JLPH: Journal of Law, Politic and Humanities
E-ISSN: 2962-2816
P-ISSN: 2747-1985
https://dinastires.org/JLPH dinasti.info@gmail.com +62 811 7404 455

DOI: https://doi.org/10.38035/jlph.v7i1
https://creativecommons.org/licenses/by/4.0/
Received: 31 Oktober 2026 | **Revised:** 01 November 2026 | **Accepted:** 05 November 2026

The Role of Village Government in Ensuring Citizens' Personal Data Confidentiality in Digital Administrative Services

Rahmat Pirdaus[1], Yandi[2], Enny Agustina[3]
[1]Universitas Pertiba, Pangkalpinang, Indonesia, rahmatpirdaus@gmail.com
[2]Universitas Pertiba, Pangkalpinang, Indonesia, yandipertiba67@gmail.com
[3]Universitas Pertiba, Pangkalpinang, Indonesia, ennyagustinadua@yahoo.com

Corresponding Author: rahmatpirdaus@gmail.com[1]

Abstract: Village digitalization has become a policy priority in Indonesia to improve village governance, but it raises legal complexities regarding the management of residents' personal data. This study examines the relationship between attributive village authority under Law Number 3 of 2024 concerning the Second Amendment to Law Number 6 of 2014 on Villages and personal data protection obligations under Law Number 27 of 2022. It addresses normative ambiguity concerning the limits of village authority and the lack of integrated legal construction between these regimes. Using a normative juridical method with statutory and conceptual approaches, this research analyzes the scope and boundaries of village authority in personal data management and its legal implications in the digitalization era. The findings show that such authority must be limited by core data protection principles, including lawfulness, purpose limitation, data minimization, and accountability, ensuring that local authority does not justify violations of constitutional rights. Key challenges include limited technical capacity and legal awareness among village officials, inadequate data security infrastructure, and weak local oversight mechanisms. The study highlights the need for regulatory harmonization, capacity building, improved infrastructure support, and participatory oversight to ensure accountable data governance.

Keywords: Village Digitalization, Personal Data Protection, Village Government Authority

INTRODUCTION

The implementation of village digitalization in Indonesia has given rise to a concrete legal issue in the form of normative ambiguity concerning the limits of village government authority in the management of villagers' personal data. Articles 18 and 19 of Law Number 3 of 2024 concerning the Second Amendment to Law Number 6 of 2014 on Villages confer attributive powers upon village governments to regulate and administer governmental affairs based on *rights of origin* (*hak asal-usul*) and village-scale local authority, which includes the authority to conduct data collection and population administration at the village level (Irfan B & Anirwan, 2024).

However, these provisions do not explicitly stipulate how such authority is to be exercised in the context of personal data processing, particularly following the enactment of Law Number 27 of 2022 on Personal Data Protection (PDP Law), which became fully effective on 17 October 2024.(Chushairi et al., 2025) This ambiguity generates legal uncertainty as to whether village governments may rely on their village-scale local authority as a valid legal basis to collect, store, and process personal data without being bound by the data protection principles set out in the PDP Law, or whether all personal data processing activities undertaken by village authorities must comply with stringent data protection standards irrespective of the source of such authority.

This lack of clarity is further exacerbated by the absence of implementing regulations that specifically govern procedures for personal data management by village governments, thereby giving rise to diverse practices that are often inconsistent with established personal data protection principles (Mirna et al., 2023).

Empirical observations indicate that the implementation of village digitalization through various platforms-such as Village Information Systems and other village administrative applications-has resulted in the large-scale accumulation of villagers' personal data without adequate protection mechanisms. According to data from the Ministry of Villages, Development of Disadvantaged Regions, and Transmigration, as of 2024 more than 50,000 villages have implemented digital village information systems, collecting personal data ranging from population identity records, household economic data, and health information to records of social assistance received by villagers (Mardinata et al., 2023).

In practice, however, such data collection is frequently carried out without providing clear notice to the public regarding the purpose of data collection, how the data will be used, and who will have access to it. More alarmingly, numerous cases have been identified in which personal data-by its nature confidential-has been publicly disclosed on village websites or social media platforms without the consent of the data subject, ostensibly in the name of transparency and accountability. This situation creates significant vulnerabilities to the misuse of personal data, including risks of data breaches, identity theft, and data-driven discrimination against certain groups within village communities (Putri Nugroho et al., 2024).

The gap between *das sollen* (the normative ideal) and *das sein* (the empirical reality) in the implementation of village digitalization becomes evident when confronting the ideal norms of personal data protection, as enshrined in the Constitution and the PDP Law, with the actual practices of data governance at the village level. Article 28G paragraph (1) of the 1945 Constitution explicitly guarantees every individual's right to personal protection, which has been interpreted by the Constitutional Court as encompassing the protection of personal data as an integral component of the right to privacy (Kusnadi, 2021).

The PDP Law further operationalizes this constitutional safeguard through fundamental principles, including lawfulness and fairness, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability, all of which must be observed in any personal data processing activity without exception. However, in reality, personal data management practices at the village level frequently contravene these principles.(Junaedi, 2025) Personal data is often collected excessively and beyond what is necessary and relevant; data is stored without adequate security standards; disclosures to third parties are made without the data subject's consent; and there is no clear accountability mechanism in the event of violations or data breaches.(Silalahi et al., 2025) This disparity demonstrates that, notwithstanding the existence of a comprehensive legal framework for personal data protection, its implementation at the village level remains far below the expected standard.

The urgency of this research lies in the pressing need to construct a clear legal framework delineating the limits of village government authority in managing personal data in

the era of digitalization. While a number of studies have examined village digitalization and personal data protection as separate issues, there has been no comprehensive analysis of the interaction and potential conflict between village governmental authority and the imperatives of personal data protection within the context of digitalization. The identified research gap encompasses three fundamental aspects: first, the absence of studies analyzing how the principles of personal data protection under the PDP Law can and should be applied within the framework of attributive village authority derived from rights of origin; second, the lack of systematic research identifying the legal, technical, and institutional challenges faced by village governments in implementing personal data protection standards; and third, the absence of a comprehensive legal construction concerning mechanisms for harmonizing village governance regulations with personal data protection laws that may serve as practical guidance for village authorities.

