Journal of International Islamic Law, Human Right and Public Policy
(JISHUP Journal) | ISSN (e): 3031-2280
Website https://jishup.org/index.php/ojs/index | Volume 4 No. 1 (2026)

LEGAL ACCOUNTABILITY FOR PERSONAL DATA BREACHES IN DIGITAL PUBLIC SERVICES IN WEST JAVA

Berna Sudjana Ermaya
Universitas Pasundan, Bandung, Indonesia
E-mail: berna.ermaya@unpas.ac.id

Received: 06/03/2026 | **Revised:** 09/03/2026 | **Accepted:** 28/03/2026 | **Published:** 30/03/2026

Abstract

The integration of digital public services raises a legal accountability problem when personal data move across government agencies and technology providers. This article examines the allocation of responsibility for personal data breaches in West Java, the relationship between administrative, compensatory, and criminal consequences, and the safeguards needed to make accountability effective. The study employs normative legal research through statutory and conceptual approaches, supported by scholarly literature and official documents concerning West Java's digital services. The analysis finds that responsibility must follow each actor's authority over processing purposes, instructions, and security arrangements. Outsourcing does not automatically release a public institution from its obligations, while a processor may bear responsibility for processing beyond authorized instructions. Breach notification, documented compliance, and accessible remedies connect preventive obligations with subsequent enforcement. Public-interest exceptions require a specific statutory justification and cannot be treated as general immunity. This article proposes a framework linking responsibility allocation, evidence preservation, coordinated incident handling, and citizen redress. It concludes that accountable digital public services require a demonstrable chain of legal responsibility throughout the processing lifecycle. The findings constitute doctrinal conclusions rather than an empirical assessment of breaches or institutional compliance in West Java.

Keywords: Digital public services; Legal accountability; Personal data breaches; Public administration; West Java.

INTRODUCTION

Digital public services change how citizens encounter the state. Applications for permits, education assistance, public complaints, and administrative documents increasingly depend on electronic systems that collect and exchange personal information. These arrangements can reduce repeated submissions and simplify access to government services. They also create a legal problem: when information is exposed, altered, lost, or accessed without authorization, citizens need to know which institution must explain the incident, restore protection, and respond to the resulting harm.

The public sector occupies a distinctive position in this relationship. Individuals may submit personal information because it is necessary to obtain a service or comply with a legal requirement. Their ability to refuse processing is consequently different from the choice available in many commercial transactions. Rahman (2025) identifies the frequently mandatory character of public-sector data collection and the risks associated with expansive interpretations of statutory exceptions. These characteristics strengthen the need to connect administrative authority with enforceable duties toward data subjects.

West Java provides a relevant setting for examining this issue. The provincial government describes Sapawarga as an integrated application through which residents can access public services, information, and channels for communicating public aspirations. Its official description establishes the existence of a digital service environment involving several administrative functions. However, a public-facing application does not, by itself, disclose the complete allocation of legal responsibility among the institutions and providers supporting each function (Government of West Java, n.d.). jabarprov.go.id Integration therefore raises questions beyond the security of an individual application. A service may involve an institution responsible for eligibility decisions, another unit operating shared infrastructure, and an external provider maintaining software. These participants do not necessarily

have identical authority over personal data. Treating all of them as interchangeable obscures the distinction between deciding why information is processed and carrying out processing on another party's instructions. Indonesia's Law No. 27 of 2022 on Personal Data Protection provides the principal statutory framework for addressing these relationships. It regulates data-subject rights, processing grounds, controller and processor obligations, administrative sanctions, dispute resolution, and criminal prohibitions. Its relevance to digital public services lies in its ability to connect institutional processing activities with identifiable legal duties (Republic of Indonesia, 2022).

Nevertheless, the existence of legislation does not resolve every question of attribution. Responsibility may become difficult to establish when decision-making authority, system operation, and incident evidence are distributed across organizations. Thompson et al. (2015) demonstrate that public-sector information problems can arise from inadequate data governance rather than technology alone. Their findings support examining who makes processing decisions, who supervises access, and which records allow those decisions to be reviewed.

