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 1 No. 3 (2023)

LEGAL SAFEGUARDS FOR PERSONAL DATA SHARING BETWEEN GOVERNMENT AGENCIES IN WEST JAVA

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

Received: 02/09/2023 | **Revised:** 08/09/2023 | **Accepted:** 25/09/2023 | **Published:** 30/09/2023

Abstract

Data sharing between government agencies can improve administrative coordination while exposing personal information to processing beyond its original purpose. This article examines the legal safeguards governing interagency personal data sharing in West Java within the regulatory framework applicable through 2023. Normative legal research combines statutory and conceptual approaches, drawing on national legislation, provincial regulations, and relevant scholarship. The analysis distinguishes institutional authority to perform a public function from authorization to disclose particular personal information. It finds that lawful sharing requires an identifiable processing basis, a specific purpose, appropriate allocation of controller responsibilities, and safeguards proportionate to the information and risks involved. Data governance roles under Satu Data arrangements do not automatically determine controller or processor status. Likewise, interoperability and simplified access procedures do not displace statutory personal data protection duties. The article develops a framework connecting authorization, limited disclosure, secure exchange, recipient accountability, and subsequent review. It concludes that interagency cooperation should preserve a demonstrable chain of responsibility throughout the information flow. These findings establish a doctrinal framework rather than evidence that particular agencies have complied with or violated the applicable requirements.

Keywords: Data sharing; Government agencies; Legal safeguards; Personal data protection; West Java.

INTRODUCTION

Government agencies increasingly need information held by other institutions to perform public functions. A resident applying for a service may reasonably expect the administration to verify relevant information without repeatedly requesting the same documents. Coordinated information use can reduce duplication, improve accuracy, and support timely decisions. However, those benefits depend on a legally defensible relationship between the purpose of the requesting agency and the information disclosed by the supplying institution. The ability to connect systems does not, by itself, answer whether a particular exchange is authorized or whether its scope is justified.

Personal data sharing creates a distinctive accountability problem because information moves beyond the institution with which the individual initially interacted. Once received elsewhere, it may enter another database, become available to additional personnel, or support a different administrative decision. Each movement can change the practical conditions of protection, even where all participating organizations belong to government. Otjacques et al. (2007) identify privacy, identification, and organizational issues associated with interoperability in electronic government. Their analysis helps explain why information exchange requires attention to institutional relationships alongside technical compatibility.

In Indonesia, Satu Data Indonesia provides an important governance framework for improving the quality and exchange of government data. Presidential Regulation No. 39 of 2019 addresses standards, metadata, interoperability, and reference arrangements, while Presidential Regulation No. 95 of 2018 supplies the broader electronic-government context. These instruments support administrative coordination, but their application must be distinguished from the assessment of whether an identifiable individual's information may be disclosed for a particular purpose. Data governance and personal data protection address connected questions without becoming interchangeable legal frameworks (Republic of Indonesia, 2018, 2019).

OPEN ACCESS

West Java has a regional setting relevant to this relationship. Provincial Regulation No. 4 of 2021 addresses communication and informatics, statistics, and cryptography, while Governor Regulation No. 47 of 2022 establishes implementing arrangements for Satu Data Jawa Barat. The latter recognizes institutional roles and procedures concerning data management and dissemination. Its Article 14 also addresses restrictions on access to certain data and confidentiality arrangements for access to excluded data. These provisions demonstrate that facilitating exchange and controlling access are both relevant to the regional framework; they do not establish unrestricted availability of every government-held record (Province of West Java, 2021, 2022). jdih.jabarprov.go.id

Law No. 27 of 2022 on Personal Data Protection adds requirements directly relevant to exchanges involving personal information. Article 55 addresses domestic transfers between controllers, while Articles 18, 20, and 47 concern arrangements involving multiple controllers, lawful processing grounds, and demonstrated accountability. Their relationship becomes important when an agency relies on its public function or participation in a shared platform to obtain information from another institution. A lawful service objective does not remove the need to examine the particular data, processing arrangement, and safeguards involved (Republic of Indonesia, 2022).

