International Journal of Educational Review, Law, and Social Sciences (IJERLAS)
ISSN: 2808-487X
Edition: Vol. 5 No.6 (2025)
https://radjapublika.com/index.php/IJERLAS/index

Personal Data Protection in West Java's Digital Public Services: An Analysis of Implementation Post-PDP Law

Berna Ermaya Sudjana[1], Ihsanul Maarif[2]
[1.2] Universitas Pasundan, Bandung, Indonesia
Email: berna.ermaya@unpas.ac.id

Keywords:
PDP Law; personal data protection; digital public services; Data governance;

Article Info:
Received:
07/10/2025
Revised:
11/10/2025
Accepted:
15/11/2025
Published:
30/11/2025

ABSTRACT

Transformation service digital public in West Java is growing rapidly and increasing efficiency service , but also gives rise to complexity risk related personal data protection community . Publishing Constitution Personal Data Protection (PDP Law) becomes runway law important For strengthen right privacy citizens and organizing data governance in the sector public . Research This aim analyze implementation of the PDP Law in service West Java digital public with review three dimensions Main : regulatory , institutional , and technical-operational . Research methods use approach descriptive qualitative through studies documents , review regulations , and interviews with the apparatus involved in data management . Research results show that implementation the beginning of the PDP Law provides a number of impact positive , such as increasing awareness institutional to importance personal data protection , improvements procedure data management through implementation principle data minimization , as well as update policy privacy on a number of digital platforms. However , the findings also identified various challenges , among others, have not yet composition regulations derivatives at the level area , the minimum officials Data Protection Officer (DPO), inequality standard security application , limitations literacy apparatus , as well as weakness mechanism monitoring and reporting incident data leak . Novelty research This lies in the approach integrative that combines analysis regulatory , institutional , and technical-operational in a way simultaneously , so that produce greater understanding comprehensive about dynamics implementation of the PDP Law at the level area . This study give contribution important for development of a more public data governance model accountable , adaptive , and sustainable in support digital transformation of government .

How to cite: Berna Ermaya Sudjana, & Ihsanul Maarif. (2025). Personal Data Protection in West Java's Digital Public Services: An Analysis of Implementation Post-PDP Law. International Journal of Educational Review, Law And Social Sciences (IJERLAS), 5(6), 278–287.
DOI: https://doi.org/10.5281/zenodo.20271970

Introduction

Transformation service digital public in Indonesia in a number of year final show very rapid The transformation of digital public services in Indonesia over the past few years has shown very rapid development, especially in West Java Province, which is often referred to as a digital province because of its success in integrating various technology-based services. Platforms such as Sapawarga, the West Java One Data System, and a number of applications for health, education, and population administration services have pushed improvements in the quality of public services through faster access, procedural efficiency, and information transparency. However, this acceleration of digitalization simultaneously increases the risk to personal data security and public privacy, especially due to the high volume of sensitive data concentrated in a single digital government ecosystem. The enactment of the Personal Data Protection Law (PDP Law) in 2022 serves as a comprehensive legal framework to protect citizens' privacy rights. Nevertheless, its implementation at the regional level, including in West Java, still faces challenges related

to limited resources, governance unpreparedness, and unequal levels of digital literacy among government apparatus.[1]. Academic studies about personal data protection generally emphasize importance three element main : security technology , governance institutional , and compliance regulatory . Research previously mention that system security adequate information , such as encryption and authentication layered , is foundation in prevent data [2]leaks . On the other hand , the literature regarding public data governance highlight the need clear *data governance framework* so that the role and responsibility answer controller and data processors do not overlapping Overlapping[3]. Furthermore, compliance with national regulations is a determinant of public institutions' accountability in managing personal data [4]. However, most studies still focus on the national level or the private sector, so the implementation of personal data protection in the context of regional public services, particularly in regions with massive digital service development, such as West Java, has not been discussed in depth.