Earlier scholarship has addressed public-sector data protection, supervisory independence, and comparative accountability mechanisms. Rahman (2025) examines the implications of Indonesia's personal data protection legislation for public institutions. Widiatedja and Mishra (2023) emphasize the importance of organizationally and functionally independent supervision. Badriah et al. (2024) discuss accountability through the comparison of Indonesian, South Korean, and Singaporean policies. These studies provide a foundation for examining how legal duties operate within an integrated provincial service environment.

The contribution of this article is to connect those discussions through the attribution of responsibility after a breach. Its central argument is that accountability requires a traceable relationship between processing authority, the applicable obligation, evidence of performance or failure, and an appropriate remedy. The analysis applies this argument to West Java's documented digital service context without assuming that a particular institution has experienced a proven breach.

LITERATURE REVIEW

Accountability as an Institutional Relationship

Accountability concerns more than the existence of an organizational commitment to comply with the law. Bovens (2007) conceptualizes it as a relationship in which an actor must explain and justify conduct before a forum capable of questioning, evaluating, and attaching consequences to that conduct. This perspective helps distinguish a general statement of responsibility from an arrangement through which responsibility can actually be examined.

Applied to digital public services, this approach directs attention to the institution making processing decisions, the information needed to evaluate those decisions, and the body authorized to review them. A statement that a system follows privacy principles remains incomplete if affected individuals cannot identify the responsible institution or obtain a reasoned response following an incident.

The framework also clarifies the relationship between internal and external accountability. Internal controls can identify operational failures and support corrective action. External review becomes necessary when the institution's explanation is contested or when a legal consequence requires a competent authority. Neither arrangement can perform effectively without reliable documentation.

Public-Sector Processing and the Public Interest

Public authorities process information for purposes connected to statutory responsibilities. That connection does not make every proposed use necessary or proportionate. Black and Stevens (2013) explain that public-sector processing requires careful consideration of the relationship between a legitimate public purpose, the necessity of processing, and the interests of the individuals concerned.

This reasoning is particularly relevant where several services share a common platform. Information collected for one administrative purpose may become technically available to another unit. Technical accessibility does not establish that the second use has an appropriate legal basis. The justification must concern the actual processing activity rather than the general desirability of integrated government.

Rahman (2025) further shows why statutory exceptions deserve close attention in Indonesia. Public institutions may interpret public-interest provisions broadly, potentially weakening the protection that legislation otherwise provides. For the present analysis, this concern supports a requirement for an identifiable legal justification whenever an institution restricts a data-subject entitlement or relies on an exception to a controller obligation.

OPEN ACCESS

Data Governance and Responsibility Attribution

Data governance concerns the allocation of authority and responsibilities over information throughout its use. Thompson et al. (2015) illustrate how inadequate governance can undermine the reliability and traceability of public-sector information systems. The relevance of their study lies in the connection between operational arrangements and the ability to determine who was responsible for particular actions.

Wu (2014) examines personal data protection in electronic government across different national settings. The study highlights the need for legal arrangements that respond to public-sector information practices. Its comparative perspective supports treating digital government as an institutional environment requiring dedicated safeguards rather than assuming that general technological progress produces adequate protection.

These studies suggest that an accountability analysis should follow the processing activity. Organizational names and procurement labels provide starting points, but they do not conclusively determine who controls a particular use of personal information. The practical distribution of authority must be examined alongside the relevant legal definitions.

Supervision and Accessible Remedies

Supervisory independence matters because public institutions can become the subjects of data protection scrutiny. Widiatedja and Mishra (2023) argue that meaningful protection in Indonesia requires an authority with both organizational and functional independence. Their argument concerns the credibility of oversight where the state is simultaneously a regulator and a major processor of personal information.