Relevant prior research includes the study by Siti Aisyah and Eddy Suriyani (2024), entitled *"Implementation of the Village Digitalization Program (Digides) in Improving Public Services in Kapar Village, Murung Pudak District, Tabalong Regency"*.(Siti Aisyah & Eddy Suriyani, 2024) published in the *Journal of Public Administration*. This study focuses on the effectiveness of village digitalization programs in enhancing the quality of public services but does not analyze the legal implications relating to personal data protection. It concludes that village digitalization significantly improves administrative efficiency, while also identifying challenges such as limited digital literacy and inadequate data security standards.

Another study by Putri, Sari, Fajrina, and Aisyah (2025), entitled *"Online Security in Social Media: The Importance of Personal Data Protection in the Digital Era (Case Study of Pematang Jering Village)"*.(Putri et al., 2024) published in the *Jurnal Pengabdian Nasional Indonesia*, examines public awareness regarding the importance of personal data protection in social media usage, but does not address the scope of village government authority in managing personal data. The study finds that awareness of personal data breach risks remains very low and recommends intensive public education on data security.

The distinguishing feature of the present research lies in its analytical focus, which positions village governmental authority as the central variable in examining the implementation of personal data protection within the context of village digitalization, as well as in its effort to construct a coherent and operational legal framework integrating the village law regime with the personal data protection regime.

Based on the foregoing, this research is directed at addressing two interrelated fundamental questions concerning the governance of personal data at the village level in the context of digital transformation. First, it examines the form and normative limits of village government authority in managing villagers' personal data, particularly in light of the expansion of administrative functions through digitalization. Second, it analyzes the legal implications arising from village digitalization, including the structural and practical challenges in implementing personal data protection within decentralized governance frameworks.

The objectives of this study are to analyze the legal construction of village governmental authority in personal data management by integrating the provisions of the Village Law and the PDP Law, as well as to identify legal implications, implementation challenges, and to formulate policy recommendations for regulatory harmonization and capacity-building of village governments in implementing personal data protection.

The theoretical contribution of this research lies in the development of the concept of conditional authority, whereby village-scale local authority must be exercised in compliance with personal data protection principles as part of the constitutional guarantee of citizens' rights. From a practical perspective, this study is expected to provide operational guidance for village governments in implementing digitalization programs in alignment with personal data

protection standards, as well as to offer input to policymakers in designing more specific implementing regulations concerning personal data governance at the village level.

METHODS

This study employs a normative (doctrinal) legal research method to analyze and construct a legal framework governing the authority of village governments in managing villagers' personal data in the digitalization era. This method is chosen due to the normative nature of the research problem, which focuses on examining legal norms, interpreting statutory provisions, and identifying gaps and inconsistencies within regulations on village authority and personal data protection. The research applies three main approaches: a statutory approach to systematically review relevant laws and regulations, including Law Number 3 of 2024 concerning the Second Amendment to Law Number 6 of 2014 on Villages and Law Number 27 of 2022 on Personal Data Protection; a conceptual approach to analyze key doctrines such as attributive authority, rights of origin, village-scale local authority, privacy, and constitutional rights; and a case approach to assess practical implementation of personal data management at the village level, including instances of violations or disputes.

The study utilizes primary, secondary, and tertiary legal materials. Primary materials include the 1945 Constitution, relevant statutes, implementing regulations, and selected village regulations; secondary materials consist of legal textbooks, journal articles, prior research, and official policy reports; while tertiary materials include legal dictionaries and encyclopedias to support terminological clarity. Data are analyzed qualitatively using a descriptive-prescriptive method, where descriptive analysis explains existing legal frameworks and practices, and prescriptive analysis formulates an ideal regulatory model and policy recommendations. Analytical techniques include grammatical, systematic, and teleological interpretation, alongside comparative analysis to identify normative conflicts between village governance and personal data protection regimes, and to propose mechanisms for legal harmonization in addressing the limits of village authority and challenges of digitalization.

RESULTS AND DISCUSSION

1. The Form and Limits of Village Government Authority in the Management of Villagers' Personal Data in the Era of Village Digitalizationsa

An analysis of the form and limits of village government authority in managing villagers' personal data in the era of digitalization requires a comprehensive understanding of the legal construction of village authority within Indonesia's constitutional system, as well as its relationship with the imperative of personal data protection as a constitutionally guaranteed right. Law Number 3 of 2024 concerning the Second Amendment to Law Number 6 of 2014 on Villages establishes a distinct paradigm of authority for village governments, differing from other governmental entities within the unitary state structure, by recognizing *rights of origin* (*hak asal-usul*) and village-scale local authority as the primary foundations of village authority (Gatot, 2025).

Article 18 of the Village Law stipulates that village authority encompasses governance administration, the implementation of village development, community development, and community empowerment, all of which are carried out based on community initiatives, rights of origin, and village customs and traditions.(Rusnan et al., 2023) This construction of authority is further elaborated in Article 19, which provides that village authority includes: authority based on rights of origin; village-scale local authority; authority delegated by the central government, provincial government, or regency/municipal government; as well as other authority assigned in accordance with prevailing laws and regulations (Lathifatul Mustofa & Yunanto, 2025).

The fundamental characteristic of this construction of village authority lies in its attributive nature, whereby authority derived from *rights of origin* (*hak asal-usul*) and village-scale local authority does not constitute a delegation from supra-village governments. Rather, it represents a formal recognition of the village as a customary law community unit that pre-existed the establishment of the Unitary State of the Republic of Indonesia. This stands in stark contrast to the classical theory of decentralization, under which the authority of autonomous regions is derived from the delegation of powers by the central government (Hariyanto, 2020).

