



**Tata Kelola dan Tanggung Jawab Hukum Perlindungan Data
Pribadi Konsumen dalam Layanan IndiHome by Telkomsel:
Studi pada PT Creative Widya Nusantara**

***Governance and Legal Responsibilities Regarding the Protection
of Consumer Personal Data in IndiHome Services by Telkomsel:
A Study of PT Creative Widya Nusantara***

**Hana Hanifia Yusrima Latifa Hanum^{1✉}, Wardah Yuspin² Kelik Wardiono³,
Khudzaifah Dimyati⁴**

^{1,2,3,4}Universitas Muhammadiyah Surakarta, Indonesia

DOI: <https://doi.org/10.63477/jols.v3i3.624>, Pages: 112-124

✉ Email Correspondence: r100250018@student.ums.ac.id

ABSTRAK

Penelitian ini menggunakan metode hukum empiris dengan pendekatan deskriptif kualitatif. Data diperoleh melalui wawancara, observasi, dan studi kepustakaan, kemudian dianalisis secara kualitatif melalui reduksi data, penyajian data, dan penarikan kesimpulan. Hasil penelitian menunjukkan bahwa Telkomsel berkedudukan sebagai Pengendali Data Pribadi (Data Controller) karena menentukan tujuan dan sarana pemrosesan data serta mengelola basis data pelanggan. PT Creative Widya Nusantara berperan sebagai mitra operasional dalam pemasaran dan registrasi pelanggan, sedangkan PT Telkom Akses menjalankan fungsi teknis dengan akses data yang terbatas. Pelindungan data pribadi diterapkan melalui mekanisme consent, pengunggahan data identitas secara mandiri, pembatasan akses data, verifikasi identitas, pemenuhan hak koreksi dan penghapusan data, serta penggunaan audit trail. Kebaruan penelitian ini terletak pada analisis pembagian tanggung jawab hukum antara Pengendali Data Pribadi dan mitra operasional dalam registrasi layanan telekomunikasi. Efektivitas pelindungan data masih perlu diperkuat melalui peningkatan kualitas consent, audit berkala, pelatihan keamanan data, dan edukasi konsumen.

Kata Kunci: Pelindungan Data Pribadi, Data Controller, Tata Kelola Data, Tanggung Jawab Hukum

ABSTRACT

This study employs an empirical legal research method with a qualitative descriptive approach. Data were gathered through interviews, observations, and literature reviews, then analyzed qualitatively via data reduction, data presentation, and conclusion drawing. The findings indicate that Telkomsel acts as the Personal Data Controller, as it determines the purposes and means of data processing and manages the customer database. PT Creative Widya Nusantara serves as an operational partner for marketing and customer registration, while PT Telkom Akses performs technical functions with limited data access. Personal data protection is implemented through mechanisms such as consent, self-uploading of identity data, data access restrictions, identity verification, fulfillment of rights regarding data correction and deletion, and the use of audit trails. The study's novelty lies in its analysis of the division of legal responsibility between the Personal Data Controller and operational partners during telecommunications service registration. The effectiveness of data protection requires further strengthening through improved consent quality, periodic audits, data security training, and consumer education.

Keywords: Personal Data Protection, Data Controller, Data Governance, Legal Responsibility

Article Info

Copyright (c) 2026, Hana Hanifia Yusrima Latifa Hanum, et al.

Received: 24-9-2026, Revised: 28-9-2026, Accepted: 29-9-2026, Published: 30-9-2026

INTRODUCTION

The development of information and communication technology has driven digital transformation across various sectors of life, including the telecommunications sector. The digitalization of services enables service providers to collect and utilize consumers' personal data for various purposes, ranging from customer registration, identity verification, service activation, and billing to customer relationship management. In this context, personal data no longer functions merely as supporting information but has become an asset of strategic value for service providers. Therefore, personal data management requires adequate protection mechanisms to safeguard privacy rights and prevent unauthorized use of data. Bygrave (2014) explains that personal data protection is an important instrument for safeguarding individuals' rights over their personal information while limiting the risks of data misuse in various digital activities.

Personal data protection is not only related to information security but also concerns the protection of privacy rights as part of individual rights in a digital society. Solove (2021) explains that personal data is closely associated with an individual's identity, such that the use, dissemination, or processing of data without a lawful basis may potentially cause legal, social, and economic harm to data subjects. Therefore, personal data protection aims to ensure that every individual retains control over the use of their personal data and obtains legal certainty regarding every form of data processing carried out by other parties.

