Nagri Pustaka: Jurnal Pendidikan, Ilmu Sejarah, dan Budaya
E-ISSN: 3032-0151 | Vol. 4 No. 4, 2026 | Pages 341-362
https://journal.yazri.com/index.php/nagripustaka

Institutional Governance of Personal Data Protection in Public Information Services: An Integrative Literature Review

Hironimus Banuel[1]✉, Zulkarnaen[2], Erdi[3], Martoyo[4]; Arifin[5], Aripin Manurung[6]

(1,2,3,4,5) Universitas Tanjungpura, Kota Pontianak, Indonesia
(1) Sekretariat DPRD Kabupaten Sanggau, Indonesia
(6) Politeknik Negeri Pontianak, Kota Pontianak, Indonesia

Received: 21-08-2026 | Revised: 11-10-202x | Accepted: 20-10-2026

Corresponding Author:
Erdi,
Universitas Tanjungpura, Jl. Profesor Dokter H. Hadari Nawawi, Bansir Laut, Kec. Pontianak Tenggara, Kota Pontianak, Kalimantan Barat 78115, Indonesia
Email: erdi@fisip.untan.ac.id

ABSTRACT

Integrating personal data protection into public information services creates a governance challenge: public organizations must ensure access to information while safeguarding personal data in administrative documents. This study examines how the literature explains this challenge and develops a framework for disclosure decisions. It uses an integrative literature review involving a structured search, appraisal, thematic synthesis, and conceptual integration. The analysis covers five domains: institutional roles and regulations, institutional capacity, governance mechanisms, service outcomes, and institutional risks. The findings indicate that effective implementation requires consistent regulatory interpretation, competent personnel, procedures, information infrastructure, and interorganizational coordination. Information classification, consequence assessment, proportionate disclosure, redaction, access control, and decision documentation translate institutional capacity into accountable practices. The study proposes a framework linking regulatory mandates, institutional capacity, administrative mechanisms, accountable decisions, and public information service outcomes. It contributes to public governance scholarship by framing personal data protection and public information disclosure as an integrated institutional decision-making process, rather than merely regulatory compliance or technological security.

Integrasi pelindungan data pribadi dalam layanan informasi publik menghadirkan tantangan tata kelola kelembagaan. Badan publik harus menjamin akses terhadap informasi sekaligus menjaga data pribadi yang tercantum dalam dokumen administratif. Penelitian ini mengkaji bagaimana literatur menjelaskan tantangan tersebut serta merumuskan kerangka integratif untuk pengambilan keputusan keterbukaan informasi. Penelitian menggunakan metode tinjauan literatur integratif melalui penelusuran terstruktur, penelaahan kritis, sintesis tematik, dan integrasi konseptual. Analisis mencakup lima ranah, yaitu peran dan regulasi kelembagaan, kapasitas kelembagaan, mekanisme tata kelola, hasil layanan informasi publik, dan risiko kelembagaan. Hasil kajian menunjukkan bahwa implementasi yang efektif memerlukan keselarasan interpretasi regulasi, kompetensi sumber daya manusia, prosedur administratif, infrastruktur informasi, serta koordinasi antarorganisasi. Klasifikasi informasi, penilaian konsekuensi, keterbukaan proporsional, penyamaran data, pengendalian akses, dan dokumentasi keputusan mendukung praktik keterbukaan yang akuntabel. Kajian ini mengusulkan kerangka yang menghubungkan mandat regulasi, kapasitas kelembagaan, mekanisme administratif, pengambilan keputusan akuntabel, dan hasil layanan informasi publik. Kerangka tersebut menempatkan pelindungan data pribadi dan keterbukaan informasi sebagai proses pengambilan keputusan kelembagaan publik yang terintegrasi.

Keywords: personal data protection, public information services, institutional governance, information disclosure

© 2026 The Author(s). Published by Yazri Aksara Nusantara, ID

This is an Open Access article distributed under the terms of the Creative Commons Attribution 4.0 International License (https://creativecommons.org/licenses/by/4.0/).

Introduction

Public institutions increasingly face the challenge of managing public information while protecting personal data contained in administrative records (Sexton et al., 2017). The expansion of digital government, electronic document management, and online information services has increased the availability and circulation of government-held information (Aribianto et al., 2026; Nabawi et al., 2026; Soulthoni & Itasari, 2025; Yani & Susanto, 2026). These developments create opportunities for transparency, public participation, and administrative accountability. At the same time, they increase institutional responsibilities to ensure that personal data are processed and disclosed in accordance with applicable legal requirements (Arifin et al., 2026; Isbandono et al., 2025; Kaplale & Maulana, 2026; Octavianus & Kurniawan, 2026). Public institutions must therefore manage two governance objectives simultaneously: facilitating access to information that supports public accountability and protecting personal data from inappropriate disclosure.

The relationship between transparency and privacy is not necessarily complementary in every administrative situation (Lestari, 2025). Transparency requires public institutions to provide information concerning their activities, decisions, and use of public resources. Personal data protection, by contrast, limits the processing and disclosure of information relating to identifiable individuals (Nugroho, 2025). These principles may intersect when requested documents contain both information relevant to public oversight and personal data that require protection (Briantama & Yopan, 2026; Marwenny et al., 2024; Tan et al., 2025). Consequently, public institutions cannot rely exclusively on a general presumption of openness or confidentiality. They need administrative procedures that assess the legal status, relevance, sensitivity, and potential consequences of disclosing specific information (Sitepu et al., 2025).

Adeoye & Ran(2024), through a systematic review of 470 articles on government transparency, identify privacy as one of the dilemmas affecting transparency outcomes. Their analysis demonstrates that transparency involves competing institutional and normative considerations that cannot be resolved merely by increasing the volume of information published. Desrochers (2024) similarly discusses the relationship between access to information and privacy in public service reform, emphasising the need for practical approaches that maintain transparency while safeguarding personal information. These studies indicate that public information governance requires institutional arrangements that reconcile access rights and privacy protection within administrative processes.

The challenge is particularly relevant in Indonesia following the enactment of Law No. 27 of 2022 concerning Personal Data Protection (PDP Law). The law establishes obligations for personal data controllers and processors, including public-sector institutions, and recognises disclosure and dissemination as activities within the scope of personal data processing. These obligations operate alongside Law No. 14 of 2008 concerning Public Information Disclosure (KIP Law), which establishes public access to information as a fundamental principle while providing legally defined grounds for restricting access. The two laws therefore create an institutional responsibility to assess public information requests through both disclosure and personal data protection considerations.

The implementation of these regulatory obligations is not determined solely by the existence of legal provisions. Public institutions must interpret the relationship between applicable regulations, assign responsibilities across organisational units, identify personal data in requested documents, assess disclosure consequences, and determine whether to release information in full or in part. Rahman (2025) identifies regulatory fragmentation and the

potential overinterpretation of personal data protection exemptions as challenges to implementing Indonesia's PDP Law in the public sector. These challenges suggest that regulatory compliance requires operational guidance and institutional coordination.

Organisational capacity also influences the implementation of these responsibilities. Pribadi et al. (2024), examining digital government implementation in four Indonesian local governments, identify employee skills, leadership, regulation, infrastructure, information and communication technology, transparency, and accountability as factors associated with digital government service implementation. Masrich et al. (2026), in their study of personal data protection implementation in Majalengka Regency, identify challenges concerning regulatory understanding, human resources, and information technology readiness. These findings indicate that institutional implementation of personal data protection requires aligning organisational competence, administrative arrangements, and technological resources.

Despite these contributions, the relationship between personal data protection and public information disclosure still requires an integrated institutional perspective. Transparency research often emphasises public access, accountability, and bureaucratic behaviour, while personal data protection studies often focus on legal compliance, privacy rights, and information security. These perspectives provide important insights but do not always explain how public institutions organise the administrative decisions required when a requested document contains both public information and personal data. In particular, the institutional relationship between regulatory mandates, organisational capacity, disclosure procedures, coordination, and accountable decisions requires further conceptual integration (Bangsu et al., 2026).