The implication of this attributive authority is that villages possess a significant degree of autonomy to regulate and administer their own governmental affairs without the need to await formal delegation from higher levels of government, provided that such matters fall within the scope of rights of origin or village-scale local authority. (Jefri & Manalu, 2025) In the context of personal data management, this construction provides a legal basis for village governments to conduct data collection, information gathering, and population administration at the village level as part of their governmental functions, without requiring explicit delegation from regency or central authorities.

Nevertheless, the attributive authority vested in village governments cannot be construed as absolute or unfettered power. Article 1 paragraph (3) of the 1945 Constitution affirms that Indonesia is a state governed by the rule of law (rechtsstaat), which implies that all governmental authority including that of village governments must be exercised in accordance with the supremacy of law and within the limits prescribed by the Constitution and statutory regulations (Rifan & Rahmawati, 2021).

In the context of personal data management, the constitutional limitations on village authority derive from Article 28G paragraph (1) of the 1945 Constitution, which guarantees every individual's right to the protection of their person, family, honor, dignity, and property under their control, as well as the right to security and protection from threats that inhibit the exercise of their fundamental rights. (Nenny Rianarizkiwati, 2024) The Constitutional Court, through its jurisprudence, has interpreted this provision as encompassing the protection of personal data as an integral component of the right to privacy and personal security. Accordingly, any governmental action involving the collection, processing, or disclosure of personal data must satisfy certain constitutional standards in order to be deemed lawful and not in violation of citizens' constitutional rights (Arrasuli & Fahmi, 2023).

The enactment of Law Number 27 of 2022 on Personal Data Protection (PDP Law), which became fully effective on 17 October 2024, marks a paradigmatic shift in personal data governance in Indonesia by operationalizing the constitutional guarantee of personal data protection into a comprehensive set of principles, obligations, and legal mechanisms. (Arafat & Alexander Tito Enggar Wirasto, 2024) The PDP Law defines personal data as any data relating to an identified or identifiable individual, whether directly or indirectly, through electronic or non-electronic systems (Hasibuan & Putri, 2024).

This definition encompasses a broad spectrum of data, ranging from basic identity information such as names and national identification numbers to more sensitive categories, including health data, financial information, biometric data, and data concerning children. In the context of village governance, nearly all administrative activities involving villagers such as the issuance of official certificates, registration for social assistance programs, data collection for village development planning, and population administration services involve the collection and processing of personal data. Accordingly, the PDP Law holds substantial normative relevance for the exercise of village governmental authority.

The fundamental principles enshrined in the PDP Law impose significant normative constraints on the scope of village authority in personal data management. Article 5 of the PDP Law provides that personal data processing must adhere to the following principles: lawfulness and fairness, purpose limitation, data adequacy and relevance, accuracy, storage limitation, integrity and confidentiality, and accountability. The principle of lawfulness and fairness, as further elaborated in Article 20, requires that any processing of personal data must be based on a valid legal ground, which may include the consent of the data subject, the performance of a contract, compliance with a legal obligation of the data controller, the performance of a task carried out in the public interest, the protection of vital interests of the data subject, or the legitimate interests of the data controller or a third party (Yudha et al., 2025).

Within the context of village governance, the most relevant legal bases are the performance of public service functions and compliance with legal obligations, implying that the collection and processing of personal data by village authorities must be conducted strictly within the scope of their statutory duties and functions.

Nevertheless, the existence of a legal basis grounded in the performance of public functions does not automatically legitimize all forms of personal data collection and processing by village governments. The principle of purpose limitation, as stipulated in Article 5 paragraph (1)(b) of the PDP Law, requires that personal data be processed for specific, explicit, and lawful purposes, and not further processed in a manner incompatible with those purposes (Anggien Suari & Sarjana, 2023). The implication of this principle is that village governments must clearly define the specific purpose of each data collection activity, and the data collected must not be repurposed for other uses without a valid legal basis and, where required, renewed consent from the data subject.

In practice, this means that personal data collected, for example, for the issuance of a domicile certificate cannot subsequently be used for unrelated purposes such as economic profiling or targeting of social assistance programs without clear legal justification and the data subject's consent.

The principle of data adequacy and relevance, commonly referred to in data protection literature as the data minimization principle, imposes further limitations on the scope of personal data that may be collected by village authorities. Article 5 paragraph (1)(c) of the PDP Law provides that personal data obtained must be adequate, relevant, and limited to what is necessary in relation to the purposes of processing (Rustam, 2025). This principle requires that village governments collect only such personal data as is strictly necessary and directly relevant to the administrative function being performed, and prohibits the excessive or indiscriminate collection of data.

In the context of village digitalization often characterized by the use of standardized electronic forms there is a tendency to collect more personal data than necessary under the pretext of building comprehensive databases or anticipating future needs. Such practices are inconsistent with the data minimization principle and may constitute a violation of the rights of data subjects. The accountability dimension in personal data management, as stipulated in Article 5 paragraph (1) (g) of the PDP Law, imposes stringent procedural constraints on the exercise of village governmental authority (Syofyan et al., 2025). The principle of accountability requires that the personal data controller in this case, the village government be responsible for all personal data processing activities it undertakes and be able to demonstrate compliance with applicable data protection principles.

This entails that village governments must maintain comprehensive documentation of each personal data processing activity, including the legal basis for processing, the purpose of processing, the categories of personal data processed, the recipients of such data, the retention period, and the technical and organizational security measures implemented.

Furthermore, village authorities must be able to demonstrate that the processing of personal data has been carried out either on the basis of valid consent from the data subject, where consent is required, or on another lawful basis as provided under the PDP Law.

The legal construction of data subject rights, as set forth in Chapter IV of the PDP Law, carries significant normative implications for the obligations of village governments in managing villagers' personal data. Articles 6 through 15 of the PDP Law confer a comprehensive set of rights upon data subjects, including the right to be informed of the existence, purpose, and accountability of parties processing their personal data; the right of access and to obtain copies of such data; the right to rectification and updating of personal data; the right to erasure under certain conditions; the right to restrict processing; the right to data portability in a structured and electronically readable format; and the right to object to the processing of personal data.

