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. 1 (2024)

PROTECTING CITIZENS' PERSONAL DATA RIGHTS IN WEST JAVA'S DIGITAL PUBLIC ADMINISTRATION

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

Received: 06/03/2024 | **Revised:** 09/03/2024 | **Accepted:** 28/03/2024 | **Published:** 30/03/2024

Abstract

Digital public administration increasingly relies on the collection and exchange of personal information, creating challenges for citizens seeking to understand and exercise their data rights. This article examines the legal protection of personal data rights in West Java's digital public administration within the regulatory framework applicable through 2024. Normative legal research is employed through statutory and conceptual approaches, drawing on legislation, scholarly publications, and official provincial documentation. The analysis identifies three requirements for effective protection: a lawful and specific processing purpose, accessible procedures for exercising rights, and identifiable institutional responsibility. Public service authority does not provide unrestricted permission to collect or reuse personal information. Likewise, consent cannot replace the legal justification required for mandatory administrative processing. Access, correction, and other statutory entitlements must be implemented with attention to their respective conditions and exceptions. The article proposes a coordinated framework connecting clear notices, proportionate identity verification, documented decisions, and accessible complaint mechanisms. It concludes that personal data protection should be integrated into ordinary administrative procedures rather than confined to technical security arrangements. These findings provide a doctrinal framework and do not constitute an empirical assessment of institutional compliance in West Java.

Keywords: Citizens' rights; Digital public administration; Personal data protection; Public services; West Java.

INTRODUCTION

Public administration increasingly depends on information supplied by the people it serves. An application for an administrative document, a public complaint, or access to a government programme may require identity details, contact information, and supporting records. Digital systems make these transactions easier to organize, but they also change how information travels between institutions. Citizens may understand the service they are requesting without knowing which organizations can access their information or how long it will remain available.

This imbalance matters because public administration exercises authority over decisions that affect everyday life. An inaccurate record may obstruct an application, while unnecessary disclosure may expose information that a resident submitted to obtain an essential service. Protecting personal data therefore concerns the quality and fairness of administrative processes as well as the prevention of unauthorized access.

West Java provides a relevant setting for examining these issues. In an official publication dated May 27, 2024, the provincial government described Sapawarga as an application bringing several public services together through an integrated access arrangement. The publication presented service simplification as a priority of provincial digital administration (Government of West Java, 2024). This establishes a documented context for examining personal data rights, although it does not establish how every underlying processing arrangement operates. jabarprov.go.id

Integration creates a tension between administrative convenience and the boundaries of legitimate information use. Residents may benefit from submitting information once, yet the same arrangement can make it difficult to distinguish the purpose of the original collection from subsequent uses. A common interface does not necessarily mean that every participating institution has the same legal authority to process every available record.

Law No. 27 of 2022 on Personal Data Protection provides a central framework for addressing this relationship. The law recognizes data-subject rights and establishes obligations concerning processing, security, accountability, and remedies. Its relevance to public administration lies in the connection it creates between the exercise of institutional authority and the protection of individuals whose information supports that authority (Republic of Indonesia, 2022).

The year 2024 is especially significant because Article 74 established a maximum two-year adjustment period from the law's promulgation on October 17, 2022. That period must be distinguished from the law's commencement: the legislation entered into force upon promulgation. Its transitional provision concerned adjustment to processing requirements, rather than postponing the existence of the law until 2024 (Republic of Indonesia, 2022, Articles 74–76).

Earlier research provides several foundations for examining this transition. Rahman (2021) discusses personal data protection within Indonesia's electronic-based government framework. Wu (2014) examines the protection of personal information in electronic government across different national settings. Thompson et al. (2015) show how weaknesses in public-sector data governance can undermine the reliability and traceability of information systems.

These studies suggest that adopting digital technology does not automatically make personal data rights usable. A right may be recognized in legislation while remaining difficult to exercise through an administrative service. Citizens need to identify the responsible institution, submit a request, receive an understandable decision, and challenge an unsatisfactory response through an appropriate mechanism.

This article addresses that practical legal relationship. It examines how personal data rights should be understood within West Java's digital public administration, how legitimate administrative processing should be distinguished from excessive collection or reuse, and which institutional procedures can support the exercise of those rights. Its contribution is a framework connecting substantive entitlements with the administrative steps needed to make them effective.