This study addresses that issue through an integrative literature review. Rather than treating personal data protection and public information disclosure as separate regulatory concerns, the study examines how public institutions can integrate both obligations into a coherent administrative decision process. Four research questions guide the review:

1. How does existing literature explain the relationship between personal data protection and public information disclosure in public-sector organisations?
2. What institutional capacities and administrative mechanisms are required to implement personal data protection in public information services?
3. What regulatory, organisational, and administrative barriers affect integrating personal data protection into public information service delivery?
4. What institutional governance framework can be developed to integrate personal data protection and public information disclosure in public-sector organisations?

The study contributes to public governance literature in three ways. First, it connects the literature on transparency and personal data protection through an institutional decision-making perspective. Second, it identifies the organisational capacities and administrative mechanisms required to translate regulatory obligations into accountable disclosure practices. Third, it develops an institutional governance framework that explains the relationship between regulatory mandates, institutional capacity, administrative mechanisms, disclosure decisions, and public information service outcomes. The framework provides a conceptual basis for examining how personal data protection is implemented in public information services, including within local legislative institutions.

Methods

This study employs an Integrative Literature Review (ILR) to examine how public-sector organisations integrate personal data protection requirements into public information disclosure services. An integrative review is appropriate for synthesising empirical and theoretical literature derived from diverse research designs and disciplinary perspectives (Whittemore & Knafl, 2005). Unlike a review that primarily summarises findings within a single research tradition, an ILR enables critical examination and conceptual integration of existing knowledge to develop new perspectives on a research problem (Torraco, 2005, 2016). Accordingly, this study brings together scholarship on public information disclosure, personal data protection, institutional capacity, administrative decision-making, and public-sector governance to develop an integrated institutional framework.

Following the methodological orientation of the previous integrative review of rural cooperatives as hybrid last-mile governance institutions (Erdi et al., 2026), this study uses a structured, purposive literature search. The structured search provides an organised basis for identifying relevant scholarly publications, while purposive selection ensures the included literature contributes substantively to the research objectives. This approach aligns with the view that literature reviews should have a clearly defined purpose, an appropriate search strategy, and transparent criteria for selecting and evaluating relevant publications (Snyder, 2019). The literature covers 2000 to 2026 to capture developments in freedom of information, privacy governance, institutional implementation, and digital public administration (Budiyanto & Putra, 2026; Figueredo & Silva, 2026; Lund-Tønnesen, 2026; Sienkiewicz-Małyjurek & Zyzak, 2025). Peer-reviewed journal articles published in English and Indonesian constitute the primary sources. Relevant conceptual studies and scholarly legal analyses are also considered when they provide substantial insights into the relationship between public information disclosure and personal data protection. International literature is included to identify broader theoretical and comparative perspectives. At the same time, Indonesian studies receive particular attention because of the institutional and regulatory context of Law No. 14 of 2008 concerning Public Information Disclosure and Law No. 27 of 2022 concerning Personal Data Protection (Budiman, 2023; Qurbani & Yuningsih, 2026).

The literature search is organised around three interconnected themes. The first concerns personal data protection and privacy governance in public-sector organisations, including regulatory compliance, institutional responsibilities, and personal data management. The second addresses public information disclosure, freedom of information, access to information, transparency, and accountability. The third focuses on institutional capacity and administrative implementation, including human resource competence, organisational coordination, information management, bureaucratic discretion, and public service delivery. Search terms combine expressions such as "personal data protection," "privacy governance," "public information disclosure," "freedom of information," "access to information," "PPID," "institutional capacity," "administrative implementation," "accountability," and "public service delivery." Combinations of these terms are used to identify studies that connect at least two of the principal thematic areas. Consistent with recommendations for transparent literature review design, the final manuscript will report the academic databases and platforms actually searched, search dates, final search expressions, and retrieval records (Snyder, 2019).

Literature selection is guided by its relevance to the research questions and its contribution to institutional governance. Studies are considered relevant when they examine institutional mandates, regulatory interpretation, organisational capacity, administrative

procedures for assessing and disclosing information, bureaucratic decision-making, interorganizational coordination, accountability, public information service outcomes, or institutional risks associated with personal data processing and information disclosure. The relevance and analytical contribution of each study are considered in relation to its research objectives, theoretical orientation, methodological design, evidence transparency, principal findings, and acknowledged limitations. This critical examination is intended to distinguish the contributions and limitations of different forms of evidence rather than treating all publications as methodologically equivalent (Whittemore & Knafl, 2005). The core synthesis excludes studies focused exclusively on technical cybersecurity, cryptographic systems, software engineering, or individual privacy behaviour unless they clearly connect to public-sector institutional responsibilities or administrative information governance (Briantama & Yopan, 2026; Sari et al., 2024). Indonesian laws, government regulations, ministerial regulations, and relevant institutional guidelines are examined separately as contextual legal sources. These regulatory documents support the interpretation of the institutional setting but are not treated as journal publications or counted as part of the scholarly literature corpus.

The selected literature is examined through a structured extraction process. Information recorded from each publication includes author and publication year, geographical and institutional context, research objectives, theoretical orientation, research design, data sources, principal findings, limitations, and implications for institutional governance. Particular attention is given to the institutional arrangements and administrative processes through which public organisations manage the relationship between disclosure obligations and personal data protection. The extracted information is subsequently organized into five analytical domains: (1) institutional roles and regulatory frameworks, covering legal mandates, allocation of authority, institutional responsibilities, and regulatory interpretation; (2) institutional capacity, covering human resource competence, regulatory understanding, leadership support, administrative resources, and information technology infrastructure; (3) governance mechanisms, covering information classification, consequence assessment, identification of personal data, disclosure grounds, partial disclosure, redaction, access control, documentation, monitoring, and coordination; (4) public information service outcomes, covering accessibility, procedural certainty, proportionality of disclosure decisions, privacy safeguards, administrative accountability, and public trust; and (5) institutional risks, covering unauthorized disclosure, excessive restriction of public information, inconsistent administrative discretion, fragmented responsibilities, inadequate documentation, and weaknesses in institutional oversight (Briantama & Yopan, 2026).

The analysis combines thematic synthesis with conceptual integration (Matthew et al., 2025; Wahyudi et al., 2026). First, the analysis identifies recurring concepts and findings and groups them according to the five analytical domains. This process examines patterns of meaning across the selected publications and organises related findings into analytically coherent themes, drawing on the principles of thematic analysis described by (Braun & Clarke, 2006). Second, the study examines relationships among the themes across empirical and conceptual literature to identify patterns, complementarities, and differences in institutional arrangements and administrative practices. Third, the study integrates the identified relationships into a conceptual framework explaining how regulatory mandates and institutional capacity shape governance mechanisms, administrative disclosure decisions, accountability arrangements, and public information service outcomes. This integrative process

follows the principle that a literature review should move beyond aggregating findings toward a critical synthesis that generates new conceptual insights (Torraco, 2005, 2016).

The synthesis focuses on the decision pathway through which public institutions identify information containing personal data, assess the legal basis and potential consequences of disclosure, determine whether information can be released wholly or partially, coordinate responsibilities among organisational units, and document the grounds for administrative decisions. Finally, the study develops conceptual propositions from the integrated findings to explain the institutional conditions under which personal data protection and public information disclosure can be implemented consistently. The study examines institutional risks and governance safeguards as cross-cutting factors that may influence each stage of the decision-making process (Briantama & Yopan, 2026; Putra et al., 2025). The study considers differences in legal systems, administrative structures, organisational capacities, and public information regimes when interpreting findings across geographical contexts. Accordingly, the resulting framework conceptually integrates the available literature rather than statistically generalising or empirically assessing a particular public institution (Marwenny et al., 2024).