Existing scholarship provides foundations for that examination. Rahman (2021) connects personal data protection with Indonesia's electronic-based government framework, while Thompson et al. (2015) show how weaknesses in governance can undermine public-sector information management. Black and Stevens (2013) examine necessity and proportionality in public-sector processing, and Widiatedja and Mishra (2023) emphasize independent supervision. Building on these contributions, this article examines the legal conditions for interagency sharing, the allocation of responsibility across participating institutions, and the safeguards needed throughout the information flow. Its contribution is a coordinated interpretation of these requirements within West Java's regulatory context through 2023.

LITERATURE REVIEW

Interoperability and the Boundaries of Permissible Sharing

Interoperability enables systems to exchange and use information, but the existence of that capability does not settle the legality of an exchange. Otjacques et al. (2007) examine identification and data sharing in electronic government, demonstrating the importance of privacy and organizational arrangements when institutions cooperate. Their work supports separating the technical question of whether information can move from the legal question of whether it should move for a specified purpose. An interface may function correctly while delivering information to a recipient whose authority, purpose, or access privileges have not been adequately examined.

Wu (2014) similarly situates personal data protection within the institutional environment of electronic government. The comparative study supports examining legal arrangements rather than assuming that increased digital capacity produces effective protection. For interagency sharing, the implication is that processing decisions must remain accountable even where exchange becomes routine or automated. A system that repeatedly supplies information should retain the capacity to identify the recipient, purpose, and applicable restrictions. The present article uses these insights conceptually and does not treat findings from other jurisdictions as evidence of actual practices in West Java.

Public Authority and Proportionality

Government agencies possess legal responsibilities, but the information needed to perform those responsibilities varies by function. Black and Stevens (2013) explain why public-sector processing requires consideration of necessity and proportionality in relation to the public interest. Their analysis is relevant where an agency requests a complete dataset even though its function may require only a limited confirmation. The appropriate inquiry concerns the connection between the requested information and the administrative task. General claims of efficiency should be translated into a specific explanation of what information is required, why it is needed, and how its use will remain bounded.

Personal data protection also addresses the imbalance between the individual and institutions controlling information. Lynskey (2014) explains how data protection rights can reduce information and power asymmetries, although the study concerns the European legal order. This conceptual perspective helps identify what can be lost when information is shared without a clear account of subsequent use. Residents may remain unaware of the recipient or unable to identify the institution responsible for correction. Safeguards should therefore support both justified institutional access and a comprehensible relationship between the individual and the agencies involved.

OPEN ACCESS

Responsibility and Reviewable Information Flows

Accountability becomes difficult when several institutions participate in processing without a clear allocation of duties. Bovens (2007) provides an institutional framework involving explanation, scrutiny, and consequences, while Thompson et al. (2015) connect public-sector information problems with weaknesses in governance and traceability. Together, these studies support documenting responsibility at each stage of an exchange. A supplying agency should be able to explain its disclosure, and a receiving agency should be able to explain subsequent use. Their responsibilities may differ, but the involvement of multiple bodies should not leave the processing activity without an identifiable explanation.

Rahman (2021) and Widiatedja and Mishra (2023) provide Indonesian perspectives on the legal framework and the importance of oversight. These contributions help position interagency sharing within a broader system of institutional obligations and external review. The remaining issue addressed here is how the national personal data protection requirements interact with regional data governance arrangements at the level of an actual information flow. The article develops that relationship by distinguishing authorization, institutional roles, operational controls, and review, rather than treating the existence of a shared platform or cooperation document as conclusive evidence of lawful processing.