The gap study This show the need further study contextual and empirical about How government area apply provisions of the PDP Law in practice everyday . Therefore that, the novelty of the research This lies in its approach which is special analyze implementation personal data protection post PDP Law in ecosystem service West Java digital public with blend perspective regulatory, institutional, and technical operational research This serve findings empirical about readiness infrastructure , governance , and competence apparatus , as well as show How dynamics local influence effectiveness data protection a aspects that have not been Lots reviewed in study previously. With Thus, the study This expected No only enrich literature about personal data protection in the sector public, but also provide input practical for government area in strengthen policies and mechanisms data security.

Research methods used is approach descriptive qualitative with analysis regulations as well as interview deep with apparatus the government involved in data management on services digital public. Approach This allows researchers get description comprehensive about practices, constraints, and opportunity repair implementation of the PDP Law at the level area. In a way overall, research This own significance in clarify to what extent is readiness and compliance government area to mandate of the PDP Law in the middle increasing digitalization service public. Because of this that, question underlying research studies This is: *How implementation personal data protection in service digital public in West Java after enactment of the PDP Law, and factors What only that affects effectiveness implementation ?*

Results and Discussion

1. Implementation Regulation of the PDP Law in West Java Digital Public Services

The enactment of the Personal Data Protection Law (PDP Law) marks a new era strengthening right privacy citizens and data governance in Indonesia . Law This No only present framework comprehensive law, but also affirms not quite enough answer government as data controller and processor in every organization service digital [5]public . In the context of West Java, regulations This become reference main for organizer service digital public for adapt procedure technical and institutional in personal data management society , especially Because province This manage sufficient volumes of population data big through integrated digital services. Implementation regulatory seen through a number of step early, such as compilation internal guidelines, updates clause policy privacy on digital platforms, strengthening mechanism consent management, and improvement awareness apparatus about classification of personal data that is general and specific[6]. These efforts show existence commitment beginning government area For adjusting governance digital services with principles applicable data protection in a way national.

Although Thus, the results interviews and reviews regulations show that implementation regulatory Not yet evenly throughout agency area . Differences readiness inter-institutional Still Enough striking, especially in services managed by agencies that have level digital literacy varies. Some service units has adopt aligned internal policies with the PDP Law and start apply standard minimum data security , such as restrictions access based on roles and procedures notification incident. However, some other Still referring

[1] Government of the Republic of Indonesia, *Law Number 27 of 2022 concerning Personal Data Protection* .
[2]Solove, Daniel J., & Schwartz, Paul M., *Information Privacy Law* , Oxford University Press, 2020.
[3]OECD, *Data Governance in the Public Sector: Enhancing Data-driven Public Value* , OECD Publishing, 2021
[4]Warren, Samuel & Brandeis, Louis, "The Right to Privacy," *Harvard Law Review* , 1890.
[5] **Government of the Republic of Indonesia, *Law Number 27 of 2022 concerning Personal Data Protection***
[6]Solove, Daniel J., & Schwartz, Paul M., *Information Privacy Law* , Oxford University Press, 2020

to old regulations such as the ITE Law or Minister of Home Affairs Regulation related System Government Electronic Based (SPBE), which does not in a way specific arrange principles personal data protection as required by the PDP Law [7].

Asynchrony This show that harmonization policy derivatives of the PDP Law at the level area Still be at the stage early. Delay compilation regulations technical at the level national, such as regulation implementer about data controllers, data processors , and compliance audit mechanisms, as well influence readiness area in translate the PDP Law operational [8]conditions the indicates the need mentoring intensive from government center especially the Ministry of Communication and Information and the Ministry of Administrative and Bureaucratic Reform so that the government area get clarity framework implementation, standardization data security, and reporting formats uniform incidents. In addition, consolidation cross-organizational in West Java is necessary strengthened because of public data governance in the regional digital ecosystem nature interconnected, so that unpreparedness One agency can potential bother integrity overall system service digital public.