Result and Discussion

Public Information Services as Institutional Governance Interfaces

Public information services constitute an administrative interface through which public institutions translate the principles of information disclosure and personal data protection into institutional decisions (Sitepu et al., 2025). In this process, public institutions do not merely provide documents. They also serve as information managers, identifying the requested information, determining its legal classification, assessing the consequences of disclosure, and deciding whether to release it in full, disclose it partially, or withhold it.

The relationship between transparency and privacy is not always straightforward. Adeoye & Ran (2024), through a systematic review of 470 articles on government transparency, identified privacy as a key dilemma shaping transparency outcomes. Their analysis shows that government transparency involves competing institutional and normative considerations, not merely publishing government-held information. In public information services, this tension becomes particularly visible when requested documents contain information relevant to public oversight while simultaneously containing personal data that requires protection.

Desrochers (2024) similarly positions access to information and privacy as interconnected considerations in public service reform. Access to information supports government accountability, whereas privacy protection limits the disclosure of personal information without an adequate legal basis. These principles require administrative procedures that enable public institutions to assess both interests within the same service process. A disclosure decision should not automatically be reduced to a binary choice between releasing or withholding an entire document. Instead, institutions need to examine the content of the requested information and determine an appropriate form of access based on applicable legal requirements and the consequences of disclosure.

In Indonesia, these principles interact in Law No. 14 of 2008 concerning Public Information Disclosure and Law No. 27 of 2022 concerning Personal Data Protection. These regulations require public institutions to balance public access with individual rights when handling information requests. Their implementation therefore involves more than regulatory compliance. It requires institutional arrangements that translate legal provisions into consistent administrative practices.

Public information services can consequently be understood through three institutional characteristics. First, they constitute a regulatory interpretation space, where officials translate legal provisions into decisions on specific information requests. Second, they constitute an administrative coordination space, because requested information may originate from different organisational units and require verification of its content and personal data components. Third, they constitute an accountability space, because decisions to disclose, partially disclose, or withhold information must have identifiable and defensible reasons.

These characteristics indicate that service quality cannot be assessed solely through response speed or the availability of online request channels. Institutional quality also depends on the consistency, proportionality, and accountability of disclosure decisions (Vieira et al., 2026; Walke & Winkler, 2025; Yang, 2026). Excessive reliance on privacy protection may lead institutions to restrict public access beyond what is legally necessary. Conversely, disclosure without adequate examination of personal data may expose individuals to inappropriate processing or disclosure (Briantama & Yopan, 2026). The central analytical issue is therefore not an abstract opposition between transparency and privacy. It concerns the institutional capacity to manage the intersection of these principles through consistent administrative decisions (Putra et al., 2025).

Institutional Roles and Regulatory Frameworks

Regulatory mandates provide the normative foundation for managing public information disclosure and personal data protection. However, implementing these mandates requires institutional interpretation because requested documents may contain different categories of information with distinct legal implications (Prastawa & Kartika, 2026). A single document may contain information concerning public expenditure that is relevant to public oversight while also including names, addresses, identification numbers, or other personal information.

Law No. 14 of 2008 establishes openness as the general principle and requires exceptions to be applied strictly and within defined limits. Article 17(h) identifies information concerning personal secrets as one category of exempt information. Article 19 requires the PPID to conduct a consequence test before determining information as exempt. Article 22(7) provides a basis for partially fulfilling information requests when only certain parts of a document contain exempt information. These provisions indicate that the exclusion of information should not automatically extend to an entire document when protected information can be separated from information that remains accessible.

Law No. 27 of 2022 adds another dimension to this administrative responsibility. Article 16 includes disclosure and dissemination within the scope of personal data processing. Article 20 regulates the legal bases for processing personal data, including the fulfilment of legal obligations and the performance of tasks in the public interest or provision of public services, subject to applicable requirements. Consequently, the presence of personal data in a public institution's document does not, by itself, determine whether the document must be withheld. Institutions must also consider the purpose, legal basis, relevance, and consequences of processing and disclosure.

The interaction between these regulatory mandates creates three challenges for institutions to interpret. The first concerns the boundary of information disclosure. Institutions must identify whether requested information is open, exempt, or contained in a document that combines both categories. The second concerns the legal basis for protecting personal data. Officials must examine the status and relevance of personal data rather than treating every

document containing personal information as automatically inaccessible—the third concerns institutional authority and responsibility. The PPID requires support from organisational units that produce or control documents to verify their substance, context, and disclosure risks (Sulaeman et al., 2026).

Choi (2018), in a study of public officials' responses to information disclosure requests in South Korea, found that the information's characteristics influenced disclosure decisions. The study also identified blame-avoidance motivations as a factor that could discourage officials from releasing information unfavourable to their agencies. These findings demonstrate that formal legal mandates do not entirely determine administrative decisions. Information characteristics, bureaucratic incentives, and organisational environments also influence how officials interpret and implement disclosure requirements.

Rahman (2025) identifies related challenges in implementing personal data protection in Indonesia's public sector. The study highlights the tendency to prioritise sectoral regulations and the potential to overinterpret personal data protection exemptions. This concern indicates that privacy protection should not become a general justification for restricting access without an adequate legal and administrative assessment. Regulatory harmonisation and clear institutional responsibilities are therefore necessary to support consistent implementation.

Galván et al. (2025) further emphasise that access to public information and personal data protection should be considered together within responsible data governance. Their analysis places attention on how data are collected, shared, published, stored, and reused. This perspective extends the discussion beyond the final decision to disclose a document and requires institutions to examine the governance arrangements that regulate information throughout its administrative lifecycle.

The analysis supports the following proposition:

Proposition 1—Regulatory Mandate Clarity: Consistency in public information service decisions increases when institutional authority, responsibilities, and the boundaries between open and exempt information are translated into clear operational guidelines understood by relevant organisational units.

Institutional Capacity and Implementation Readiness

Regulatory compliance requires organisational resources and capabilities that enable public institutions to translate legal obligations into administrative practices. Institutional capacity in public information services includes human resource competence, regulatory understanding, administrative procedures, technological infrastructure, organisational leadership, and resources to support information management (Judijanto et al., 2024; Nugroho, 2025).

Evidence from Indonesian digital governance illustrates the relevance of organisational capacity. Pribadi et al. (2024), using survey data from 424 employees across four local governments, found that employee skills, leadership, regulation, infrastructure, information and communication technology, transparency, and accountability were positively associated with the implementation of digital government services. Their findings suggest that digital public services depend on the interaction between organisational, regulatory, and technological factors rather than on technology alone.

These findings are relevant to personal data protection because managing public information increasingly involves digital documents, electronic records, online request systems, and data exchange between organisational units. These processes require officials to

understand the legal distinction between public information and personal data, recognise potentially sensitive information, and apply appropriate safeguards. Digital infrastructure can support these activities, but it cannot independently replace administrative judgment or regulatory competence.

Masrich et al. (2026), in their study of personal data protection implementation at the Communication and Informatics Service in Majalengka Regency, identified challenges related to regulatory understanding, human resources, and information technology readiness. Their findings indicate that implementation requires strengthening regulations and infrastructure. The study suggests that institutional readiness is not determined merely by the existence of a personal data protection law or supporting policy. It also depends on whether officials possess the knowledge and resources required to apply those provisions in daily administrative work.

Institutional capacity can be examined through five interconnected dimensions. First, human resource competence concerns officials' ability to identify personal data, understand information classifications, conduct consequence testing, and prepare decisions concerning full or partial disclosure. Second, regulatory understanding concerns the extent to which officials understand the relationship between public information disclosure requirements and personal data protection obligations. Third, administrative capacity concerns the availability of standard operating procedures, documentation systems, request-handling mechanisms, and internal guidance. Fourth, technological and information infrastructure concerns secure document storage, access management, electronic records, redaction facilities, and systems for tracking information requests. Fifth, organisational leadership and resource support concern the institutional commitment to allocate personnel, time, infrastructure, and oversight for information management (Putra et al., 2025).

