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 2 No. 3 (2024)

PERSONAL DATA PROTECTION COMPLIANCE IN LOCAL GOVERNMENT DIGITAL SERVICES IN WEST JAVA

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

Received: 02/09/2024 | **Revised:** 08/09/2024 | **Accepted:** 25/09/2024 | **Published:** 30/09/2024

Abstract

The expansion of local government digital services requires public institutions to demonstrate that personal data processing complies with legal obligations. This article examines the requirements for personal data protection compliance in West Java within the legal framework applicable through 2024. Normative legal research is conducted through statutory and conceptual approaches, supported by scholarly literature and official provincial documentation. The analysis distinguishes the existence of a digital service from evidence that its processing activities meet legal requirements. Compliance requires an identifiable processing basis, purpose limitation, appropriate security, accessible data-subject procedures, and documented responsibility across participating institutions and providers. Service integration does not independently authorize unrestricted data sharing, while outsourcing does not automatically release a controller from statutory obligations. The article develops a compliance assessment framework connecting legal requirements with records that can support institutional review. It also proposes incorporating privacy review into service planning, procurement, operation, and incident response. The study concludes that compliance should be assessed through the relationship between applicable duties and demonstrated implementation. Its findings establish a normative assessment framework rather than measured compliance levels or verified violations among local governments in West Java.

Keywords: Compliance; Digital public services; Local government; Personal data protection; West Java.

INTRODUCTION

Local government digital services increasingly depend on personal information. Residents provide identity details, contact information, and supporting documents when applying for administrative services, accessing public programmes, or submitting complaints. Electronic processing can simplify these transactions, but it also places responsibility on public institutions to justify how information is collected, used, shared, and retained. The legal issue extends beyond preventing unauthorized access. Information may be stored securely while being collected without a sufficient processing basis, used beyond its original purpose, or retained longer than justified. Personal data protection compliance therefore requires examination of the whole processing activity rather than an assessment of cybersecurity alone. West Java provides a relevant setting for this inquiry. An official provincial publication dated May 27, 2024, described Sapawarga as an integrated application supporting access to several public services. The publication emphasized simplification and the optimization of existing applications as part of the provincial government's digital service direction (Government of West Java, 2024). This documented policy context raises an important question: how should institutions demonstrate compliance when a service involves several administrative functions? A common interface may make the service easier to use without making institutional responsibilities equally clear. Residents may interact with one application while their information is processed by different government units and technology providers. Each participant may perform a distinct function, making it necessary to identify who determines processing purposes, who carries out instructions, and who responds when a legal obligation is not fulfilled. Indonesia's Law No. 27 of 2022 on Personal Data Protection supplies the principal framework for examining those questions. It establishes processing grounds, data-subject rights, controller and processor obligations, accountability requirements, and legal consequences. These provisions make personal data protection a matter of institutional conduct supported by evidence, rather than a general assurance that an application

is safe (Republic of Indonesia, 2022). The year 2024 represents an important point in that framework. Article 74 established a maximum two-year adjustment period following promulgation on October 17, 2022. The law itself entered into force upon promulgation; the adjustment period should therefore be distinguished from its commencement. By the end of the period in October 2024, institutions were expected to have adjusted their processing arrangements to the statutory requirements. Research on digital government helps explain why this adjustment involves organizational decisions. Mergel et al. (2019) describe digital transformation as a broader change in public-sector processes and relationships. Their analysis supports examining whether the introduction of technology is accompanied by changes in responsibilities, decision-making procedures, and institutional capacity.

Personal data protection scholarship identifies related concerns. Rahman (2021) examines the legal framework for protecting personal information in Indonesia's electronic-based government system. Thompson et al. (2015) demonstrate how weaknesses in public-sector data governance can affect the reliability and traceability of information. Widiatedja and Mishra (2023) emphasize the importance of independent supervision in Indonesia. Building on these studies, this article develops a framework for examining compliance in West Java's local government digital services. It addresses three questions: which legal requirements should guide compliance assessment, what evidence can support an assessment of implementation, and how can compliance be incorporated into ordinary service governance? Its contribution is the connection between legal obligations and reviewable institutional practices, without claiming to have measured the performance of particular local governments.