2. Institutional Governance and the Role of Data Controllers

The PDP Law requires existence separation role between *Data Controller* (data controller) and *Data Processor* (data processor) as mechanism purposeful accountability guard security and integrity of personal data in every process of collection , storage , and data [9]processing . However in in practice , structure organization government area Still Not yet fully accommodate separation function said. Many services digital public at the level province and districts / cities including in West Java managed by the service or technical units that double as as maker policy , management system , data processor , and supervisor internal compliance. Duplicate pattern function This in a way direct contradictory with principle recommended segregation of *duties* in modern data [10]governance. Analysis results show existence several institutional problems that hinder implementation effectiveness of the PDP Law in the region :

Not yet available officials functional specifically for Data Protection Officers (DPO)

Although the PDP Law and standards international data protection as GDPR requires existence officials or special unit in charge answer on compliance personal data management , some big agency government areas in West Java have not yet own personnel specially designated as a DPO [11]. Apart from the absence nomenclature position functional support role this, ability technical and legal about data privacy is also still limited. Assigned apparatus often originate from background behind IT alone , without understanding deep about aspect law data protection.

Coordination inter-agency not optimal

Coordination cross-organizational is element important in public data governance, especially Because Lots digital sharing services or each other connecting different database. However, many regional digital platforms Still walk in silos, so that data exchange no own uniform governance standards . Situation This No only increase risk inconsistency policy data security , but also makes it difficult implementation principle *data minimization*, validation access, and internal[12] control audits. Fragmentation coordination This

[7]Ministry of Communication and Information of the Republic of Indonesia, *Guidelines System Government Electronic Based* , 2023.

[8]OECD, *Digital Government Review: Enhancing Data Governance in the Public Sector* , OECD Publishing, 2021.

[9] Government of the Republic of Indonesia, *Law Number 27 of 2022 concerning Personal Data Protection* .
[10] OECD, *Data Governance in the Public Sector*, OECD Publishing, 2021.
[11] Voigt, Paul & Von dem Bussche, Axel, *The EU General Data Protection Regulation (GDPR): A Practical Guide*, Springer, 2017.
[12] Janssen, M. & Van den Hoven, J., "Big Data and Public Sector Governance," *Government Information Quarterly*, 2015.

the more seen when there is difference perception inter-agency about obligation reporting incident data leaks and procedure giving access to party third.

The gap literacy and capacity apparatus

Literacy level apparatus government to principle base data protection is still varies. Many employees have not understand in a way comprehensive draft *data minimization*, *lawful processing* , *consent management* , and *data breach notification* which are foundation main in the PDP Law and global data [13]protection policy . As a result, a number of practice field data collection Still done in a way over - *collection* , storage No in accordance standard security , and mechanisms agreement No explained in a way transparent to inhabitant . Problem institutional the show that transition towards mature data governance No only need regulations , but also changes structural and cultural in organization government area . Regulation without supported mechanism strong institutions will produce *compliance gap* , where the rules only adopted formally but No implemented in a way substantive [14]. Therefore that , strengthening institutional is prerequisite main For ensure that PDP Law requirements can implemented in a way effective , consistent and sustainable throughout ecosystem service West Java digital public .

3. Readiness Infrastructure and Security Technology

Aspect technical-operational is foundation main in ensure protection of personal data , because weakness technical potential become door enter to leakage and data misuse . In some year Lastly , West Java has show commitment For increase digital infrastructure , including through development regional data center , use technology encryption , implementation protocol security network , as well as utilization *cloud services* For support cross-service [15]data storage and integration . This effort in line with standard security information international such as ISO/IEC 27001 which emphasizes the need management security information in a way comprehensive , starting from control access until mitigation risk systemic [16]. However Thus , the findings field disclose existence a number of challenges that still exist hinder implementation personal data protection optimally :

