

Data Leakage of Consumer Personal Data in Telecommunications Services Customer Registration: Who Is Responsible?

Kebocoran Data Pribadi Konsumen dalam Registrasi Pelanggan Jasa Telekomunikasi: Siapa yang Bertanggung Jawab?

Winda Fitri¹, Hari Sutra Disemadi¹, Monica Rindiyan¹

¹ Faculty of Law, Universitas Internasional Batam, Batam, Riau Islands, Indonesia

* Corresponding author: 2051061.monica@uib.edu

Abstract

The Indonesian government mandates users of SIM cards to register their National Identification Number (NIK) and Family Card number (KK) correctly to activate their prepaid numbers. However, the prepaid card registration policy invites irresponsible individuals who use that personal data without the owner's permission. Therefore, the main issue in this research is, the legal regulations governing the protection of personal data in Indonesia, the role of telecommunications service providers in maintaining the confidentiality of consumer data, and how government agencies play a role in efforts to protect personal data in Indonesia. Type of research used in this research is normative legal research and used data collection technique through literature research. The findings of this study can be summarized as follows, regarding Law No. 27 of 2022 on Personal Data Protection (PDP Law) that provides a strong legal basis for protecting consumer personal data, regulating individual rights to their personal data, and establishing obligations for personal data managers. As well as telecommunications service providers have the responsibility to provide clear and transparent information to consumers about how their personal data will be used and processed. Along with the government agencies function to enact and supervise personal data protection regulations and educate public about data privacy awareness.

Keywords

Personal Data Protection; Telecommunications Service Providers; Government Agencies



Copyrights © 2024 Author(s) and published by the Faculty of Law, Universitas Sultan Ageng Tirtayasa, Banten, Indonesia. All works published in the **Yustisia Tirtayasa** are licensed under a Creative Commons Attribution 4.0 International License. All writings published in this journal are personal views of the authors and do not represent the views of this journal and the author's affiliated institutions.

Abstrak

Pemerintah Indonesia mewajibkan pengguna kartu SIM untuk mendaftarkan Nomor Induk Kependudukan (NIK) dan Nomor Kartu Keluarga (KK) untuk mengaktifkan nomor prabayar. Namun, kebijakan registrasi kartu prabayar ini mengundang oknum yang tidak bertanggung jawab untuk menggunakan data pribadi tersebut tanpa izin pemiliknya. Oleh karena itu, isu utama dalam penelitian ini adalah, peraturan perundang-undangan yang mengatur perlindungan data pribadi di Indonesia, peran penyedia layanan telekomunikasi dalam menjaga kerahasiaan data konsumen, dan bagaimana lembaga pemerintah berperan dalam upaya melindungi data pribadi di Indonesia. Jenis penelitian yang digunakan dalam penelitian ini adalah penelitian hukum normatif dan menggunakan teknik pengumpulan data melalui studi pustaka. Penelitian ini dapat disimpulkan sebagai berikut, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) yang memberikan dasar hukum yang kuat untuk melindungi data pribadi konsumen, mengatur hak individu atas data pribadi mereka, dan menetapkan kewajiban bagi pengelola data pribadi. Selain itu, penyedia layanan telekomunikasi memiliki tanggung jawab untuk memberikan informasi yang jelas dan transparan kepada konsumen tentang bagaimana data pribadi mereka akan digunakan dan diproses. Bersamaan dengan itu, lembaga pemerintah berfungsi untuk membuat dan mengawasi peraturan perlindungan data pribadi serta mengedukasi masyarakat tentang kesadaran privasi data.

Kata Kunci

Perlindungan Data Pribadi; Penyedia Layanan Telekomunikasi; Lembaga Pemerintah

HOW TO CITE:

Winda Fitri, Hari Sutra Disemadi, Monica Rindiyani. Data Leakage of Consumer Personal Data in Telecommunications Services Customer Registration: Who Is Responsible?, *Yustisia Tirtayasa : Jurnal Tugas Akhir*, Vol.4 No.1, hlm.98-112

Introduction

In recent years, the use of technology in education, science, and the economy has increased rapidly. This use of technology is very helpful in increasing the potential for improving the welfare of the community on a national and international scale¹. The increasing development of technology is evidenced by the growing use of mobile phones by the public. Activities in telecommunications and information cannot be separated from the use of various types of providers or prepaid cards as supporting means. If we talk about telecommunications providers, they are companies that provide services for mobile phone users. As of June 2023, Indonesia has four telecommunications providers, namely Telkomsel, Indosat Ooredoo Hutchison, XL Axiata, and Smartfren, with a combined user count reaching 346.8 million². However, along with the development of this use of technology, problems that can harm the community have emerged, such as transactions for the sale of personal data, fraud, misuse of personal data, and others. These problems prove that there are shortcomings and weaknesses in the supervision of the implementation of personal data protection³.

The protection of personal information is explicitly regulated in Indonesian legislation, namely Article 28G, paragraph (1) of the 1945 Constitution, which states that "every person has the right to the protection of their personal self, family, honor, dignity, and possessions under their control, as well as the right to a sense of security and protection from threats and fear of doing or not doing something that is a human right". The Head of the General Directorate of Aptika at the Ministry of Communication and Information, Samuel, explained that personal data is a valuable asset/commodity in big data and the digital economy. Therefore, the protection of personal data will minimize privacy breaches and the misuse of personal data.