LITERATURE REVIEW

Compliance as Demonstrated Institutional Conduct

Compliance concerns whether conduct conforms to applicable legal requirements. In personal data protection, the adoption of a policy is relevant but does not establish that every processing activity follows that policy. An assessment must connect the rule with the activity and the evidence available to evaluate it. Bovens (2007) provides a useful conceptual foundation by examining accountability as a relationship involving explanation, scrutiny, and consequences. Applied to compliance, this perspective suggests that institutions should be able to explain their processing decisions before a competent reviewing body. Documentation serves that relationship when it records actual decisions and actions. A processing inventory, for example, becomes useful when it accurately identifies the information being used, the purpose of processing, and the responsible institution. Its existence alone does not establish the lawfulness of those activities.

Digital Transformation and Data Governance

Digital transformation changes administrative processes as well as their technological form. Mergel et al. (2019) show why an organizational perspective is necessary when examining public-sector digitalization. Personal data compliance belongs within that perspective because processing decisions arise throughout service design and delivery. Thompson et al. (2015) connect public-sector information problems with weaknesses in governance. Their findings support examining who authorizes access, who maintains records, and how institutional decisions can be traced. These issues matter when a service combines information from several administrative sources. Wu (2014) further demonstrates the relevance of legal arrangements to personal data protection in electronic government. The study's comparative perspective supports distinguishing technological development from the institutional safeguards needed to govern information practices.

Public Authority and Proportionate Processing

Public institutions process information to perform legally assigned functions. However, a general administrative mandate does not establish that every proposed collection or transfer is justified. Black and Stevens (2013) examine public-sector processing through the relationship between necessity, proportionality, and public interest. This approach directs attention to the specific activity. The question is whether the information is needed for an identifiable purpose and whether its use is proportionate to that purpose. Technical convenience should not replace the legal explanation. Rahman (2021) places personal data protection within Indonesia's electronic government framework. Read alongside the subsequent Personal Data Protection Law, the study provides a basis for examining how sectoral administrative arrangements should relate to broader processing safeguards.

Organizational Measures and Supervision

Tikkinen-Piri et al. (2018) examine the organizational implications of European data protection requirements for companies. Their study arises from a different jurisdiction and sector, but it illustrates why compliance may

OPEN ACCESS

require changes to policies, responsibilities, and operational practices. It does not establish that European requirements automatically apply to West Java's local governments. Supervision supplies another dimension. Widiatedja and Mishra (2023) argue for organizationally and functionally independent personal data protection oversight in Indonesia. Badriah et al. (2024) similarly connect accountability with institutional arrangements, reporting, sanctions, and compensation. Together, these studies indicate that compliance requires both internal implementation and the possibility of external scrutiny. The present article develops that insight into an assessment framework suited to local government digital services.

METHOD

This study employs normative legal research using statutory and conceptual approaches. The statutory approach identifies obligations relevant to personal data processing in local government digital services. The conceptual approach uses compliance, accountability, proportionality, and data governance scholarship to connect those obligations with assessable institutional practices. The temporal scope extends through December 31, 2024. Legal developments, judicial interpretations, and publications after that date are excluded. The article provides a retrospective assessment framework for the 2024 legal setting rather than describing the position under subsequent developments.

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, Presidential Regulation No. 95 of 2018 on Electronic-Based Government Systems, and Government Regulation No. 71 of 2019 on the Operation of Electronic Systems and Transactions. The regional context is examined through West Java Provincial Regulation No. 4 of 2021 on Communication and Informatics, Statistics, and Cryptography, together with Governor Regulation No. 41 of 2022 concerning cryptography for information security within the provincial government. An official publication from 2024 establishes the context of integrated digital services.

Materials are selected according to their relevance to processing grounds, institutional responsibility, security, data-subject procedures, and accountability. Scholarly publications support conceptual interpretation. Official service descriptions establish context but are not treated as independent verification of operational compliance. The analysis identifies each relevant duty, determines the activity to which it applies, and proposes records that could support its assessment. Existing legal obligations are distinguished from recommended administrative methods. The proposed framework is not a statutory certification scheme or a validated numerical index. No questionnaires, interviews, unpublished contracts, technical inspections, or institutional audit files form part of the research. Accordingly, the article does not assign compliance scores or determine violations by particular public bodies. Its findings concern legal interpretation and the design of a review framework.

RESULTS AND DISCUSSION

The Legal Baseline for Compliance in 2024

The first finding is that compliance should be assessed against the relationship between several regulatory functions. The Personal Data Protection Law governs personal data processing, while public service and electronic government instruments establish related administrative and operational responsibilities.