These dimensions indicate that institutional capacity should not be understood as a single organisational attribute. It represents the alignment of competence, regulatory understanding, procedures, technology, and leadership. Weakness in one dimension can constrain the effectiveness of the others. Trained PPID personnel, for example, may still be unable to implement proportionate disclosure when the institution lacks document redaction facilities or cooperation from the units responsible for the requested records (Ghofar et al., 2026; Prabowo et al., 2025).

The literature supports the following proposition:

Proposition 2—Institutional Capacity Alignment: Institutional readiness to integrate personal data protection into public information services increases when human resource competence, regulatory understanding, administrative procedures, technological infrastructure, and organisational leadership are aligned with the complexity of information processing and disclosure decisions.

Governance Mechanisms and Administrative Disclosure Decisions

Institutional capacity provides the resources necessary for implementation, but administrative governance mechanisms determine how those resources are applied in actual information service decisions. Governance mechanisms include information classification, consequence testing, legal basis assessment, data minimisation, redaction, access control, documentation, coordination, monitoring, and accountability (Gao et al., 2026; Levantis et al., 2026).

The relationship between capacity and governance is important because organisational resources do not automatically produce consistent administrative decisions. Officials may

understand the legal framework but still apply it differently when institutions lack standardised procedures. Governance mechanisms reduce this variation by establishing decision stages, defining responsibilities, and requiring officials to record the reasons for their actions (van Popering-Verkerk et al., 2022).

A proportionate disclosure process can be organised into six administrative stages:

1. **Request identification**. The institution identifies the requested document, the information required, and the organisational unit responsible for the records.
2. **Information and personal data identification**. The responsible unit examines the document to identify its substantive information, public-interest content, and personal data components.
3. **Legal and consequence assessment**. The institution examines relevant legal provisions, the basis for processing or disclosure, applicable exemption grounds, and potential consequences.
4. **Disclosure determination**. The institution determines whether the document can be disclosed in full, partially disclosed, or withheld.
5. **Protection and document preparation**. When only certain information requires protection, the institution separates or redacts relevant elements while preserving access to non-exempt information.
6. **Documentation and accountability**. The institution records the decision, legal basis, assessment, responsible officials, and reasons for any restriction.

These stages should be understood as an integrated decision pathway rather than independent administrative activities. Identifying personal data informs the legal assessment; the legal assessment informs the disclosure decision; and the decision determines the required protection and documentation. Failure at an earlier stage can affect the accuracy of later decisions.

Febriyani et al. (2022) illustrate the importance of coordination: their study of the relationship between main and supporting PPIDs in Central Java found that coordination and leadership commitment contributed to public information service performance. Supporting PPIDs supplied the information the main PPID needed to respond to public requests. This finding demonstrates that information disclosure cannot be treated as an isolated administrative function assigned exclusively to one officer or unit.

Governance mechanisms must also connect administrative efficiency with personal data safeguards. Access control, document version management, secure storage, and redaction procedures help institutions prevent unauthorised disclosure while maintaining the availability of information that can legally be released. These safeguards should be proportionate to the sensitivity of the information and the risks associated with its processing.

The analysis supports the following proposition:

Proposition 3—Governance Mechanism Integration: Institutional capacity is more likely to produce accountable disclosure decisions when it is operationalised through standardised procedures for information identification, legal assessment, consequence testing, redaction, documentation, coordination, and monitoring.

Public Information Service Outcomes and Proportional Disclosure

Information classification is a central mechanism for reconciling public information disclosure and personal data protection. It enables public institutions to distinguish among accessible information, exempt information, and documents that contain both. The

classification process should therefore examine the information's content rather than rely solely on document titles, originating units, or broad categories of administrative records (Gao et al., 2026; Ignaczak et al., 2026).

The principle of proportional disclosure is particularly important when a requested document contains personal data alongside information relevant to public accountability. Withholding the entire document may unnecessarily restrict access to information that should remain available. Conversely, releasing the document without removing protected personal information may expose individuals to risks that are not necessary to achieve the purpose of public disclosure (Amelia & Wiraguna, 2026).

Articles 17(h), 19, and 22(7) of Law No. 14 of 2008 provide an important legal basis for this approach. They establish grounds for protecting personal secrets, require consequence testing, and allow partial fulfilment of information requests. Read together, these provisions support an administrative approach in which institutions assess the relevant information and determine whether protected elements can be separated from the remainder of a document.

The concept of proportional disclosure involves three analytical considerations. First, relevance to public interest concerns how the information contributes to public oversight, accountability, participation, or understanding of government activities. Second, personal data sensitivity concerns the nature of the information and the potential consequences of disclosing it. Third, the availability of less restrictive alternatives concerns whether the institution can fulfil the request without disclosing protected information through redaction, anonymisation, partial disclosure, or removing specific document elements, where legally appropriate (Warthon, 2024).

Yan & Zhang (2022), in their analysis of personal information protection in government information disclosure during major public health emergencies, demonstrate the importance of contextual assessment. Their analysis indicates that disclosure decisions may depend on the information's sensitivity, the public value of disclosure, the surrounding circumstances, and the intended audience. Although the study concerns a specific policy context, it supports the broader argument that information disclosure should be assessed by its purpose and consequences rather than through an undifferentiated approach.

Galván et al. (2025) also emphasise responsible data governance in the relationship between access to information and personal data protection. Their perspective supports examining the consequences of data publication and reuse, not merely the initial decision to provide access. Disclosure can create further risks when information is copied, redistributed, combined with other datasets, or used outside its original administrative context.

Public information service outcomes should therefore be assessed through the relationship between accessibility, privacy protection, procedural certainty, and accountability. Accessibility concerns whether applicants can obtain legally open information. Privacy protection concerns whether personal data are managed in accordance with applicable requirements. Procedural certainty concerns whether officials and applicants can understand the decision process. Accountability concerns whether the institution can explain and document the basis for disclosure or restriction (Ghofar et al., 2026).

The analysis leads to the following proposition:

Proposition 3—Governance Mechanism Integration: The balance between public information access and personal data protection is more likely when institutions apply content-based classification, consequence assessment, and proportionate redaction to distinguish information that can be disclosed from information that requires protection.

Institutional Risks, Administrative Discretion, and Governance Safeguards

Integrating public information disclosure and personal data protection creates institutional risks when regulations, organisational capacities, and administrative procedures are not adequately aligned. These risks may arise from unauthorised disclosure, excessive restriction of public information, inconsistent interpretation of legal provisions, fragmented organisational responsibilities, or inadequate documentation of administrative decisions (Kholis et al., 2026; Sipahutar & Jannah, 2023).

The first risk is unauthorised disclosure of personal data. This may occur when officials release documents without identifying personal data components or applying appropriate safeguards. The consequences can extend beyond the initial service transaction because disclosed information may be copied, redistributed, or combined with other information (Suhardi, 2025).

The second risk is excessive restriction of public information. Institutions may interpret personal data protection provisions too broadly and withhold documents that contain information relevant to public oversight (Cahyadewi & Afifah, 2026). Rahman (2025) highlights the potential for overinterpretation and overuse of personal data protection exemptions in the Indonesian public sector. This concern indicates that privacy protection should not become a general justification for restricting access without an adequate legal and administrative assessment.

The third risk is inconsistent administrative discretion. Choi (2018) demonstrates that information characteristics and organisational incentives, including blame avoidance, can influence officials' disclosure decisions. When institutional procedures are unclear, officials may rely heavily on personal judgment, resulting in different decisions for requests involving similar information.

The fourth risk is fragmented institutional responsibility. When the PPID and document-producing units lack clear responsibilities, information verification and decision-making may be delayed or incomplete. Fragmentation can also make it difficult to identify which unit is accountable when inappropriate disclosure or unjustified restriction occurs (Machmudi, 2025).

The fifth risk is weak administrative traceability. Institutions that do not record the basis, process, and authorisation of disclosure decisions may struggle to explain their actions during complaints, information disputes, audits, or internal evaluations (Rahman, 2025).

