

Ideal Formulation Of Legal Protection For Personal Data Security In Electronic Transactions Based On The Value Of Justice

Achmad Nur Rochman¹⁾ & Andri Winjaya Laksana²⁾

¹⁾ Faculty of Law, Universitas Islam Sultan Agung (UNISSULA) Semarang, Indonesia,
E-mail: achmadnurrochman.std@unissula.ac.id

²⁾ Faculty of Law, Universitas Islam Sultan Agung (UNISSULA) Semarang, Indonesia,
E-mail: andri.w@unissula.ac.id

Abstract. *Legal protection of personal data security in electronic transactions in Indonesia, as part of the right to privacy guaranteed by the 1945 Constitution of the Republic of Indonesia, is strengthened by the Human Rights Law, the Electronic Information and Transactions (ITE) Law, Government Regulation 71/2019, and Law No. 27 of 2022 concerning Personal Data Protection, amidst increasing data processing in various digital services. Increasing internet penetration and the use of data-driven platforms increase the risk of personal data leaks and misuse in the banking, health, transportation, and marketplace sectors, as demonstrated by a number of real-life cases such as illegal online loans and misuse of customer data. Given these conditions, this study emphasizes the urgency of strengthening oversight, law enforcement, and institutional integrity to ensure effective personal data protection and provide certainty and a sense of security for the public in online transactions. The approach used in compiling this thesis is normative legal research. The specifics of this research are descriptive analysis. The theories used include legal protection theory and justice theory. Research results: (1) Legal protection of personal data security in electronic transactions in Indonesia is based on the guarantee of the right to privacy in the constitution and international human rights instruments, then strengthened through sectoral regulations until it is comprehensively affirmed in Law No. 27 of 2022 concerning Personal Data Protection. This framework regulates the definition, scope, obligations of organizers, and enforcement mechanisms through lawsuits and sanctions, but its effectiveness is largely determined by the formation of LOPDP, compliance of perpetrators, strengthening of supervision, and coordination of law enforcement. (2) The ideal concept of personal data protection based on the value of justice affirms personal data as a human right, so that its processing must be lawful, limited to the purpose, secure, transparent, and remain under the control of the data subject. Effective*

protection requires a multi-faceted approach and the establishment of an independent supervisory authority, authorized to act on and resolve disputes quickly, including through international cooperation to ensure that protection is maintained in cross-border data transfers.

Keywords: *Electronic Transactions; Ideal Concept; Personal Data Protection.*

1. Introduction

Indonesia is a state based on law (*rechtsstaat*) which requires all government administration to be based on law and respect for human rights, including the protection of personal data.¹The basic guarantee of protection comes from the 1945 Constitution of the Republic of Indonesia, specifically Article 28G Paragraph (1) which confirms the right of every person to protection of themselves, their family, their honor, their dignity and their property, as well as the right to feel safe from the threat of fear.²The strengthening of these regulations can also be seen in Article 29 Paragraph (1) of Law Number 39 of 1999 concerning Human Rights, which states that everyone has the right to protection of themselves, their families, their honor, their dignity, and their property rights. The series of legal bases above shows the state's obligation to provide legal protection for citizens' personal data through the formation and implementation of laws and regulations that regulate the authority, limitations, and responsibilities of parties processing personal data.³

The rapid development of technology and information has brought significant benefits to human life. Its impact is felt in many activities, such as increasingly efficient transportation, easily accessible tourism through digital services, expanding trade through marketplaces, the financial industry supported by electronic banking services, and governments increasingly relying on app-based service systems.⁴

The use of information technology and science also aligns with the national development goal of sustainably improving the quality of Indonesian society, as access to information, education, and public services becomes faster, broader, and more cost-effective. This change contributes to a new, connected lifestyle, where citizens' data, identities, and activities are increasingly recorded digitally.⁵

¹Rika Marlina, Division of Power in the Governance of Government in Indonesia, *Jurnal Daulat Hukum*, Vol. 1, No. 1, 2018, pp. 171-178.

²Siti Mardiyati, Constitutionality of Personal Data Protection as Part of the Right to a Sense of Security, *Discipline: Journal of the Academic Community of the Youth Pledge School of Law*, Vol. 31, No. 3, 2025, pp. 209-222.