In Indonesia, the regulation of personal data protection has obtained a more comprehensive legal foundation through Law Number 27 of 2022 concerning Personal Data Protection. The law regulates the principles of personal data processing, the rights of data subjects, the obligations of Personal Data Controllers and Personal Data Processors, as well as accountability mechanisms in cases of violations of personal data protection. The enactment of the Personal Data Protection Law demonstrates that personal data protection is no longer viewed merely as a technical issue but also as part of the protection of citizens' rights in the digital environment (Attidhira & Permana, 2022). Palit and Purba (2025) also emphasize that personal data protection is closely related to the protection of privacy rights as part of human rights that must be respected and protected by the state and by parties involved in processing personal data.

The telecommunications sector is one of the sectors characterized by intensive personal data processing. Telecommunications service providers routinely collect and manage various types of customer data to support service delivery. This situation has become increasingly complex following the integration of IndiHome services into the Telkomsel ecosystem. In the provision of IndiHome by Telkomsel services, the customer registration process involves not only Telkomsel as the service provider but also PT Creative Widya Nusantara (PT CWN) as an operational marketing partner, Sales Force personnel as customer registration officers, and PT Telkom Akses as the party responsible for network surveys and installation. During this process, customers are required to provide various types of personal data, including full name, telephone number, email address, National Identification Number (NIK), a photograph of their Identity Card (KTP), installation address, and customer location information. The involvement of several parties in a single service process indicates that personal data processing is not carried out solely by the service provider but also involves other parties that have access to customer data at specific stages.

PT Creative Widya Nusantara is a company engaged in marketing and sales force management that collaborates with various telecommunications service providers, including Telkomsel (Creative Widya Nusantara, 2024). In the provision of IndiHome by Telkomsel services, PT Creative Widya Nusantara assists in marketing and customer registration processes through Sales Force personnel who interact directly with consumers. Meanwhile, PT Telkom Akses is a company engaged in the development and management of telecommunications infrastructure and is responsible for conducting network surveys and installing services for customers (Telkom Akses, 2024). The involvement of various parties creates a need for clear and accountable personal data protection governance capable of ensuring the security of consumer data throughout the service delivery process.

This condition raises several legal issues that are relevant for examination. First, it is necessary to analyze how consumer personal data is governed and managed in IndiHome by Telkomsel services, which involve several parties with different functions. Second, it is necessary to determine the legal status of each party involved in personal data processing, particularly to identify the party acting as the Personal Data Controller and the parties performing operational functions in data processing. Third, it is necessary to examine how personal data protection is implemented in practice, including consent mechanisms, restrictions on data access, the fulfillment of data subject rights, and supervision of the use of personal data. Fourth, it is necessary to analyze the allocation of legal responsibilities when problems arise in relation to the processing of consumer personal data. These issues are highly relevant because they are directly related to the protection of consumer rights as personal data owners in their legal relationship with telecommunications service providers (Hadjon, 1987).

Research on personal data protection has been conducted from various perspectives. Attidhira and Permana (2022) examined the development of personal data protection regulations in Indonesia and their implications for the national legal system. Syailendra, Lie, and Sudiro (2024) discussed the challenges and opportunities in implementing the Personal Data Protection Law in digital services. Judijanto, Solapari, and Putra (2024) highlighted the gap between normative regulations on personal data protection and their implementation in practice. Maleno (2024) analyzed the comparison between Indonesia's Personal Data Protection Law, the General Data Protection Regulation (GDPR), and the California Consumer Privacy Act (CCPA). Triyanti (2025) examined the need for personal data governance reform within the population administration system. These studies demonstrate that research on personal data protection has developed across the areas of regulation, privacy rights, and electronic system governance. However, studies specifically addressing the governance and legal responsibility for personal data protection within operational partnership schemes in telecommunications services remain relatively limited.

This study differs from previous research by focusing on the relationship between Telkomsel as the Personal Data Controller and PT Creative Widya Nusantara as an operational partner directly involved in the customer registration process. This focus is important because, in practice, personal data processing is not conducted solely by the service provider as the data controller but also involves other parties that have access to customer data at specific stages. Accordingly, this study not only examines the normative aspects of personal data protection but also analyzes data management governance, the implementation of personal data protection, and the

allocation of legal responsibilities within operational partnerships in telecommunications services.