Sjoraida (2025), examining public information disclosure policy implementation in West Java, identifies bureaucratic and institutional conditions that influence transparency practices. This finding demonstrates that formal organisational arrangements do not automatically ensure effective implementation. Institutional culture, established bureaucratic practices, and the actual distribution of authority can influence how transparency policies operate in practice.

These risks demonstrate that administrative discretion cannot be eliminated. Information requests differ in content, context, and potential consequences. However, discretion needs to operate within defined legal and procedural boundaries. Institutions can reduce arbitrary decisions through clear classification criteria, documented consequence assessments, standardised redaction procedures, access controls, internal review, and complaint mechanisms (Kharin et al., 2026; Wahyudi et al., 2026).

The analysis supports the following proposition:

Proposition 5—Institutional Governance Safeguards: The risks of unauthorised personal data disclosure and unjustified restriction of public information decrease when institutions

combine clear decision procedures with access controls, documented assessments, internal oversight, complaint mechanisms, and periodic evaluation.

Institutional Governance Framework and Design Implications

The preceding synthesis indicates that effective implementation requires an institutional design that connects regulatory mandates, organisational capacity, administrative mechanisms, and accountability arrangements. A policy framework that focuses exclusively on regulatory compliance may fail to address operational constraints. Similarly, investments in digital infrastructure may not produce accountable disclosure when institutions lack clear procedures and competent personnel (Alqarni et al., 2026; Israyudin et al., 2025; Ramdhan & Kusumawati, 2026).

An integrated institutional design should include six components (Sulaeman et al., 2026).

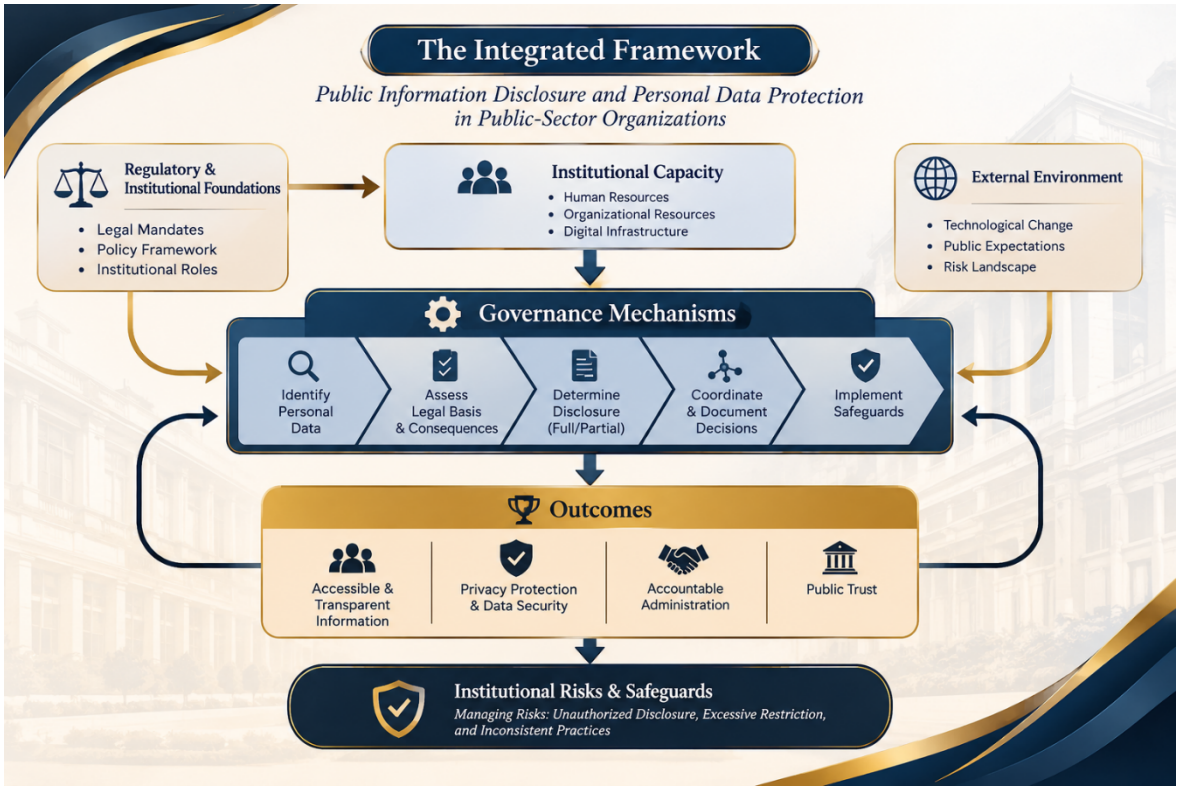
The study identifies six institutional priorities: (1) regulatory and procedural alignment through clear guidance on disclosure, data protection, and institutional responsibilities; (2) competence development through continuous training in information classification, legal assessment, redaction, and complaint handling; (3) integrated information management supported by reliable document inventories, secure storage, and access controls; (4) standardised disclosure decisions through documented assessment, partial disclosure, and written justification; (5) cross-unit coordination and accountability by clarifying the responsibilities of PPID and document-producing units; and (6) monitoring and institutional learning through regular evaluation of service performance, disclosure consistency, complaints, and data protection incidents.

Table 1. Institutional Governance Design for Personal Data Protection in Public Information Services

Governance component	Core administrative requirement	Expected institutional contribution
Regulatory alignment	Operational guidelines and clear authority	Consistent regulatory interpretation
Competence development	Training and technical guidance	Accurate information assessment
Information management	Document inventory and secure systems	Reliable and controlled information access
Disclosure procedures	Classification, assessment, and redaction	Proportionate disclosure
Coordination and accountability	Defined responsibilities and decision records	Traceable institutional decisions
Monitoring and learning	Evaluation, complaints, and corrective action	Continuous institutional improvement

The framework indicates that institutional design should not place all responsibility on the PPID. The PPID functions as the service coordination and decision-management point, while document-producing units contribute substantive verification and institutional leadership provides authority, resources, and oversight. Relevant legal, information technology, and administrative functions support safeguard implementation within their respective responsibilities.

The integrated framework can be summarized as follows:



Institutional risks and governance safeguards operate across the entire framework. Risks may emerge during regulatory interpretation, information processing, or officials' disclosure decisions. Safeguards such as internal review, access controls, documentation, oversight, and complaint mechanisms help institutions manage these risks.

The framework advances three institutional arguments. First, the integration of transparency and personal data protection should be analysed as a problem of institutional translation. Legal mandates do not implement themselves. Public institutions must translate regulatory requirements into operational procedures, role assignments, and decisions concerning specific information requests.

Second, institutional capacity should be understood as a condition that enables procedural governance rather than as an outcome in itself. Competent personnel, technology, and organisational resources become meaningful when institutions use them through standardised and accountable decision mechanisms. This distinction explains why organisational capacity and administrative procedures must be analysed together (Asetya, 2026; Muallidin, 2026; Rajasa, 2026).

Third, public value depends on the institution's ability to produce proportionate disclosure decisions. The objective is not to maximise disclosure regardless of privacy consequences or to maximise confidentiality regardless of public accountability. Instead, the institution must identify which information can be disclosed, which information requires protection, and how the decision can be justified under applicable legal provisions (Azhar et al., 2026).

The framework also identifies a limitation in treating digital transformation as the primary solution to information governance problems. Digital systems can improve document retrieval, access management, request tracking, and administrative efficiency. However, technology

cannot independently determine the legal status of information or replace institutional responsibility for disclosure decisions. Digital capability must therefore operate within a governance arrangement that includes competent officials, clear procedures, and accountability mechanisms.

Theoretical Implications for Public Governance

The synthesis contributes to public governance scholarship by positioning personal data protection in public information services as an institutional decision-making problem. Existing discussions of transparency often focus on access rights, accountability, and the availability of government information. Personal data protection literature, in contrast, frequently emphasises legal compliance, data security, processing principles, and individual rights. The intersection of these perspectives requires an analytical framework that explains how public institutions translate both regulatory obligations into administrative decisions (Tan et al., 2025).