³Jeremy Zefanya Yaka Arvante, "The Impact of Online Loan Problems and Legal Protection for Online Loan Consumers," *Indonesian Law Student Writers Association Law Journal*, Vol. 2, No. 1, 2022, pp. 73-87.

⁴Afika Febri Nur Safitri et al., Multisector Digital Transformation: Impact Analysis on Economy, Banking, and Tourism in the Industrial Era 4.0, *INOMATEC: Journal of Innovation and Contemporary Multidisciplinary Studies*, Vol. 1, No. 02, 2025, pp. 273-280.

⁵I. Gede Iwan Sudipa, et al, *Information Technology & SDGs*, Sonpedia Publishing Indonesia, Jambi, 2023, p. 5

Information technology is often seen as a “double-edged sword” because besides increasing human welfare, progress and civilization, technology can also be used as a means of committing unlawful acts, including criminal acts known as cybercrime.⁶ Advances in information and communication technology also open up opportunities for misuse in the data and information management sector, particularly in the management of personal data that requires protection. Technological developments are narrowing the boundaries of privacy, making personal data easier to access, copy, and distribute without permission. This situation becomes even more vulnerable as the use of digital services continues to increase, as more activities require people to submit data to platforms, applications, or service providers, whether for transactions, identity verification, or daily communication. Various cybercrimes are increasingly emerging that exploit technological advances, such as carding (credit card fraud), ATM/EDC skimming, hacking, cracking, phishing (internet banking fraud), and the spread of malware (viruses, worms, trojans, and bots).⁷

2. Research Methods

The type of research used in this study is Normative Legal Research, which is legal research conducted based on primary legal materials by examining theories, concepts, legal principles, and laws and regulations related to this research. This approach is also known as a library approach, namely by studying books, laws and other documents related to this research.⁸ Normative legal research is also known as doctrinal research, which is research that analyzes both the law written in books (law as written in the book) and the law decided by judges through a process.⁹

3. Results and Discussion

3.1. Legal Protection for Personal Data Security in Electronic Transactions in Indonesia

The increasingly advanced development of technology presents new challenges, particularly regarding the fulfillment of the right to privacy. The use of data-dependent internet-based services is increasingly widespread in Indonesia. This is evident in the banking, healthcare, trade transactions, online transportation, and

⁶Ari Dermawan and Akmal Akmal, The Urgency of Legal Protection for Victims of Information Technology Crimes, *Journal of Science and Social Research*, Vol. 2, No. 2, 2020, pp. 39-46.

⁷Uni Sabadina, Criminal Law Politics for Combating Information Technology Crimes Related to Personal Data Leaks by Online-Based Corporations, *Lex Renaissance*, Vol. 6, No. 4, 2021, pp. 799-814.

⁸Ahamad Rosidi et al., Methods in Normative and Sociological Legal Research (Field Research), *Journal of Law and Government*, Vol. 2, No. 1, 2024, pp. 46-58.

⁹I. Made Pasek Diantha, *Normative Legal Research Methodology in Justifying Legal Theory*, Prenada Media, Jakarta, 2016, p. 8

various other activities that require the collection of personal data. This situation presents its own challenges, particularly in addressing the need for guaranteed personal data protection. At the global economic level, Indonesia is seen as having a strategic position in international trade, including electronic transactions, which encourage the widespread circulation of personal data. This situation increases the risk of the dissemination and use of personal data, making the need for adequate regulation and protection even more crucial.¹⁰

The discussion of personal data protection is closely related to the concept of privacy. The law has recognized the concept of privacy in relation to physical disturbances in the form of trespass (entering another person's yard without permission) which is known in criminal law. In its development, the law also provides protection for human emotions and intellect. Everyone has the right to privacy, the constitution has guaranteed protection of the right to privacy, so that privacy is a basic right that is inherent in everyone without exception. In Indonesia, the right to privacy has received constitutional guarantees since the amendment to the 1945 Constitution. Article 28G paragraph (1) of the 1945 Constitution confirms the recognition of the right of every person to obtain protection for themselves, their families, honor, dignity, and property under their control, as well as the right to a sense of security and protection from the threat of fear in exercising human rights. Article 28H paragraph (4) of the 1945 Constitution also states that everyone has the right to own private property and no one may arbitrarily seize it.¹¹

