Implementation of Personal Data Protection on Online Tax Websites DKI Jakarta

Indra Nurmansyah[1]*, Luthy Yustika[2]

[1,2]Faculty of Law, Universitas Esa Unggul, Jakarta, Indonesia
Correspondent Author:
E-mail:indranurmansyah30@student.esaunggul.ac.id

Abstract

This study aims to analyze the implementation of Law Number 27 of 2022 on Personal Data Protection (PDP Law) in the management of data on the DKI Jakarta Online Tax website. The research problem focuses on data governance, protection mechanisms, access restrictions, fulfillment of data subject rights, and preparedness for incident response. The study employs a qualitative approach through in-depth interviews with officials and system and data administrators at the DKI Jakarta Regional Revenue Agency (Bapenda) and the Tangerang Regency Regional Revenue Agency. The findings indicate that Bapenda collects personal data such as National Identification Numbers (NIK), names, addresses, marital status, and other personal information for the purposes of taxpayer validation and policy formulation. Data protection measures are implemented through encryption, role-based access control, activity monitoring and logging, as well as periodic security audits. Mechanisms for taxpayer services have been established to facilitate requests for data access, rectification, and objections in accordance with the provisions of the PDP Law. In addition, Bapenda has established incident response procedures implemented by an internal Computer Security Incident Response Team (CSIRT) through processes of identification, analysis, recovery, and notification within 3×24 hours in the event of a data breach. The challenges encountered include harmonization between the PDP Law and government archival regulations, as well as the enhancement of security awareness and literacy among employees and taxpayers. This study concludes that the implementation of personal data protection on the DKI Jakarta Online Tax website has generally been effective; However, further improvements are required in data retention policies and the formal appointment of a Data Protection Officer.

Keywords:*Personal Data Protection, Online Tax System, Data Governance.*

1. INTRODUCTION

Digital transformation in the government sector has brought significant changes to the way public services are delivered, including regional tax services. The DKI Jakarta Online Tax website has become a crucial tool, facilitating taxpayers in fulfilling their administrative obligations electronically. However, this ease of digital access is accompanied by an increased risk of personal data misuse. The enactment of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) reinforces the urgency of data protection in the provision of technology-based public services (Mariyam, 2024).

Based on this, this study is urgently needed to examine whether the management of personal data within a Tax service on the DKI Jakarta Online Tax Website is in line with applicable national legal provisions. Inconsistencies in personal data processing with the principles of legality, purpose limitation, and security as stipulated in the PDP Law have the potential to create legal issues. Furthermore, the potential inconsistency between the obligations of government agencies to maintain tax archives and the rights of data subjects under the PDP Law poses a challenge for the DKI Jakarta Regional Revenue Agency (Bapenda) as a digital service provider (Wahyudi et al., 2024). This issue is increasingly relevant considering that the DKI Jakarta Online Tax website manages sensitive data such as National Identity Number (NIK), addresses, and residency status, which require a robust security system. Therefore, this study is needed to understand how legal regulations regarding personal data protection are practically implemented in the DKI Jakarta Online Tax system.

In this context, this study aims to explain the compliance of personal data management practices at the Jakarta Regional Revenue Agency (Bapenda) with the principles stipulated in the Personal Data Protection Law (PDP). The main idea of this study is that personal data protection must be implemented comprehensively, starting from the legal basis and internal policies to technical and administrative mechanisms. Supporting ideas supporting this study include the importance of internal access control, the use of encryption, incident response procedures, and mechanisms for serving the rights of personal data subjects. Supporting data was obtained through in-depth interviews with officials from the Jakarta Regional Revenue Agency (Bapenda) and officials from the Tangerang Regency DPMPTSP who handle information systems, data policies, and information security, thus providing an empirical picture of the implementation of data protection in practice (Widiarti, 2024).

Based on the background above, the problem formulation in this study is divided into two, namely (1) What are the legal regulations regarding personal data protection according to Law Number 27 of 2022 concerning Personal Data Protection? and (2) How is personal data protection implemented on the DKI Jakarta Online Tax website?