Badriah et al. (2024) complement this discussion by connecting accountability with reporting arrangements, sanctions, and compensation mechanisms. Their analysis indicates that legal protection depends on the relationship between substantive duties and the processes through which failures are addressed.

The remaining question is how these elements should be connected within an integrated service arrangement. This article addresses that question through a framework linking authority, obligations, evidence, and remedies. It uses the literature to evaluate the coherence of legal responsibility rather than to claim an empirically demonstrated level of compliance in West Java.

METHOD

This study employs normative legal research using statutory and conceptual approaches. The statutory approach examines the relationship between personal data protection obligations, electronic system governance, public service responsibilities, and relevant West Java regulations. The conceptual approach draws on accountability, proportionality, and data governance scholarship to interpret responsibility within services supported by multiple organizations.

The principal legal material is Law No. 27 of 2022 on Personal Data Protection. Supporting instruments include Law No. 25 of 2009 on Public Services, Law No. 14 of 2008 on Public Information Disclosure, Government Regulation No. 71 of 2019 on the Operation of Electronic Systems and Transactions, and Presidential Regulation No. 95 of 2018 on Electronic-Based Government Systems. The regional context is examined through West Java Provincial Regulation No. 4 of 2021 and Governor Regulation No. 41 of 2022.

Constitutional Court Decision No. 151/PUU-XXII/2024 is considered because it affects the interpretation of the appointment requirements for officials or personnel performing personal data protection functions. The Court held that the conjunction in Article 53(1)(b) must be understood as "and/or," addressing an interpretation that treated the listed conditions as cumulative (Constitutional Court of the Republic of Indonesia, 2025). Mahkamah Konstitusi RI

Official descriptions of Sapawarga are used to establish the provincial service context. They are not treated as evidence of the application's complete technical architecture, contractual arrangements, or compliance performance. Scholarly sources are selected for their relevance to public-sector processing, accountability, data governance, and institutional supervision.

The analysis proceeds by identifying the processing actors, determining their applicable obligations, distinguishing the legal consequences of different failures, and evaluating the evidence necessary for review. Interpretive findings are separated from recommendations for institutional practice. Proposed safeguards are therefore presented as the article's normative recommendations unless a specific statutory provision establishes the obligation.

Developments reported during 2026 are treated cautiously. An official BPOM publication reports preparations concerning Government Regulation No. 33 of 2026. Because its complete authenticated text was not examined for

OPEN ACCESS

this study, the article does not attribute detailed obligations, commencement provisions, or enforcement procedures to that instrument (Badan Pengawas Obat dan Makanan, 2026). The substantive analysis remains anchored in the verified statutory provisions identified above.

No interviews, questionnaires, incident logs, or unpublished contracts form part of the research material. The study consequently does not determine the occurrence, frequency, or causes of actual breaches in West Java. Its findings concern the interpretation and organization of legal accountability within the documented regulatory and service context.

RESULTS AND DISCUSSION

Allocating Responsibility Across Digital Public Service Participants

The first finding is that responsibility should be attributed according to authority over the relevant processing activity. Under the Personal Data Protection Law, the distinction between controllers and processors is central to this assessment. An institution's role must be connected to its decisions about processing purposes and its relationship with parties carrying out processing activities (Republic of Indonesia, 2022, Article 1).

A public institution that determines the information required for a service and the purpose for which it will be used cannot assume that responsibility moves entirely to a software provider. Article 51(3) places processing performed through an appointed processor within the controller's responsibility. Outsourcing therefore changes the operational arrangement without automatically eliminating the public institution's statutory obligations.

The provider's position also requires careful examination. Processing must follow the controller's instructions, and the involvement of another processor requires written approval under the conditions established by Article 51. Where processing exceeds the controller's instructions and specified purposes, Article 51(6) attributes responsibility for that processing to the processor. Article 52 additionally extends specified obligations to processors (Republic of Indonesia, 2022).