According to Holvast, privacy is synonymous with freedom, control, and self-determination. However, there is still no consensus on the definitive meaning of privacy. Meanwhile, according to Solove, there are at least six definitions of privacy:¹²

1. *The right to be left alone*(right to be alone)
2. *Limited access to the self*(the right to isolate oneself from others)
3. *Secrecy*(the right to keep certain things from others)
4. *Control over the personal information*(right to control personal information)

¹⁰Aditya Ahmad Fauzi et al., *Utilization of Information Technology in Various Sectors in the Society 5.0 Era*, PT. Sonpedia Publishing Indonesia, Jambi, 2023, p. 5

¹¹Badrut Tamam and Moh Bagas Fadhli Dzil Ikrom, *Legal Protection of Citizens' Privacy Rights against Personal Data Leaks in Indonesia*, *Constitution Journal*, Vol. 3, No. 2, 2024, pp. 139-154.

¹²Siti Yuniarti, *Legal Protection of Personal Data in Indonesia*, *BECOSS JOURNAL (Business Economic, Communication, and Social Sciences)*, Vol.1, No.1, 2019, pp. 147-154

5. *Personhood*(right to protect personality)

6. *Intimacy*(the right to relate to others)

The concept of privacy as a human right that must be protected is recognized in Article 12 of the Universal Declaration of Human Rights, which states that: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attack." This provision emphasizes that no one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor shall he be subjected to attacks on his honor and reputation. Everyone has the right to the protection of the law against any such interference or attack.¹³

Danrivanto Budhijanto explained that the protection of private rights as part of human rights will strengthen humanitarian values, improve relations between individuals and society, increase independence or autonomy to exercise control and obtain appropriateness, foster a tolerant attitude and prevent discriminatory treatment, while limiting government authority.¹⁴

Privacy is indeed a human right, but there are exceptions to its application, so it is not absolute. The personal data protection guidelines published by the Organization for Economic Co-Operation and Development (OECD) allow for exceptions for national sovereignty, national security, and public policy, as long as the restrictions are minimal and publicly known. Warren and Brandeis also emphasize that privacy has limits, including:¹⁵

1. Personal information may be published for public interest.
2. Privacy protection does not apply if no harm has been experienced.
3. Privacy protection does not exist if the person concerned has expressed consent to the dissemination of his or her personal information.
4. Consent and privacy deserve legal protection because the losses that arise are often difficult to measure, especially because they concern a person's mental

¹³Edi Saputra Hasibuan and Elfirda Ade Putri, Security Protection of Personal Data in Cyberspace, *Sasana Law Journal*, Vol. 10, No. 1, 2024, pp. 70-83.

¹⁴Vincent Pane, Legal Protection for Hacked Consumer Personal Data Based on Government Regulation Number 80 of 2019 Concerning Electronic Commerce, *Lex Privatum*, Vol. XI, No. 2, 2023, pp. 1-9

¹⁵Siti Yuniarti, *Op. Cit.*, p. 150.

condition so that the impact can be felt more severely than the physical losses resulting from the disruption of private life.

The United Nations General Assembly, in its document, *The Right to Privacy in the Digital Age*, acknowledged that advances in communications technology have enabled people to connect globally, but have also increased the ability of governments, companies, and individuals to conduct surveillance, eavesdropping, and data collection that potentially threaten human rights. Privacy protection is essential for both online and offline activities.

Terms frequently used in discussions of personal data protection are "personal information" and "personal data." The United States generally uses the term personally identifiable information, while Europe uses personal data, and current regulations in Indonesia use the term personal data. Personal data is understood as any information relating to an identified or identifiable individual (data subject). The General Data Protection Regulation (GDPR) details the scope of personal data more specifically, including name, identity number, location data, online identifier, or one or more specific elements related to a person's physical, physiological, genetic, mental, economic, cultural, or social condition, including data disguised through pseudonymization that can still identify a person when combined with additional information.¹⁶

Before Law Number 27 of 2022 was passed, regulations regarding personal data protection in Indonesia were scattered across various provisions and had not been comprehensively formulated. One regulation containing these provisions was Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law). This law does recognize personal data protection, but its provisions are still incomplete. Article 26 Paragraph (1) states that, "Unless otherwise stipulated by statutory regulations, the use of any information through electronic media concerning a person's personal data must be carried out with the consent of the person concerned." Article 26 Paragraph (2) also gives the injured party the right to file a lawsuit for losses arising under this law.