Based on the foregoing discussion, this study addresses the research questions of how consumer personal data is governed and managed, how the legal status of the parties involved in personal data processing is determined, how personal data protection is implemented, and how legal responsibility is allocated in the provision of IndiHome by Telkomsel services at PT Creative Widya Nusantara. This study aims to analyze the governance of consumer personal data management, the legal status of the parties involved in personal data processing, the implementation of personal data protection, and legal responsibility in the provision of IndiHome by Telkomsel services.

Theoretically, this study is expected to contribute to the development of personal data protection law scholarship, particularly regarding the relationship between Personal Data Controllers and operational partners in the provision of telecommunications services. Practically, this study is expected to provide input for telecommunications service providers in strengthening consumer personal data protection governance. The novelty of this study lies in its analysis of governance and the allocation of legal responsibilities between the Personal Data Controller and operational partners who interact directly with consumers during the telecommunications service registration process, an area that remains relatively limited in existing personal data protection research in Indonesia.

METHOD

This study is an empirical legal study that examines law as social behavior and its implementation in the practice of community life (Salim, 2022). The approach used is descriptive qualitative research to obtain an understanding of the governance and legal responsibilities for the protection of consumer personal data in IndiHome by Telkomsel services at PT Creative Widya Nusantara.

The research data consist of primary and secondary data. Primary data were obtained through field observations and semi-structured interviews with informants selected purposively, namely Tunjung Aribowo Harimurti as the Manager of the Surakarta Operational Region of PT Creative Widya Nusantara, a representative of PT Telekomunikasi Selular (Telkomsel), Sales Force personnel of PT Creative Widya Nusantara, and technicians of PT Telkom Akses. The selection of informants was based on their involvement in the management and protection of consumer personal data in IndiHome by Telkomsel services. Secondary data were obtained through a literature review covering laws and regulations, books, scientific journals, company documents, and privacy policies related to personal data protection.

Data validity was tested using source triangulation by comparing information obtained from interviews, observations, company documents, and the literature used in the study. The collected data were analyzed qualitatively through the stages of data reduction, data presentation, and conclusion drawing, as proposed by Miles, Huberman, and Saldaña (2014). The analysis was conducted to identify patterns, relationships, and meanings related to personal data management governance, the legal status of the parties involved, the implementation of personal data protection, and legal responsibilities in IndiHome by Telkomsel services.

The research was conducted in accordance with research ethics principles by obtaining consent from the informants prior to the interviews, maintaining the

confidentiality of information obtained during the research, and using all research data solely for academic purposes and the advancement of scientific knowledge.

RESULT AND DISCUSSION

Governance of Consumer Personal Data Management in IndiHome by Telkomsel Services

The governance of consumer personal data management in IndiHome by Telkomsel services is implemented through the distribution of functions and authorities among the parties involved. The research findings show that the processes of collecting, transmitting, storing, and using data involve Telkomsel, PT Creative Widya Nusantara (PT CWN), Sales Force personnel, and PT Telkom Akses according to their respective roles.

Telkomsel acts as the service provider that manages the customer system and database, PT CWN serves as an operational marketing partner that assists in customer acquisition and registration, while PT Telkom Akses performs technical functions in the form of network surveys and service installation. Tunjung Aribowo Harimurti, as the Manager of the Surakarta Operational Region of PT CWN, explained that PT CWN performs its function as a *marketing agency* through Sales Force personnel. The registration data are subsequently transmitted to the Telkomsel system through the Digital Sales Information (DSI) or Digipos application for service activation (Interview with Tunjung Aribowo Harimurti, 2026). This structure demonstrates a division of functions among the parties that collect, manage, and use data for service purposes.

The initial stage of data processing takes place during customer registration. Based on the results of interviews with Sales Force personnel of PT CWN, prospective customers provide their full name, telephone number, email address, installation address, and location coordinates. The data are used for service administration, network availability verification, and determination of the installation location by technicians. Thus, the data collected are not only related to customer identity but also include information that supports the operation of telecommunications services (Interview with Sales Force PT CWN, 2026).