The definition of individual privacy rights is the right to enjoy a private life without interference, the right to communicate with others without unlawful investigation, and the right to control information about their personal life and their own personal data⁴. When examined further, the right to privacy is not limited to the right to information or communication, but also includes the following: 1) Information privacy, which involves the creation of regulations governing the collection and handling of personal data such as financial information, email address, social security number, medical records; 2) Bodily privacy, which concerns the protection of a person's physical self against invasive

¹ Bambang Warsita, "Kecenderungan Global Dan Regional Dalam Pemanfaatan Teknologi Informasi Dan Komunikasi Untuk Pendidikan," *Jurnal Teknodik* 10, no. 19 (2018): 069–098, <https://doi.org/10.32550/teknodik.v10i19.394>.

² Nur Hidayati, "Per Juni 2023, Jumlah Pengguna Layanan Seluler Mencapai 346,8 Juta," Kompas, 2023.

³ M Rafifnafia Hertianto, "Sistem Penegakan Hukum Terhadap Kegagalan Dalam Perlindungan Data Pribadi Di Indonesia," *Kertha Patrika* 43, no. 1 (2021): 93–109, <https://doi.org/10.24843/KP.2021.v43.i01.p07>.

⁴ Lia Sautunnida, "Urgensi Undang-Undang Perlindungan Data Pribadi Di Indonesia; Studi Perbandingan Hukum Inggris Dan Malaysia," *Kanun Jurnal Hukum* 20, no. 2 (2018): 369–84, <https://doi.org/10.24815/kanun.v20i2.11159>.

procedures such as drug testing and cavity searches; 3) Communication privacy, this type of privacy protects a person's communications from being intercepted or read without their consent which includes the security and privacy of mail, telephone, email, and other forms of communication; 4) Territorial privacy, which concerns the regulation of the limits of intrusion into one's environment from being entered or searched without their consent⁵.

Law No. 11 of 2008 Concerning Information and Electronic Transactions, in Article 16, stipulates that electronic system providers must provide a reliable and secure electronic system, be responsible for the operation of the system, and apply minimum requirements for the implementation of electronic systems. In the government's effort to protect the security of personal data of provider users, the Ministry of Communication and Information Technology (Kominfo) on October 31, 2017, has implemented a policy that requires all prepaid SIM card users to register their National Identification Number (NIK) and Family Card number (KK). These numbers are personal information from the Indonesian population database. The purpose of this policy is to protect consumers from fraud and misuse of their personal data, and to promote a single identity system in Indonesia⁶.

In 2016, the Indonesian Ministry of Communication and Information Technology (Kominfo) issued Ministerial Regulation Number 12 of 2016 on the Registration of Telecommunications Service Customers. This regulation replaced the previous regulation from 2005 and has undergone several changes through Ministerial Regulation Number 14 of 2017 and Ministerial Regulation Number 21 of 2017. The most striking change was the introduction of customer data validation using population data from the Directorate General of Population and Civil Registration (Dukcapil) of the Ministry of Internal Affairs. Through this validation and verification, customers must use an identity that is consistent with their population data, especially their NIK (National Identity Number) and KK (Family Card Number). This data will be checked against the population database, and if it is correct, the prepaid number will be activated. However, if it is not correct, the customer must activate the number through an operator gallery or outlet designated by the mobile operator. For Foreign Nationals who do not have an NIK, activation must be done at the operator gallery using an identity such as a passport/KITAP/KITAS⁷.

After the registration of prepaid cards was closed, uncertainty and incidents of misuse of personal information by foreign individuals emerged. The registration process did not provide adequate information and the organizers did not comply with existing regulations. Changes in regulations that do not impose restrictions on the number of

⁵ Hertianto, "Sistem Penegakan Hukum Terhadap Kegagalan Dalam Perlindungan Data Pribadi Di Indonesia."

⁶ Arinta Rachmawati, Rinitami Njatrijani, and Suradi Suradi, "Perlindungan Hukum Pelanggan Prabayar XL Axiata Terhadap Kebijakan Menkominfo Terkait Registrasi Ulang Nomor Handphone Di Semarang," *Diponegoro Law Journal* 8, no. 1 (2019): 142–58, <https://ejournal3.undip.ac.id/index.php/dlr/article/view/25330>.

⁷ Iwan Krisnadi and Sindhu Permadhie, "Analisis SWOT Kewajiban Registrasi Pelanggan Jasa Telekomunikasi," 2018, https://www.academia.edu/download/55255041/Analisis_SWOT_Kewajiban_Registrasi_Pelanggan_Jasa.pdf.

numbers that can be registered with one identity increase the potential risk of illegal registration by cyber criminals⁸. The prepaid card registration policy also opens opportunities for irresponsible individuals to engage in the trade of KK and NIK numbers without the consent of the owners. Meutya Viada Hafid, Vice Chairman of the DPR Commission I, showed that there is a potential risk of data leaks in the prepaid card registration process⁹. This data leak threat includes the banking sector and population information and includes many stages in the registration process itself. The Elsam Institute asserted that this policy could threaten the privacy rights of citizens, especially due to the lack of validation by operators and the ambiguity in regulations that can be exploited for illegal collection of personal data¹⁰.

In 2020, the public was shocked by the leakage of personal data carried out by an outsourcing employee of the telecommunications service provider Telkomsel, with the victim being a social media influencer, Denny Siregar. His personal data was widely disseminated on the internet, including details about the devices he used. This data breach undoubtedly caused both material and immaterial losses to him. Subsequently, Denny Siregar filed a civil lawsuit against Telkomsel for the data breach, seeking compensation in the amount of 1 trillion Indonesian Rupiah¹¹. Furthermore, there are cases of the use of more than 50 similar National Identification Numbers (NIK) and Family Card Numbers (KK) for the re-registration of SIM cards for Indosat Ooredoo users with different numbers¹². Victims of this crime have complained, and they have also reported it to the police due to the theft of personal data. However, there has been no follow-up on the handling of this case by the police.