Inequality infrastructure between service

Not all service digital public in West Java has standard same security . Some applications has apply *multi-factor authentication* and systems modern encryption , while application other Still depend on method authentication simple like *single password login* . Conditions This show existence imbalance in level maturity technology between the organizing units services . Inequality This can increase risk attack cyber Because service with security low can become point enter for attacker For access other connected systems in regional [17]digital ecosystem **.**

Limitations budget security cyber

Shopping technology information government area generally focused on development application new and integration service , but Not yet in a way proportional allocate budget For improvement security cyber . Many agencies Not yet carry out update system in a way periodically , not yet conduct a security audit independent , and not operate testing vulnerability (*penetration testing*) as routine activities . Conditions This contradictory with principle *security by design* and *security by default* which are part important in personal data protection according to framework regulations international and the PDP Law [18]. As a result , the potential vulnerability technical often No detected until incident happen .

Potential leaks from third parties (IT vendors)

[13] Solove, Daniel J., *Understanding Privacy*, Harvard University Press, 2008.

[14] Lodge, M. & Wegrich, K., *The Problem-Solving Capacity of the Modern State*, Oxford University Press, 2014.
[15] Kemenkominfo RI, *Laporan Pembangunan Infrastruktur TIK Nasional*, 2023.
[16] ISO/IEC 27001:2013, *Information Security Management Systems Requirements*.
[17] ENISA (European Union Agency for Cybersecurity), *Threat Landscape Report*, 2021.
[18] Voigt, P. & Von dem Bussche, A., *The EU GDPR: A Practical Guide*, Springer, 2017.

In developing digital systems, local governments often collaborate with third parties or technology vendors. This reliance on vendors can pose additional risks if not accompanied by a Data Processing Agreement (*DPA*) that regulates data security obligations, data usage restrictions, and liability in the event of a breach [19]. The absence of a DPA can lead to weak oversight mechanisms for how vendors manage personal data, increasing the risk of data leaks, *data scraping* , and data misuse for purposes beyond public services. These findings emphasize that personal data protection cannot be viewed as a purely technical issue, but requires strong integration between technological security, institutional governance, and regulatory compliance.[6] These three form [20]an interdependent ecosystem; weaknesses in one aspect can erode the effectiveness of others. Therefore **,** that , the effort increase personal data protection in West Java demands approach holistic that is not only build infrastructure technology , but also strengthen human resource capacity , ensuring compliance law , and create coordination solid inter-agency .

4. Challenges in Implementing the PDP Law in Regional Government Environments

Based on regulatory, institutional, and technical analysis, several fundamental challenges affect the effective implementation of the PDP Law in West Java. These challenges indicate that regional government preparedness is uneven and requires strengthening of policies, organizational structures, apparatus competencies, and oversight mechanisms. Broadly speaking, these challenges can be grouped into the following five main categories:

Normative Challenges

One of the biggest obstacles to the implementation of the Personal Data Protection Law at the regional level is the lack of derivative legal instruments in the form of Regional Regulations (Perda) or Governor Regulations (Pergub) that regulate personal data management more operationally.1 [21]The absence of derivative regulations means that regional agencies lack uniform technical guidelines for implementing the principles of the Personal Data Protection Law, such as data processing mechanisms, risk classification, or minimum security standards. Furthermore, several operational guidelines still refer to outdated provisions such as the ITE Law and the SPBE regulation, which were not specifically designed to regulate personal data protection [22]. This regulatory disharmony creates uncertainty in interpretation, resulting in inconsistent implementation of the Personal Data Protection Law across agencies.

Challenge Organizational

From the side institutional , lack of officials functional *Data Protection Officer* (DPO) becomes inhibitor main . In fact , DPO is actor responsible key answer monitor compliance , providing recommendations , and become connector between institutions and authorities supervisor [23]. Lack of specialized human resources cause not quite enough answer frequent data protection held by IT employees or administration that is not own competence law and privacy . In addition , it has not the existence of a special unit that handles supervision PDP compliance causes the internal monitoring process to not be walk systematic . Many agencies Not yet own internal audit mechanisms and structured *risk assessment* . This condition hinders the early detection of data breach risks .