The proposed framework connects five analytical elements: institutional roles and regulatory mandates, institutional capacity, administrative governance mechanisms, public information service outcomes, and institutional risks. These elements form a sequence of institutional relationships rather than independent implementation factors.

Regulatory mandates establish the legal obligations and boundaries that guide information disclosure and personal data protection. Institutional capacity determines whether public organisations possess the personnel, knowledge, procedures, infrastructure, and leadership required to implement these mandates. Administrative governance mechanisms translate institutional capacity into operational practices. Accountable decision processes represent the immediate institutional output of the interaction between mandates, capacity, and governance mechanisms. Public information service outcomes emerge when institutional decisions provide meaningful access to information while protecting personal data and maintaining administrative accountability.

This framework advances three theoretical arguments. First, it analyses the integration of transparency and personal data protection as an institutional translation problem. Second, institutional capacity enables procedural governance when organisations convert resources into consistent administrative practices. Third, public value depends on the institution's ability to produce proportionate disclosure decisions that maintain information accessibility while protecting personal data.

This review's theoretical contribution lies in connecting the governance of information disclosure with the institutional implementation of personal data protection. It shifts the analytical focus from the existence of legal provisions or digital systems to the administrative decision pathway through which public institutions reconcile access rights and privacy obligations. The framework provides a basis for further empirical examination of institutional arrangements, administrative discretion, and accountability in public information services (Budiman, 2023; Cahyono et al., 2026).

Conclusion

Bagian This integrative literature review examined how public-sector organisations can integrate personal data protection into public information services through institutional governance arrangements. The synthesis indicates that regulatory compliance or technological safeguards alone do not adequately address the relationship between information disclosure and personal data protection. It requires institutional procedures that translate legal obligations into consistent, proportionate, and accountable administrative decisions.

The review identifies five interrelated analytical domains: institutional roles and regulatory frameworks, institutional capacity, governance mechanisms, public information service outcomes, and institutional risks. The synthesis demonstrates that clear regulatory interpretation establishes the basis for implementation, while human resource competence, administrative procedures, infrastructure, and leadership determine institutional readiness. Governance mechanisms, including information classification, consequence assessment, proportionate redaction, access control, documentation, and coordination, translate institutional capacity into accountable disclosure practices.

The study develops an institutional governance framework connecting regulatory mandates, institutional capacity, administrative governance mechanisms, accountable decision processes, and public information service outcomes. Institutional risks and governance safeguards operate as cross-cutting conditions that shape implementation. The framework frames the integration of personal data protection and public information disclosure as an institutional decision-making process, not solely a matter of regulatory compliance or technological security.

For public institutions, the framework suggests establishing clear operational guidelines, strengthening personnel competence, integrating document management systems, standardising disclosure assessments, defining responsibilities across organisational units, and conducting periodic monitoring. These arrangements should enable institutions to protect personal data without unnecessarily restricting information that is relevant to public accountability.

This review has limitations. The synthesis is dependent on the scope and quality of the literature selected and cannot establish the actual implementation conditions of every public institution. Differences in legal systems, administrative structures, organisational resources, and information management practices may affect the framework's applicability across institutional settings. Further empirical research is therefore required to examine how the proposed framework operates in specific public organisations, particularly local government institutions and legislative secretariats. Such research can assess the consistency of information classification, the implementation of consequence testing, the role of PPID coordination, and the accountability of decisions involving documents that contain personal data.

Acknowledgment

The authors thank the colleagues and academic peers whose scholarly insights and constructive feedback contributed to the development of this article. The authors also acknowledge the institutional and academic environment that supported the intellectual process underlying this study. Any remaining limitations or errors are the sole responsibility of the authors.

References

Adeoye, O., & Ran, B. (2024). Government transparency: paradoxes and dilemmas. *Public Management Review*, *26*(8), 2194–2217. https://doi.org/10.1080/14719037.2023.2181981

Alqarni, W., ZA, S., Muallidin, I., Afrijal, A., & Akhyar, M. N. (2026). The Role of Institutional Quality in Shaping Digital Governance in Decentralised Indonesia. *Journal of Contemporary Governance and Public Policy*, *7*(1), 83–106. https://doi.org/10.46507/jcgpp.v7i1.793

Amelia, S. R., & Wiraguna, S. A. (2026). Juridical Construction of Data Accuracy Principles in Personal Data Protection Governance: A Comparative Analysis of Indonesia and Singapore. *Journal of Law, Politic and Humanities*, *6*(5), 4308–4316. https://doi.org/10.38035/jlph.v6i5.3621

Aribianto, Kustiningsih, N., & Sundjoto. (2026). The Implementation of Analog-to-Digital Records Management in Government Institutions to Support the Adoption of an Electronic-Based Government System (A Study at the Office of the Trade Order Supervision Center (BPTN) Surabaya, Ministry of Trade of the R. *Jurnal Ragam Pengabdian*, *3*(1 (Spesial Issue)), 1919–1927. https://doi.org/10.62710/n4hws148

Arifin, F., Refliandi, I., & Rahmadhani, S. (2026). *PUBLIC INFORMATION DISCLOSURE UNDER LAW NO . 14 OF 2008 : STRENGTHENING TRANSPARENCY , ACCOUNTABILITY , INTRDUCTION At present , many countries , including Indonesia , continue to seek effective governance systems capable of creating institutional stabili*.

Asetya, D. R. (2026). Institutional Transformation and Governance in Indonesia: Democracy, Decentralization, and the Persistence of Oligarchy. *Journal of International Political Economy and Strategy*, *1*(1), 1–9. https://journal.privietlab.org/index.php/JIPES/article/view/1796

Azhar, A. W., Ahmad, H., & Hatiboruah, D. (2026). *Custodia : Journal of Legal , Political , and Humanistic Inquiry Personal Data Protection in Indonesia ' s Digital Public Services : Implementation and Accountability*. *2*(1).

Bangsu, M. N. A., Brahmanto, D. E., & Shifa, A. (2026). Legal Protection of Personal Data in Indonesia Following the Enactment of Law No. 27 of 2022 on Personal Data Protection. *Advances in Community Services Research*, *4*(2), 210–224. https://doi.org/10.60079/acsr.v4i2.968

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Briantama, A., & Yopan, M. (2026). An Analysis of Digital Institutional Capacity and Personal Data Protection Policy Implementation in Indonesia : A Systematic Literature Review. *Journal of Law, Politic and Humanities*, *6*(4), 2522–2532. https://doi.org/10.38035/jlph.v6i4.3253

Budiman, R. (2023). The Development of Personal Data Protection Law in Indonesia: Challenges and Prospects for the Implementation of Law No. 27 of 2022. *Jurnal Smart Hukum (JSH)*, *2*(1), 24–36. https://doi.org/10.55299/jsh.v2i1.1352

Budiyanto, M. N., & Putra, R. (2026). *Digital Governance Effectiveness in Public Organizations : a Systematic Literature Review of Institutional Capacity and Organizational Culture*. *5*(5), 2715–2722.

Cahyadewi, B., & Afifah, W. (2026). Right to be Forgotten vs. Public Information Disclosure to Public Officials in Indonesia. *Mimbar Keadilan*, *19*(1), 109–121. https://doi.org/10.30996/mk.v19i1.132922

Cahyono, D., Rahayu, D. W. S., Siahaan, M. M., & Edwards, J. (2026). Legal Governance of Personal Data Protection in Indonesian Digital Business. *Legal Autonomous Web-Based Governance (LAW)*, *1*(1), 95–108. https://doi.org/10.68012/law.v1i1.113

Choi, J. M. (2018). Factors influencing public officials' responses to requests for information disclosure. *Government Information Quarterly*, *35*(1), 30–42. https://doi.org/10.1016/j.giq.2017.11.007

Desrochers, P. R. (2024). Access to Information and Privacy: Practical Approaches for Public Service Reform. *Canadian Public Administration*, *67*(4), 562–572. https://doi.org/10.1111/capa.12582

Erdi, Hengki, H., Aryada, K. T., Mujib, Zalviwan, M., & Rudiyanto, Y. (2026). *Rural Cooperatives as Hybrid Last-Mile Governance Institutions : An Integrative Literature Review*. *01*, 160–175.