Another common issue experienced by the public is receiving phone calls or Short Message Service (SMS) messages containing promotions or information involving threats or fraud. Data registration for SIM cards includes NIK and mobile phone numbers owned by the Ministry of Communication and Information Technology Kominfo also suspected of being leaked. This information has been circulating on social media and it is said that 1.3 billion data with a data size of 87 GB were affected by this incident. Alfons Tanujaya,

⁸ Moh. Muttaqin, "Kesadaran Pengguna Jasa Telekomunikasi Seluler Dalam Melindungi Data Kependudukan Setelah Pemberlakuan Registrasi Nomor MSISDN," n.d.

⁹ Fadhel Achmad Ar. Ridha, "Jual Beli Nomor Kartu Keluarga Dan Nomor Induk Kependudukan Melalui Media Sosial (Tinjauan Hukum Ekonomi Syariah Dan Hukum Positif)," *Diss. Pasca Sarjana*, 2020, <http://idr.uin-antasari.ac.id/15978/>.

¹⁰ Ahmad Budiman, "Perlindungan Data Pribadi Dalam Kebijakan Registrasi Kartu Prabayar," *Jurnal Pusat Penelitian Badan Keahlian DPR RI* 10, no. 06 (2018): 25–30, <https://berkas.dpr.go.id/sipinter/files/sipinter--039-20200707130131.pdf>.

¹¹ Erfan Maaruf, "Kasus Kebocoran Data, Hakim Tunda Sidang Gugatan Denny Siregar Ke Telkomsel," *Sindonews*, 2021, <https://nasional.sindonews.com/read/293756/13/kasus-kebocoran-data-hakim-tunda-sidang-gugatan-denny-siregar-ke-telkomsel-1610031687>.

¹² Kustin Ayuwuragil, "Kominfo Akui 'Pencurian' NIK Dan KK Saat Registrasi Kartu SIM," *CNN Indonesia*, 2018, <https://www.cnnindonesia.com/teknologi/20180305204703-213-280691/kominfo-akui-pencurian-nik-dan-kk-saat-registrasi-kartu-sim>.

cyber security observer from Vaksincom, stated that the mobile phone numbers in the data are valid and had checked with several numbers¹³.

Based on the background that has been explained, this study will focus on several main issues. First, the legal regulations governing the protection of personal data in Indonesia will be analyzed. Second, the role of telecommunications service providers in maintaining the confidentiality of consumer data will be investigated in more depth. Finally, the study will evaluate how government agencies play a role in efforts to protect personal data in Indonesia.

Research Method

Type of research used in this research is normative legal research, and used data collection technique through literature research, namely the legal materials used will be collected by reviewing, studying, and examining journals, legal research results, and reviewing various official documents in the form of legislation, and literature related to the problems to be studied¹⁴.

Result and Discussion

A. Legal Regulations on Personal Data Protection in Indonesia

Personal data protection is a strategic asset that is often abused, so further regulations are needed to avoid the negative consequences of personal data abuse, namely selling for commercial purposes without the consent of the data owner. The Indonesian government has enacted several laws and regulations to protect personal data. One of them is Law No. 11 of 2008 on Information and Electronic Transactions (ITE Law), which was then further developed through the amendment of ITE Law with the issuance of Law Number 19 of 2016 on Amendments to Law Number 11 of 2008 on Information and Electronic Transactions. ITE Law was established on the basis of being able to protect the legal interests of freedom of expression, both verbally and in writing. The ITE Law regulates the principle of confidentiality of communication and personal data in electronic systems. This creates a legal basis to protect personal data from illegal access or misuse within the scope of the law¹⁵.

Data protection is often associated with the protection of privacy rights. In fact, in the Explanation of the ITE Law, the right to personal data is explained as one part of privacy rights, which has the following meaning: 1) Personal rights are the right to enjoy

¹³ Novina Putri Bestari, "Duh! 1,3 Miliar Data Registrasi SIM Card Kominfo Diduga Bocor," CNBC Indonesia, 2022, <https://www.cnbcindonesia.com/tech/20220901125852-37-368451/duh-13-miliar-data-registrasi-sim-card-kominfo-diduga-bocor>.

¹⁴ Yati Nurhayati, Ifrani, and M. Yasir Said, "Metodologi Normatif Dan Empiris Dalam Perspektif Ilmu Hukum," *Jurnal Penegakan Hukum Indonesia* 2, no. 1 (2021): 1–20, <https://doi.org/10.51749/jphi.v2i1.14>.

¹⁵ Muhammad Fikri and Shelvi Rusdiana, "Ruang Lingkup Perlindungan Data Pribadi: Kajian Hukum Positif Indonesia," *Ganesha Law Review* 5, no. 1 (2023): 39–57.

one's private life and be free from all kinds of interference; 2) Personal rights are the right to be able to communicate with others without being spied on; 3) Personal rights are the right to monitor access to information about one's personal life and data¹⁶.

ITE Law is perceived as cyberlaw in Indonesia, which is expected to regulate all matters of the internet world, including punishing cybercrime perpetrators. ITE Law It is not only directed to a specific legal subject but is directed to everyone as a confirmation of the phrase "every person who intentionally commits the crime of insult and/or defamation". The government considers the ITE Law to be a form of general prevention (general prevention) provided by the state to everyone¹⁷. In the 2016 revision of the ITE Law, it was stipulated that in order to guarantee the recognition and respect for the rights and freedoms of others, and to meet fair demands. The term "guaranteeing respect and the rights and freedoms of others" is used, but in fact, the community seems to be gagged by the norms in the ITE Law. In other words, the revision did not essentially change the problems in the ITE Law. The real problem lies in the issues of "criminalization" and "interpretation of norms". The elastic, problematic, and ambiguous articles in the ITE Law have claimed many victims. However, creating an interpretation guideline for the ITE Law is not the right step to overcome this problem¹⁸. Which then gave rise to the idea of drafting a law that could fully protect personal data.