LITERATURE REVIEW

Personal Data Protection in Public Administration

Personal data protection regulates the relationship between individuals and organizations that process information about them. Its scope extends beyond secrecy. Information may be accurate and securely stored while still being collected excessively, retained without sufficient justification, or used for an unrelated purpose.

Rahman (2021) examines the legal framework for personal data protection in Indonesia's electronic-based government system. The study is relevant because it connects digital administration with legal safeguards. Its pre-2022 perspective also provides a useful baseline for considering the subsequent introduction of comprehensive personal data protection legislation.

Wu (2014) approaches the issue through a cross-country study of electronic government. The research demonstrates the importance of examining legal and institutional arrangements alongside technological development. For the present article, this perspective supports evaluating digital administration through the treatment of personal information rather than through the availability of applications alone.

The distinction has practical consequences. A service may become faster while leaving residents uncertain about how to correct an inaccurate record. Evaluating personal data protection therefore requires attention to the relationship between information practices and citizens' ability to influence decisions concerning their own data.

Public Interest and Proportionate Processing

Public authorities often process information to perform legally assigned tasks. However, the existence of a public task does not establish that every category of information is necessary for its performance. Black and Stevens (2013) examine this issue through the relationship between public interest, necessity, and proportionality in public-sector processing.

Their analysis supports asking whether a particular processing activity is connected to an identifiable administrative purpose and whether its scope is justified. The relevant question is more precise than whether digitalization benefits government. It concerns why specific information is needed for a particular function and what consequences follow from its use.

This distinction also helps explain why consent requires careful treatment. Residents may have limited practical freedom to refuse processing associated with an essential service. A consent form cannot resolve every issue concerning administrative authority, excessive collection, or secondary use. The processing institution must identify a legal basis appropriate to the activity.

OPEN ACCESS

Accountability and the Exercise of Rights

Bovens (2007) conceptualizes accountability as a relationship in which an actor explains and justifies conduct before a forum capable of evaluating it. Applied to personal data rights, this perspective highlights the need for identifiable responsibility and reviewable decisions.

An access or correction mechanism becomes meaningful when the responsible institution can explain what it holds, why it processes the information, and how it decided the request. A general assurance that personal information is protected does not provide the same opportunity for scrutiny.

Thompson et al. (2015) complement this perspective by examining governance weaknesses in public-sector information systems. Their findings connect operational problems with uncertainty over responsibilities and records. The implication for rights protection is that institutions must be able to trace decisions affecting personal information.

Supervision and Effective Protection

Widiatedja and Mishra (2023) argue that organizationally and functionally independent supervision is important to meaningful personal data protection in Indonesia. Their discussion is particularly relevant where public institutions are themselves responsible for processing large amounts of personal information.

Badriah et al. (2024) examine accountability in personal data protection policy through comparisons involving Indonesia, South Korea, and Singapore. Their analysis connects protection with reporting mechanisms, institutional arrangements, sanctions, and compensation.

Taken together, these studies establish that rights require organizational support. The remaining issue examined here is how to connect legal entitlements with ordinary administrative procedures in an integrated provincial service environment. The proposed contribution concerns that connection rather than a claim that personal data protection in public administration has not previously been studied.

METHOD

This article employs normative legal research through statutory and conceptual approaches. The statutory approach examines legislation relevant to personal data protection and digital public administration. The conceptual approach draws on proportionality, accountability, and data governance scholarship to evaluate how statutory rights can be implemented through administrative procedures.

The temporal scope covers legal instruments and publications available by December 31, 2024. Subsequent legislation, judicial interpretations, and institutional developments are excluded. The article is therefore a retrospective analysis of the 2024 framework, rather than a description of the legal position in later years.

The principal legal material is Law No. 27 of 2022 on Personal Data Protection. Supporting instruments include Law No. 14 of 2008 on Public Information Disclosure, 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 provincial publication from 2024 establishes the context of integrated service delivery.

Legal materials are selected according to their relevance to processing authority, data-subject entitlements, institutional obligations, and administrative remedies. Scholarly publications support the interpretation of these issues. Official descriptions of digital services are used to establish context and are not treated as independent verification of technical security or legal compliance.