The fulfillment of these data subject rights is not a matter of policy discretion for village governments, but rather constitutes a mandatory legal obligation. (Maulidina, 2024) Accordingly, village authorities must establish effective and accessible mechanisms enabling villagers to exercise their rights over their personal data. This includes providing clear procedures for submitting requests for data access, correction, or deletion, as well as ensuring timely and appropriate responses to such requests within the statutory timeframes prescribed by the PDP Law.

From the perspective of authority theory in administrative law, the authority of village governments in managing personal data may be classified as conditional authority, whereby the legitimacy and legality of its exercise are contingent upon compliance with substantive and procedural requirements as stipulated in the PDP Law. Although the Village Law confers attributive authority upon villages to regulate and administer their governmental affairs including population administration and the management of villagers' data the exercise of such authority must remain subject to the principles and mechanisms of personal data protection as an integral component of the constitutional guarantee of citizens' rights (Iswandari, 2021).

Accordingly, village-scale local authority cannot be invoked as a justification for personal data management practices that fail to meet established data protection standards, as such practices would contravene the hierarchy of legal norms, in which constitutional rights prevail over administrative authority. This construction of conditional authority necessitates the harmonization of village administrative functions with the imperatives of personal data protection, ensuring that administrative efficiency is not achieved at the expense of fundamental rights, particularly the right of individuals to the protection of their personal data (Hariansah & Qhistina, 2026).

From an operational standpoint, the limits of village governmental authority in personal data management are manifested across several concrete dimensions. First, there are limitations concerning the types and categories of personal data that may be collected. Village governments are only permitted to collect personal data that is directly relevant to the administrative function being performed and strictly limited to what is necessary. The collection of sensitive personal data such as health data, biometric data, or data relating to an individual's sexual life may only be undertaken where there is a clear and specific legal basis, and with the explicit consent of the data subject, except in narrowly defined circumstances as provided under the PDP Law.

Second, there are limitations relating to the purpose of data processing. Each data collection activity must have a specific and explicit purpose, and the data obtained may not be used for other purposes without a valid legal basis or the consent of the data subject. Third, there are limitations concerning the retention period of personal data. Personal data may only be retained for as long as necessary to fulfill the purpose of processing or as

required by applicable laws and regulations, and must be erased or destroyed once the purpose has been achieved or the legal obligation has been satisfied.

Fourth, there are limitations regarding the disclosure or transfer of personal data to third parties. Village governments are prohibited from disclosing or sharing villagers' personal data with third parties without a lawful basis or the data subject's consent. Where such disclosure is lawfully carried out, it must be ensured that the recipient is likewise bound by corresponding obligations to safeguard the personal data in accordance with applicable data protection standards.

2. Legal Implications and Implementation Challenges of Village Digitalization for the Protection of Villagers' Personal Data

The implementation of village digitalization within the scope of village governmental authority gives rise to multidimensional and complex legal implications for the protection of villagers' personal data. The most fundamental implication is the transformation of the legal status of village governments from traditional local administrative entities into personal data controllers, as defined in Article 1 point (6) of Law Number 27 of 2022 on Personal Data Protection namely, any individual, public body, or international organization that, individually or jointly, determines the purposes of and exercises control over the processing of personal data (Bahary, 2025).

This transformation entails that village governments traditionally characterized as simple, community-based administrative units grounded in local wisdom must now comply with a complex and technical legal regime governing personal data protection, which applies universally to all data controllers without exception. Consequently, village authorities can no longer rely on informal and undocumented administrative practices in managing personal data. Instead, they are required to implement structured data governance systems that meet the technical and organizational standards mandated by the PDP Law.

The second legal implication concerns the emergence of comprehensive new legal obligations imposed on village governments in their capacity as data controllers. Articles 27 through 45 of the PDP Law set forth detailed obligations, including the duty to formulate and implement internal personal data protection policies; the obligation to conduct a Data Protection Impact Assessment (DPIA) for high-risk data processing activities; the requirement to establish complaint-handling and dispute resolution mechanisms for data subjects; the obligation to maintain systematic and comprehensive records of data processing activities; the duty to notify personal data breaches to the relevant data protection authority and affected data subjects within a prescribed timeframe; and the requirement to appoint a Data Protection Officer (DPO) under certain conditions (An Nafisa et al., 2025).

These obligations are mandatory in nature and cannot be disregarded on the grounds of limited institutional capacity or resources. Failure to comply may result in the imposition of administrative sanctions and, in certain circumstances, criminal penalties, as provided under the PDP Law. The dimension of legal liability constitutes a third, highly critical legal implication (Hariansah, 2022). The PDP Law establishes a regime of graduated and proportionate sanctions, ranging from administrative measures such as written warnings, temporary suspension of personal data processing activities, and the deletion or destruction of personal data to administrative fines of up to 2 percent of annual revenue or turnover. In addition, it provides for criminal sanctions, including imprisonment of up to six years and/or fines of up to IDR 6,000,000,000 (six billion rupiah), for specific offenses such as the unlawful acquisition or collection of personal data, unlawful disclosure of personal data, or the falsification of personal data (Shafa Salsabila & Sidi Ahyar Wiraguna, 2025).

Within the context of village governance, such liability may be imposed not only on the village government as an institutional entity but also personally upon individual village officials involved in personal data violations, including the Village Head, Village Secretary, or other administrative personnel who exercise access to and control over villagers' personal data. This creates significant legal exposure for village apparatus, who often lack sufficient understanding of the complexities of personal data protection and the legal consequences arising from non-compliance.

The fourth legal implication pertains to the right of action (right to sue) available to citizens in cases of personal data violations committed by village governments. Articles 48 to 50 of the PDP Law provide mechanisms for dispute resolution that may be pursued by data subjects who suffer harm as a result of violations of their personal data rights, either through alternative dispute resolution mechanisms or through civil litigation before the courts (Claudia, 2024).

In the village governance context, this means that villagers are equipped with legal instruments to hold village authorities accountable for breaches of personal data protection, including the right to claim compensation for both material and immaterial damages arising from such violations. The prospect of civil litigation introduces a substantial financial risk for village governments, particularly given that, in the digitalization era where personal data is processed on a large scale a single data breach incident may affect hundreds or even thousands of villagers, each of whom may have standing to bring a claim (Anisyah Sutopo & Ahyar Wiraguna, 2025).