Currently, regulations governing the protection of personal data of Indonesian citizens have been passed, as stated in Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). Article Number (1) of the PDP Law states that, "Personal Data is data about individuals who are identified or can be identified individually or combined with other information either directly or indirectly through electronic or non-electronic systems", in Number 2 states that, "Personal

¹⁶Guswan Hakim et al., *Comparative Legal Analysis of Personal Data Protection Regulations Between the European Union and Indonesia*, Halu Oleo Legal Research, Vol. 5, No. 2, 2023, pp. 443-453.

Data Protection is the overall effort to protect Personal Data in the series of Personal Data processing to guarantee the constitutional rights of Personal Data subjects". In both articles, it has been emphasized that personal data is protected by law as a guarantee of the basic rights of citizens.¹⁷

A person's personal data consists of several processes, including information collection, storage, processing, and data transfer from one industry to another. The more data collected, the greater the risk of misuse. The right to personal data is a property right inherent in every individual as a personal data subject. Personal data protection applies to every individual, both Indonesian citizens and foreign nationals in Indonesia, regarding all personal data processing, including collection, use, storage, transfer, and deletion.¹⁸

The use of the internet in various aspects of life not only makes things easier, but also raises various issues, including legal issues related to the protection of personal data. Often, when someone makes a transaction or registers with an organization or service on the internet, the user is asked to submit certain personal data. Regarding the protection of personal data, there are several categories of legal subjects that need to be regulated, one of which is "Personal Data Managers," namely individuals, public or private legal entities, and other community organizations that individually or jointly manage personal data. Personal Data Managers carry out "personal data management" in the form of activities or a series of actions regarding personal data, using either automatic or manual data processing tools, carried out in a structured manner with a data storage system, including, among other things, the processing of collection, use, disclosure, dissemination, and security of personal data.

Data is a crucial element because it contains various personal information frequently used in activities on digital platforms. Data is generally requested to obtain services on a digital medium, yet not all providers are able to guarantee the security of their users' personal data. This situation opens up opportunities for misuse of personal data, which is then difficult to hold accountable. Electronic system organizers are any individuals, government agencies, business actors, or elements of society that provide, manage, and/or operate electronic systems, either independently or jointly, for use by electronic system users, both for their own benefit and for the benefit of other parties. The obligations of Electronic System Organizers in protecting personal data, as stated in the Regulation of the

¹⁷Beni Kharisma Arrasuli and Khairul Fahmi, Positive Legal Protection in Indonesia Against Personal Data Misuse Crimes, *UNES Journal of Swara Justisia*, Vol. 7, No. 2, 2023, pp. 369-392.

¹⁸Siti Rahmah and Fitri Wahyuni, Legal Protection of Personal Data in the Big Data Era, *Indragiri Journal of Multidisciplinary Research*, Vol. 4, No. 3, 2024, pp. 43-50.

Minister of Communication and Information Technology Number 20 of 2016 concerning the Protection of Personal Data of Internet Users, are:¹⁹

1. Carry out certification of the Electronic Systems it manages in accordance with the provisions of laws and regulations.
2. Maintaining the truth, validity, confidentiality, accuracy and relevance as well as suitability for the purposes of obtaining, collecting, processing, analyzing, storing, displaying, announcing, sending, disseminating and destroying Personal Data.
3. Notify the Personal Data Owner in writing if there is a failure to protect the confidentiality of Personal Data in the Electronic System that he/she manages, with the following notification provisions:
 - a. Must be accompanied by the reasons or causes for the failure to protect the confidentiality of Personal Data.
 - b. This can be done electronically if the Personal Data Owner has given Consent for this purpose, which is stated at the time of obtaining and collecting the Personal Data.
 - c. It must be ensured that it has been received by the Personal Data Owner if the failure contains potential losses for the person concerned.
 - d. Written notification shall be sent to the Personal Data Owner no later than 14 (fourteen) days after the failure is discovered.
4. Have internal rules regarding the protection of Personal Data in accordance with the provisions of laws and regulations.
5. Provide an audit trail of all activities in the Electronic System it manages.
6. Provide options to Personal Data Owners regarding the Personal Data they manage which may/or may not be used and/or displayed by/to third parties with their consent as long as it is related to the purpose of obtaining and collecting Personal Data.