The Personal Data Protection Bill (PDP Bill), or RUU PDP as it is more commonly known, was initially discussed and became the main topic of President Jokowi's state address to the DPD and DPR on August 16, 2019¹⁹. Then, the Indonesian government began to develop a comprehensive regulation to protect personal data. In 2019, the government submitted the PDP Bill to the House of Representatives. The General Data Protection Regulation (GDPR) had a major influence on the PDP Bill, including the regulation of the rights of data subjects as a crucial point in the implementation of the right to personal data protection²⁰.

The long journey of the PDP Bill that ended with the enactment of Law No. 27 of 2022 on Personal Data Protection (PDP Law). PDP Law originated from the thought that the protection of personal data is one of human rights and the need for legal basis to provide security over personal data. PDP Law regulates the rights and obligations related

¹⁶ Faiz Rahman, "Kerangka Hukum Perlindungan Data Pribadi Dalam Penerapan Sistem Pemerintahan Berbasis Elektronik Di Indonesia," *Jurnal Legislasi Indonesia* 18, no. 1 (2021): 81–102, https://www.researchgate.net/profile/Faiz-Rahman-6/publication/350648863_Kerangka_Hukum_Perlindungan_Data_Pribadi_dalam_Penerapan_Sistem_Pemerintahan_Berbasis_Elektronik_di_Indonesia/links/606bfbfc492851e91b1a6db22/Kerangka-Hukum-Perlindungan-Data-Pribadi-

¹⁷ Anton Hendrik Samudra, "Pencemaran Nama Baik Dan Penghinaan Melalui Media Teknologi Informasi Komunikasi Di Indonesia Pasca Amandemen UU ITE," *Jurnal Hukum & Pembangunan* 50, no. 1 (2020): 91–105, <https://doi.org/10.21143/jhp.vol50.no1.2485>.

¹⁸ Atikah Mardhiya Rohmy, Teguh Suratman, and Arini Indah Nihayat, "UU ITE Dalam Perspektif Perkembangan Teknologi Informasi Dan Komunikasi," *Jurnal Dakwah Dan Komunikasi Islam* 7, no. 2 (2021): 309–39, <https://www.ejournal.iainsyarifuddin.ac.id/index.php/dakwatuna/article/download/1202/498>.

¹⁹ Moh Hamzah Hisbulloh, "Urgensi Rancangan Undang-Undang (RUU) Perlindungan Data Pribadi," *Jurnal Hukum UNISSULA* 37, no. 2 (2021): 119–33, <https://doi.org/10.26532/jh.v37i2.16272>.

²⁰ Deanne Destriani Firmansyah Putri and Muhammad Helmi Fahrozi, "Upaya Pencegahan Kebocoran Data Konsumen Melalui Pengesahan RUU Perlindungan Data Pribadi (Studi Kasus E-Commerce Bhinneka.Com)," *Borneo Law Review* 5, no. 1 (2021): 46–68, <http://jurnal.borneo.ac.id/index.php/bolrev/article/viewFile/2014/1429>.

to personal data, which includes the definition of personal data, the rights of individuals to their personal data, and the obligations of personal data controllers. Individual rights include the right to access, correct, delete, or transfer their personal data. In addition, the PDP Law also regulates the requirements for consent for the collection and processing of personal data, which must be given voluntarily by the data owner²¹.

PDP Law regulates the rights of data subjects as follows: 1. The right to information (Article 5); 2. The right to complete (Article 6); 3. The right to access (Article 7); 4. The right to terminate, delete, and/or destroy processing (Article 8); 5. The right to withdraw consent for processing (Article 9); 6. The right to object to automated decision-making and profiling (Article 10); 7. The right to delay or restrict processing (Article 11); 8. The right to sue and receive compensation for personal data breaches (Article 12); and 9. The right to data portability (Article 13)²².

There are four violations that can be subject to criminal penalties as regulated in the Personal Data Protection Law (PDP Law). First, disclosing personal data that is not your own or doxing. The perpetrator can be sentenced to a maximum of four years in prison and a maximum fine of Rp 4 billion. Second, collecting personal data illegally, perpetrators can be sentenced to a maximum of five years in prison and a maximum fine of Rp5 billion. Third, using personal data that is not your own. An example of this violation is registering a SIM card with someone else's ID card. The perpetrator is threatened with a maximum of 5 years in prison and a maximum fine of Rp5 billion. Fourth, creating false or counterfeiting personal data. The perpetrator of the violation will be given a maximum penalty of six years in prison and a fine of Rp6 billion. In addition to regulating criminal penalties, the PDP Law also regulates administrative sanctions, which will be imposed when there is a violation of the provisions on obligations. The administrative sanctions that are given are in the form of a written warning, temporary suspension of personal data processing activities, deletion or destruction of personal data, and administrative fines. For administrative fines, the amount is a maximum of 2 percent of annual income or revenue against the violation variable²³.

In the context of consumer data breaches in telecommunications service registration, the PDP Law and ITE Law play an important role. For example, when a data security breach occurs that results in the leakage of consumer personal data, the PDP Law can be used to determine the responsibility of the data controller and provide rights to individuals affected, including the right to obtain information about the data breach. Meanwhile, the ITE Law can also be used to prosecute those involved in a data security breach, especially if the breach involves illegal access or alteration of electronic data. The articles in the ITE Law that prohibit illegal acts in the cyber world can be used as a legal basis for law enforcement against data breach perpetrators.