The fifth legal implication pertains to the principles of transparency and public accountability in the management of personal data by village governments. Article 7 of the PDP Law grants data subjects the right to obtain clear information regarding the identity of the data controller, the legal basis for processing, the purpose of data collection and use, and the accountability of the party requesting the personal data (Marsya Iffah Erisar Raib et al., 2025).

This entails that village governments must be capable of providing comprehensive, clear, and intelligible explanations to villagers regarding how their personal data is managed, the purposes for which it is collected, the parties who have access to such data, the duration of data retention, and the mechanisms available for individuals to exercise their data subject rights. This obligation of transparency necessitates a paradigm shift in village governance, moving away from traditionally paternalistic and opaque practices toward a more participatory and accountable model of governance (Setyaningrum et al., 2024).

However, notwithstanding the comprehensive legal framework established by the PDP Law, the practical realization of these provisions at the village level faces a range of complex and interrelated challenges. The first, and most fundamental, challenge is the limited human resource capacity at the village level to understand and implement personal data protection standards (Aulia Alayna Suvil et al., 2024).

Low levels of digital literacy and limited awareness of the importance of personal data protection constitute significant barriers, particularly in regions that remain economically and educationally disadvantaged. Most village officials lack formal training in information technology or law, and therefore encounter substantial difficulties in comprehending technical concepts such as data encryption, role-based access control, audit trails, and Data Protection Impact Assessments (DPIA).

This situation is further exacerbated by the lack of comprehensive and systematic training and capacity-building programs from central or regional governments concerning the implementation of the PDP Law at the village level (Ashar et al., 2025). Existing training initiatives are generally sporadic, unstructured, and tend to focus primarily on the

technical operation of village information systems rather than on the critical aspects of personal data protection. As a result, many village governments implement digitalization programs without an adequate understanding of the legal risks and data protection implications associated with their activities.

The second challenge relates to the limited financial resources and technical infrastructure available to implement adequate personal data security standards (Renanda & Rosidin, 2025). Compliance with the PDP Law requires substantial investment in secure information technology infrastructure, including data encryption systems, firewalls, backup and disaster recovery mechanisms, strict access control systems, and comprehensive monitoring and audit frameworks. However, the high cost of implementation often constitutes a significant barrier, particularly for village governments with limited fiscal capacity.

In practice, most villages in Indonesia operate under severely constrained budgets, with village funds largely allocated to priority programs such as physical infrastructure development, community economic empowerment, and basic social services (Kamuli et al., 2023). Investment in data security infrastructure is frequently deprioritized in village budgeting processes, as it is perceived as less tangible and unlikely to yield immediate, visible benefits for the community. As a consequence, personal data collected through village digitalization programs is often stored in systems lacking adequate security safeguards, and in many cases merely kept on personal computers of village officials or in simple, unencrypted spreadsheet applications accessible to anyone with physical access to such devices.

The third challenge concerns the complexity of coordination and system integration between village-level information systems and those of higher levels of government. Village digitalization initiatives promoted by the central government presuppose the integration of village information systems with national population databases, regional government systems, and various sectoral information systems, such as those related to health, education, and social assistance (Hadi & Widnyani, 2024).

In practice, however, such integration faces significant technical and regulatory obstacles. From a technical perspective, discrepancies in data format standards, security protocols, and technological platforms across different levels of government often impede system interoperability. Many information systems at the regency or provincial level are developed independently without due consideration for integration with village systems, resulting in data silos that cannot effectively communicate with one another.

From a regulatory standpoint, there remains an absence of a clear and comprehensive legal framework governing inter-agency data sharing, including the legal basis for data exchange, required consent procedures, limitations on data usage, and accountability mechanisms in the event of personal data breaches during data-sharing processes. This regulatory vacuum generates legal uncertainty and creates the risk of data-sharing practices that contravene the principles of purpose limitation and data minimization as enshrined in the PDP Law (Wicaksono & Yasin, 2024).

The fourth challenge relates to the socio-cultural characteristics of village communities, which create structural barriers to the effective implementation of personal data protection. In rural settings where paternalistic and hierarchical norms remain deeply entrenched, there is a prevailing tendency for community members to comply with directives issued by village authorities without questioning the purpose or consequences of disclosing their personal data. This dynamic gives rise to information asymmetry and power imbalance between village governments as data collectors and villagers as data subjects, whereby individuals often lack sufficient bargaining power to refuse data requests or to scrutinize how their personal data will be used.

Under such conditions, the notion of "free, specific, informed, and unambiguous consent", as required under the PDP Law, becomes highly problematic in practice. Villagers frequently provide their personal data not on the basis of a clear and informed understanding of the implications, but rather due to a perceived absence of alternatives or as a result of social pressure to comply with local authority (Elvina Putri Maheswari & Sidi Ahyar Wiraguna, 2025). This situation is further exacerbated by the low level of legal literacy among rural communities regarding their personal data rights. Consequently, many villagers remain unaware that they possess the right to refuse the provision of personal data, the right of access, the right to rectification of inaccurate data, and the right to object to certain forms of data processing.

The fifth challenge concerns the absence of effective oversight and enforcement mechanisms at the local level. Although the PDP Law mandates the establishment of an independent data protection authority at the national level, endowed with supervisory and enforcement powers, its capacity to exercise effective oversight down to the village level remains severely constrained, particularly given Indonesia's vast number of villages exceeding 74,000.

In practice, oversight of personal data protection at the village level is virtually non-existent, enabling village governments to engage in questionable data management practices without meaningful checks and balances. The lack of oversight also means that violations of personal data protection frequently go undetected and unaddressed, either because villagers are unaware that their rights have been infringed or because there are no accessible and responsive complaint mechanisms through which such violations can be reported. This condition fosters a culture of impunity, which risks perpetuating practices that undermine the fundamental right to personal data protection within village communities.