¹⁹Wenderlin Koswara, "Implementation of Personal Data Protection Rules by Electronic System Organizers in Relation to the Theory of Justice and Legal Certainty," *Journal of Development Law Paradigms*, Vol. 7, No. 2, 2022, pp. 86-103.

7. Provide access or opportunity to Personal Data Owners to change or update their Personal Data without disrupting the Personal Data management system, unless otherwise stipulated by statutory regulations.
8. Destroy Personal Data in accordance with the provisions in this Ministerial Regulation or the provisions of other laws and regulations that specifically regulate each Sector Supervisory and Regulatory Agency for that purpose.
9. Provide a contact person who can be easily contacted by the Personal Data Owner regarding the management of their Personal Data.

The obligations of Electronic System Organizers are also explained in Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, which explains that Electronic System Organizers are required to operate Electronic Systems that meet the following minimum requirements:²⁰

1. Can re-display Electronic Information and/or Electronic Documents in full in accordance with the retention period stipulated by statutory regulations.
2. Can protect the availability, integrity, authenticity, confidentiality and accessibility of Electronic Information in the implementation of the Electronic System.
3. Can operate in accordance with procedures or instructions in the implementation of the Electronic System.
4. Equipped with procedures or instructions announced in language, information or symbols that can be understood by the parties concerned with the implementation of the Electronic System.
5. Have an ongoing mechanism to maintain the currency, clarity, and accountability of procedures or instructions.

3.2. The Ideal Concept of Legal Protection for Personal Data Security in Electronic Transactions Based on Justice Values

Protection of personal data has been affirmed in Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia which states that "every person has the right to protection of themselves, their families, their honor, their dignity, and their property under their control, and has the right to a sense of security and

²⁰Nathanias Salsabila Marikar Sahib et al., Problems with regulations for electronic system operators (PSE) in Indonesia, *Pancasakti Law Journal (PLJ)*, Vol. 1, No. 1, 2023, p. 61-74.

protection from the threat of fear to do or not do something that is a basic human right." In addition, Article 28H paragraph (4) also stipulates that "Every person has the right to have personal property rights and these property rights may not be taken over arbitrarily by anyone." Based on the provisions of these articles, the state has an obligation to make efforts to protect every person, including protection of the soul and body, as well as everything they own, including information that is classified as personal data.²¹

A key definition in personal data protection regulations is "personal data processing." Essentially, personal data processing is defined as the entire series of actions related to personal data, including but not limited to collecting, recording, organizing, storing, modifying, using, disclosing, restricting, and deleting personal data; and/or transferring personal data across borders.²²

The process for data protection must require a multifaceted approach encompassing supervision, self-regulation, and management systems for personal information management, personal data security, administrative oversight, and industry self-regulation. Controversial jurisdictions can be addressed with a multifaceted approach: personal information litigation occurs across the network and in real society. Therefore, efforts should be made to achieve unified national legislation, strengthen implementation oversight, enhance corporate data security management, and support the establishment of industry self-regulation. This will not only be beneficial for punishing violators but also serve as a public warning to society, deter violations, and further maintain social harmony and stability.²³

The idea of personal data protection initially developed from the idea of personal data protection as a fundamental human right, as proposed by Warren and Brandeis who formulated that privacy is the right to enjoy one's life and the right to have one's feelings and thoughts respected, which should not be disturbed by others (right to be alone). This view is emphasized in Article 17 of the International Covenant on Civil and Political Rights (ICCPR) through the Human Rights Committee's General Comment No. 16 on the Rights to Respect of Privacy, Family, Home, and Correspondence, and Protection of Honour and Reputation and Article 12 of the Universal Declaration of Human Rights which states that, "no one shall be subjected to arbitrary interference with his privacy, family, home or

²¹Juan Matheus and Ariawan Gunadi. Establishment of a personal data protection supervisory agency in the digital economy era: A comparative study with the KPPU. *Justisi*, Vol. 10, No. 1, 2024, pp. 20-35.