II. RESEARCH METHOD

The method applied in implementing this research is an empirical legal approach, namely an approach that examines the effectiveness of the application of legal norms through empirical data in the field (Muhaimin, 2020).

Regarding data types and sources, the researcher used primary and secondary data. Primary data was collected through interviews with two sources from the Jakarta Regional Revenue Agency (Bapenda) and one source from the Tangerang Regency DPMPTSP:

1. Informant 1: Fransiskus Petta Messakh, System and Data Manager of the DKI Jakarta Regional Revenue Agency (Bapenda).
2. Informant 2: Andri Mauli Rizal, Head of the Extension Implementation Unit of the DKI Jakarta Regional Revenue Agency (Bapenda).
3. Informant 3: Ana Yusrina, Investment and Licensing Supervision, DPMPTSP, Tangerang Regency.

Meanwhile, the secondary data used by researchers is in the form of legislation, scientific journals, and legal literature related to data protection.

Then, the data collection technique was carried out through in-depth interviews using 10 structured questions covering the implementation of the PDP Law, security mechanisms, data subject rights, data retention, and incident handling.

Researchers applied data analysis techniques using an interactive analysis model, which includes data reduction, data presentation, and conclusion drawing. Cross-checking was also conducted between informants' answers and the provisions of the PDP Law to maintain validity.

III. RESULTS AND DISCUSSION

Legal Regulations for Personal Data Protection According to Law Number 27 of 2022 concerning Personal Data Protection

Law Number 27 of 2022 concerning Personal Data Protection serves as the primary basis for every government agency, including the Jakarta Regional Revenue Agency (Bapenda), in managing personal data in online system services. The provisions of the Personal Data Protection Law emphasize the responsibility of data controllers to ensure data processing complies with the principles of legality, purpose limitation, data minimization, accuracy, security, and accountability. In the context of the Jakarta Online Tax service, Bapenda serves as the Data Controller because it collects, stores, and processes taxpayer data for the purposes of tax services and administration.

The personal data protection arrangements on the DKI Jakarta Online Tax website must comply with the security standards required by the Personal Data Protection Law. This includes the use of security technologies, including encryption, authentication systems, role-based internal access control, and logging mechanisms. The Online Tax system is also required to implement purpose restrictions to ensure that collected data is processed solely for tax service purposes and is not used for any other purpose. This principle also ensures that data controllers do not engage in excessive processing that could violate taxpayers' privacy rights (Wiraguna & Barthos, 2025).

In addition to technical aspects, the Data Protection and Data Protection Law also requires data controllers to provide mechanisms for fulfilling data subjects' rights. In the Online Tax system, this is implemented through service facilities for data access requests, data corrections, and objection handling. Verification procedures are implemented to ensure that requests originate from the data owner, thereby preventing identity theft. This regulation demonstrates the principles of accuracy and transparency in taxpayer services.

The PDP Law also requires reporting of personal data breaches. To fulfill this obligation, Bapenda established the Computer Security Incident Response Team (CSIRT) as an incident response unit. This dedicated unit works continuously to address cybersecurity issues through system monitoring, threat identification, incident analysis, and rapid response to ensure data and systems remain protected.

The presence of CSIRT in the digital space is becoming increasingly important because it is tasked with identifying, analyzing, handling, and notifying insThe team complies with the 72-hour time limit stipulated in the Data and Information Technology (PDP) Law. The presence of this team demonstrates that accountability and data security obligations have been internalized within the organizational structure of the Jakarta Regional Revenue Agency (Bapenda).

Through these normative regulations, the DKI Jakarta Online Tax website has essentially been directed to meet all security and personal data governance standards required by the Personal Data Protection Law. However, the effectiveness of its implementation remains dependent on consistent internal procedures, human resource readiness, and the harmonization of taxation and personal data protection policies (Cahyani & Marianata, 2024).