METHOD

This study employs normative legal research through statutory and conceptual approaches. Its temporal scope includes legislation and publications available through December 31, 2023, and excludes later implementing measures and judicial developments. The statutory approach examines the interaction between personal data protection, electronic government, interoperability, and West Java's regional data governance arrangements. The conceptual approach draws on proportionality, accountability, and information governance scholarship to interpret the safeguards needed when personal information moves between agencies. This design supports legal analysis without claiming to reconstruct an exchange that has been verified through institutional records.

The principal legal material is Law No. 27 of 2022 on Personal Data Protection. Supporting national instruments include Law No. 14 of 2008 on Public Information Disclosure, Presidential Regulation No. 95 of 2018 on Electronic-Based Government Systems, Presidential Regulation No. 39 of 2019 on Satu Data Indonesia, and Minister of Communication and Informatics Regulation No. 1 of 2023 on interoperability. The regional analysis considers West Java Provincial Regulation No. 4 of 2021 and Governor Regulation No. 47 of 2022. Scholarly publications are selected for their relevance to interagency exchange, public-sector processing, and institutional responsibility.

The analysis first identifies the legal character of the information and proposed exchange, then examines processing authority, institutional roles, protective measures, and subsequent accountability. The tables present an analytical framework and do not report observed practices, compliance scores, or incident frequencies. No unpublished agreements, access logs, technical audits, or interviews form part of the research material. Consequently, conclusions concerning an actual agency's compliance would require additional evidence. Existing statutory duties are distinguished throughout from recommended implementation methods, so that the article does not present every proposed administrative safeguard as an expressly prescribed legal requirement.

RESULTS AND DISCUSSION

Domestic Transfers Require Continuing Protection

The first finding is that sharing personal information between domestic public institutions remains a regulated processing activity. Article 55 permits a controller to transfer personal data to another controller within Indonesia and requires both the transferring and receiving controllers to protect the information in accordance with the Personal Data Protection Law. The provision establishes continuing responsibility on both sides of the transfer. It should therefore be read alongside the requirements governing processing grounds, purposes, security, and accountability rather than treated as a stand-alone authorization for every exchange (Republic of Indonesia, 2022).

An agency's authority to perform a public function and its justification for receiving particular information are related but distinct matters. A legally assigned task may establish a relevant processing basis, yet the institution must still identify the information needed for that task and the scope of the proposed use. The supplying institution likewise needs a defensible explanation for disclosure. This interpretation connects Article 55 with Article 20's processing grounds and Article 16's principles. It avoids assuming that information becomes available for unrestricted reuse merely because the sender and recipient both exercise governmental functions.

OPEN ACCESS

Satu Data Roles and Personal Data Protection Roles

West Java's Satu Data framework identifies roles such as data producers, data custodians, and supporting custodians. These roles organize activities within the regional governance arrangement, but they do not automatically settle controller or processor status for every personal data operation. The relevant assessment must examine the authority exercised over the particular processing activity. An institution's responsibility for distributing a statistical dataset does not, by itself, establish its authority over every identifiable record held by another public body. The regulatory terminology should therefore be connected to the actual function rather than used as an automatic legal classification.

Three relationships require separate consideration. Agencies may exchange information as distinct controllers, jointly determine aspects of processing under an arrangement involving multiple controllers, or use a participant that processes information on instructions. Article 18 establishes minimum conditions for processing involving two or more controllers, including an agreement addressing roles and responsibilities, related purposes and jointly determined processing methods, and a jointly appointed contact person. Articles 51–52 address processors. These requirements should be applied according to the arrangement concerned; participation in the same system does not independently establish that every participant has the same status (Republic of Indonesia, 2022).

Table 1. Distinguishing Institutional Relationships in Interagency Sharing

Relationship	Central legal question	Relevant provision	Implication for responsibility
Transfer between distinct controllers	What processing does each institution control?	Article 55	Both transferring and receiving controllers retain applicable protection duties.
Processing involving multiple controllers	Are the conditions for the arrangement under Article 18 satisfied?	Article 18	Roles, responsibilities, related purposes, processing methods, and contact arrangements require attention.
Processing on another institution's instructions	Does the participant act within the authorized instructions and purposes?	Articles 51–52	Processor obligations apply, while controller responsibility must also be examined.
Performance of a Satu Data governance role	What does the regional role authorize for the particular dataset?	Governor Regulation No. 47 of 2022	The governance role must be distinguished from controller or processor classification.