These provisions support an activity-specific analysis. A technology provider should not be classified solely by the wording of a procurement contract. If it uses information for a purpose outside authorized instructions, the legal assessment must address that conduct. Conversely, the fact that an incident occurs within infrastructure operated by a vendor does not establish that every relevant failure originated with that vendor.

For West Java's integrated services, the practical implication is the need for documented responsibility at the level of each service function. The official Sapawarga description indicates the presence of several public service categories, but it does not establish which institution determines every processing purpose. Any assessment of an actual incident would therefore require further evidence concerning institutional mandates, processing arrangements, and the affected information flow.

The provincial government, a city or regency institution, and an external provider should not be presumed to share identical responsibilities merely because residents access their functions through one interface. Their respective duties must be determined from the applicable law and facts. This approach prevents a common accountability problem: a unified service experience accompanied by an unclear chain of institutional explanation.

Table 1. Principal Accountability Issues in Digital Public Services

Issue	Relevant legal basis	Implication for accountability
Responsibility for processing decisions	Personal Data Protection Law, Article 1	Identify the actor determining the relevant processing purposes and control.
Processing through an appointed provider	Article 51(1)–(3)	Appointment of a processor does not automatically remove controller responsibility.
Additional processors	Article 51(4)–(5)	Examine authorization and the documented processing chain.
Processing beyond instructions	Article 51(6)	Assess the processor's responsibility for the unauthorized processing activity.
Demonstration of compliance	Article 47	Require records that allow compliance to be evaluated.
Protection functions within organizations	Articles 53–54, read with the Constitutional Court decision	Ensure the relevant protection function is appointed and able to perform its duties.

OPEN ACCESS

Preventive Duties and the Evidence Needed to Assess Compliance

Legal accountability begins before a breach occurs. Security arrangements, processing records, access permissions, and supervision determine both the level of protection and the quality of evidence available after an incident. Article 47 is especially significant because it requires controllers to take responsibility for processing and demonstrate compliance with personal data protection principles (Republic of Indonesia, 2022).

Demonstration requires more than producing a privacy notice. A notice explains aspects of the relationship with the data subject, while compliance evidence concerns what the institution actually does. An assessment may require processing records, authorization documents, access histories, security assessments, and records of corrective action. The appropriate evidence depends on the particular obligation under examination.

Risk assessment provides a further connection between prevention and accountability. Article 34 requires a personal data protection impact assessment for processing with a high potential risk to data subjects. In integrated services, the relevant inquiry concerns the processing operation rather than the public value of the application as a whole. Data combination, specific personal information, or decisions with significant consequences may require closer scrutiny under the statutory criteria.

The article recommends incorporating these assessments into service design and procurement review. Before a new function is introduced, the institution should identify the necessary information, authorized recipients, retention arrangements, and likely consequences of misuse. This recommendation translates the legal analysis into an administrative practice; it is not presented as proof that West Java institutions currently lack such arrangements.

The appointment of personnel performing protection functions must also have practical significance. Following the Constitutional Court's interpretation of Article 53, public service processing cannot be excluded from the appointment requirement merely because other listed conditions are absent. The organizational task is then to provide the appointed personnel with sufficient access to relevant decisions and documentation.

Thompson et al. (2015) help explain why this matters. Their public-sector audit analysis connects information problems with deficiencies in governance and traceability. Applied here, the implication is that security controls should support an identifiable administrative decision-making process. When no reliable record shows who authorized access or approved a transfer, both prevention and subsequent legal review become weaker.

Breach Notification and the Limits of Public-Interest Exceptions

A failure of personal data protection is broader than the publication of information on the internet. The elucidation of Article 46 encompasses failures affecting confidentiality, integrity, and availability, including relevant loss, alteration, destruction, disclosure, or unauthorized access. An institution must therefore assess the nature of an incident before describing it as a routine technical disruption.