²¹ Elfian Fauzi and Nabila Alif Radika Shandy, "Hak Atas Privasi Dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi," *Lex Renaissance* 7, no. 3 (2022): 445–61.

²² Nenny Rianarizkiwati, "Ius Constituendum Hak Atas Pelindungan Data Pribadi: Suatu Perspektif Hak Asasi Manusia," *Jurnal Hukum Sasana* 8, no. 2 (2022): 324–41, <https://doi.org/dx.doi/sasana.10.59999/v8i2.1604>.

²³ Krista Yitawati et al., "Implikasi Dan Sosialisasi Undang-Undang Perlindungan Data Pribadi Dalam Menjaga Kerahasiaan Data Pribadi Seseorang," *DAYA - MAS : Media Komunikasi Hasil Pengabdian Dan Pemberdayaan Masyarakat* 7, no. 2 (2022): 90–95, <http://dayamas.unmermediun.ac.id/index.php/dayamas/article/download/92/89>.

However, it is important to note that the ITE Law is more focused on the aspect of electronic transactions and illegal acts in the cyber world in general, while the PDP Law is more specific in regulating the protection of personal data, while the PDP Law has a more specific role in protecting the privacy of individual personal data²⁴. Therefore, both ITE Law and PDP Law were created in response to the rapid growth of information technology. It aims to protect the rights and freedoms of individuals in the online world, while also ensuring public safety, moral considerations, religious values, and security concerns.

B. The Role of Telecommunications Service Providers in Protecting Consumer Personal Data

Telecommunication service providers are key players in the modern communication ecosystem. In an era where information and communication technology (ICT) is increasingly dominating everyday life, the role of telecommunication service providers is becoming increasingly important in providing reliable and secure telecommunications services to consumers. One important aspect that is increasingly being highlighted is the protection of consumer personal data in the registration of telecommunication service customers. Customer personal data, such as identification numbers, addresses, and other sensitive information, are becoming increasingly vulnerable to potential data security breaches. Telecommunications service providers are substances that collect, store, and manage customer personal data in the context of customer registration and use of telecommunications services. Personal data collected by telecommunications service providers includes sensitive information such as identification numbers, home addresses, phone numbers, and other information that can be linked to an individual's identity²⁵. Therefore, telecommunications service providers have a great responsibility to maintain the confidentiality and security of customer personal data.

Telecommunications service providers are obliged to implement appropriate security measures to prevent the leakage of customer personal data. This includes the use of security technology, careful data access management, and monitoring of potential security threats. Telecommunications service providers also have the responsibility to provide clear and transparent information to consumers about how their personal data will be used and processed²⁶. Furthermore, they must obtain consumer consent before collecting and managing personal data. In addition, data privacy regulations are becoming increasingly strict in many countries, including Indonesia. For example, the enactment of Law Number 27 of 2022 on Personal Data Protection (PDP Law) in Indonesia is a significant step in improving the protection of consumer personal data. The PDP Law

²⁴ Gillang Achmad Riyadi and Toto Tohir Suriaatmadja, "Perlindungan Hukum Atas Kebocoran Data Pribadi Konsumen PT PLN Dihubungkan Dengan Hak Atas Keamanan Pribadi Ditinjau Dari Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi," *Bandung Confrence Series: Law Studies* 3, no. 1 (2023): 226–31, <https://doi.org/https://doi.org/10.29313/bcsls.v3i1.4945>.

²⁵ Sukarelawati Permana, "Pengaturan Perlindungan Data Pribadi Konsumen Jasa Keuangan Dalam Penggunaan Uang Elektronik Berbasis Server," *Veritas et Justitia* 8, no. 2 (2022): 386–414, <https://doi.org/https://doi.org/10.25123/vej.v8i2.5213>.

²⁶ Trias Palupi Kurnianingrum, "Urgensi Perlindungan Data Pribadi Konsumen Di Era Ekonomi Digital," *Kajian* 25, no. 3 (2023): 197–216, <https://doi.org/http://dx.doi.org/10.22212/kajian.v25i3.3893>.

regulates rights and obligations related to personal data, including licensing requirements, individual rights to their personal data, and the obligations of personal data managers²⁷. Therefore, telecommunications service providers need to understand and comply with the provisions of the PDP Law in protecting consumer personal data.

If a data breach occurs, telecommunications service providers have a legal and ethical obligation to immediately report the breach to the relevant authorities and to the affected individuals. Emergency response measures must also be taken to stop the breach and mitigate losses. Telecommunications service providers also have the responsibility to cooperate with regulatory authorities that oversee the protection of personal data, such as the Central Statistics Agency (BPS) or the Personal Data Protection Commission (KPPD) in Indonesia. They must comply with applicable regulations and participate in the audit and supervision process²⁸.

A report by Indonesia's Ombudsman between 2018 and August 2022 found over 300 complaints regarding telecommunication services provided by PT Telkom Indonesia, particularly Indihome. The most complaints, at nearly 150, were filed in 2020, with Indihome being the target of most grievances that year. PT Telkom Indonesia as a Personal Data Controller based on the Personal Data Protection Law, which can be through non-litigation which prioritizes the final result of a win-win solution and litigation channels which the final result is a win-lose solution²⁹.

C. The Role of Government Agencies in Efforts to Protect Personal Data in Indonesia

The role of government agencies in the effort to protect personal data in Indonesia is highly relevant in regulating, supervising, and ensuring the implementation of regulations related to personal data protection. In this context, government agencies play the role of law enforcers, supervisors, and facilitators in maintaining the security and privacy of individual personal data³⁰. Government agencies have a leading role in the development of personal data protection regulations. In the context of Indonesia, the regulation of personal data protection is primarily governed by Law Number 27 of 2022 on Personal Data Protection (PDP Law). Government agencies, such as the Ministry of Communication and Information Technology (Kemkominfo) and the Personal Data Protection Commission (KPPD), have played a key role in the drafting and enforcement of this PDP Law.

