independently reviewable, rather than the absence of a general statutory framework.

The findings support an accountability framework in which each public digital service maintains identifiable legal grounds, documented processing purposes, clearly allocated controller and processor responsibilities, and verifiable records of data sharing and security measures. The proposed institutional measures include service-level processing inventories, standardized controller-processor arrangements, risk-based impact assessments, interoperable audit records, and integrated procedures for incident documentation, notification, investigation, and corrective action. These measures represent operational recommendations derived from the statutory obligations and comparative accountability analysis, rather than evidence of practices already implemented throughout the public sector. The transition preceding the commencement of Government Regulation No. 33 of 2026 provides a regulatory opportunity to align administrative procedures with the existing PDP Law and the forthcoming implementing requirements. Effective supervisory arrangements are also necessary to connect institutional compliance with independent review and enforceable administrative responsibility. An accountable digital-government framework ultimately requires a continuous and auditable chain of legal and institutional responsibility extending from the initial authorization of personal-data processing to its subsequent use, supervision, and lawful termination.

.

REFERENCES

Chick, R. C., Clifton, G. T., Peace, K. M., Propper, B. W., Hale, D. F., Alseidi, A. A., & Vreeland, T. J. (2020). Using technology to maintain the education of residents during the COVID-19 pandemic. *Journal of surgical education*, *77*(4), 729-732. https://doi.org/10.1016/j.jsurg.2020.03.01

Abdurrahman, M., Suherman, D., Bhimasena, A., & Carlos, F. M. (2025). Indonesia's digital transformation: How e-government is revolutionizing public services. *Indonesia Discourse, 2*(1), 107–134. https://doi.org/10.15294/indi.v2i1.23037

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). https://doi.org/10.46924/jihk.v7i2.385

Alsarraf, H. A., Aljazzaf, S., & Ashkanani, A. M. (2023). Do you see my effort? An investigation of the relationship between e-government service quality and trust in government. *Transforming Government: People, Process and Policy, 17*(1), 116–133. https://doi.org/10.1108/TG-05-2022-0066

Bowen, C. M. (2024). Government data of the people, by the people, for the people: Navigating citizen privacy concerns. *Journal of Economic Perspectives, 38*(2), 181–200. https://doi.org/10.1257/jep.38.2.181

Distel, B., Koelmann, H., Plattfaut, R., & Becker, J. (2022). Watch who you trust! A structured literature review to build a typology of e-government risks. *Information Systems and e-Business Management, 20*, 789–818. https://doi.org/10.1007/s10257-022-00573-4

Eom, S.-J., & Lee, J. (2022). Digital government transformation in turbulent times: Responses, challenges, and future direction. *Government Information Quarterly, 39*(2), 101690. https://doi.org/10.1016/j.giq.2022.101690

European Union. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation).* https://eur-lex.europa.eu/eli/reg/2016/679/oj

Figueroa, V., Sánchez Crespo, L. E., Santos-Olmo, A., Rosado, D. G., & Fernández-Medina, E. (2025). Building a holistic cybersecurity framework for e-government based on a systematic analysis of proposals. *International Journal of Information Security, 24*, 121. https://doi.org/10.1007/s10207-025-01024-0

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

General Elections Commission of the Republic of Indonesia. (2023). *National final voter list for the 2024 election: 204,807,222 voters.* https://www.kpu.go.id/

Gray, J. W. Y. (2023). What do data portals do? Tracing the politics of online devices for making data public. *Data & Policy, 5*, e10. https://doi.org/10.1017/dap.2023.7

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*, 1089–1105. https://doi.org/10.1007/s10796-024-10497-8

Huang, Z.-X., & Huang, T.-Y. (2023). Privacy calculus theory in the digital government context: The case of Taiwan's new eID policy. *Social Science Computer Review, 41*(5), 1745–1766. https://doi.org/10.1177/08944393221117500

Jansen, B., Kadenko, N., Broeders, D., van Eeten, M., Borgolte, K., & Fiebig, T. (2023). Pushing boundaries: An empirical view on the digital sovereignty of six governments in the midst of geopolitical tensions. *Government Information Quarterly, 40*(4), 101862. https://doi.org/10.1016/j.giq.2023.101862

Kanaan, A., Al-Hawamleh, A., Abulfaraj, A., Al-Kaseasbeh, H. M., & Alorfi, A. (2023). The effect of quality, security and privacy factors on trust and intention to use e-government services. *International Journal of Data and Network Science, 7*(1), 185–198. https://doi.org/10.5267/j.ijdns.2022.11.004

Kementerian Komunikasi dan Digital Republik Indonesia. (2026, 22 Juli). *Indonesia menyiapkan otoritas perlindungan data pribadi yang independen*.

Kementerian Komunikasi dan Informatika Republik Indonesia. (2024, 24 Juni). *BSSN identifikasi serangan ransomware pada Pusat Data Nasional Sementara*.

.

Lestari, Y., & Mujib, M. M. (2022). Optimizing personal data protection legal framework in Indonesia: A comparative law study. *Supremasi Hukum, 11*(2). https://doi.org/10.14421/sh.v11i2.2729

Li, Y., & Shang, H. (2023). How does e-government use affect citizens' trust in government? Empirical evidence from China. *Information & Management, 60*(7), 103844. https://doi.org/10.1016/j.im.2023.103844

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

Mahkamah Konstitusi Republik Indonesia. (2025). *Putusan Nomor 151/PUU-XXII/2024*.