Article 46 establishes written notification within a maximum of three times twenty-four hours to the affected data subjects and the designated institution. The prescribed content concerns the exposed information, when and how the exposure occurred, and the controller's handling and recovery measures. The provision also requires public notification in certain circumstances (Republic of Indonesia, 2022). peraturan.bpk.go.id

This obligation should be supported by an internal escalation process. Technical staff need a clear route for informing responsible officials when an incident may affect personal information. Legal personnel should assess the notification obligation while the incident team investigates the facts. The institution should record when relevant information became available and distinguish established facts from matters still under investigation.

The statutory exceptions require separate attention. Article 50 identifies particular obligations that may be excepted for specified interests and requires the exception to operate in implementing statutory provisions. Its reference to Article 46(1)(a) concerns notification to data subjects; it does not list Article 46(1)(b), which concerns notification to the institution. The scope of an exception must therefore be examined at the level of the particular provision.

The interpretive conclusion is that a general reference to public interest is insufficient to establish comprehensive immunity. A public body should identify the statutory basis, the obligation affected, and the connection between disclosure and the protected interest. This reasoning is consistent with Black and Stevens's (2013) emphasis on necessity and proportionality, although their analysis arises from a different legal setting.

Communication should also enable protective action. Affected residents need a comprehensible explanation of the information involved, the measures taken, and the available contact channel. Publishing technical details that expose additional vulnerabilities may be inappropriate, but withholding useful information requires a lawful justification. Institutional embarrassment does not itself establish such a justification.

OPEN ACCESS

Public information disclosure obligations should be considered alongside privacy protection. Law No. 14 of 2008 contains a framework for disclosure and exceptions, including protection concerning personal information. The article therefore recommends publishing appropriately aggregated information about incident handling and corrective action while protecting affected individuals from further exposure (Republic of Indonesia, 2008).

Distinguishing Administrative, Compensatory, and Criminal Consequences

The second major finding is that different forms of legal accountability must be assessed separately. An incident may reveal a failure to fulfil a processing obligation without establishing every element necessary for compensation or a criminal conviction. Conversely, recovery of the system does not necessarily resolve the legal consequences of an earlier violation.

Administrative accountability concerns compliance with statutory duties. Article 57 provides sanctions for specified violations and identifies written warnings, temporary suspension of processing, deletion or destruction of personal data, and administrative fines. Applying a particular consequence requires attention to the violated provision, the competent authority, and the governing procedure (Republic of Indonesia, 2022).

For a public service, corrective action should also consider continuity. Restricting an unsafe processing operation may be necessary, while an indiscriminate interruption could obstruct essential services. The article recommends identifying which functions can continue safely and which require temporary restrictions. This is a proposal for proportionate implementation, not an assertion that every incident permits the same administrative response.

Compensatory accountability addresses harm experienced by the data subject. Article 12 recognizes the right to bring a claim and obtain compensation for violations involving the processing of personal data. Article 64 provides a framework for dispute settlement. These provisions establish an avenue for redress without determining the outcome of every possible claim.

A compensation assessment must examine the relevant violation, the claimed injury, the connection between them, and the applicable evidentiary requirements. A resident's allegation of financial loss or other harm should be investigated rather than automatically accepted or dismissed. The existence of a breach is a starting point for analysis, not a substitute for determining the legal basis and extent of compensation.

Criminal accountability concerns conduct satisfying the statutory elements of an offence. Articles 65–68 address prohibited conduct involving personal data and the corresponding offences. Unauthorized acquisition, disclosure, use, or falsification must be assessed according to the specific prohibition and required mental elements. A security incident alone does not establish an official's or provider's criminal guilt.

This distinction is particularly important when a third party attacks a public system. The attacker's conduct and the service provider's compliance are separate subjects of inquiry. Criminal investigation of unauthorized access does not remove the need to examine whether the controller fulfilled its own obligations. Equally, identifying weaknesses in institutional governance does not establish that an individual committed an intentional personal data offence.