Before the PDP Law was enacted, legal regulations regarding personal data protection were regulated in Article 26Article (1) of Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Electronic Information and Transactions "the use of any information through electronic media concerning a person's personal data must be carried out with the consent of the person concerned" (Anggen Suari & Sarjana, 2023). The weaknesses of this regulation include not clearly defining the type of personal data, not fully regulating the rights of data subjects, there is no specific binding administrative sanctions regime and the sanctions are limited to only applying to the electronic sector.

Then Law No. 71 of 2019 concerning "Electronic Data Storage and Management (PSTE) requires maintaining the confidentiality, integrity, and availability of data and providing notification if"data protection failures occur". However, the regulation still has weaknesses, it does not clearly differentiate between data controllers and data processors. It also does not systematically regulate the rights of data subjects.

In addition, there are other sectoral arrangementsSuch as Law No. 10 of 1998 concerning Banking which stipulates that "Banks are obliged to keep confidential information regarding Customers, Depositors and their deposits."

Law No. 23 of 2006jo. Law No. 24 of 2013 Article 79 paragraph (1) regulates that "personal data and population documents must be kept and their confidentiality protected by the state". Law No. 36 of 2009 concerning "Health also strictly regulates the prohibition on disclosing a person's identity and health data which is expressly regulated in health law because everyone has the right to the confidentiality of their personal health condition that has been disclosed to health service providers". This provision is part of the protection of the right to privacy and confidentiality of patient medical records.

Then according to Article 3 letter g of the LawNumber 43 of 2009 concerning "Archives" regulates that the implementation of archives aims to guarantee the safety and security of archives as evidence of national accountability and protection of state interests and the civil rights of the people.

Law Number 14 of 2008 concerning Public Information Disclosure (UU KIP) also prohibits the disclosure of personal data. Of these laws, all only partially and sectorally regulate data confidentiality, not as a comprehensive digital human right. However, digital transactions and information are currently growing rapidly. Therefore, a comprehensive law governing personal data protection is needed, not a partial one.

How the law rulesWhat are the criminal sanctions for violations of personal data abuse before the enactment of the PDP Law? Criminal remedies depend on the type of violation. For example, perpetrators can be subject to criminal sanctions under Articles 30, 32, and 48 of the ITE Law (illegal access, destruction, or transfer of electronic data). Criminal penalties are generally regulated under Article 378 of the Criminal Code (fraud) if data is used for deception and Article 263 of the Criminal Code (forgery) if a forged document is used. However, there is no specific offense called a "personal data breach," and victim protection is limited. This is because before the PDP Law, personal data protection was not systematic, resulting in a lack of legal certainty. The application of criminal provisions was still scattered across several legal regulations and there was no independent supervisory authority, resulting in unclear and unenforceable data subject rights. This resulted in disproportionate sanctions and a lack of deterrent effect.

The PDP Law then emerged to establish a comprehensive personal data protection regime, affirming the rights of data subjects, regulating the obligations of data controllers and processors, and providing structured administrative, civil, and criminal sanctions.

Implementation of Personal Data Protection on the DKI Jakarta Online Tax Website

The subjects of this study were officials and system managers at the Jakarta Regional Revenue Agency (Bapenda) and Tangerang Regency DPMPTSP officials who understand the application of personal data protection in the Online Tax service. The object of this study was the implementation of personal data protection on the Jakarta Online Tax website, including policies, technical procedures, and taxpayer data management.

The Jakarta Regional Revenue Agency (Bapenda) manages a large amount of taxpayer data. Based on the latest data as of December 31, 2024, the number of registered taxpayers is presented in the following table:

Table 1. Number of Taxpayers in DKI Jakarta as of December 31, 2024

Number of Taxpayers until December 31, 2024	
Per Person	7,188,375

Business entity	322,014
Total	7,510,389

The implementation of personal data protection on the DKI Jakarta Tax Online website for taxpayers' data is carried out through technical and administrative measures in accordance with the provisions of the Personal Data Protection Law. With more than 7.5 million taxpayers, the Tax Online system must ensure that data processing is secure, limited to tax purposes, and accessible only to authorized parties.