The analysis proceeds through four stages: identifying the relevant rights, examining the lawful grounds and limits of processing, assessing procedures needed to exercise those rights, and developing recommendations for institutional implementation. Existing legal requirements are distinguished from the article's proposed administrative safeguards.

No interviews, surveys, unpublished administrative records, or technical audits form part of the research. The findings consequently do not establish the prevalence of violations or the performance of particular institutions. They provide a doctrinal assessment of the relationship between legal rights and administrative arrangements.

OPEN ACCESS

RESULTS AND DISCUSSION

Personal Data Rights as Part of Administrative Fairness

The first finding is that personal data rights should be treated as part of the administrative relationship between citizens and public institutions. A resident who submits information for a service remains entitled to the protection provided by law. Submission does not convert personal information into a resource available for unrestricted institutional use.

Access and correction are particularly relevant to administrative fairness. An individual may be unable to challenge an inaccurate decision without knowing which information supported it. A correction procedure can therefore affect more than the quality of a database; it may influence the institution's ability to reach a properly informed decision.

Articles 5–13 of the Personal Data Protection Law recognize several entitlements concerning information, correction, access, termination or deletion, withdrawal of consent, objections to certain automated decisions, processing restrictions, compensation, and the use or transfer of personal data. These entitlements have different conditions and should not be presented as interchangeable or unconditional (Republic of Indonesia, 2022).

The distinction matters in public administration. Withdrawal of consent does not necessarily terminate processing that rests on another valid legal basis. Similarly, a deletion request requires consideration of the applicable statutory grounds and exceptions. An institution should identify the right being exercised before deciding whether the request can be fulfilled.

Table 1. Personal Data Rights and Their Administrative Implications

Right or entitlement	Principal provision	Administrative implication
Information concerning processing	Article 5	Explain the relevant legal basis, purpose, and institutional accountability.
Completion, updating, and correction	Article 6	Provide a route for addressing inaccurate or incomplete information.
Access and copies	Article 7	Enable individuals to obtain their information subject to applicable requirements.
Termination, deletion, or destruction	Article 8	Assess the request against statutory conditions and applicable exceptions.
Withdrawal of consent	Article 9	Determine which processing relies on consent and the consequences of withdrawal.
Objection to certain automated decisions	Article 10	Assess whether the decision falls within the statutory scope.
Postponement or restriction	Article 11	Examine the request in relation to the processing purpose and legal limits.
Claims and compensation	Article 12	Provide information concerning the relevant redress mechanism.
Obtaining, using, or transferring data	Article 13	Examine format, secure interoperability, and applicable exceptions.

Source: Author's synthesis of Republic of Indonesia (2022).

The table identifies legal entitlements without assuming that a particular West Java application already provides every corresponding function. Establishing implementation would require examining the actual interface, administrative procedures, and institutional records.

A further distinction concerns access to personal information and access to public information. Law No. 14 of 2008 regulates public information disclosure, while the Personal Data Protection Law establishes entitlements concerning an individual's personal data. Institutions should determine which legal mechanism applies instead of treating every request as an ordinary demand for public disclosure.

Lawful Processing Beyond Routine Consent

The second finding concerns the relationship between administrative authority and processing grounds. Article 20 recognizes several legal bases, including consent, legal obligations, and the performance of public-interest tasks,

OPEN ACCESS

public services, or lawful authority. Consent is therefore one basis within a broader statutory framework (Republic of Indonesia, 2022).

For mandatory administrative functions, the institution should explain the relevant legal obligation or public authority. Presenting all processing as a voluntary agreement can mislead residents about the consequences of refusal. It may also obscure the institution's duty to justify what information is necessary.

The opposite assumption is equally problematic. A public institution cannot rely on its general mandate to justify every possible use of personal information. The processing purpose should relate to the particular service or administrative function. Article 16's principles provide a basis for examining the specificity, legality, transparency, accuracy, and security of that activity.

Black and Stevens (2013) support this approach through their analysis of necessity and proportionality. Applied to West Java's integrated service context, the implication is that an institution should distinguish information needed to perform a function from information that would merely be convenient to possess.

Optional features require separate consideration. Information used for a voluntary notification preference or another additional function should not automatically be treated as necessary for the underlying service. The article recommends separating mandatory processing explanations from optional choices so that residents can understand the relationship between their decisions and access to the service.