Table 2. Distinct Purposes of Legal Accountability

Form	Principal inquiry	Relevant material	Potential legal response
Administrative	Was a specified processing or protection obligation violated?	Compliance records, instructions, assessments, notification documents	Statutory sanctions and corrective measures
Compensatory	Does a legally supportable claim connect a violation with compensable harm?	Evidence of the violation, injury, and relevant causal connection	Compensation or another legally available remedy
Criminal	Does the conduct satisfy the elements of a personal data offence?	Evidence of prohibited conduct, attribution, and required mental elements	Criminal proceedings and penalties where proved

Source: Author's synthesis of Republic of Indonesia (2022). The evidentiary categories are analytical guidance rather than an exhaustive procedural checklist.

Maintaining these distinctions improves legal precision. Citizens can seek an appropriate remedy without assuming that all proceedings have the same purpose. Institutions can address compliance failures while investigators assess suspected offences. Findings from one process may be relevant to another, but each forum must act within its own authority.

OPEN ACCESS

Making Accountability Work Within West Java's Service Environment

West Java's regional instruments provide an institutional setting for applying national obligations. Provincial Regulation No. 4 of 2021 addresses communication and informatics, statistics, and cryptography. Governor Regulation No. 41 of 2022 concerns the implementation of cryptography for information security within the provincial government. These instruments should be read alongside the Personal Data Protection Law, Government Regulation No. 71 of 2019, and Presidential Regulation No. 95 of 2018.

The regional framework does not remove the need to identify the controller and processor for each activity. Nor should the provincial government automatically be treated as the controller of every service operating geographically within West Java. A service may belong to a provincial institution, a city or regency institution, or another legally distinct public body. Geography establishes the context of the study; it does not settle legal attribution.

The article proposes four connected administrative arrangements. First, each integrated service should maintain a record of processing responsibilities. The record should identify the responsible institution, the purpose and legal basis of processing, participating providers, and the official responsible for coordinating a response. Its purpose is to make the legal relationship understandable before a dispute occurs.

Second, service and procurement agreements should support the fulfilment of statutory duties. Relevant provisions include authorized instructions, access restrictions, additional processor approval, incident escalation, evidence preservation, and the return or deletion of information. Contractual allocation can clarify cooperation and recourse between participants, but it cannot eliminate statutory duties owed to data subjects.

Third, incident handling should preserve both technical and administrative evidence. Investigators may need access histories and system records, while legal review may require approval documents, processing instructions, and notification decisions. Preserving only technical logs can leave unanswered questions about institutional authority. Preserving only administrative correspondence may fail to establish what happened to the information.

Fourth, residents should have an accessible entry point for complaints. They should not be required to understand the full relationship between infrastructure operators, service institutions, and vendors before reporting harm. A coordinated channel can receive the complaint, identify the responsible body, and explain the available next step. Such coordination does not merge the legal identities of the participating institutions.

This proposal connects with Bovens's (2007) accountability relationship by identifying the actor, the explanation required, and the reviewing forum. It also develops Badriah et al.'s (2024) concern with reporting, sanctions, and compensation into an arrangement suitable for integrated services. Its practical value lies in reducing the distance between a statutory right and an institution capable of responding to it.

Independent scrutiny remains essential. Internal assessment can support prompt correction, but it cannot substitute for review by a competent external body where the law provides that avenue. Widiatedja and Mishra's (2023) argument for functional independence is relevant because the credibility of an explanation depends partly on whether it can be questioned outside the institution responsible for the processing.

Contribution and Limitations

The article's contribution is an integrated account of how processing authority, compliance evidence, and remedies should relate to one another. It develops accountability as a chain that can be examined throughout the processing lifecycle. The central question becomes whether a responsible actor can explain a particular activity through reliable evidence before a competent forum.

Its geographic application is limited to the documented West Java regulatory and service context. No conclusion is drawn about the performance of a particular agency, the security of Sapawarga, or the prevalence of personal data breaches. Establishing those matters would require additional material, including incident records, contracts, technical assessments, and interviews with relevant officials.