Source: Author's synthesis of Republic of Indonesia (2022) and Province of West Java (2022).

Purpose Limitation and the Scope of Disclosure

A lawful information flow should begin with an identifiable administrative purpose. Requests framed only as supporting coordination or improving services may be too general to explain why particular personal information is required. The article recommends describing the task, intended use, requested data categories, authorized recipient, and expected duration of access before an exchange begins. These records make the decision reviewable and support the statutory processing principles. They are proposed as practical methods of demonstrating justification, rather than as a claim that the legislation prescribes one standardized form for every interagency request.

The scope of disclosure should then be assessed against that purpose. Where a function requires only verification of a particular fact, supplying a complete record may create unnecessary exposure. A limited confirmation can sometimes meet the administrative need, although its own processing still requires a lawful basis and appropriate safeguards. Black and Stevens's (2013) proportionality analysis supports considering less intrusive arrangements when they can achieve the legitimate objective. This article does not establish that one technical design is suitable for all services; it identifies a legal question that should guide design and authorization.

Further use requires renewed attention when the recipient's purpose changes. Information received for one function should not be assumed to support unrelated activities merely because the recipient already holds a copy. The relevant assessment concerns the proposed processing ground, purpose, and applicable restrictions. A documented sharing arrangement can help explain those boundaries, but its wording cannot legalize an activity that lacks the required authority. Likewise, the initial sending institution's justification cannot automatically substitute for the recipient's explanation of a later use. Each institution should remain able to account for the conduct it controls.

OPEN ACCESS

Open Data and Restricted Personal Information

Satu Data arrangements promote accessibility and reuse within their legal scope, but accessibility should not be confused with unrestricted public disclosure. The classification of a dataset matters. Government-held information may consist of aggregate statistics, administrative records concerning identifiable individuals, or information whose combination with other material creates identification risks. Removing a person's name does not necessarily remove the personal character of the information. An assessment should consider the content and context before deciding whether open dissemination, restricted interagency access, or another arrangement is appropriate.

Governor Regulation No. 47 of 2022 provides a concrete regional basis for examining this distinction. Article 14 addresses dissemination, the proposal of access restrictions through the regional Satu Data forum, and confidentiality arrangements for access to excluded data. Its scope must nevertheless be respected: the regulation provides a particular regional data governance framework, not a complete authorization for every exchange of personal administrative records. Law No. 14 of 2008 also contains public information disclosure rules and exceptions concerning personal information. The analytical conclusion is that openness, confidentiality, and personal data protection must be assessed together within the applicable provisions (Republic of Indonesia, 2008; Province of West Java, 2022).

Cooperation Documents Cannot Replace Legal Authority

A cooperation document can clarify responsibilities, permitted activities, security arrangements, and the handling of subsequent requests. However, an agreement is not an independent substitute for a processing basis. The relevant legal question remains whether each institution possesses authority for the particular disclosure or use. This distinction is especially important where the parties rely on general cooperation language that does not identify the data involved. A document may demonstrate that officials agreed to cooperate while leaving unresolved whether the contemplated processing satisfies the Personal Data Protection Law.

Documentary requirements also need to be stated precisely. Presidential Regulation No. 39 of 2019 provides simplified access arrangements for government institutions using the Satu Data Indonesia portal, including access without certain separate cooperation documents. That simplification should not be converted into either a universal obligation to sign a memorandum before every exchange or a universal exemption from all documentation. Article 18 of the Personal Data Protection Law expressly requires an agreement where its conditions apply. The article's interpretation is that portal access procedures and substantive personal data duties must be read according to their respective scope and legal level. Sekretariat Kabinet Republik Indonesia

Security and Traceability During Exchange

The safeguards governing exchange must operate while information is transmitted and after it reaches the recipient. Minister of Communication and Informatics Regulation No. 1 of 2023 provides a particularly relevant instrument because it addresses interoperability within electronic government and Satu Data Indonesia. Its requirements include technical protections and transaction records within the regulated interoperability framework. These provisions connect the ability to exchange information with the capacity to maintain its protection and trace the exchange. A successful connection is therefore only one part of the relevant operational assessment (Ministry of Communication and Informatics, 2023).