Technical Challenges

Challenge technical appear from inequality quality security application between service digital public . Some applications has apply authentication dual , encryption , and control access based role ; however Still Lots other applications that do not fulfil minimum safety standards cyber . This is enlarge potential gap security vulnerabilities . [24]Furthermore, regional IT infrastructure has not fully adopted

[19] Information Commissioner's Office (ICO), *Guidance on Data Processing Agreements*, UK, 2020.
[20] OECD, *Digital Government Review: Enhancing Data Governance in the Public Sector*, OECD Publishing, 2021.
[21]Rosadi, Otong, *Personal Data Protection Law in Indonesia* , 2023.
[22]Ministry of Communication and Information of the Republic of Indonesia, *Guidelines System Government Electronic Based* , 2021.
[23]Voigt, P. & Von dem Bussche , A., *The EU General Data Protection Regulation (GDPR): A Practical Guide* , Springer, 2017.
[24]ENISA, *Cybersecurity Threat Landscape Report* , EU, 2022.

international standards such as ISO/IEC 27001 for information security management. [25]*Budget* constraints and spending priorities focused on developing new applications often lead to the neglect of security updates and system audits.

Challenge Culture and Literacy

Culture organization and level literacy apparatus become factor important things that are often ignored . Awareness employee to importance personal data protection Still low , so that procedure security often viewed as burden administrative solely [26]. In some case , personal data considered as " general data " so that can accessed and shared without procedure adequate security . This show that training literacy privacy and security cyber not optimal. Habits less organization discipline in documentation data processing , management digital archives , and use device personal (*Bring Your Own Device*) enlarge risk undetected data leaks detected .

Challenge Oversight and Accountability

Supervision is element important in governance data protection . However , internal audit mechanisms and external in many agency government area Not yet walk effective . There is no routine audit obligations result in an evaluation process security No systematic and vulnerable find problem in a way too late . In addition , reporting personal data incident (*data breach notification*) has not been become habit organization [27]. Many incidents technical No recorded formally because No There is standard agreed reporting or concern will impact reputational . As a result , the response to incident become slow and frequent No in accordance with standard international which emphasizes transparency and mitigation fast . Challenges the show existence wide *implementation* gap between mandate normative PDP Law and reality operational in the area **[28].** This gap No only due to limitations source Power technical and institutional factors , but also by factors culture organization and not yet maturity of public data governance . Therefore Therefore , the implementation of the PDP Law requires approach holistic involving harmonization regulation , strengthening human resource capacity , improvement infrastructure security , as well as formation mechanism clear and continuous supervision .

5. Impact Implementation of the PDP Law on West Java Digital Public Services

Although implementation of the Personal Data Protection Law (PDP Law) in the environment government area Still face a number of challenge regulatory , institutional , technical , and cultural , implementation beginning regulations This has bring a number of impact positive to governance improvements service digital public in West Java. Impact This show existence shift paradigm from an efficiency - oriented service model administrative solely going to attentive service aspect protection right privacy citizen .

Improvement Awareness Institutional

One of most significant impact is increasing awareness institutional to importance personal data protection as component main in organization service public . Apparatus government area start understand that data protection is not only obligation law , but also part from improvement quality services and efforts build trust Public awareness is reflected in increased internal discussions, public awareness of personal data categories, and the emergence of internal policy [29]- making initiatives related to data processing. This institutional awareness also encourages agencies to be more cautious in collecting and storing data, and to begin considering the legal and reputational risks that can arise from privacy breaches [30].