Febriyani, A. R., Yuliyanto, M., Naryoso, A., & Tuti, A. (2022). Synergy of Public Information Openness Practices between Main PPID with Supporting PPID in Central Java. *Proceedings of the 6th International Conference on Social and Political Enquiries, ICISPE 2021, 14-15 September 2021, Semarang, Indonesia*. https://doi.org/10.4108/eai.14-9-2021.2321356

Figueredo, E., & Silva, L. C. S. (2026). Challenges of Digital Services in Public Administration in the Era of Digital Transformation: A Systematic Literature Review. *Journal of the Knowledge Economy*, *17*(4), 11926–11955. https://doi.org/10.1007/s13132-026-03277-z

Galván, C., Berrino Malaccorto, R., & Herrero, J. (2025). Access to public information and personal data protection: how do they dialogue? *International Data Privacy Law*, *15*(4), 328–371. https://doi.org/10.1093/idpl/ipaf009

Gao, F., Wang, D., Wang, J., & Tu, Y. (2026). Data Classification and Grading as an Information Governance Mechanism: A Review of Regulatory Practices, Sectoral Implementation, and Operationalization Gaps in China. *Information*, *17*(6), 602. https://doi.org/10.3390/info17060602

Ghofar, A., Hendra, A., Sariwulan, T., & Arifin, A. L. (2026). Managing Public Information Governance in Indonesia: A SMART Transparency Approach Based on Information Technology and Artificial Intelligence. *Dinasti International Journal of Education Management and Social Science*, *7*(4), 3775–3789. https://doi.org/10.38035/dijemss.v7i4.6385

Ignaczak, L., Martins, M. G., Costa, C. A. da, & Kunst, R. (2026). A value-based approach for information classification. *International Journal of Information Security*, *25*(1), 9. https://doi.org/10.1007/s10207-025-01174-1

Isbandono, P., Utami, D. A., Prastyawan, A., Gamaputra, G., & Lestari, Y. (2025). Transparency and Accountability in Public Services and Policies in Administrative Law: A Comparative Study of Indonesia and Norway. *Pena Justisia: Media Komunikasi Dan Kajian Hukum*, *24*(1), 3998–4016. https://doi.org/10.31941/pj.v24i2.6029

Israyudin, R., Arrofi, F. M., & Dwiardi, A. R. (2025). Digital Transformation through Electronic-Based Government System Policy in Indonesia: A Policy Narrative Analysis. *Journal La Sociale*, *6*(2), 281–292. https://doi.org/10.37899/journal-la-sociale.v6i2.1825

Judijanto, L., Sono, M. G., & Bunyamin, I. A. (2024). Analysis of Regulatory Quality, Interagency Coordination, and Institutional Capacity on the Effectiveness of Public Services in Jakarta. *West Science Social and Humanities Studies*, *2*(10), 1633–1642. https://doi.org/10.58812/wsshs.v2i10.1345

Kaplale, M. I., & Maulana, D. (2026). Legal Protection of Personal Data in Indonesia's Digital Ecosystem: Challenges for Regulatory Enforcement and Legal Certainty. *Journal of Lex et Justitia*, *2*(2), 18–32. https://doi.org/10.67171/d1qff634

Kharin, J., Harahap, C. N., Judira, S. M., Cakrawangsa, M. G. U., Muthmainah, A., & Sinurat, M. O. (2026). Legal Boundaries Of Administrative Innovation Within State Public Services.

Indonesian Journal of Innovation Studies, *27*(4), 2–5. https://doi.org/10.21070/ijins.v27i4.2448

Kholis, M. N., Nanung, A., Dirjon, S., Simamora, D. K., & Kusumo, I. S. (2026). Enforcement of Law No. 19/2016 on Electronic Information and Personal Data Protection in Indonesia. *Jurnal Multidisiplin West Science*, *5*(08), 1838–1846. https://doi.org/10.58812/jmws.v5i08.3833

Lestari, N. (2025). Open Data Policy AND Privacy Challenges: Balancing Transparency AND Security in Digital Governance in Indonesia. *Asian Digital Governance Problems*, *2*(2), 68–77. https://doi.org/10.71435/685955

Levantis, N., Sgora, A., Tsipis, A., & Polykalas, S. (2026). Operationalising AI Governance in Public Administration: An Integrated Regulatory and Risk Management Framework. *Information*, *17*(10), 962. https://doi.org/10.3390/info17100962

Lund-Tønnesen, J. (2026). Digital surveillance governance: understanding developments in the use of personal data in public sector reform. *Public Management Review*, 1–28. https://doi.org/10.1080/14719037.2026.2620546

Machmudi, E. A. A. P. (2025). Navigating the Institutional Vacuum of Personal Data Protection and Public Trust in Indonesia. *International Journal of Law Dynamics Review*, *3*(2), 113–123. https://doi.org/10.62039/ijldr.v3i2.114

Marwenny, E., Syafwar, R., & Yani, P. (2024). Personal Data Protection in Public Services. *Jurnal Ilmiah Ekotrans & Erudisi*, *4*(2), 74–85. https://doi.org/10.69989/yjew5p90

Masrich, A., Yanto, T., & Supriyono, E. (2026). Implementation of Law Number 27 of 2022 concerning Personal Data Protection (PDP) at the Communication and Information Service in Majalengka Regency. *Jurnal Ilmiah Administrasi Pemerintahan Daerah*, *18*(1), 11–20. https://doi.org/10.33701/jiapd.v18i1.5561

Matthew, B., Wagiman, W., & Prasetyo, S. (2025). KETERKAITAN ANTARA HUKUM DAN ADMINISTRASI PUBLIK: HUBUNGAN YANG MEMASTIKAN BAHWA KEBIJAKAN DILAKSANAKAN DALAM BATASAN HUKUM. *The Indonesian Journal of Public Administration (IJPA)*, *11*(1), 1–17. https://doi.org/10.52447/ijpa.v11i1.8196

Muallidin, I. (2026). The politicization of public policy in Indonesia: A Global South perspective. *Journal of Public Policy*. https://doi.org/10.1017/S0143814X26101202

Nabawi, I. H., Bajari, A., Erwina, W., & Khadijah, U. L. S. (2026). The Digital Shock: Administrative Burden and the Governance–Service Trade-Off in Indonesia's Public Service Reform. *Administrative Sciences*, *16*(3), 159. https://doi.org/10.3390/admsci16030159

Nugroho, E. R. S. (2025). Balance Between Transparency and Data Protection in Digital Government as Public Information Disclosure Implementation in Indonesia. *Greenation International Journal of Law and Social Sciences*, *3*(2), 558–563. https://doi.org/10.38035/gijlss.v3i2.495

Octavianus, Y. Y., & Kurniawan, E. (2026). Legal Policy on the Law Enforcement of Personal Data Protection in Indonesia. *Journal of Law, Society and Living Norms*, *1*(3), 137–142. https://doi.org/10.66111/m8x80p84

Prabowo, S., Abdurohman, M., Nuha, H. H., & Sutikno, S. (2025). Identifying and Validating Critical Factors in Designing a Comprehensive Data Protection Impact Assessment (DPIA) Framework for Indonesia. *International Journal of Safety and Security Engineering*, *15*(1), 113–126. https://doi.org/10.18280/ijsse.150113

Prastawa, R. T., & Kartika. (2026). Legal Protection for PLN in The Disclosure of Customer Data to Law Enforcement Agencies. *Journal of Law, Society and Living Norms*, *1*(3), 132–136. https://doi.org/10.66111/tfdnnx31