The sixth challenge pertains to local political dynamics and the potential misuse of personal data for political purposes (Endah Astuti et al., 2024). Within the context of village governance often dominated by local elites with particular political interests there exists a tangible risk that personal data collected through village digitalization initiatives may be instrumentalized for political gain. Such misuse may include voter targeting in village head elections or general elections, the mobilization of political support, or even the intimidation of community groups whose political positions diverge from those of the incumbent village authorities (Bahram, 2025). This risk is further amplified by the fact that village information systems frequently contain highly comprehensive personal data, encompassing the economic, social, and even political profiles of villagers. In the wrong hands, such data may be exploited for purposes that are fundamentally incompatible with the principles of personal data protection. However, preventing the misuse of personal data for political purposes at the village level remains particularly challenging, given the limited oversight mechanisms and the fragility of checks and balances within local governance structures.

CONCLUSION

This study concludes that the authority of village governments in managing villagers' personal data in the digital era is derived from attributive authority under Law Number 3 of 2024 concerning the Second Amendment to Law Number 6 of 2014 on Villages, particularly authority based on rights of origin (*hak asal-usul*) and village-scale local authority. This authority provides a legitimate legal basis for village administrations to conduct data collection and population administration as part of their governmental functions. Nevertheless, such authority is not absolute and must be exercised in accordance with the principles of personal data protection as regulated in Law Number 27 of 2022 on Personal Data Protection, as well

as the constitutional guarantees under Article 28G paragraph (1) of the 1945 Constitution. Accordingly, all processes involving the collection, storage, processing, and dissemination of personal data must adhere to principles such as lawfulness, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability. Village-scale local authority therefore cannot be used to justify practices that conflict with national legal standards or constitutional protections of personal data.

Furthermore, the implementation of village digitalization carries significant legal implications by positioning village governments as personal data controllers with corresponding responsibilities. This requires the establishment of internal policies, adequate data security infrastructure, and accountability mechanisms aligned with personal data protection principles. However, its implementation faces substantial challenges, including limited digital literacy among village officials, inadequate financial resources and infrastructure, inconsistent technical standards, weak supervisory mechanisms, and risks of political misuse of personal data. Therefore, coordinated efforts between central and regional governments, along with community participation, are essential to strengthen institutional capacity, improve infrastructure, develop technical regulations, and ensure participatory oversight. These measures are crucial to ensure that villagers are not merely passive data subjects but active stakeholders in safeguarding their personal data.

REFERENCES

An Nafisa, T., Alam, Moch. Z., & Maharani, D. P. (2025). Analisis Pengaturan Pengalihan Data Pribadi Lintas Negara Pasca Akuisisi Dalam Undang-Undang Perlindungan Data Pribadi. *Jurnal Dialektika Hukum*, *7*(1), 97–135. https://doi.org/10.36859/jdh.v7i1.3548

Anggen Suari, K. R., & Sarjana, I. M. (2023). Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, *6*(1), 132–142. https://doi.org/10.38043/jah.v6i1.4484

Anisyah Sutopo, H., & Ahyar Wiraguna, S. (2025). Sanksi Hukum Terhadap Pelanggaran Perlindungan Data Pribadi Dalam Praktik Kampanye Politik: Analisis Praktik Pencatutan Ktp Tanpa Persetujuan: Dasar Hukum Perlindungan Data Pribadi, Bentuk Pengawasan Bawasalu dalam Mengawasi Pencatutan KTP oleh Partai Politik, Sanksi dan Pertanggungjawaban Partai Politik terhadap Korban Pencatutan Data Diri untuk Pemenuhan Persyaratan Peserta Pemilu. *NALAR: Journal Of Law and Sharia*, *3*(1). https://doi.org/10.61461/nlr.v3i1.117

Arafat, M. & Alexander Tito Enggar Wirasto. (2024). Kebijakan Kriminal dalam Penanganan Siber di Era Digital: Studi Kasus di Indonesia. *Equality : Journal of Law and Justice*, *1*(2), 220–241. https://doi.org/10.69836/equality-jlj.v1i2.170

Arrasuli, B. K., & Fahmi, K. (2023). Perlindungan Hukum Positif Indonesia Terhadap Kejahatan Penyalahgunaan Data Pribadi. *UNES Journal of Swara Justisia*, *7*(2), 369. https://doi.org/10.31933/ujsj.v7i2.351

Ashar, A., Irwan, I., & Herman Dema. (2025). Pemanfaatan Teknologi Informasi dalam Pelaksanaan E-Government di Desa Sipodeceng. *SOSMANIORA: Jurnal Ilmu Sosial Dan Humaniora*, *4*(2), 421–428. https://doi.org/10.55123/sosmaniora.v4i2.5255

Aulia Alayna Suvil, Firdaus Firdaus, M. Arif Ramadhan, Wanda Darma Putra, & Dwi Putri Lestarika. (2024). Implementasi Perlindungan Data Pribadi Berdasarkan Undang-Undang Nomor 11 Tahun 2020. *JURNAL HUKUM, POLITIK DAN ILMU SOSIAL*, *3*(4), 70–80. https://doi.org/10.55606/jhpis.v3i4.4235

Bahary, F. S. (2025). Tantangan Implementasi UU Pelindungan Data Pribadi Bagi Investor Asing di Indonesia. *SENTRI: Jurnal Riset Ilmiah*, *4*(9), 2214–2224. https://doi.org/10.55681/sentri.v4i9.4653

Bahram, M. (2025). Tanggung Jawab Konstitusional Pemerintah Dalam Menjamin Hak Konstitusional Atas Informasi Di Era Digital. *SINERGI : Jurnal Riset Ilmiah*, *2*(9), 4380–4406. https://doi.org/10.62335/sinergi.v2i9.1753

Chushairi, S. M., Fithry, A., & Rusfandi, R. (2025). Perlindungan Hukum Bagi Korban Atas Kebocoran Pusat Data Nasional Sementara (Pdns) Perspektif Perlindungan Data Pribadi. *Jurnal Jendela Hukum*, *12*(2), 89–122. https://doi.org/10.24929/jjh.v12i2.4664