Technically, the Pajak Online website uses the https protocol with an active SSL certificate to ensure that all data sent over the network is encrypted and protected from potential eavesdropping. HTTPS, or HyperText Transfer Protocol Secure, secures communication between a website and a user's browser by encrypting it. Ensuring security is crucial when exchanging data online, especially when sharing personal and financial information. HTTPS provides this security by using the SSL (Secure Sockets Layer) or TLS (Transport Layer Security) protocols.

HTTPS is indicated by the phrase https:// appearing in the website's address bar and usually marked with a padlock icon. This means all communications between the website and the browser are encrypted, preventing third parties from accessing this data (Syailendra Putra et al., 2024). This encryption protects sensitive user information (usernames, passwords, credit card information, etc.), thereby reducing the risk of fraud and data theft.

The use of https demonstrates that the Pajak Online server meets basic security standards for digital public services. Furthermore, the system's database is protected by internal encryption, preventing unauthorized access to information such as National ID Numbers (NIK), population data, and taxpayer information. The system is also equipped with a firewall to block malicious external activity and prevent attacks such as brute force attacks, injection attacks, and other unauthorized access.

These security measures are reinforced by regular backup procedures to safe storage, which aim to maintain service continuity and prevent data loss in the event of a system failure or cyberattack. These backups also ensure that data recovery can be performed quickly without causing significant disruption to taxpayers.

From an internal governance perspective, Bapenda's implementation of role-based access control (RBAC) is a model for granting users access to systems, applications, and data based on their assigned roles. For example, a security analyst has the authority to configure the firewall but not access customer data, while a salesperson can access customer data without the authority to change firewall settings.

In the RBAC system, administrators assign specific roles to each user, each with different access rights or permissions. Each employee can only access data according to their function and authority, thereby reducing the risk of data misuse internally. This procedure ensures that personal data cannot be viewed, modified, or distributed by unauthorized parties, in line with the principle of minimizing access stipulated in the PDP Law. Internal activity is recorded through a logging system, which allows monitoring and tracking of any access or changes made to taxpayer data.

In addition, the Jakarta Regional Revenue Agency (Bapenda) provides a service mechanism to fulfill data subject rights, including the right to access, the right to correct data, and the right to object. An identity verification process is carried out before processing requests, ensuring that the request originates from the data owner (Silalahi et al., 2025). This step demonstrates the implementation of the principles of accuracy, transparency, and accountability required by the Data Protection and Data Protection Law.

The establishment of the Computer Security Incident Response Team (CSIRT) by the Jakarta Regional Revenue Agency (Bapenda) is intended as an information security incident response unit. This team handles the identification, analysis, mitigation, and reporting of suspected personal data breaches. Incident notification is required within a maximum of three working days as mandated by the PDP Law. The presence of the CSIRT strengthens the agency's readiness to face security threats and ensures that risk management is carried out in a measured manner.

Overall, the implementation of personal data protection on the DKI Jakarta Online Tax website has covered technical, administrative, and incident response aspects in line with the provisions of the Personal Data Protection Law. However, researchers have found that the DKI Jakarta Online Tax website has not provided any notification to users that all data attached or submitted to the DKI Jakarta Online Tax application is guaranteed confidentiality by the DKI Jakarta Revenue Agency in accordance with the provisions of the PDP Law. Therefore, citizens who use the DKI Jakarta Online Tax website application need not worry because their personal data cannot be misused. Therefore, according to researchers, it is necessary to increase human resource capacity, harmonize internal policies, and periodically evaluate system security so that the implementation of personal data protection can be maintained optimally and sustainably (Pradana & Saragih, 2024).

The researchers then compared the implementation of personal data protection on the SiPinter (Integrated Licensing Service Information System) website in Tangerang Regency. The results of this study indicate that the implementation of personal data protection on the DKI Jakarta Online Tax website and the Tangerang Regency SiPinter website demonstrate a similar approach based on Law Number 27 of 2022 concerning Personal Data Protection.

Although both have the same legal basis, there are significant differences in regulatory transparency, data processing mechanisms, technical security, and system governance. These differences are particularly evident in how each service provides information to the public and how data protection processes are operationally implemented.