Pribadi, U., Iqbal, M., Ibrahim, M. A., Juhari, & Ahdarrijal, Y. (2024). Nexus of public organization, transparency, and accountability in Indonesia's digital governance. *Journal of Public Affairs*, *24*(3). https://doi.org/10.1002/pa.2940

Putra, R. K., Agustin, Y., Nurul Ihsan, L., & Ahmad Dafiqi, Z. (2025). Institutional Dysfunction in Personal Data Protection: A Legal-Political Analysis Based on New Institutional Theory. *Perkara : Jurnal Ilmu Hukum Dan Politik*, *3*(2), 938–949. https://doi.org/10.51903/bkktey52

Qurbani, A. S., & Yuningsih, H. (2026). Analisis Yuridis terhadap Tindak Pidana Pelanggaran Data Pribadi oleh Media Massa dalam Sistem Hukum Pidana Indonesia. *Jurnal Antologi Hukum*, *5*(2), 258–271. https://doi.org/10.21154/antologihukum.v5i2.5338

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

Rajasa, A. (2026). Bureaucratic Reform in Post-Authoritarian Indonesia: A Bibliometric-Informed Critical Review (1966–2026). *Public Administration and Development*. https://doi.org/10.1002/pad.70122

Ramdhan, F. A., & Kusumawati, L. (2026). Governance Challenges in Public Service Regulation and the Evolution of Administrative Accountability in Indonesia. *Qriset Indonesia Journal of Law*, *1*(1), 20–27. https://doi.org/10.63668/qijl.v1i1.53

Sari, J. A., Yuliani, I., Akadira, T., Sunarya, A., & Ating, R. (2024). Data Security and Individual Privacy from the Perspective of Public Administration. *Ilomata International Journal of Social Science*, *5*(3), 818–830. https://doi.org/10.61194/ijss.v5i3.1297

Sexton, A., Shepherd, E., Duke-Williams, O., & Eveleigh, A. (2017). A balance of trust in the use of government administrative data. *Archival Science*, *17*(4), 305–330. https://doi.org/10.1007/s10502-017-9281-4

Sienkiewicz-Małyjurek, K., & Zyzak, B. (2025). Digital Technologies in Public Administration Networks: Systematic Literature Review and Research Avenues. *Administration & Society*, *57*(8–9), 1051–1087. https://doi.org/10.1177/00953997251369090

Sipahutar, M. Y., & Jannah, L. M. (2023). INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES Personal Data Protection Law in Indonesia: Institutional Challenges. *International Journal of Law Management & Humanities*, *6*(4), 1–17. https://doij.org/10.10000/IJLMH.115352

Sitepu, E. N., Philia, I. T., Simbolon, J. A., Saragih, J., Aulia, N., Purba, R. O., Situmeang, T. A., & Ramadhan, T. (2025). Tinjauan Yuridis Sengketa Informasi Publik dalam Administrasi Negara: Studi Kasus Putusan PTUN Nomor 410/G/KI/2024/PTUN.JKT. *JOURNAL OF ADMINISTRATIVE AND SOCIAL SCIENCE*, *6*(1), 34–46. https://doi.org/10.55606/jass.v6i1.1835

Sjoraida, D. F. (2025). Bureaucratic practices and the struggle for transparency: a case study of public information disclosure policy implementation in West Java, Indonesia. *Asian Anthropology*, *24*(4), 391–395. https://doi.org/10.1080/1683478X.2025.2508603

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*(August), 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Soulthoni, H. P. N., & Itasari, M. (2025). The Implementation of Electronic-Based Archiving to Accelerate Government Digitalization in Indonesia. *Indonesian Journal of Innovation and Applied Sciences (IJIAS)*, *5*(1), 49–57. https://doi.org/10.47540/ijias.v5i1.1735

Suhardi, M. (2025). STATE RESPONSIBILITY IN PERSONAL DATA PROTECTION WITHIN THE ELECTRONIC-BASED GOVERNMENT SYSTEM. *Jurnal Kecerdasan Buatan Dan Teknologi Informasi*, *4*(3), 292–302. https://doi.org/10.69916/jkbti.v4i3.458

Sulaeman, D., Fatra, F., Syah, M. G. F., Qori, I. M., & Lubis, M. (2026). *Privacy and Data Protection Governance for Implementing Indonesia ' s Personal Data Protection Law (Law No . 27 / 2022): A Structured Literature Review*. *4*(1), 8–17. https://doi.org/10.62123/enigma

Tan, W., Karo, R. P. P. K., Situmeang, A., Rusdiana, S., & Razak, S. S. A. (2025). Protection of Public Services Personal Data in The Delivery of Public Services: Comparative Study in Indonesia and Malaysia. *SASI*, 33–43. https://doi.org/10.47268/sasi.v31i1.2415

Torraco, R. J. (2005). Writing Integrative Literature Reviews: Guidelines and Examples. *Human Resource Development Review*, *4*(3), 356–367. https://doi.org/10.1177/1534484305278283

Torraco, R. J. (2016). Writing Integrative Literature Reviews. *Human Resource Development Review*, *15*(4), 404–428. https://doi.org/10.1177/1534484316671606

van Popering-Verkerk, J., Molenveld, A., Duijn, M., van Leeuwen, C., & van Buuren, A. (2022). A Framework for Governance Capacity: A Broad Perspective on Steering Efforts in Society. *Administration & Society*, *54*(9), 1767–1794. https://doi.org/10.1177/00953997211069932

Vieira, K. M., dos Reis Lehnhart, E., Battistella, L. F., Alves, J. N., da Silva Zonatto, V. C., Ravanello, R. P., & Flôres, F. D. (2026). PS-DigQual: scale development and validation for digital public service quality. *Quality and Quantity*, *60*(5), 15465–15495. https://doi.org/10.1007/s11135-026-02790-2

Wahyudi, H., Maulana, J., & Rosidin, A. (2026). Administrative Discretion and the Risk of Abuse of Authority in Indonesian Public Administration. *LEGAL BRIEF*, *15*(2), 156–167. https://doi.org/10.35335/legal.v15i2.1648

Walke, F., & Winkler, T. J. (2025). Assessing Omnichannel Service Quality in the Public Sector. *Public Administration*, *103*(2), 581–599. https://doi.org/10.1111/padm.13038

Warthon, M. (2024). Restricting access to AI decision-making in the public interest: The justificatory role of proportionality and its balancing factors. *Internet Policy Review*, *13*(3). https://doi.org/10.14763/2024.3.1801

Whittemore, R., & Knafl, K. (2005). The integrative review: updated methodology. *Journal of Advanced Nursing*, *52*(5), 546–553. https://doi.org/10.1111/j.1365-2648.2005.03621.x

Yan, Z., & Zhang, M. (2022). Protection of Personal Information in Government Information Disclosure Based on the Administrative Regulation Perspective. *BCP Social Sciences & Humanities*, *19*, 434–443. https://doi.org/10.54691/bcpssh.v19i.1726

Yang, W. (2026). Institutional Pressures and Bureaucratic Responsiveness: Why Do Public Agencies Respond to Freedom of Information Requests? *Public Administration Review*, *86*(2), 354–370. https://doi.org/10.1111/puar.70013

Yani, R. A. W., & Susanto, T. D. (2026). The effect of internal policies, application development, knowledge management, risk management, and information security management on electronic based administrative and public services in Indonesia: A Systematic Literature Review. *Procedia Computer Science*, *284*, 428–435. https://doi.org/10.1016/j.procs.2026.07.021

Policy and Regulatory Sources

Instruksi Presiden Republik Indonesia Nomor 9 Tahun 2025 tentang Percepatan Pembentukan Koperasi Desa/Kelurahan Merah Putih.

Peraturan Menteri Koperasi Republik Indonesia Nomor 2 Tahun 2025 tentang Pengembangan Koperasi Desa/Kelurahan Merah Putih.

Peraturan Gubernur Kalimantan Barat Nomor 23 Tahun 2025 tentang dukungan dan pelaksanaan kebijakan Koperasi Desa/Kelurahan Merah Putih.