Claudia, Z. (2024). Penyelesaian Sengketa Perlindungan Data Pribadi Melalui Arbitrase di Era Society 5.0. *Jurnal Supremasi*, 114–129. https://doi.org/10.35457/supremasi.v14i2.2794

Elvina Putri Maheswari & Sidi Ahyar Wiraguna. (2025). Urgensi Persetujuan Pemilik Data dalam Pengelolaan Data Pribadi oleh Platform Digital. *Jurnal Ilmu Komunikasi Dan Sosial Politik*, *2*(4), 908–914. https://doi.org/10.62379/jiksp.v2i4.2498

Endah Astuti, Ade Maman Suherman, & Tri Setiady. (2024). Implikasi Hukum Pidana Penyalahgunaan Data Pribadi Kasus Dharma Pongrekun Pilkada Jakarta Berdasarkan Teori Penegakan Hukum. *Hukum Inovatif : Jurnal Ilmu Hukum Sosial Dan Humaniora*, *2*(1), 81–95. https://doi.org/10.62383/humif.v2i1.997

Gatot, R. Y. (2025). Transformasi Hukum Pemerintahan Desa: Perbandingan UU No. 5 Tahun 1979 dan UU No. 6 Tahun 2014 tentang Desa. *TheJournalish: Social and Government*, *6*(3). https://doi.org/10.55314/tsg.v6i3.977

Hadi, I., & Widnyani, I. A. P. S. (2024). Modernisasi dan Digitalisasi Public Servis: Mewujudkan Indonesia Emas Melalui Harmonisasi Sistem Pemerintahan Berbasis Elektronik (SPBE). *JURNAL KRIDATAMA SAINS DAN TEKNOLOGI*, *6*(02), 639–658. https://doi.org/10.53863/kst.v6i02.1398

Hariansah, S. (2022). Analisis Implementasi Nilai-Nilai Budaya Hukum dalam Kehidupan Berbangsa dan Bernegara: Studi Kritis Pendekatan Masyarakat, Budaya dan Hukum. *KRTHA BHAYANGKARA*, *16*(1), 121–130. https://doi.org/10.31599/krtha.v16i1.1000

Hariansah, S., & Qhistina, L. (2026). *Toward Algorithmic Due Process: Constitutional Challenges and Human Rights Risks in Indonesia's Digital State*.

Hariyanto, H. (2020). Hubungan Kewenangan antara Pemerintah Pusat dan Pemerintah Daerah Berdasarkan Negara Kesatuan Republik Indonesia. *Volksgeist: Jurnal Ilmu Hukum Dan Konstitusi*, *3*(2), 99–115. https://doi.org/10.24090/volksgeist.v3i2.4184

Hasibuan, E. S., & Putri, E. A. (2024). Perlindungan Keamanan Atas Data Pribadi Di Dunia Maya. *Jurnal Hukum Sasana*, *10*(1), 70–83. https://doi.org/10.31599/sasana.v10i1.2134

Irfan B, & Anirwan, A. (2024). Explorasi Implementasi Digitalisasi Desa: Studi Literatur. *Indonesian Journal of Intellectual Publication*, *5*(1), 1–8. https://doi.org/10.51577/ijipublication.v5i1.546

Iswandari, B. A. (2021). Jaminan Atas Pemenuhan Hak Keamanan Data Pribadi Dalam Penyelenggaraan E-Government Guna Mewujudkan Good Governance. *Jurnal Hukum Ius Quia Iustum*, *28*(1). https://doi.org/10.20885/iustum.vol28.iss1.art6

Jefri, & Manalu, E. F. (2025). Analisis Yuridis Terhadap Dampak Kebijakan Pemerintah Pusat Pada Kemandirian Hukum Masyarakat Desa Lumban Binanga. *Al-Zayn : Jurnal Ilmu Sosial & Hukum*, *3*(3), 1750–1757. https://doi.org/10.61104/alz.v3i3.1460

Junaedi, A. M. (2025). Urgensi Perlindungan Data Pribadi Dalam Era Digital: Analisis Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi. *KNOWLEDGE: Jurnal Inovasi Hasil Penelitian Dan Pengembangan*, *5*(2), 247–257. https://doi.org/10.51878/knowledge.v5i2.5269

Kamuli, S., Wantu, S. M., Hamim, U., Djafar, L., Sahi, Y., & Dahiba, H. (2023). Pemberdayaan Berkelanjutan Melalui Pemanfaatan Dana Desa Bagi Masyarakat Pesisir di Desa

Momalia Kecamatan Posigadan Provinsi Sulawesi Utara. *Jambura Journal Civic Education*, *3*(2). https://doi.org/10.37905/jacedu.v3i2.21827

Kusnadi, S. A. (2021). Perlindungan Hukum Data Pribadi Sebagai Hak Privasi. *AL WASATH Jurnal Ilmu Hukum*, *2*(1), 9–16. https://doi.org/10.47776/alwasath.v2i1.127

Lathifatul Mustofa, L. S., & Yunanto, S. E. (2025). Teknokratisasi Kewenangan Desa Dalam Pembangunan Dan Pemberdayaan Masyarakat Lokal di Desa Keputran Kecamatan Kemalang Kabupaten Klaten. *Journal of Indonesian Rural and Regional Government*, *9*(1), 65–74. https://doi.org/10.47431/jirreg.v9i1.608

Mardinata, E., Cahyono, T. D., & Muhammad Rizqi, R. (2023). Transformasi Digital Desa Melalui Sistem Informasi Desa (SID): Meningkatkan Kualitas Pelayanan Publik dan Kesejahteraan Masyarakat. *Parta: Jurnal Pengabdian Kepada Masyarakat*, *4*(1), 73–81. https://doi.org/10.38043/parta.v4i1.4402