Based on interviews with the DKI Jakarta Regional Revenue Agency (Bapenda), the data collected includes Population Identification Numbers, addresses, population identities, and other taxpayer information (Sijabat & Widjaja, 2025). All of this data is used for validation processes, tax services, and the formulation of data-based public policies. However, the DKI Jakarta Online Tax website does not directly state the legal basis for personal data protection according to the PDP Law on its public page and, as stated above, DKI Jakarta Online Tax also does not provide notifications that can be accessed directly by users, either via SMS (Short Message Service) or WhatsApp messages on mobile phones or via incoming messages to each application user's personal email.

The absence of such a display does not diminish the legality of data processing because the authority of the DKI Jakarta Tax Office has been regulated in the DKI Jakarta Regional Government Regulation. However, from the perspective of the principle of transparency according to the provisions of the PDP Law, the absence of regulatory information on the public page indicates a lack of care on the part of the DKI Jakarta Dispenda. Therefore, for future improvements, the DKI Jakarta Dispenda needs to directly include the legal basis for personal data protection according to the PDP Law on its public page and also provide notifications that can be directly accessed by users, either notifications via messages on mobile phones via SMS (Short Message Service) or WhatsApp or via inboxes to each application user's personal email. This is an implication or implementation of legal protection for the personal data belonging to users of the DKI Jakarta Online Tax Website application.

In contrast, the SiPinter Tangerang Regency website has displayed a different implementation, so that the implications of this service have included regulatory information on the PDP Law and emphasized that personal data management has been adjusted to the security standards of the Communication and Information Department and the National Cyber and Crypto Agency. Based on interviews between researchers and officials from the Tangerang Regency Investment and One-Stop Integrated Services Agency (DPMPTSP), the SiPinter application regularly undergoes audits from the National Cyber and Crypto Agency (BSSN) and adjusts all security procedures according to the directions of authorized national institutions. Thus, SiPinter Tangerang Regency demonstrates a higher level of transparency in providing information regarding the legal basis for personal data protection according to the PDP Law on its public page.

Significant differences are also evident in the technical aspects of data security. The DKI Jakarta Online Tax website utilizes encryption, role-based access control, system activity logging, security monitoring, and incident handling through the CSIRT. Meanwhile, SiPinter Tangerang Regency implements a notification process through two-factor authentication in the form of an OTP code sent to the user's phone number. Furthermore, sensitive data such as the National Identity Number (NIK) is masked on the verifier's screen, minimizing the potential for data misuse by internal parties. According to the source, this data masking is part of the implementation of the principles of data minimization and access restriction, which are essential elements in personal data protection.

Regarding third-party management, the Tangerang Regency DPMPTSP provided a more detailed explanation. Application development and maintenance are carried out by experts working under a cooperation agreement and a Non-Disclosure Agreement, a written agreement that binds the parties to maintain the confidentiality of certain information obtained in a legal relationship and prohibits the disclosure, use, or distribution of such information to other parties without permission. This aims to provide clear legal boundaries regarding the obligation to maintain data confidentiality. Interviews regarding DKI Jakarta Online Tax did not provide such detailed information, although its technical governance still follows internal mechanisms and is monitored by the local government.

Implementation challenges also differ between the two systems. Jakarta's Online Tax faces regulatory harmonization challenges, particularly regarding differences in data retention rules between archiving provisions and the Data and Information Technology Law. Conversely, Tangerang Regency's SiPinter faces challenges related to user behavior. Prior to the implementation of OTP authentication, there were cases of account misuse by unauthorized parties. To prevent this, the Tangerang Regency DPMPTSP implemented a policy that requires one National Identification Number (KTP) to be used for only one account in the Online Tax system.

Overall, both services have strived to comply with personal data protection requirements. DKI Jakarta's Online Taxation is more mature in managing large-scale data and has a stable security structure. On the other hand, Tangerang Regency's SiPinter demonstrates stronger public transparency practices, tighter login security, and clearer third-party governance. This comparison demonstrates that each region has implemented the principles of the Personal Data Protection Law according to its respective context and public service needs.