In addition to general identification data, the registration process also uses the National Identification Number (NIK) and a photograph of the Identity Card (KTP) to verify customer identity. According to Tunjung Aribowo Harimurti, such data are used to ensure the validity of identity, prevent the use of fictitious identities, and support administrative validation, including the identification of customer history such as outstanding payments or previous administrative issues (Interview with Tunjung Aribowo Harimurti, 2026). NIK, KTP photographs, installation addresses, and location information have relatively high risks if accessed by unauthorized parties. Therefore, their processing must be carried out in a limited and proportional manner and in accordance with the predetermined purposes, as stipulated under the principles of Law Number 27 of 2022 concerning Personal Data Protection.

These risks demonstrate the importance of implementing the principle of *data minimization*. Bygrave (2014) explains that personal data processing must be carried out proportionally by limiting the collection and use of data to information relevant to the purposes of the service. In IndiHome by Telkomsel services, NIK and KTP photographs are used for identity verification, while installation addresses and location coordinates are used for network surveys and installation. Thus, the types of data collected are related to the needs of service provision.

Customer data entry is conducted through the Digital Sales Information (DSI) or Digipos application, which is integrated with the Telkomsel system. Sales Force personnel are only authorized to enter basic data such as name, telephone number, email address, and installation location information. Subsequently, customers receive a follow-up registration link to upload their KTP photograph and enter their NIK independently. This mechanism reduces field personnel's access to sensitive identification data because the data are transmitted directly by customers to the Telkomsel system (Interview with Sales Force PT CWN, 2026).

The management and storage of customer data are centrally carried out by Telkomsel. Data submitted through the registration system are entered into the company's database and used for service activation, account management, data changes, complaint handling, billing, and service termination. PT CWN does not have the authority to store or manage the data after the registration process has been completed. This condition demonstrates that control over the system and database rests with Telkomsel (Interview with Telkomsel Representative, 2026).

Access restrictions are implemented at the operational level. Sales Force personnel do not have access to NIK and KTP photographs because the data are uploaded directly by customers. Under certain circumstances, Sales Force personnel may assist customers, particularly elderly customers, but such assistance is provided in the use of the system without altering the mechanism for independent data uploading (Interview with Sales Force PT CWN, 2026).

Similar restrictions are applied to PT Telkom Akses. Technicians can only access customer names, telephone numbers, and installation addresses required for network surveys and installation. Technicians do not have access to NIK, KTP photographs, or other identities that are not required. Additional location information is obtained through communication with customers when necessary (Interview with PT Telkom Akses Technician, 2026).

The research findings show that personal data management governance applies the principles of access limitation and data minimization. Bygrave (2014) emphasizes that access to personal data should be limited only to parties who require it to perform specific functions. In IndiHome by Telkomsel services, Telkomsel centrally manages and stores the data, PT CWN assists with customer acquisition and registration, while PT Telkom Akses uses the data necessary for technical functions. This pattern limits the circulation of data and supports the security and confidentiality of customer information.

Legal Status of Telkomsel and PT Creative Widya Nusantara in Consumer Personal Data Management

Determining the legal status of the parties is important because it relates to the distribution of authority and responsibility in personal data processing. Not all parties involved have the same legal status. Therefore, it is necessary to identify the parties that determine the purposes of processing, control the system, manage the database, and make decisions regarding the use of data.

Law Number 27 of 2022 concerning Personal Data Protection distinguishes between Personal Data Controllers and Personal Data Processors. Article 1 number 4 defines a Personal Data Controller as a party that determines the purposes and exercises control over personal data processing, while Article 1 number 5 defines a Personal Data Processor as a party that carries out processing on behalf of a Personal

Data Controller. Thus, legal status is determined based on the authority to determine the purposes and means of data processing.

The research findings show that the authority to determine the purposes and means of data processing in IndiHome by Telkomsel services rests with Telkomsel. Based on an interview with a Telkomsel representative, all customer data enter the Telkomsel system and database and are used for activation, account management, data changes, billing, complaint handling, customer relationship management, and service termination. Telkomsel also determines the registration mechanism, types of data collected, verification procedures, and procedures for fulfilling data subject rights (Interview with Telkomsel Representative, 2026).