Law No. 25 of 2009 places public service delivery within a framework of institutional obligations and service accountability. Presidential Regulation No. 95 of 2018 concerns electronic-based government, while Government Regulation No. 71 of 2019 regulates electronic system operation. These instruments provide relevant context but should not be treated as substitutes for the specific requirements of the Personal Data Protection Law (Republic of Indonesia, 2009, 2018, 2019, 2022).

West Java's regional instruments support the examination of local information governance. Provincial Regulation No. 4 of 2021 addresses communication and informatics, statistics, and cryptography. Governor Regulation No. 41 of 2022 concerns information security arrangements within the provincial government (Province of West Java, 2021, 2022).

Their geographic and institutional scope requires careful treatment. A provincial regulation does not, by itself, establish the responsibility of every city or regency institution for every digital service. An assessment must identify the public body operating the relevant function and the legal instruments applicable to it.

The 2024 adjustment deadline also requires precision. Completion of the statutory adjustment period does not establish that all institutions became compliant. It establishes the temporal expectation against which their arrangements may be examined. Evidence of implementation remains necessary.

OPEN ACCESS

This distinction prevents two unsupported conclusions: that institutions were compliant merely because the deadline had passed, or that they were noncompliant because digital administration involved complex information flows. Neither conclusion follows without examining the relevant activity and evidence.

Lawful Grounds and Purpose Limitation

A compliance assessment should begin by identifying why information is processed. Article 20 recognizes several processing grounds, including consent, legal obligations, and public-interest tasks, public services, or lawful authority. The correct ground depends on the activity rather than on a standard consent statement used across an application (Republic of Indonesia, 2022).

Mandatory administrative processing should be explained through its applicable legal basis. When residents must supply information to obtain a service required by law, presenting the entire relationship as a freely negotiable agreement can obscure the institution's authority and the limits of individual choice.

However, the existence of public authority does not justify unrelated uses. Article 16 establishes processing principles that include specificity, legality, transparency, accuracy, security, and consistency with purpose. An assessment should therefore examine whether the information collected is connected to the stated administrative function.

Black and Stevens (2013) support this reasoning through their discussion of necessity and proportionality. Applied here, the compliance inquiry concerns the information needed to perform the function, the scope of its use, and the justification for any additional processing.

Relevant evidence may include the service mandate, a processing inventory, collection forms, explanatory notices, and documented decisions concerning information sharing. These records help establish what the institution intended to do, but they should be compared with actual processing arrangements before a definitive compliance conclusion is reached.

Optional functions require separate consideration. A service may include voluntary communications or other additional features alongside mandatory processing. The article recommends distinguishing these purposes so that residents can understand which information is required and which choices concern additional activities.

Responsibility Across Institutions and Providers

Integrated services can involve several organizations without giving each organization identical authority. Compliance assessment should identify the controller and processor for the particular processing activity, rather than relying solely on the name displayed on the application.

Article 51 is important where a controller appoints a processor. Processing must follow the controller's instructions, and the article preserves controller responsibility for processing through the appointed arrangement. It also addresses additional processors and processing beyond authorized instructions (Republic of Indonesia, 2022).

Procurement documents can help clarify those relationships, but contractual wording is not conclusive when it conflicts with the parties' actual conduct. An assessment should examine who determines the purpose of processing and how instructions are implemented.

The article recommends reviewing agreements for provisions concerning authorized activities, access restrictions, incident escalation, additional processors, and the return or deletion of information. These provisions can support implementation; they do not eliminate statutory duties or conclusively prove that the duties have been fulfilled.

Responsibility should remain clear when a service changes. Introducing a new feature, recipient institution, or provider may change the processing arrangement. A review conducted only when the original contract was signed may no longer reflect the service being delivered.

The official 2024 Sapawarga publication establishes a context of integrated access. It does not disclose the complete controller–processor relationships for all participating functions. Determining those relationships would require additional institutional documents, which were not available within this study.

A Framework Connecting Obligations with Evidence

The second finding is that compliance review becomes more precise when each duty is connected to evidence. Article 47's accountability requirement supports examining whether the institution can demonstrate its fulfilment of personal data protection obligations.

OPEN ACCESS

The framework in Table 1 organizes this inquiry. The listed evidence is indicative: its adequacy depends on the processing activity and legal requirement. The absence of a document bearing a particular title does not automatically establish a violation if equivalent reliable evidence exists.