²²Abdul Rauf, et al. Legal Protection of Personal Data in Indonesia. *SISITI: Scientific Seminar on Information Systems and Information Technology*. Vol. 14. No. 2. 2025.

²³Siti Rahmah, Darmiwati, and Fitri Wahyuni. Legal Protection of Personal Data in the Big Data Era, *Indragiri Journal of Multidisciplinary Research*, Vol. 3, No. 2, February 2023, pp. 43-52

correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."²⁴

Referring to this, as a country based on law, the Indonesian Government should provide guarantees for the protection of personal data as part of fundamental human rights. This perspective is in line with Scheltema's thinking as quoted by Ahmad Redi, who outlined the five main characteristics of a state based on law (Rule of Law/Rechtsstaat). One of these characteristics is respect, recognition, and protection of human rights that uphold the dignity of every individual. At the national level, personal data protection is a form of respect for fundamental human rights and has received constitutional guarantees through Article 28G paragraph (1) and Article 28H of the 1945 Constitution of the Republic of Indonesia. Article 28G paragraph (1) states that, "everyone has the right to protection of themselves, their families, honor, dignity, and property under their control, and has the right to a sense of security and protection from the threat of fear to do or not do something that is a human right" while Article 28H paragraph (4) states that, "everyone has the right to have personal property rights and such property rights may not be taken over arbitrarily by anyone."²⁵ This mandate is reaffirmed in Law No. 1 of 2024 concerning Electronic Information and Transactions, specifically in the Explanation of Article 26 of the ITE Law, which states that personal data protection falls within the realm of personal rights, also known as the right to privacy. Most recently, with the enactment of Law No. 27 of 2022, the strengthening of personal data protection in Indonesia has become increasingly evident as a guarantee of people's basic rights.²⁶

The existence of various regulations that establish the right to personal data protection as a fundamental human right demonstrates that the state is present to protect all citizens, both in terms of protecting one's life and body as well as protecting personal data. This also aligns with the goals of the Indonesian state, as mandated in the Fourth Paragraph of the Preamble to the 1945 Constitution of the Republic of Indonesia, which states, "...to protect the entire Indonesian nation and all of Indonesia's territory."²⁷

²⁴Herol Hansen Samin, Legal Protection Against Personal Data Leaks by Data Controllers Through a Progressive Legal Approach. *Scientific Journal of Research Student*, Vol. 1, No. 3, 2024, pp. 1-15.

²⁵Siti Mardiyati, The Constitutionality of Personal Data Protection as Part of the Right to a Sense of Security. *Consensus: Journal of Legal Studies*, Vol. 4, No. 2, 2025, pp. 221-233.

²⁶Pardamean Sihombing, Wiwik Sri Widiarty, and Binoto Nadapdap. Legal Protection of Consumer Personal Data in E-Commerce Transactions in Indonesia. *Journal of Social Technology*, Vol. 6, No. 1, 2026, pp. 373-382.

²⁷Cahya Supena and Cecep Cahya Supena. A review of the concept of the Indonesian legal state before and after the amendment to the 1945 Constitution of the Republic of Indonesia. *Moderat: Scientific Journal of Government Science*, Vol. 9, No. 2, 2023, pp. 372-388.