Based on the interview results described above, the researcher then conducted a theoretical analysis of the empirical findings (Setiawan & Samosir, 2023). The researcher employed a legal approach, comparing the provisions of Law Number 27 of 2022 concerning Personal Data Protection with data management practices on the DKI Jakarta Online Tax website. In this approach, the researcher believes that law is viewed not only as written norms but also as institutional behavior in carrying out its obligations. Therefore, the analysis was conducted by comparing the principles of the Personal Data Protection Law with the practices described directly by Bapenda officials in interviews.

Normatively, the PDP Law establishes the principles of legality, purpose limitation, data minimization, accuracy, security, and accountability (Martien, 2023). Research results indicate that most of these principles have been implemented. The use of role-based access control illustrates the restriction of access according to task requirements, in line with the principles of data minimization and purpose limitation. The implementation of encryption and monitoring and logging systems reflects the implementation of data security and integrity principles. Monitoring can be defined as the process of continuously monitoring and evaluating database performance to identify potential problems and ensure system optimization (Hapsari & Endang Wirjatmi TL, 2023). Meanwhile, logging is a mechanism for recording all activities or events in a database, which is useful for tracking changes, analyzing problems, and securing data (Joshua & W. Chandra, 2024). This reflects that data protection obligations are implemented not only as regulations but also as part of daily operations.

The incident response procedures implemented by the Jakarta Regional Revenue Agency's internal CSIRT (Central Data Service Agency) also demonstrate the concrete implementation of the incident notification obligations stipulated in the Personal Data Protection Law (PDP). The stages of identification, analysis, recovery, and notification reflect the implementation of the principles of accountability and institutional responsibility for any risk of personal data breaches (SA et al., 2024). Therefore, the implementation of the law within the Jakarta Regional Revenue Agency (Bapenda) is not merely administrative, but also technical and structured (Gunardi, 2022).

Data subject rights, such as the rights of access and correction, have also been fulfilled through verification mechanisms and official services. These practices demonstrate the implementation of the principles of accuracy and transparency required by the PDP Law. Verification mechanisms ensure that any data changes are carried out legally and securely, while also preventing identity theft.

However, empirical approaches demonstrate a gap between norms and practices, particularly regarding the harmonization of the PDP Law with government archiving regulations, which still require long-term tax data retention. This situation suggests that the effectiveness of law implementation is affected by overlapping regulations binding government agencies. Furthermore, challenges in employee and user security literacy are non-technical factors that can impact the effectiveness of data protection, suggesting that successful law implementation also depends on human resource readiness.

Overall, the empirical analysis shows that the Jakarta Regional Revenue Agency (Bapenda) has implemented the principles of the Personal Data Protection Law (PDP) in various aspects, both technical and administrative. However, improvements to internal policies, such as including the regulatory basis for the PDP Law and providing notifications to each user of the Online Tax Website application, are still needed. Harmonization of archive retention and the formal appointment of a Data Protection Officer are still needed to ensure optimal implementation of personal data protection in accordance with the applicable legal framework.

IV. CONCLUSION

This research shows that personal data protection in the DKI Jakarta Online Tax service is based on the legal framework established by Law Number 27 of 2022 concerning Personal Data Protection. The provisions of this law provide clear guidance regarding the obligations of data controllers, including the principles of legality, purpose limitation, data minimization, accuracy, security, and accountability. Based on the analysis, this legal regulation serves as the primary foundation for the DKI Jakarta Regional Revenue Agency (Bapenda) in developing data protection policies and mechanisms for its digital services. However, the effectiveness of these regulations remains dependent on the consistency of their operational implementation.