The article recommends connecting access permissions to identifiable users or institutional functions, limiting disclosure to authorized purposes, and retaining records that permit appropriate review. Protective measures should reflect the nature of the information and risks involved. A transfer record can help establish who received information and when, but it does not independently prove the lawfulness of the underlying purpose. Equally, a legally justified request does not excuse an insecure method of delivery. Authorization and security are complementary safeguards, and an institution should be able to explain both within the processing activity it controls.

Recipient governance becomes crucial once information enters another system. Copies, downloaded files, and subsequent exports may create additional points of exposure beyond the original interface. Thompson et al. (2015) explain why information governance must address responsibilities and traceability rather than depend solely on the technology used. Applied to sharing, this supports identifying who can authorize onward disclosure, how access is reviewed, and how unnecessary copies are handled. These are proposed implementation questions, not findings that West Java agencies currently lack such arrangements. Their application would require examination of actual practices and records.

OPEN ACCESS

Assessing Risk Before Linking Datasets

Combining datasets can reveal information that was not apparent in either source considered separately. A sharing arrangement may therefore change the risk profile even when each agency originally collected its information lawfully. Article 34 of the Personal Data Protection Law identifies categories of high-risk processing, including relevant data matching or combination activities, for which an impact assessment is required. The assessment of applicability should concern the actual operation rather than the public benefit claimed for the programme. A general assurance that integration improves administration does not answer the statutory risk question (Republic of Indonesia, 2022).

An appropriate review should consider what the linkage enables, which individuals may be affected, and whether the intended purpose can be achieved through a more limited arrangement. It should also examine data quality because incorrect matching may lead to inaccurate administrative conclusions. The resulting record should inform the authorization decision and protective measures, rather than exist only as an attachment produced after implementation. This article recommends reviewing the arrangement again when purposes, recipients, or information categories change materially. Such review supports continuing accountability without assuming that every modification necessarily triggers identical legal requirements.

Table 2. Safeguards Across the Information Flow

Stage	Question requiring resolution	Relevant safeguard	Record supporting review
Request	Why does the recipient need the information?	Specific purpose and appropriate processing basis	Task description and legal justification
Selection	Which information is necessary for that purpose?	Limited and justified disclosure	Requested fields and reasons for inclusion
Authorization	Who may approve disclosure and receipt?	Identifiable institutional responsibility	Approval and role allocation
Exchange	How will authorized information move?	Secure access and traceable transactions	Access permissions and transaction records
Recipient use	What may the recipient do with the information?	Purpose boundaries and controlled onward sharing	Processing instructions or relevant arrangements
Correction	How will inaccurate shared information be addressed?	Coordinated examination and appropriate updates	Correction decisions and follow-up
Retention or closure	What remains necessary after the purpose ends?	Lawful retention, restriction, return, or deletion	Retention justification and completion records

Source: Author's proposed framework informed by Republic of Indonesia (2022), Ministry of Communication and Informatics (2023), and Province of West Java (2022). The listed records are indicative rather than a universal statutory checklist.

Citizens' Rights and Coordinated Institutional Responses

Information sharing should preserve an understandable relationship between residents and the institutions processing their data. A person requesting access or correction may not know which agency supplied the record or which body made a subsequent change. The legal assessment must respect the specific rights and exceptions under the Personal Data Protection Law, while administrative coordination should help identify the institution competent to respond. A shared contact arrangement required under Article 18 can perform an important role where that provision applies, but it should not be presumed to replace the responsibilities of all participating controllers.