Pham, L., Limbu, Y. B., Le, M. T. T., & Nguyen, N. L. (2023). E-government service quality, perceived value, satisfaction, and loyalty: Evidence from a newly emerging country. *Journal of Public Policy, 43*(4), 812–833. https://doi.org/10.1017/S0143814X23000296

Rahman, F. (2025). Safeguarding personal data in the public sector: Unveiling the impact of the new Personal Data Protection Act in Indonesia. *UUM Journal of Legal Studies, 16*(1), 1–18. https://doi.org/10.32890/uumjls2025.16.1.1

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

Razi, F., Tuasikal, H., & Markus, D. P. (2024). Implementation and challenges of the Personal Data Protection Law in Indonesia. *Jurnal Indonesia Sosial Teknologi, 5*(12), 6559–6565. https://doi.org/10.59141/jist.v5i12.1285

Republik Indonesia. (2018). *Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.*

Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.*

Republik Indonesia. (2023). *Peraturan Presiden Nomor 82 Tahun 2023 tentang Percepatan Transformasi Digital dan Keterpaduan Layanan Digital Nasional.*

Republik Indonesia. (2024). *Peraturan Presiden Nomor 174 Tahun 2024 tentang Kementerian Komunikasi dan Digital.*

Republik Indonesia. (2026a). *Peraturan Pemerintah Nomor 33 Tahun 2026 tentang Pelaksanaan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.*

Riemann, L. T., Hähner, F. P. S., Schmitz, A.-K., Ataian, M., Jaster, M., & Ückert, F. (2023). An open-source software tool to facilitate data protection impact assessments. *Applied Sciences, 13*(20), 11230. https://doi.org/10.3390/app132011230

Roselin, S., & Syailendra, M. R. (2025). Personal data subject rights protection: A comparative study between Indonesian PDP Law and the UK Data Protection Act. *Jurnal USM Law Review, 8*(2), 825–835. https://doi.org/10.26623/julr.v8i2.12076

Rukanova, B., van Engelenburg, S., Ubacht, J., Tan, Y.-H., Geurts, M., Sies, M., Molenhuis, M., Slegt, M., & van Dijk, D. (2023). Public value creation through voluntary business-to-government information sharing enabled by digital infrastructure innovations: A framework for analysis. *Government Information Quarterly, 40*(2), 101786. https://doi.org/10.1016/j.giq.2022.101786

Safitri, M. Y., & Mahfud, M. (2023). The ASEAN cross-border personal data transfer instrument: Has Indonesia's Personal Data Protection Law followed it? *Jurnal Magister Hukum Udayana, 12*(3). https://doi.org/10.24843/JMHU.2023.v12.i03.p06

Spinelli, M., & Terzidou, K. (2022). Quis custodiet ipsos custodes? Data protection in the judiciary in EU and EEA Member States. *International Data Privacy Law, 12*(2), 93–112. https://doi.org/10.1093/idpl/ipac002

Syailendra, M. R., Lie, G., & Sudiro, A. (2024). Personal data protection law in Indonesia: Challenges and opportunities. *Indonesia Law Review, 14*(2), Article 4. https://doi.org/10.15742/ilrev.v14n2.4

Syifa, S. N., Abdillah, M. T., & Fadil, S. J. (2025). The legal responsibility of the General Elections Commission in the 2024 election data leak: Integration of personal data protection laws and the

.

principle of Sadd al-Dharī‘at. *Justicia Islamica, 22*(1). https://doi.org/10.21154/justicia.v22i1.10390

Tan, W., Karo Karo, R. P. P., Situmeang, A., Rusdiana, S., & Abd Razak, S. S. (2025). Protection of public services personal data in the delivery of public services: Comparative study in Indonesia and Malaysia. *SASI, 31*(1), 33–43. https://doi.org/10.47268/sasi.v31i1.2415

Taufiq, M., & Kenyo, A. S. (2025). The legal protection of personal data in the digital era: A comparative study of Indonesian law and the GDPR. *International Journal of Business, Law, and Education, 6*(2). https://doi.org/10.56442/ijble.v6i2.1178

Virnandes, S. R., Shen, J., & Vlahu-Gjorgievska, E. (2024). Building public trust through digital government transformation: A qualitative study of Indonesian civil service agency. *Procedia Computer Science, 234*, 1183–1191. https://doi.org/10.1016/j.procs.2024.03.114

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

Yusliwidaka, A., Abqa, M. A. R., & Wardana, K. A. (2024). A discourse of personal data protection: How Indonesia responsible under domestic and international law? *Pandecta Research Law Journal, 19*(2), 453–482. https://doi.org/10.15294/pandecta.v19i2.13279

Zhao, Y., Liang, Y., Yao, C., & Han, X. (2022). Key factors and generation mechanisms of open government data performance: A mixed methods study in the case of China. *Government Information Quarterly, 39*(4), 101717. https://doi.org/10.1016/j.giq.2022.101717