This status is reinforced by Telkomsel's control over the data management system and infrastructure. Registration data are stored directly in the Telkomsel system through DSI or Digipos and are not stored by PT CWN or other marketing parties. Telkomsel controls the mechanisms for collecting, storing, using, modifying, and deleting customer data. These are the primary characteristics of a Personal Data Controller.

These findings are consistent with Kuner, Bygrave, and Docksey (2020), who explain that a *data controller* is a party that determines the purposes and means of personal data processing. In IndiHome by Telkomsel services, Telkomsel determines the types of data, registration system, verification procedures, and use of data for service provision. Based on these characteristics, Telkomsel fulfills the elements of a Personal Data Controller both normatively and empirically.

PT Creative Widya Nusantara has a different legal status. The research findings show that PT CWN does not determine the purposes of data use or data processing policies. Tunjung Aribowo Harimurti explained that PT CWN acts as a *marketing agency* that assists with marketing and registration through Sales Force personnel. Registration data are transmitted to the Telkomsel system through the designated application and are not stored in the PT CWN database (Interview with Tunjung Aribowo Harimurti, 2026).

This condition indicates that PT CWN does not fulfill the elements of a Personal Data Controller because it does not determine the purposes of processing, does not control the system, and does not control the customer database. Its role is limited to operational marketing and registration functions. Accordingly, PT CWN is more appropriately understood as an operational partner that assists in the processing process without having the authority to independently determine the purposes and means of processing.

PT Telkom Akses also has a different status from that of a Personal Data Controller. The company is only involved in network surveys and installation, with access to data necessary for technical work. Technicians obtain customer names, telephone numbers, and installation addresses through *work orders*, but do not have access to NIK, KTP photographs, or other unnecessary data. PT Telkom Akses also does not determine the purposes of data use or manage the customer database (Interview with PT Telkom Akses Technician, 2026).

The distribution of authority among Telkomsel, PT CWN, and PT Telkom Akses demonstrates a separation of functions. Telkomsel is responsible for database management, system control, identity verification, fulfillment of data subject rights, and data security. PT CWN is responsible for marketing, registration, and supervision of Sales Force personnel, while PT Telkom Akses performs technical functions with

access according to work requirements. This structure reflects the application of the accountability principle because each party exercises its authority in accordance with its respective functions and responsibilities.

Based on the overall findings, Telkomsel can be classified as a Personal Data Controller because it determines the purposes and means of processing, controls the system, and manages the customer database. PT CWN performs operational marketing and registration functions, while PT Telkom Akses uses the data necessary for technical functions. Therefore, the primary responsibility for managing and protecting consumer personal data rests with Telkomsel, while PT CWN and PT Telkom Akses perform functions within the scope of their respective authorities.

Implementation of Personal Data Protection in the IndiHome by Telkomsel Partnership Scheme

The implementation of personal data protection in IndiHome by Telkomsel services is carried out from the registration stage through the use of the service. This mechanism involves Telkomsel as the Personal Data Controller, PT CWN as the operational partner, and PT Telkom Akses as the technical function provider. Protection is implemented through consent, independent identity uploading, access restrictions, identity verification, fulfillment of data subject rights, and monitoring of processing activities.

Customer consent serves as the basis for the legitimacy of data processing during registration. Based on interviews with Sales Force personnel of PT CWN, prospective customers receive explanations regarding the purposes of data collection for registration, identity verification, network installation, administration, handling of disruptions, and billing. After receiving such information, customers decide whether to proceed with registration through the Telkomsel system (Interview with Sales Force PT CWN, 2026). Attidhira and Permana (2022) explain that valid consent must be given consciously, specifically, and based on adequate information. Therefore, the effectiveness of consent depends on customers' understanding of the data collected, the purposes of its use, the parties that have access, and their rights as data subjects.

Protection is also implemented through independent uploading of identification data. After the initial data are entered through DSI or Digipos, the Telkomsel system sends a follow-up registration link to customers to upload their KTP photographs and enter their NIK directly. This mechanism reduces field personnel's access to sensitive data and ensures that the data are stored directly in the Telkomsel system (Interview with Tunjung Aribowo Harimurti and Sales Force PT CWN, 2026).

Access restrictions constitute a primary mechanism in service provision. Sales Force personnel only access data for initial registration, while NIK and KTP photographs cannot be accessed because they are uploaded directly by customers. PT Telkom Akses technicians only obtain names, telephone numbers, and installation addresses for surveys and installation, without access to other identification documents (Interview with PT Telkom Akses Technician, 2026). This implementation reflects the principle of *data minimization*, namely that data processing is limited to information that is relevant and necessary for specific purposes.