Repair Procedure Data Management

[25]ISO/IEC 27001:2013, *Information Security Management Systems Requirements* .
[26] Solove, Daniel J., *Understanding Privacy*, Harvard University Press, 2008
[27] Information Commissioner's Office (ICO), *Data Breach Reporting Guidelines*, UK, 2020.
[28] Lodge, M. & Wegrich, K., *The Problem-Solving Capacity of the Modern State*, Oxford University Press, 2014.
[29] Warren, S. & Brandeis, L., *The Right to Privacy*, Harvard Law Review, 1890.
[30] OECD, *Digital Government Review: Enhancing Trust in Public Sector Data Governance*, 2021

The implementation of the PDP Law encourages a number of service digital public for repair procedure personal data management . Some application start apply principle *data minimization* , namely only collect real data required For objective services [31]. In addition , the flow data storage and processing into more clear , including identification responsible actor answer on every stage data management . This reform covers implementation mechanism control access based on role - *based access control* , related SOP updates data processing , as well as improvement practice security system through encryption and monitoring activity This effort marks the first step towards more systematic data governance that meets international privacy standards.

Standardization of Digital Privacy Policy

Another positive impact is the initial standardization of privacy policies *across* various digital platforms in West Java. Many services have updated their privacy policy pages to include the purpose of data processing, the legal basis for processing, the data retention period, and data subject rights, such as the right to access, correct, and delete personal data [32]. This change is an important step because privacy policies serve as a transparency tool between the government and the public. This transparency is the foundation for building digital trust , which is essential in a technology-based public service ecosystem [33].

Impacts are Still Partial and Limited Implementation

Although a number of change positive has visible , impact implementation of the PDP Law is still nature partial and not yet comprehensive throughout agency government area . Many service units have not yet renew policy privacy , not yet apply mechanism *consent management* , and not yet have SOP for handling incident data leaks . In addition , the practice data processing is still often done without documentation adequate , and a number of application Still collect data in a excessive without base clear law . Limitations This show that success implementation of the PDP Law is not only depends on regulations , but also requires readiness institutional , availability source Power humans , as well as support budget and infrastructure technical [34]. In other words, the implementation of the PDP Law is still be at the stage transition towards better data governance mature , and its impact will more significant if government area capable overcome challenge structural that has been identified previously .

6. Integrative Approach in Understanding PDP Implementation

The novelty of this research lies in its integrative approach, which simultaneously combines three layers of analysis: regulatory, institutional, and technical-operational. This approach differs from most previous research, which tends to view personal data protection issues sectorally from a separate legal, information technology, or government administration perspective [35]. By integrating these three dimensions, this research provides a more comprehensive and contextual understanding of the dynamics of the implementation of the Personal Data Protection Law at the local government level.

Regulatory Dimension

In the first layer, this study analyzes how the PDP Law is interpreted and translated into regional-level policies, including Gubernatorial Regulations, technical guidelines, and internal SOPs. This analysis is crucial because the effective implementation of the PDP Law depends heavily on the harmonization of national and regional policies [36]. This approach allows researchers to identify *policy gaps* and normative barriers that would otherwise be invisible if research focused solely on formal legal aspects.

Institutional Dimension

[31] Voigt, P. & Von dem Bussche, A., *The EU GDPR: A Practical Guide*, Springer, 2017.
[32] Information Commissioner's Office (ICO), *Guide to Privacy Notices*, UK, 2020.
[33] Janssen, M., Charalabidis, Y., & Zuiderwijk, A., "Transparency in Digital Government," *Government Information Quarterly*, 2012.
[34] Lodge, M. & Wegrich, K., *The Problem-Solving Capacity of the Modern State*, Oxford University Press, 2014.
[35] Yakowitz, Jane, "Tragedy of the Data Commons," *Harvard Journal of Law & Technology*, 2011.
[36] Rosadi, Otong, *Hukum Perlindungan Data Pribadi di Indonesia*, 2023.