Kemkominfo, as one of the government agencies with authority in the field of communication and information technology, plays a leading role in ensuring the existence

²⁷ Zendik Anggriawan, Ratih Kemala, and Erry Praditya, "Analisis Perlindungan Hukum Terhadap Data Konsumen Marketplace Di Indonesia Berdasarkan Undang-Undang No. 27 Tahun 2022" 1, no. 2 (2023): 36–40, <https://doi.org/https://doi.org/10.37010/hmr.v1i02.10>.

²⁸ Sahat Maruli Tua Situmeang, "Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber," *SASI* 27, no. 1 (2021): 38–52, <https://doi.org/10.47268/sasi.v27i1.394>.

²⁹ Indah Ipa, Theresia Louize Pesulima, and Ronald Fadly Sopamena, "Perlindungan Konsumen Pelanggan Indihome Terhadap Kebocoran Data Pribadi," *Pattimura Law Study Review* 1, no. 2 (2023): 445–51, <https://doi.org/https://doi.org/10.2047268/palasrev.v1i2.12070>.

³⁰ Muhammad Bayu Satrio and Men Wih Widiatno, "Perlindungan Hukum Terhadap Data Pribadi Dalam Media Elektronik (Analisis Kasus Kebocoran Data Pengguna Facebook Indonesia)," *JCA of Law* 1, no. 1 (2020).

of an appropriate and relevant framework for personal data protection. They also play a role in issuing more detailed implementing regulations, such as the Ministry of Communication and Information Technology Regulation Number 20 of 2016 on Personal Data Protection in Electronic Systems (Permenkominfo 20/2016), which provides practical guidance on the management of personal data in electronic systems. In addition, the KPDP is an institution established in accordance with the Personal Data Protection Law and is responsible for overseeing the implementation and enforcement of the Personal Data Protection Law. The KPDP has the authority to receive reports of personal data breaches, investigate these breaches, and impose sanctions on violators in accordance with applicable laws. With the existence of the KPDP, government agencies provide a guarantee that personal data protection regulations are applied consistently and effectively³¹.

Government agencies also play a role in providing guidance and guidance to entities that manage personal data, including telecommunications service providers. These guidelines and guidelines cover best practices in the collection, processing, and storage of personal data in accordance with the principles of personal data protection. Apart from that, government agencies also provide guidance regarding reporting data breaches and the steps that must be taken to deal with them. Kemkominfo and KPDP, together with other relevant government agencies, play a role in providing guidance to manage personal data to understand and comply with the provisions of the PDP Law, ITE Law, and related regulations. In this case, government agencies act as facilitators in ensuring that appropriate and secure personal data management practices are widely implemented in various sectors.

The development of public awareness about personal data protection is an important aspect in data protection efforts. The more aware the public is about the rights and risks associated with their personal data, the more they can play an active role in protecting their own personal data security³². Government agencies play a key role in facilitating these awareness campaigns and providing the necessary resources. Government agencies are also involved as mediators in resolving personal data disputes. They can facilitate the mediation process between individuals who feel their privacy has been violated and entities that manage personal data. Mediation is one way to resolve disputes without having to go through a more complex and expensive court process.

In addition, government agencies also play a role in international cooperation related to personal data protection. In the era of globalization and increasing connectivity, personal data can easily flow across borders. Therefore, international cooperation in personal data protection is crucial.

³¹ Denico Doly, "Pembentukan Lembaga Pengawas Pelindungan Data Pribadi Dalam Perspektif Pembentukan Lembaga Negara Baru (Establishment of a Personal Data Protection Supervisory Agency in the Perspective of the Establishment of a New State Institution)," *Negara Hukum: Membangun Hukum Untuk Keadilan Dan Kesejahteraan* 12, no. 2 (2021): 223–44, <https://doi.org/https://doi.org/10.22212/jnh.v12i2.2357>.

³² Indriana Firdaus, "Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi Dari Kejahatan Peretasan," *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia* 4, no. 2 (2022): 23–31.

Conclusion

This study reveals that the legal framework for personal data protection in Indonesia has undergone positive development, especially with the enactment of Law Number 27 of 2022 on Personal Data Protection (PDP Law). The PDP Law provides a strong legal basis for protecting consumer personal data, regulating individual rights to their personal data, and establishing obligations for personal data managers. In addition to regulation, the role of telecommunications service providers in ensuring the security and privacy of consumer personal data is very important. They have an ethical and legal responsibility to protect the data they manage, implement effective security measures, and provide clear information to consumers about the use of their personal data. In order to achieve harmony between technological development and personal data protection, cooperation between the government, telecommunications service providers, and the public is essential. This joint effort will help create an environment where consumers can use telecommunications services with confidence and without fear of personal data breaches.