Identity verification is also implemented to maintain the security of data processing. Based on an interview with a Telkomsel representative, requests for data changes must undergo verification using registered communication channels, such as telephone numbers, email addresses, or short message services. This procedure

ensures that data changes are carried out by the legitimate data owner (Interview with Telkomsel Representative, 2026).

The implementation of the right to rectification is also available. Customers can correct inaccurate or inappropriate data, such as telephone numbers, email addresses, or service ownership information, through verification procedures. Utami (2024) explains that the right to correct data is a fundamental right related to the principle of data accuracy. The correction mechanism enables data to remain relevant and up to date.

The right to erasure is also accommodated. Customers who no longer use the service may submit a request for deletion through official Telkomsel channels or GraPARI by completing identity verification (Interview with Sales Force PT CWN, 2026). Although this mechanism is available, the research findings indicate that information regarding the deletion period, notification after deletion, and the status of data that remain stored require greater transparency. Such clarity is important to ensure that the right to erasure can be effectively exercised.

Monitoring is conducted through access controls and verification mechanisms. A Telkomsel representative explained that data access is granted based on work requirements and the authority of each party. Data changes also undergo verification procedures documented in the system, thereby creating an activity trail that can be traced when necessary (Interview with Telkomsel Representative, 2026). In personal data protection, an *audit trail* functions as an instrument of accountability and oversight. Its effectiveness needs to be supported by authority-based access restrictions as well as periodic evaluations and audits.

Based on the overall findings, the implementation of personal data protection in the IndiHome by Telkomsel partnership scheme includes customer consent, independent identity uploading, access restrictions, identity verification, fulfillment of the rights to rectification and erasure, and the use of an *audit trail*. These findings are consistent with Attidhira and Permana (2022) and Utami (2024), who emphasize that the effectiveness of data protection is determined not only by regulations but also by the implementation of technical and organizational mechanisms that ensure security, confidentiality, and accountability.

Legal Responsibilities and Challenges of Personal Data Protection in the IndiHome by Telkomsel Partnership Scheme

Legal responsibility for personal data protection is determined by the position and authority of each party. The research findings show that Telkomsel, as the party that controls the system, determines the purposes of processing, and manages the database, has the primary responsibility for personal data protection. PT CWN is responsible for the operational aspects of registration and supervision of personnel involved in data collection.

Telkomsel is responsible for the overall process of managing customer data, including account management, data changes, billing, customer relationship management, service termination, identity verification, access restrictions, and fulfillment of data subject rights (Interview with Telkomsel Representative, 2026). This position demonstrates that the security, confidentiality, and use of personal data constitute part of Telkomsel's responsibilities as the party that determines the purposes and means of processing.

This responsibility has legal consequences. Hadjon (1987) explains that legal protection aims to ensure the fulfillment of the rights of legal subjects within a legal relationship. In IndiHome by Telkomsel services, such rights include the security and confidentiality of data, information regarding processing, and control over the use of personal data. If a failure in protection originates from the data management system, Telkomsel is responsible based on its status as the Personal Data Controller.

PT CWN's responsibility focuses on operational aspects. PT CWN assists in marketing and registration activities through Sales Force personnel and is responsible for supervising personnel compliance with data protection procedures. The company is required to ensure that Sales Force personnel do not request, store, copy, or use data beyond registration needs and to provide guidance, training, and supervision to field personnel (Interview with Tunjung Aribowo Harimurti, 2026).

The research also shows the existence of disciplinary mechanisms for personnel who misuse customer data. Any suspected violation is followed up through internal mechanisms and coordinated with Telkomsel. Sanctions are imposed on personnel proven to have violated procedures or used data for purposes outside their duties. Thus, PT CWN's responsibility relates to personnel supervision and operational compliance (Interview with Tunjung Aribowo Harimurti, 2026).

The potential misuse of data by Sales Force personnel constitutes one of the challenges. Although the Telkomsel system restricts access to NIK and KTP photographs, risks may still arise when Sales Force personnel assist customers who experience difficulties using digital devices, particularly elderly customers. Under certain circumstances, customers may request assistance in uploading documents or entering data using their devices. Such situations require stricter supervision and increased compliance with data protection procedures (Interview with Sales Force PT CWN, 2026; Interview with Tunjung Aribowo Harimurti, 2026).