Correction requires particular care because an inaccurate record can move through several systems. Updating the source may not automatically update every recipient, while deleting information indiscriminately may conflict with another valid obligation. The article recommends a documented process for examining whether a correction affects previously shared information and what lawful follow-up is necessary. This recommendation concerns coordinated implementation rather than a claim that every correction must trigger the same technical response. Its purpose is to prevent organizational boundaries from leaving an established inaccuracy unresolved within the relevant administrative process.

Incident handling presents a related coordination problem. The parties should be able to identify the affected processing, preserve relevant records, and evaluate applicable notification duties under Article 46. An internal

OPEN ACCESS

arrangement that designates one coordinator should not be assumed to remove another controller's statutory obligations. Bovens's (2007) accountability framework supports a response in which each actor can explain its own conduct before an appropriate forum. Widiatedja and Mishra (2023) additionally underscore the value of external scrutiny when internal explanations are contested. Together, these perspectives support cooperation that clarifies responsibility instead of dispersing it.

Implementation Priorities and Research Limitations

The year 2023 must be understood within the statutory transition. Article 74 allowed a maximum two-year adjustment period from the promulgation of the Personal Data Protection Law, while the law itself entered into force in October 2022. The transition did not establish that existing interagency practices were automatically lawful, nor does the present study determine how any particular agency adjusted them. A defensible implementation approach would examine existing exchanges, identify the relevant processing relationships, and assess whether purposes, access arrangements, and protective measures correspond to the applicable requirements.

For West Java, the main institutional priority is to connect regional data governance with the legal character of each exchange. The Satu Data framework supplies relevant roles and procedures, while the Personal Data Protection Law establishes duties concerning personal information. The proposed approach brings them together without assuming that the regional framework covers every operational database. Its limitations remain substantial: no actual exchange agreements, access records, or risk assessments were evaluated. Empirical research would be needed to establish whether institutions implement these safeguards, how they resolve disputed responsibilities, and what difficulties arise in practice.

CONCLUSION

Legal safeguards for personal data sharing between government agencies in West Java require a justified relationship between administrative authority, the information disclosed, and the recipient's intended use. Within the framework available through 2023, domestic transfers remain subject to protection duties on both sides, while arrangements involving multiple controllers and processors require distinct analysis. Satu Data roles, interoperability, and simplified portal access do not independently determine personal data authority or remove applicable statutory requirements. The article proposes connecting authorization, limited disclosure, secure exchange, recipient governance, correction, and subsequent review throughout the information flow. This approach supports administrative cooperation while preserving a demonstrable chain of responsibility. The conclusions remain doctrinal and do not establish compliance or violations by particular agencies; those findings require examination of actual processing arrangements and institutional evidence.

REFERENCES

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

Lynskey, O. (2014). Deconstructing data protection: The 'added-value' of a right to data protection in the EU legal order. *International & Comparative Law Quarterly, 63*(3), 569–597. https://doi.org/10.1017/S0020589314000244

Ministry of Communication and Informatics. (2023). *Peraturan Menteri Komunikasi dan Informatika Nomor 1 Tahun 2023 tentang Interoperabilitas Data dalam Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik dan Satu Data Indonesia*. https://peraturan.bpk.go.id/Details/255562/permenkominfo-no-1-tahun-2023

Otjacques, B., Hitzelberger, P., & Feltz, F. (2007). Interoperability of e-government information systems: Issues of identification and data sharing. *Journal of Management Information Systems, 23*(4), 29–51. https://doi.org/10.2753/MIS0742-1222230403

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 47 Tahun 2022 tentang Peraturan Pelaksanaan Satu Data Jawa Barat*. https://jdih.jabarprov.go.id/page/info/produk/30532

OPEN ACCESS

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

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. (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 Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia*. https://peraturan.bpk.go.id/Details/108813/perpres-no-39-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

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