Table 1. Proposed Framework for Assessing Personal Data Protection Compliance

Compliance dimension	Principal legal basis	Indicative evidence
Lawful processing	Article 20	Identification of the processing ground and relevant administrative mandate
Purpose and processing principles	Article 16	Processing inventory, collection forms, sharing justifications, and retention arrangements
Processing records	Article 31	Records showing relevant processing activities
High-risk processing assessment	Article 34	Documented assessment of whether statutory high-risk criteria apply and the required impact assessment
Security and supervision	Articles 35–39	Access arrangements, security procedures, monitoring records, and corrective actions
Data-subject procedures	Articles 5–14 and corresponding controller duties	Request channels, recorded responses, and evidence of completed action
Breach response	Article 46, subject to applicable exceptions	Incident records, notification decisions, and handling documentation
Demonstrated accountability	Article 47	Review records connecting duties with implementation
Processor arrangements	Articles 51–52	Instructions, agreements, approvals, and oversight records
Personal data protection functions	Articles 53–54	Assessment of appointment requirements and records of assigned functions

Source: Author's synthesis of Republic of Indonesia (2022), using the statutory text applicable within the study's 2024 scope.

A review should distinguish documented policy from demonstrated operation. A security policy may establish the intended procedure, while access records and corrective actions provide evidence of implementation. Neither category should automatically replace the other.

The framework also distinguishes applicability from performance. For instance, an impact assessment requirement must first be evaluated against the statutory high-risk criteria. A reviewer should not conclude that every service requires an identical assessment without examining the processing involved.

Where evidence is incomplete, the appropriate finding may be that compliance cannot yet be determined. This differs from a verified violation. Maintaining that distinction makes the framework more useful for institutional review and avoids overstating what limited documentation can establish.

Security and the Management of Information Throughout the Service

Security should be assessed in relation to the information and risks involved. The relevant inquiry concerns whether protective arrangements correspond to the processing activity. Merely listing security products or technical features provides an incomplete basis for evaluation.

Access control illustrates the connection between security and administration. A service should identify which roles need access and how permissions are changed when staff responsibilities change. The article recommends periodic review of permissions as a means of supporting the statutory protection and supervision duties.

Data quality requires similar attention. Inaccurate or outdated information can affect service decisions even when no external attack occurs. Compliance review should therefore consider how records are corrected and how relevant updates are communicated within authorized processing arrangements.

Retention also belongs within the assessment. Institutions should determine when information remains necessary and which legal requirements justify continued storage. Indefinite retention should not be assumed to follow from the public character of a service.

OPEN ACCESS

Thompson et al. (2015) help explain why these issues require governance as well as technology. Their public-sector audit analysis connects information weaknesses with unclear responsibilities and inadequate management arrangements. Applied to local digital services, the implication is that security and data quality should have identifiable institutional owners.

Tikkinen-Piri et al. (2018) provide complementary insight into the organizational changes associated with data protection requirements. Although their research concerns European rules and companies, it supports the narrower conceptual point that compliance requires coordinated operational practices. Indonesian law remains the governing basis for this article's assessment framework.

Data-Subject Procedures as Evidence of Compliance

Residents' ability to exercise statutory rights provides another important dimension of compliance. A privacy notice may explain those rights, but an institution must also have arrangements capable of receiving and deciding relevant requests.

Article 14 recognizes recorded electronic or nonelectronic applications for exercising the rights identified in Articles 6–11. Accordingly, compliance review should examine whether the available procedure is consistent with the statutory framework, including the applicable conditions and limits (Republic of Indonesia, 2022).

Identity verification should protect residents from unauthorized disclosure or alteration. Its design should nevertheless remain proportionate to the request. Requiring unnecessary additional information can create new processing risks without improving the reliability of the response.

Response records can demonstrate whether the institution granted access, corrected information, explained a restriction, or refused a request. A generic acknowledgment shows receipt but does not establish fulfilment. The reviewer should examine the decision and, where relevant, the completion of the required action.

Integrated services create an additional coordination issue. The office receiving a request may not operate the underlying record. The article recommends an internal referral process that preserves traceability and provides the resident with a clear explanation of responsibility.

Statutory exceptions must also be assessed precisely. Articles 15 and 50 concern specified rights and obligations; they should not be treated as blanket exemptions for all government processing. A compliance record should identify the provision relied upon and its relationship with the particular administrative function.

Incident Handling and Reviewable Decisions

Incident response provides a test of whether responsibilities and procedures can operate together. Article 46 establishes notification obligations following a personal data protection failure, including written notification within a maximum of three times twenty-four hours to the specified recipients, subject to applicable statutory exceptions (Republic of Indonesia, 2022).