The level of consumer digital literacy also affects the effectiveness of data protection. Some customers do not yet have adequate ability to understand digital registration mechanisms and the risks associated with the use of personal data and therefore remain dependent on assistance from Sales Force personnel. This finding is consistent with Syailendra, Lie, and Sudiro (2024), who state that low public awareness and understanding of data subject rights and processing risks constitute challenges to personal data protection in Indonesia. This condition may increase consumer vulnerability to data misuse.

Challenges also arise from institutional and supervisory aspects. Judijanto, Solapari, and Putra (2024) explain that there remains a gap between normative regulation and the implementation of personal data protection. The research findings show that the effectiveness of protection within the partnership scheme depends on procedural consistency, internal supervision, and personnel commitment. Therefore, strengthening a culture of compliance and awareness of data protection at the organizational level is important.

Strengthening the registration system and internal supervision is necessary to improve the effectiveness of data protection. Tunjung Aribowo Harimurti explained that a self-registration system that allows customers to carry out the registration process directly can reduce personnel interaction with personal data, with the Sales Force referral code used only as a marketing identifier. Such strengthening needs to be accompanied by access restrictions based on work requirements (*need-to-know*

basis), periodic training, and evaluation of data security mechanisms (Interview with Tunjung Aribowo Harimurti, 2026).

The need to strengthen supervision is consistent with Triyanti (2025), who emphasizes that reforming personal data governance cannot rely solely on regulations but also requires effective supervisory and compliance mechanisms. Data protection can function effectively when every party understands the limits of its authority, implements procedures, and complies with supervisory mechanisms capable of preventing and addressing violations. This is important in IndiHome by Telkomsel services because data processing involves several entities with different functions.

Based on the research findings, the primary responsibility for protecting consumer personal data rests with Telkomsel as the Personal Data Controller that determines the purposes, means, and policies of processing and centrally manages the customer database. PT Creative Widya Nusantara is responsible for operational aspects through the supervision of registration and Sales Force compliance with data protection procedures. The effectiveness of protection still faces challenges in the form of risks of data access at the operational level, low digital literacy among some customers, and the need to continuously strengthen supervision and data governance. The success of data protection within a partnership scheme depends not only on the distribution of legal responsibilities but also on the ability of the parties to establish a data management system that is secure, accountable, and oriented toward protecting consumer rights.

CONCLUSION

This study shows that the governance of consumer personal data protection in IndiHome by Telkomsel services is implemented through the distribution of authority among Telkomsel as the Personal Data Controller, PT Creative Widya Nusantara as the operational partner, and PT Telkom Akses as the technical function provider. Telkomsel has the authority to determine the purposes and means of data processing and to manage the customer database, while the operational and technical partners have restricted access according to their respective job requirements. Procedurally, personal data protection has been supported through customer consent, independent uploading of identification data, identity verification, data access restrictions, fulfillment of the rights to data rectification and erasure, and the use of an *audit trail*. Nevertheless, the substantive effectiveness of protection still faces challenges in the form of consumers' level of understanding of consent, the risk of data access at the field operational level, and the need for greater transparency in the implementation of data subject rights.

Improvements in personal data protection should be directed toward developing consent mechanisms that are simpler, more informative, and easier to understand, accompanied by consumer education regarding their rights and the risks of personal data misuse. Supervision should also be strengthened through internal audits and periodic evaluations to ensure that access restrictions, identity verification, and *audit trails* operate in accordance with established policies. In addition, periodic training for Sales Force personnel and other relevant staff is necessary to improve their understanding of data protection principles, access limitations, and the legal consequences of personal data misuse. Future research is recommended to involve more service providers and stakeholders to obtain a more comprehensive understanding of personal data protection practices and the effectiveness of

implementing Law Number 27 of 2022 concerning Personal Data Protection in the telecommunications sector in Indonesia.