The institutional dimension examines how organizational structures and key roles such as *Data Controller* , *Data Processor* , and *Data Protection Officer* (DPO) are established and implemented within the context of local government [37]. Previous research rarely places institutions as a primary variable, even though the success or failure of PDP implementation is heavily influenced by organizational capacity, inter-agency coordination, and the competence of staff. This approach demonstrates how non-technical factors are the primary determinants of data protection effectiveness.

Technical-Operational Dimension

This dimension examines how digital systems, IT infrastructure, and cybersecurity standards play a role in supporting or hindering the implementation of the Personal Data Protection Law. By incorporating technical-operational aspects into the analytical framework, this study demonstrates that data protection cannot be separated from the readiness of infrastructure and technological security mechanisms [38]. This technical dimension is rarely examined in depth in public policy research related to personal data. This integrative approach produces a more comprehensive picture than previous research that separates Personal Data Protection issues into specific analytical silos. Thus, this study enriches scientific understanding of the implementation of Personal Data Protection at the regional level and makes a significant contribution to the development of public data governance models in Indonesia [39]. This approach can also be used as a basis for formulating a framework for evaluating Personal Data Protection policies at the subnational level, which has been limited to date.

Conclusion

The implementation of the Personal Data Protection Law (PDP Law) in the digital public service ecosystem in West Java indicates that local governments are in a transition phase toward more mature, accountable data governance oriented toward protecting citizens' privacy rights. The study revealed that although various initial steps have been taken—such as adjusting privacy policies, increasing awareness among officials, and improving some data management procedures—these efforts remain uneven across all regional apparatuses. From a regulatory perspective, the lack of derivative regulations in the form of Regional Regulations (Perda) or Governor Regulations (Pergub) has resulted in a lack of synchronization in operational guidelines and policy interpretations between agencies. From an institutional perspective, the absence of a dedicated *Data Protection Officer* (DPO), weak cross-organizational coordination, and low literacy among officials pose significant obstacles to the implementation of personal data protection principles. Meanwhile, from a technical-operational perspective, the disparity in application security quality, limited cybersecurity budgets, and risks posed by third parties demonstrate that data protection cannot be separated from the readiness of infrastructure and technological security mechanisms. Overall, the implementation of the Personal Data Protection Law in West Java has shown initial progress, but strategic and systematic steps are still needed to ensure consistent, effective, and sustainable protection of people's personal data. Local governments need to strengthen regulatory harmonization, improve institutional capacity, standardize technical security, and build a more privacy-sensitive organizational culture. These integrated efforts are key to ensuring that West Java's digital transformation goes hand in hand with respect for citizens' fundamental rights.

[37] Voigt, P. & Von dem Bussche, A., *The EU GDPR: A Practical Guide*, Springer, 2017.
[38] ENISA, *Privacy and Data Protection Engineering*, European Union Agency for Cybersecurity, 2021.
[39] OECD, *Digital Government Review: Data Governance and Public Sector Accountability*, 2021.

References

Book

Lodge, Martin, and Kai Wegrich. 2014. *The Problem-Solving Capacity of the Modern State* . Oxford: Oxford University Press.

Rosadi, Otong. 2023. *Personal Data Protection Law in Indonesia* . Jakarta: Kencana.

Solove, Daniel J. 2008. *Understanding Privacy* . Cambridge: Harvard University Press.

Solove, Daniel J., dan Paul M. Schwartz. 2020. *Information Privacy Law*. Oxford: Oxford University Press.

Voigt, Paul, dan Axel von dem Bussche. 2017. *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Switzerland: Springer.

Jurnal

Bărcanescu, Emilia D. 2020. "Cybersecurity Threats and Data Breaches: Awareness and Privacy Protection in the Digital Era." *Journal of Information Systems & Operations Management* 14(1): 23–34.

Cavelty, Myriam Dunn. 2014. "Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities." *Science and Engineering Ethics* 20(3): 701–715.