This recommendation does not imply that all information collected through integrated administration is excessive. It provides a method for evaluating the collection: identify the purpose, determine the legal basis, examine necessity, and document the decision. The assessment must concern actual processing arrangements.

Service Integration and the Boundaries of Information Sharing

The official 2024 description of Sapawarga establishes a policy direction toward integrated access to public services. It does not establish that all participating functions operate through one database or that every institutional participant can view every record. Those technical and legal details require additional evidence.

Nevertheless, integration raises a clear normative issue. Information that becomes technically accessible across services should not automatically become legally available for unrelated purposes. An identity verification process, for example, may justify a limited exchange without justifying unrestricted access to the supporting documents.

The article therefore proposes a documented assessment before a new information-sharing arrangement is introduced. The assessment should identify the sending and receiving institutions, the information involved, the intended use, the applicable authority, and the measures limiting access. These are recommended administrative records for demonstrating the justification of sharing.

Responsibility must also remain identifiable. Under Article 51, appointing a processor does not automatically remove the controller's responsibility for processing performed through that arrangement. A resident should not lose access to a meaningful response because several organizations support the same service.

Thompson et al. (2015) demonstrate why traceability deserves attention. Their analysis connects public-sector information problems with weaknesses in governance and responsibility. For integrated administration, the practical implication is that institutions should know which participant can retrieve, correct, restrict, or otherwise act on the relevant information.

Coordination does not require treating all participating institutions as a single legal entity. Each institution's role must follow the applicable law and actual processing authority. A common service interface can simplify the citizen's experience while preserving an accurate internal allocation of responsibilities.

Accessible Procedures for Exercising Rights

Recognition of rights is incomplete without a usable procedure. Article 14 provides that requests concerning the rights in Articles 6–11 may be submitted through recorded electronic or nonelectronic applications to the controller. The provision is particularly relevant to accessibility because it does not confine those requests to a single digital channel (Republic of Indonesia, 2022).

An institution should consequently avoid making one application the only practical route for every request. A resident may lack reliable internet access, have lost access to an account, or require assistance in understanding the procedure. Assisted channels can support the exercise of rights while preserving a record of the request.

Identity verification remains necessary to prevent unauthorized disclosure. However, the verification process should correspond to the risk. Collecting extensive additional documents for a limited correction request can create

OPEN ACCESS

further exposure. The article recommends using existing verification arrangements where appropriate and requesting additional evidence only when justified.

Responses should explain the substance of the decision. A message stating that a request has been "processed" may leave the resident unable to determine whether information was corrected, access was granted, or the request was refused. A reasoned response should identify the action taken and any relevant limitation.

Requests affecting several institutions require coordination. A receiving office should be able to identify the responsible unit and explain the next step without repeatedly requiring the resident to reconstruct the information flow. This recommendation concerns service organization and does not assume a statutory entitlement to one particular channel design.

Table 2. Proposed Procedure for Handling Personal Data Rights Requests

Stage	Recommended institutional action	Purpose
Receipt	Record the request and provide an acknowledgment.	Establish a traceable starting point.
Verification	Confirm identity through proportionate measures.	Prevent unauthorized access or alteration.
Allocation	Identify the responsible controller and relevant unit.	Avoid organizational ambiguity.
Assessment	Examine the requested right, legal basis, and applicable limits.	Support a legally reasoned decision.
Response	Explain the action taken or reasons for refusal.	Make the outcome understandable.
Review	Identify the available complaint or review route.	Enable the resident to challenge the response.
Follow-up	Document completion and coordinate necessary updates.	Reduce repeated errors and conflicting records.

Source: Author's normative proposal, informed by Republic of Indonesia (2022) and Bovens (2007).

The proposed procedure translates accountability into observable administrative actions. Each stage produces information that can be reviewed. It also separates the institution's legal assessment from the technical operation required to carry out the decision.

Public-Interest Exceptions and Reasoned Restrictions

Personal data rights are subject to statutory limits. Article 15 identifies exceptions concerning specified entitlements for listed interests, including public-interest administration, and requires those exceptions to operate in implementing statutory provisions. Article 50 separately addresses exceptions to particular controller obligations.