Further research should examine whether responsibility records, notification procedures, and complaint arrangements operate as described in institutional documents. It should also assess subsequent implementing legislation through authenticated texts. Such work would test the proposed framework against actual practice while preserving the distinction between doctrinal interpretation and empirical findings.

CONCLUSION

Legal accountability for personal data breaches in West Java's digital public services should follow each participant's authority and conduct within the processing activity. A public institution cannot automatically transfer its statutory responsibility by appointing a technology provider, while a processor's unauthorized activity requires a

OPEN ACCESS

separate assessment. Administrative sanctions, compensation, and criminal proceedings serve different purposes and depend on their respective legal requirements. Notification duties and public-interest exceptions must be interpreted with attention to the particular statutory provision rather than through assumptions of institutional immunity. The article proposes documented responsibility allocation, enforceable processing arrangements, coordinated incident handling, evidence preservation, and accessible complaint channels as connected safeguards. These measures would make it easier to identify who must explain an incident, which records support that explanation, and where affected residents can seek review. The conclusions remain normative and do not establish that a breach or compliance failure has occurred within any particular West Java institution.

REFERENCES

Badan Pengawas Obat dan Makanan. (2026, September 15). BPOM perkuat kesiapan penerapan pelindungan data pribadi. https://pusdatin.pom.go.id/berita/bpom-perkuat-kesiapan-penerapan-pelindungan-data-pribadi

Badriah, L., Indiahono, D., & Sukarso. (2024). Accountability in personal data protection policy in Indonesia: Learning from South Korea and Singapore. Matra Pembaruan: Jurnal Inovasi Kebijakan, 8(2), 89–102. https://doi.org/10.21787/mp.8.2.2024.89-102

Black, G., & Stevens, L. (2013). Enhancing data protection and data processing in the public sector: The critical role of proportionality and the public interest. SCRIPTed, 10(1), 93–122. https://doi.org/10.2966/scrip.100113.93

Bovens, M. (2007). Analysing and assessing accountability: A conceptual framework. European Law Journal, 13(4), 447–468. https://doi.org/10.1111/j.1468-0386.2007.00378.x

Constitutional Court of the Republic of Indonesia. (2025). Decision No. 151/PUU-XXII/2024 concerning the judicial review of Law No. 27 of 2022 on Personal Data Protection. July 30, 2025.

Government of West Java. (n.d.). Aplikasi Sapawarga. Retrieved October 29, 2026, from https://jabarprov.go.id/sapawarga

Province of West Java. (2021). Peraturan Daerah Provinsi Jawa Barat Nomor 4 Tahun 2021 tentang Penyelenggaraan Komunikasi dan Informatika, Statistik, dan Persandian. https://jdih.jabarprov.go.id/page/info/produk/25581

Province of West Java. (2022). Peraturan Gubernur Jawa Barat Nomor 41 Tahun 2022 tentang Peraturan Pelaksanaan Persandian untuk Pengamanan Informasi di Lingkungan Pemerintah Daerah Provinsi Jawa Barat. https://peraturan.bpk.go.id/Details/259115/pergub-prov-jawa-barat-no-41-tahun-2022

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

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

Republic of Indonesia. (2008). Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik. https://peraturan.bpk.go.id/Details/39047/uu-no-14-tahun-2008

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

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

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

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

Thompson, N., Ravindran, R., & Nicosia, S. (2015). Government data does not mean data governance: Lessons learned from a public sector application audit. Government Information Quarterly, 32(3), 316–322. https://doi.org/10.1016/j.giq.2015.05.001

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

OPEN ACCESS

Wu, Y. (2014). Protecting personal data in E-government: A cross-country study. Government Information Quarterly, 31(1), 150–159. https://doi.org/10.1016/j.giq.2013.07.003

OPEN ACCESS