Marsya Iffah Erisar Raib, Sinta Dewi Rosadi, & Amelia Cahyadini. (2025). Perbandingan Penerapan Prinsip Transparansi Antara Indonesia dengan Irlandia dalam Hal Terjadinya Kegagalan Pelindungan Data Pribadi. *Eksekusi : Jurnal Ilmu Hukum Dan Administrasi Negara*, *3*(2), 51–71. https://doi.org/10.55606/eksekusi.v3i2.1815

Maulidina, E. I. (2024). Urgensi Uji Kebutuhan dan Proporsionalitas dalam Pengecualian Hak-Hak Subjek Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, *7*(2), 143–159. https://doi.org/10.38043/jah.v7i2.5464

Mirna, M., Judhariksawan, & Maskum. (2023). Analisis Pengaturan Keamanan Data Pribadi Di Indonesia. *JURNAL ILMIAH LIVING LAW*, *15*(1), 16–30. https://doi.org/10.30997/jill.v15i1.4726

Nenny Rianarizkiwati. (2024). Ius Constituendum Hak Atas Pelindungan Data Pribadi: Suatu Perspektif Hak Asasi Manusia. *Jurnal Hukum Sasana*, *8*(2). https://doi.org/10.31599/sasana.v8i2.1283

Putri, A., Sari, N., Fajrina, P., & Aisyah, S. (2024). Keamanan Online dalam Media Sosial: Pentingnya Perlindungan Data Pribadi di Era Digital (Studi Kasus Desa Pematang Jering). *Jurnal Pengabdian Nasional (JPN) Indonesia*, *6*(1), 38–52. https://doi.org/10.35870/jpni.v6i1.1097

Putri Nugroho, F. N., Listanto, M. F., Amelia, N., & Annisa, S. (2024). Analisis Kebocoran Data Pribadi Dalam Media Sosial. *Fibonacci : Jurnal Ilmu Ekonomi, Manajemen Dan Keuangan*, *1*(2), 58–65. https://doi.org/10.63217/fibonacci.v1i2.70

Renanda, A. A., & Rosidin, A. (2025). Efektivitas Pelayanan Digital Dalam Mempermudah Birokrasi Dan Pengelolaan Data Publik. *Jurnal Penelitian Multidisiplin Bangsa*, *1*(8), 1651–1657. https://doi.org/10.59837/jpnmb.v1i8.310

Rifan, M., & Rahmawati, L. (2021). Konstitusi Desa dan Eksistensinya dalam Regulasi di Indonesia. *Jurnal Konstitusi*, *18*(1), 022–043. https://doi.org/10.31078/jk1812

Rusnan, R., Sarkawi, S., & Koynja, J. J. (2023). Kewenangan Pemerintah Desa Dalam Pembentukan Peraturan Desa Di Desa Parampuan Kecamatan Labuapi Kabupaten Lombok Barat. *Jurnal Diskresi*, *2*(2). https://doi.org/10.29303/diskresi.v2i2.3725

Rustam, M. R. (2025). Tanggung Jawab Hukum Platform Fintech Per To Peer Lending Terhadap Penyalahgunaan Data Pribadi Nasabah Berdasarkan Uu No. 27 Tahun 2022 Tentang Perlindungan Data Pribadi. *IBLAM LAW REVIEW*, *5*(2), 172–180. https://doi.org/10.52249/ilr.v5i2.636

Setyaningrum, A., Dewi, M. W., & Kusuma, I. L. (2024). Pengaruh Akuntabilitas, Transparansi, dan Partisipasi Masyarakat terhadap Pengelolaan Dana Desa dalam Mewujudkan Good Governance. *Jurnal Ilmiah Keuangan Akuntansi Bisnis*, *3*(3), 581–589. https://doi.org/10.53088/jikab.v3i3.104

Shafa Salsabila & Sidi Ahyar Wiraguna. (2025). Pertanggungjawaban Hukum atas Pelanggaran Data Pribadi dalam Perspektif Undang-Undang Pelindungan Data Pribadi Indonesia.

Konsensus : Jurnal Ilmu Pertahanan, Hukum Dan Ilmu Komunikasi, *2*(2), 145–157. https://doi.org/10.62383/konsensus.v2i2.736

Silalahi, J. A. S., Purba, Y. Y., & Nasution, M. F. (2025). Analisis Yuridis terhadap Mekanisme Perlindungan Data Pribadi dalam Sistem Informasi Elektronik Berdasarkan Perspektif Hukum Pidana di Indonesia. *Jurnal Minfo Polgan*, *14*(1), 604–613. https://doi.org/10.33395/jmp.v14i1.14810

Siti Aisyah & Eddy Suriyani. (2024). Implementasi Program Digitalisasi Desa (Digides) Dalam Meningkatkan Pelayanan Publik Di Desa Kapar Kecamatan Murung Pudak Kabupaten Tabalong. *JAPB*, *7*(2), 2073–2088. https://doi.org/10.35722/japb.v7i2.1139

Syofyan, Y., Nazmi, D., & Arfiani, A. (2025). Tanggung Gugat Pemerintah Atas Kebocoran Data Pribadi Masyarakat Dalam Perspektif Undang-Undang Pelindungan Data Pribadi. *Nagari Law Review*, *8*(3), 556. https://doi.org/10.25077/nalrev.v.8.i.3.p.556-581.2025

Wicaksono, A. T., & Yasin, I. F. (2024). Criminal Law Reformulation Through Omnibus Law as a Solution to Sectoral Cyber Protection: Reformulasi Hukum Pidana Melalui Omnibus Law Sebagai Solusi Perlindungan Siber Yang Bersifat Sektoral. *Al-Jinayah : Jurnal Hukum Pidana Islam*, *10*(2), 237–261. https://doi.org/10.15642/aj.2024.10.2.237-261

Yudha, Iran Sahril, & Dhody A.R. Widjaja Atmadja3. (2025). Perlindungan Data Pribadi Konsumen, Dokumen dan Tanda Tangan Elektronik yang Dipergunakan oleh Pihak Ketiga dalam Transaksi E-Commerce. *CENDEKIA : Jurnal Penelitian Dan Pengkajian Ilmiah*, *2*(2), 173–189. https://doi.org/10.62335/cendekia.v2i2.897