These provisions require attention to the right or obligation actually at issue. An institution should not assume that one exception suspends the entire personal data protection framework. Nor should it assume that every request involving government-held information must be granted without examining the applicable conditions.

A defensible decision should identify the relevant provision and explain its connection to the administrative activity. Where information must remain available for a lawful function, the institution should explain that basis rather than relying on a general claim that government records cannot be changed or deleted.

The proportionality analysis developed by Black and Stevens (2013) provides useful conceptual support. It encourages examination of the relationship between the protected public purpose and the restriction imposed. This is an interpretive approach used by the article, rather than a claim that every element of their framework appears expressly in Indonesian legislation.

Reason-giving also supports accountability. A resident can assess or challenge a restriction only when its basis is sufficiently clear. The institution's explanation should therefore distinguish a statutory limitation from a technical difficulty, missing documentation, or an unresolved internal allocation of responsibility.

Security, Transparency, and Redress

Security measures protect the conditions under which personal data rights can be exercised. Unauthorized access can expose information, while unauthorized alteration can undermine the accuracy of administrative decisions. Security must therefore be connected to the protection of confidentiality, integrity, and availability.

Government Regulation No. 71 of 2019 provides a framework for electronic system operation. Within West Java, Provincial Regulation No. 4 of 2021 and Governor Regulation No. 41 of 2022 supply a relevant regional

OPEN ACCESS

context for information governance and security. These instruments complement the personal data protection framework rather than replacing the need to examine specific data-subject rights.

Article 47's requirement to demonstrate accountability connects security with documentation. Institutions need records that allow relevant processing decisions and protective measures to be examined. The appropriate evidence will depend on the activity, but a general assurance of security cannot answer every question about access, correction, or information sharing.

Transparency should be designed around the resident's decision. Notices should explain the responsible institution, the processing purpose, and the available route for exercising rights. Long legal statements may contain relevant information while remaining difficult to use during an actual application.

When an alleged violation occurs, complaint handling and legal redress serve related but different purposes. An administrative complaint may resolve a correction or explanation issue. A compensation claim under Article 12 requires assessment under the applicable law and procedure. The existence of an error does not automatically determine compensation, while correcting the error does not necessarily resolve every claim arising from it.

Widiatedja and Mishra (2023) explain the importance of independent supervision in this setting. Internal handling can provide a prompt response, but contested conduct may require scrutiny outside the institution responsible for processing. Badriah et al. (2024) similarly connect accountability with reporting, institutional authority, and remedies.

The proposed approach is therefore to make complaints accessible while accurately explaining their limits. Institutions should identify which office can correct a record, which body can review a contested decision, and which legal route concerns compensation. Residents should receive information suited to the issue they are raising.

Implications for West Java and Research Limitations

West Java's integrated service policy makes coordination a central concern. The legal implication is not that integration should be avoided, but that service simplification should be accompanied by an equally clear explanation of institutional responsibility and citizens' rights.

Three priorities follow from the analysis. Processing should have an identifiable purpose and legal basis. Rights requests should move through a recorded and accessible procedure. Institutional decisions should remain open to review through reliable documentation and appropriate complaint mechanisms.

These priorities could inform service standards and internal procedures without assuming that every institution faces identical risks. The appropriate arrangements depend on the sensitivity of the information, the processing purpose, and the relationship between participating bodies.

The study remains limited to legal and documentary analysis. It does not establish whether Sapawarga or another West Java service fulfils the proposed safeguards. Further research should examine actual notices, request procedures, processing agreements, and complaint outcomes. Such evidence would allow the normative framework to be evaluated against institutional practice.

CONCLUSION

Protecting citizens' personal data rights in West Java's digital public administration requires a connection between lawful processing and usable administrative procedures. The framework applicable through 2024 recognizes important entitlements, but their exercise depends on the particular legal conditions and exceptions governing each request. Public service authority must be linked to a specific processing purpose, and consent should not obscure the legal basis of mandatory administration. Integrated services should preserve identifiable responsibility, proportionate verification, reasoned decisions, and accessible review. The article proposes incorporating these safeguards into ordinary service procedures so that residents can understand how their information is used and obtain an appropriate response when they seek access, correction, or another statutory entitlement. These conclusions provide a doctrinal basis for institutional development and require empirical examination before claims about actual compliance in West Java can be made.

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

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. (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

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