The implementation of personal data protection on the DKI Jakarta Online Tax website demonstrates that most of the principles and obligations of the Personal Data Protection Law have been implemented through concrete actions. The use of the HTTPS protocol and SSL certificates, database encryption, firewalls, regular backup systems, and the implementation of internal access restrictions demonstrate that technical aspects of data security have been prioritized. Furthermore, the presence of the CSIRT and mechanisms for fulfilling data subject rights reflect efforts to uphold the principles of accountability and transparency. However, internal policy improvements must continue, such as incorporating the regulatory basis for the Personal Data Protection Law and providing notifications to each user of the Online Tax Website application, as a form of legal protection for personal data. Several challenges, such as harmonizing tax archive retention, improving employee security literacy, and strengthening internal oversight structures, also require attention to ensure more comprehensive personal data protection.

V. SUGGESTION

Based on these findings, this study recommends that the Jakarta Regional Revenue Agency (Bapenda) strengthen its personal data protection governance by establishing a more formal oversight structure, enhancing human resource capacity related to information security, and periodically evaluating the Online Tax system to ensure ongoing compliance. Furthermore, regulatory harmonization between personal data protection rules and government archiving provisions is needed to avoid policy conflicts in the management of taxpayer data. Comprehensive improvements in data security and governance are expected to achieve digital tax services that are safe, reliable, and compliant with applicable laws.

REFERENCES

[1] Anggen Suari, KR, & Sarjana, IM (2023). Maintaining privacy in the digital era: Personal data protection in Indonesia. Journal of Legal Analysis, 6(1), 132–142. https://doi.org/10.38043/jah.v6i1.4484

[2] Cahyani, WD, & Marianata, A. (2024). Analysis of personal data protection policies in Bengkulu City: Study of the implementation of the PDP Law in the digital era. Journal of Law and Public Policy Studies, 2(1), 623–626. https://jurnal.kopusindo.com/index.php/jkhkp/article/view/473

[3] Gunardi. (2022). Legal research methods. Damera Press.

[4] Hapsari, NW, & Wirjatmi TL, HTGE (2023). Optimization of monitoring and evaluation activities in the regional research. Journal of Applied Media Administration (JMAT), 4(1), 19–25.

[5] Joshua, I., & Chandra, DW (2024). Analysis of logging and auditing of SQL database access via remote connections using AnyDesk. JATI (Journal of Informatics Engineering Students), 7(6), 3180–3186. https://doi.org/10.36040/jati.v7i6.8072

[6] Mariyam, YS (2024). E-government in public services. CV Azka Pustaka.

[7] Martien, D. (2023). Legal protection of personal data. Mitra Ilmu.

[8] Muhaimin. (2020). Legal research methods. Mataram University Press.

[9] Pradana, MAE, & Saragih, H. (2024). The principle of accountability in the Personal Data Protection Act against GDPR and its legal consequences. Journal of Social Science Research, 4(4), 3412–3425.

[10] R., SA, Sadi, M., Rani, FH, & Arda, DJ (2024). Legal protection. CV Doki Course and Training.

[11] Setiawan, IKO, & Samosir, T. (2023). Legal research methodology. Reka Cipta Publisher.

[12] Sijabat, FM, & Widjaja, G. (2025). Cybersecurity and data protection in digital taxation system. Sibatik Journal, 4(4), 325–334. https://publish.ojs-indonesia.com/index.php/SIBATIK

[13] Silalahi, JAS, Purba, YY, & Nasution, MF (2025). A legal analysis of personal data protection mechanisms in electronic information systems based on a criminal law perspective in Indonesia. Jurnal Minfo Polgan, 14(1), 604–613. https://doi.org/10.33395/jmp.v14i1.14810

[14] Syailendra Putra, MR, Purwanti, PA, & Istisofani, AS (2024). Data security analysis in legal telematics: Between privacy and transparency. Journal of Legal Accounting and Education, 1(2), 633–642. https://doi.org/10.57235/jahe.v1i2.3875

[15] Wahyudi, I., Yunus, S., Lutfi, M., Musdayati, & Jaya, AH (2024). Journal of Politics and Regional Government, 6(1), 177–188.

[16] Widiarti, WS (2024). Legal research methods. Global Medika Publication.

[17] Wiraguna, SA, & Barthos, M. (2025). Privacy law & personal data protection in Indonesia. Widina Media Utama.