Funding

None

References

- Anggriawan, Zendik, Ratih Kemala, and Erry Praditya. "Analisis Perlindungan Hukum Terhadap Data Konsumen Marketplace Di Indonesia Berdasarkan Undang-Undang No. 27 Tahun 2022" 1, no. 2 (2023): 36–40. <https://doi.org/https://doi.org/10.37010/hmr.v1i02.10>.
- Ayuwuragil, Kustin. "Kominfo Akui 'Pencurian' NIK Dan KK Saat Registrasi Kartu SIM." CNN Indonesia, 2018. <https://www.cnnindonesia.com/teknologi/20180305204703-213-280691/kominfo-akui-pencurian-nik-dan-kk-saat-registrasi-kartu-sim>.
- Bestari, Novina Putri. "Duh! 1,3 Miliar Data Registrasi SIM Card Kominfo Diduga Bocor." CNBC Indonesia, 2022. <https://www.cnbcindonesia.com/tech/20220901125852-37-368451/duh-13-miliar-data-registrasi-sim-card-kominfo-diduga-bocor>.
- Budiman, Ahmad. "Perlindungan Data Pribadi Dalam Kebijakan Registrasi Kartu Prabayar." *Jurnal Pusat Penelitian Badan Keahlian DPR RI* 10, no. 06 (2018): 25–30. <https://berkas.dpr.go.id/sipinter/files/sipinter--039-20200707130131.pdf>.
- Doly, Denico. "Pembentukan Lembaga Pengawas Pelindungan Data Pribadi Dalam Perspektif Pembentukan Lembaga Negara Baru (Establishment of a Personal Data Protection Supervisory Agency in the Perspective of the Establishment of a New State Institution)." *Negara Hukum: Membangun Hukum Untuk Keadilan Dan Kesejahteraan* 12, no. 2 (2021): 223–44. <https://doi.org/https://doi.org/10.22212/jnh.v12i2.2357>.
- Fauzi, Elfian, and Nabila Alif Radika Shandy. "Hak Atas Privasi Dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi." *Lex Renaissance* 7, no. 3 (2022): 445–61.

- Fikri, Muhammad, and Shelvi Rusdiana. "Ruang Lingkup Perlindungan Data Pribadi: Kajian Hukum Positif Indonesia." *Ganesha Law Review* 5, no. 1 (2023): 39–57.
- Firdaus, Indriana. "Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi Dari Kejahatan Peretasan." *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia* 4, no. 2 (2022): 23–31.
- Hertianto, M Rafifnafia. "Sistem Penegakan Hukum Terhadap Kegagalan Dalam Perlindungan Data Pribadi Di Indonesia." *Kertha Patrika* 43, no. 1 (2021): 93–109. <https://doi.org/10.24843/KP.2021.v43.i01.p07>.
- Hidayati, Nur. "Per Juni 2023, Jumlah Pengguna Layanan Seluler Mencapai 346,8 Juta." *Kompas*, 2023.
- Hisbulloh, Moh Hamzah. "Urgensi Rancangan Undang-Undang (RUU) Perlindungan Data Pribadi." *Jurnal Hukum UNISSULA* 37, no. 2 (2021): 119–33. <https://doi.org/10.26532/jh.v37i2.16272>.
- Ipa, Indah, Theresia Louize Pesulima, and Ronald Fadly Sopamena. "Perlindungan Konsumen Pelanggan Indihome Terhadap Kebocoran Data Pribadi." *Pattimura Law Study Review* 1, no. 2 (2023): 445–51. <https://doi.org/https://doi.org/10.%2047268/palasrev.v1i2.12070>.
- Krisnadi, Iwan, and Sindhu Permadhie. "Analisis SWOT Kewajiban Registrasi Pelanggan Jasa Telekomunikasi," 2018. https://www.academia.edu/download/55255041/Analisis_SWOT_Kewajiban_Registrasi_Pelanggan_Jasa.pdf.
- Kurnianingrum, Trias Palupi. "Urgensi Perlindungan Data Pribadi Konsumen Di Era Ekonomi Digital." *Kajian* 25, no. 3 (2023): 197–216. <https://doi.org/http://dx.doi.org/10.22212/kajian.v25i3.3893>.
- Maaruf, Erfan. "Kasus Kebocoran Data, Hakim Tunda Sidang Gugatan Denny Siregar Ke Telkomsel." *Sindonews*, 2021. <https://nasional.sindonews.com/read/293756/13/kasus-kebocoran-data-hakim-tunda-sidang-gugatan-denny-siregar-ke-telkomsel-1610031687>.
- Muttaqin, Moh. "Kesadaran Pengguna Jasa Telekomunikasi Seluler Dalam Melindungi Data Kependudukan Setelah Pemberlakuan Registrasi Nomor MSISDN," n.d.
- Nurhayati, Yati, Ifrani, and M. Yasir Said. "Metodologi Normatif Dan Empiris Dalam Perspektif Ilmu Hukum." *Jurnal Penegakan Hukum Indonesia* 2, no. 1 (2021): 1–20. <https://doi.org/10.51749/jphi.v2i1.14>.
- Permana, Sukarelawati. "Pengaturan Perlindungan Data Pribadi Konsumen Jasa Keuangan Dalam Penggunaan Uang Elektronik Berbasis Server." *Veritas et Justitia* 8, no. 2 (2022): 386–414. <https://doi.org/https://doi.org/10.25123/vej.v8i2.5213>.
- Putri, Deanne Destriani Firmansyah, and Muhammad Helmi Fahrozi. "Upaya Pencegahan Kebocoran Data Konsumen Melalui Pengesahan RUU Perlindungan Data Pribadi (Studi Kasus E-Commerce Bhinneka.Com)." *Borneo Law Review* 5, no. 1 (2021): 46–68. <http://jurnal.borneo.ac.id/index.php/bolrev/article/viewFile/2014/1429>.
- Rachmawati, Arinta, Rinitami Njatrijani, and Suradi Suradi. "Perlindungan Hukum Pelanggan Prabayar XL Axiata Terhadap Kebijakan Menkominfo Terkait Registrasi Ulang Nomor Handphone Di Semarang." *Diponegoro Law Journal* 8, no. 1 (2019): 142–58. <https://ejournal3.undip.ac.id/index.php/dlr/article/view/25330>.
- Rahman, Faiz. "Kerangka Hukum Perlindungan Data Pribadi Dalam Penerapan Sistem Pemerintahan Berbasis Elektronik Di Indonesia." *Jurnal Legislasi Indonesia* 18, no. 1