Custers, Bart, Eduard de Bruin, dan Simone van der Hof. 2019. "Data Protection and Privacy in Public Sector Innovation: Balancing Public Value and Privacy Risks." *Government Information Quarterly* 36(4): 101392.

Gellert, Raphaël, dan Serge Gutwirth. 2013. "The Legal Construction of Privacy and Data Protection." *Computer Law & Security Review* 29(5): 522–530.

Janssen, Marijn, Yannis Charalabidis, dan Anneke Zuiderwijk. 2012. "Benefits, Adoption Barriers and Myths of Open Data and Open Government." *Government Information Quarterly* 29(4): 485–493.

Janssen, Marijn, dan Jeroen van den Hoven. 2015. "Big Data and Public Sector Governance: Promises and Pitfalls." *Government Information Quarterly* 32(3): 257–264.

Warren, Samuel, dan Louis Brandeis. 1890. "The Right to Privacy." *Harvard Law Review* 4(5): 193–220.

Kuhlmann, Sabine, dan Hellmut Wollmann. 2019. "Digital Era Governance and Administrative Capacity." *Public Administration Review* 79(3): 335–346.

Koops, Bert-Jaap. 2014. "The Trouble with European Data Protection Law." *International Data Privacy Law* 4(4): 250–261.

Meijer, Albert, dan Manuel Pedro Rodríguez Bolívar. 2016. "Governing the Transition to Open Government: Challenges and Opportunities." *Information Polity* 21(4): 249–260.

Nissenbaum, Helen. 2004. "Privacy as Contextual Integrity." *Washington Law Review* 79(1): 119–157.

Regan, Priscilla M. 2019. "Privacy and Data Protection in the Digital Era: European and U.S. Approaches." *Annual Review of Political Science* 22: 243–259.

Ruijer, Erna, Stephan Grimmelikhuijsen, dan Albert Meijer. 2017. "Open Government Data and Public Sector Accountability: Understanding the Effects." *Government Information Quarterly* 34(1): 45–55.

Schneider, C. Johannes. 2022. "Digital Trust: A Foundational Component of Public Sector Digitalization." *Government Information Quarterly* 39(2): 101676.

Solove, Daniel J. 2007. "A Taxonomy of Privacy." *University of Pennsylvania Law Review* 154(3): 477–564.

Warren, Samuel, dan Louis Brandeis. 1890. "The Right to Privacy." *Harvard Law Review* 4(5): 193–220.

Wirtz, Bernd W., Jan C. Weyerer, dan Carolin Geyer. 2019. "Artificial Intelligence and the Public Sector—Applications and Challenges." *International Journal of Public Administration* 42(7): 596–615.

Yakowitz, Jane. 2011. "Tragedy of the Data Commons." *Harvard Journal of Law & Technology* 25(1): 1–67.

Dokumen Organisasi / Standar Internasional

ENISA. 2021. *Cybersecurity Threat Landscape Report*. European Union Agency for Cybersecurity.

ENISA. 2021. *Privacy and Data Protection Engineering Guidelines*. European Union Agency for Cybersecurity.

ISO. 2013. *ISO/IEC 27001:2013 Information Security Management Systems Requirements*. Geneva: International Organization for Standardization.

OECD. 2021. *Digital Government Review: Enhancing Data Governance in the Public Sector*. Paris: OECD Publishing.

Regulasi

Indonesia. 2022. *Law Number 27 of 2022 concerning Personal Data Protection* . Ministry of Communication and Informatics of the Republic of Indonesia. 2021. *Guidelines System Government Electronic Based (SPBE)* .

Website

Information Commissioner's Office (ICO). 2020. "Guide to Privacy Notices." Accessed 12 January 2025. https://ico.org.uk

.

Information Commissioner's Office (ICO). 2020. "Data Breach Reporting Guidelines." Accessed 12 January 2025. https://ico.org.uk .