Compliance assessment should examine how the institution identifies an incident, escalates relevant information, evaluates notification duties, and records its decisions. The article recommends linking technical response procedures with legal and administrative review so that these activities do not proceed in isolation.

Notification does not by itself establish complete compliance. An institution may notify affected individuals while still needing to address the underlying failure. Conversely, restoring a service does not answer whether notification or another legal obligation was fulfilled.

Evidence should distinguish confirmed facts from matters still under investigation. This protects the reliability of institutional explanations and avoids presenting assumptions as established causes. Records should also show subsequent corrective action where required.

Independent scrutiny remains relevant when an institution's explanation is contested. Widiatedja and Mishra (2023) emphasize functional independence in oversight, while Badriah et al. (2024) connect accountability with reporting and remedial arrangements. These perspectives support retaining evidence that can be examined beyond the operational team.

Incorporating Compliance into Service Governance

The third finding is that compliance should be reviewed throughout the service lifecycle. A review limited to launch cannot account for later changes in processing purposes, providers, or institutional access.

During planning, the institution should identify the intended processing and applicable legal basis. Procurement should translate relevant responsibilities into operational arrangements. Testing should examine

OPEN ACCESS

whether the service implements the intended controls and procedures. Subsequent reviews should respond to material changes and identified problems.

These stages are proposed administrative methods for supporting statutory duties. They are not presented as a separate procedure expressly prescribed in this form by the Personal Data Protection Law.

Table 2. Proposed Compliance Review Across the Service Lifecycle

Service stage	Review focus	Expected record
Planning	Purpose, legal basis, information needed, and risks	Processing description and applicability assessment
Procurement	Provider responsibilities and processing instructions	Documented arrangements and approvals
Development and testing	Access, notices, request procedures, and protective measures	Review findings and corrective actions
Operation	Changes in processing, permissions, and service practices	Updated records and periodic review results
Incident response	Escalation, legal duties, evidence, and recovery	Incident chronology and reasoned decisions
Modification or closure	Continued necessity, transfer, return, retention, or deletion	Documented completion of the relevant actions

Source: Author's normative proposal informed by Republic of Indonesia (2022), Mergel et al. (2019), and Thompson et al. (2015).

This approach connects compliance with ordinary administrative decisions. It also gives management a basis for assigning work and reviewing unresolved issues without assuming that responsibility belongs entirely to technical staff.

For West Java, the framework can accommodate differences between provincial, city, and regency institutions. The common requirement is to connect the processing activity with the responsible body and applicable duty. The particular evidence will depend on the service and organizational arrangement.

Contribution and Limitations

The article contributes a legal framework for distinguishing service availability, policy adoption, and demonstrated compliance. It identifies the records needed to connect legal obligations with institutional conduct, while preserving the distinction between a verified failure and insufficient evidence.

Its findings remain doctrinal. No compliance percentage, institutional ranking, or verified violation is reported. Applying the framework empirically would require access to processing records, agreements, request outcomes, security assessments, and incident documentation.

Further research should examine whether the proposed dimensions can be assessed consistently across different local services. Such research could refine the evidence requirements without converting a limited document review into an unsupported claim about overall institutional compliance.

CONCLUSION

Personal data protection compliance in West Java's local government digital services should be assessed through the relationship between applicable legal duties and evidence of implementation. Within the framework applicable through 2024, lawful processing, purpose limitation, security, data-subject procedures, processor oversight, and demonstrated accountability form connected requirements. Integrated access does not independently authorize unrestricted information sharing, and outsourcing does not automatically remove controller responsibility. The proposed framework connects those requirements with reviewable records and incorporates assessment into planning, procurement, operation, modification, and incident response. Its practical implication is that compliance becomes an ongoing administrative responsibility supported by identifiable decisions and evidence. The study does not establish actual compliance levels among West Java institutions; that determination requires examination of their operational records and practices.

OPEN ACCESS

REFERENCES

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

Government of West Java. (2024, May 27). *Jabar bisa jadi contoh pemda provinsi dalam penggunaan aplikasi layanan publik terintegrasi*. https://jabarprov.go.id/berita/jabar-bisa-jadi-contoh-pemda-provinsi-dalam-penggunaan-aplikasi-layanan-publik-terintegra-13673

Mergel, I., Edelmann, N., & Haug, N. (2019). Defining digital transformation: Results from expert interviews. *Government Information Quarterly, 36*(4), Article 101385. https://doi.org/10.1016/j.giq.2019.06.002

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

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

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review, 34*(1), 134–153. https://doi.org/10.1016/j.clsr.2017.05.015

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