- (2021): 81–102. https://www.researchgate.net/profile/Faiz-Rahman-6/publication/350648863_Kerangka_Hukum_Perlindungan_Data_Pribadi_dalam_Penerapan_Sistem_Pemerintahan_Berbasis_Elektronik_di_Indonesia/links/606bfbc492851c91b1a6db22/Kerangka-Hukum-Perlindungan-Data-Pribadi-
- Rianarizkiwati, Nenny. “Ius Constituendum Hak Atas Pelindungan Data Pribadi: Suatu Perspektif Hak Asasi Manusia.” *Jurnal Hukum Sasana* 8, no. 2 (2022): 324–41. <https://doi.org/dx.doi/sasana.10.59999/v8i2.1604>.
- Ridha, Fadhel Achmad Ar. “Jual Beli Nomor Kartu Keluarga Dan Nomor Induk Kependudukan Melalui Media Sosial (Tinjauan Hukum Ekonomi Syariah Dan Hukum Positif).” *Diss. Pasca Sarjana*, 2020. <http://idr.uin-antasari.ac.id/15978/>.
- Riyadi, Gillang Achmad, and Toto Tohir Suriaatmadja. “Perlindungan Hukum Atas Kebocoran Data Pribadi Konsumen PT PLN Dihubungkan Dengan Hak Atas Keamanan Pribadi Ditinjau Dari Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.” *Bandung Confrence Series: Law Studies* 3, no. 1 (2023): 226–31. <https://doi.org/https://doi.org/10.29313/bcsls.v3i1.4945>.
- Rohmy, Atikah Mardhiya, Teguh Suratman, and Arini Indah Nihayaty. “UU ITE Dalam Perspektif Perkembangan Teknologi Informasi Dan Komunikasi.” *Jurnal Dakwah Dan Komunikasi Islam* 7, no. 2 (2021): 309–39. <https://www.ejournal.iaisyarifuddin.ac.id/index.php/dakwatuna/article/download/1202/498>.
- Samudra, Anton Hendrik. “Pencemaran Nama Baik Dan Penghinaan Melalui Media Teknologi Informasi Komunikasi Di Indonesia Pasca Amandemen UU ITE.” *Jurnal Hukum & Pembangunan* 50, no. 1 (2020): 91–105. <https://doi.org/10.21143/jhp.vol50.no1.2485>.
- Satrio, Muhamad Bayu, and Men Wih Widiatno. “Perlindungan Hukum Terhadap Data Pribadi Dalam Media Elektronik (Analisis Kasus Kebocoran Data Pengguna Facebook Indonesia).” *JCA of Law* 1, no. 1 (2020).
- Sautunnida, Lia. “Urgensi Undang-Undang Perlindungan Data Pribadi Di Indonesia; Studi Perbandingan Hukum Inggris Dan Malaysia.” *Kanun Jurnal Hukum* 20, no. 2 (2018): 369–84. <https://doi.org/10.24815/kanun.v20i2.11159>.
- Situmeang, Sahat Maruli Tua. “Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber.” *SASI* 27, no. 1 (2021): 38–52. <https://doi.org/10.47268/sasi.v27i1.394>.
- Warsita, Bambang. “Kecenderungan Global Dan Regional Dalam Pemanfaatan Teknologi Informasi Dan Komunikasi Untuk Pendidikan.” *Jurnal Teknodik* 10, no. 19 (2018): 069–098. <https://doi.org/10.32550/teknodik.v10i19.394>.
- Yitawati, Krista, Yuni Purwati, Sarjiyati, and Bambang Sukarjono. “Implikasi Dan Sosialisasi Undang-Undang Tentang Perlindungan Data Pribadi Dalam Menjaga Kerahasiaan Data Pribadi Seseorang.” *DAYA - MAS: Media Komunikasi Hasil Pengabdian Dan Pemberdayaan Masyarakat* 7, no. 2 (2022): 90–95. <http://dayamas.unmermadiun.ac.id/index.php/dayamas/article/download/92/89>.

Author's Biography



Winda Fitri, S.H., M.H. studied Bachelor of Laws from 2012 to 2016 at Universitas Internasional Batam (UIB) and studied Master of Laws from 2016 to 2018 also at UIB and is currently pursuing further doctoral studies in Law at Pelita Harapan University, Jakarta. Starting from 2019 until now she has been active as a permanent lecturer at UIB Bachelor of Laws Program. Apart from actively teaching in the fields of Environmental Law, Islamic Law, and business law, she is also active in research activities and Community Service (PKM) activities every year. She is also active in national and international scientific forums, at national forums she has participated in focus group discussions with research teams from the DPR RI and participated in joint international conference activities.



Hari Sutra Disemadi, S.H., M.H. is a lecturer in business law at the Faculty of Law, Universitas Internasional Batam (UIB). He has a deep research interest in the field of business law, particularly Intellectual Property Rights. Hari has produced various works, including books and publications in both international and national journals. Currently, he is pursuing a doctoral degree in law at Universitas Pelita Harapan, Jakarta, demonstrating his dedication to advancing his knowledge and contributing to the academic community.



Monica Rindiyanis is currently pursuing a Bachelor of Laws degree at Universitas Internasional Batam (UIB). The power of language and argument, and the opportunity to help others navigate complex situations all draw me to this field. Law offers a challenging and stimulating career path that allows me to continuously learn and make a positive impact on society.