Acknowledgments

The author would like to express gratitude to the Master's Program in Law, Universitas Muhammadiyah Surakarta, for the academic support provided throughout the conduct of this research. The author would also like to express sincere appreciation to Prof. Dr. Kelik Wardiono, S.H., M.H., Prof. Dr. Khudzaifah Dimyati, S.H., M.Hum., and Wardah Yuspin, S.H., M.Kn., Ph.D. for their guidance, feedback, and supervision throughout the preparation of this article. Appreciation is also extended to PT Creative Widya Nusantara, PT Telekomunikasi Selular (Telkomsel), PT Telkom Akses, and all informants who provided access to the data and information required for this research.

REFERENCE

- Attidhira, Safira Widya, & Permana, Yana Sukma. (2022). Review of Personal Data Protection Legal Regulations in Indonesia. *Awang Long Law Review*, 5(1), 280–294. <https://doi.org/10.56301/awl.v5i1.562>
- Bygrave, Lee A. (2014). *Data Privacy Law: An International Perspective*. Oxford University Press.
- Creative Widya Nusantara. (2024). *Profil Perusahaan*. <https://creativewidyanusantara.co.id/>
- Hadjon, Philipus M. (1987). *Perlindungan Hukum bagi Rakyat Indonesia: Sebuah Studi tentang Prinsip-Prinsipnya, Penanganannya oleh Peradilan dalam Lingkungan Peradilan Umum dan Pembentukan Peradilan Administrasi Negara*. Bina Ilmu.
- Judijanto, Loso, Solapari, Nuryati, & Putra, Irman. (2024). An Analysis of the Gap Between Data Protection Regulations and Privacy Rights Implementation in Indonesia. *The Easta Journal Law and Human Rights*, 3(1), 20–29. <https://doi.org/10.58812/eslhr.v3i01.351>
- Kuner, Christopher, Bygrave, Lee A., & Docksey, Christopher (Eds.). (2020). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press.
- Maleno, M. (2024). Comparative Analysis of Indonesia's Personal Data Protection Law with GDPR and CCPA. *ILCA Law Review*. <https://ejournal.psthi.or.id/index.php/ILCALaw/article/view/21>
- Miles, Matthew B., Huberman, A. Michael, & Saldaña, Johny. (2014). *Qualitative Data Analysis: A Methods Sourcebook* (3rd ed.). Sage Publications.
- Palit, Sharon M. L., & Purba, T. L. D. (2025). Legal Perspective on Data Privacy Protection as a Human Right in Indonesia. *The Easta Journal Law and Human Rights*, 4(1). <https://doi.org/10.58812/eslhr.v4i01.783>
- Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
- Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.
- Salim, H. S. (2022). *Teori dan Metode Penelitian Hukum Empiris*. Rajawali Pers.
- Solove, Daniel J. (2021). *Understanding Privacy*. Harvard University Press.
- Syailendra, Moody Rizqy, Lie, Gunardi, & Sudiro, Ahmad. (2024). Personal Data Protection Law in Indonesia: Challenges and Opportunities. *Indonesia Law Review*, 14(2). <https://scholarhub.ui.ac.id/ilrev/vol14/iss2/4/>

- Telkom Akses. (2024). *Tentang Perusahaan*. <https://www.telkomakses.co.id/>
- Telkomsel. (2024a). *Digital Sales Information*. <https://www.telkomsel.com/explore/DSI>
- Telkomsel. (2024b). *IndiHome by Telkomsel*. <https://www.telkomsel.com/indihome>
- Telkomsel. (2024c). *Kebijakan Privasi*. <https://www.telkomsel.com/kebijakan-privasi>
- Triyanti, N. (2025). Legal Gaps in Personal Data Protection: Reforming Indonesia's Population Administration System. *Hasanuddin Law Review*. <https://doi.org/10.20956/halrev.v11i1.6177>
- Utami, S. S. K. (2024). Personal Data Protection and Its Regulatory Framework in Indonesia. *De Lega Lata: Jurnal Ilmu Hukum*. <https://doi.org/10.24002/dlc.v1i2.9894>
- Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.
- Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi.
- Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.
- Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Wawancara dengan Tunjung Aribowo Harimurti, S.Sos., Manager Wilayah Operasional Surakarta PT Creative Widya Nusantara, 8 Juni 2026.
- Wawancara dengan Perwakilan PT Telekomunikasi Selular (Telkomsel), 9 Juni 2026.
- Wawancara dengan Sales Force PT Creative Widya Nusantara, 9 Juni 2026.
- Wawancara dengan Teknisi PT Telkom Akses, 10 Juni 2026.