Although the Government has enacted various laws to strengthen individual privacy rights, their implementation has not been optimal. One of the main causes is the lack of an authoritative institution as mandated by Article 58 paragraph (2) of the PDP Law, which functions to supervise, enforce the law, and resolve disputes in the field of personal data protection. The absence of this institution creates a gap between established legal norms and implementation mechanisms in the field. This condition indicates that personal data protection in Indonesia is still in a transition phase, from normative regulations to a strong and independent institutional system. Therefore, the establishment of a personal data protection institution is urgent, not only to ensure the effective implementation of the PDP Law, but also to emphasize the state's commitment to guaranteeing citizens' constitutional rights to privacy amidst the complexities of the digital era.²⁸

The absence of a dedicated agency responsible for protecting personal data creates a legal vacuum (*rechtsvacuum*), which directly impacts legal uncertainty and weakens the protection of citizens' rights to digital privacy. This vacuum creates a situation where oversight and law enforcement mechanisms for personal data breaches are ineffective. Consequently, this leaves room for various forms of violations, such as data leaks, misuse of personal information by unauthorized parties, and cross-border data transfers without adequate oversight and accountability. From the perspective of a democratic state governed by the rule of law, this situation contradicts the principles of legal certainty and due process of law, as the state should ensure the existence of an institutional structure capable of effectively enforcing and protecting citizens' digital privacy rights.²⁹

To bridge this gap, many European countries have established independent and authoritative personal data oversight institutions from the outset. This model stems from the recognition that data protection requires a supervisory institution capable of regulating the processing of personal data. The existence of an independent institution ensures the public that their privacy rights are protected by a system that operates effectively and systematically. With this strong institutional foundation, European countries can develop comprehensive data protection practices before harmonization through the GDPR is implemented regionally.

²⁸Gunawan Widjaja and Fransiska Milenia Cesarianti. The Urgency of Establishing a Personal Data Protection Supervisory Agency in Indonesia Based on Article 58 Juncto Article 59 and Article 60 of Law Number 27 of 2022 Concerning Personal Data Protection. *Sinergi: Jurnal Riset Ilmiah*, Vol. 1, No. 4, 2024, pp. 234-242.

²⁹Haikal Akbar and Prasetyo Budi Wicaksana. Legal Protection Against Personal Data Leaks Due to Cybercrime: The Perspective of Law Number 27 of 2022. *Serambi Hukum Research Journal*, Vol. 18, No. 2, 2025, pp. 239-248.

Before the EU GDPR came into effect, data protection in Europe was already established through each country's national framework. Germany is often cited as a pioneer because, from the outset, it viewed personal data as part of citizens' constitutional rights. Therefore, its protection extends beyond administrative matters to human dignity and limits on the power of both the state and businesses. This policy direction has led to faster data protection regulations in Germany than in many other European countries.³⁰

In Germany, one of the earliest milestones was the data protection regulation in the West German state of Hesse, often considered one of the first modern data protection laws. This early regulation arose from the need to control the use of data by public administrations, particularly as computing technology began to be used to manage population information. Developments at the state level later led to the establishment of a more uniform framework at the federal level to ensure clear minimum standards for data processing by state institutions and the private sector.

4. Conclusion

Based on the research and discussion, it can be concluded that the implementation of the Deposit Insurance Corporation (LPS) regulations in the liquidation of Sharia Rural Banks (BPRS) has a strong and structured legal basis. The authority of the Deposit Insurance Corporation (LPS) in carrying out the liquidation of failed banks is clearly regulated in Law Number 24 of 2004 concerning the Deposit Insurance Corporation, as amended by Law Number 7 of 2009, and is further elaborated in the Deposit Insurance Corporation Regulation Number 1 of 2022 concerning Bank Liquidation. This regulation provides full legitimacy to the Deposit Insurance Corporation to form a liquidation team that acts as a liquidator, controls and manages bank assets, collects receivables, and represents the bank in litigation proceedings in court.

5. References

Al-Qur'an:

Al-Qur'an Surat Al-Baqarah Ayat 42, <https://quran.nu.or.id/al-baqarah/42>

Al-Qur'an Surat Al-Isra' Ayat 15, <https://quran.nu.or.id/al-isra'/15>

³⁰Syafira Agata Ramadhani. Comparison of Personal Data Protection in Indonesia and the European Union. *Lex Generalis Law Journal*, Vol. 3, No. 1, 2022, pp. 73-84.

Al-Qur'an Surat Al-Maidah Ayat 38, <https://quran.nu.or.id/al-maidah/38>

Books:

Abdul Halim Barkatullah, 2019, Hukum Transaksi Elektronik di Indonesia: Sebagai Pedoman Dalam Menghadapi Era Digital Bisnis e-commerce di Indonesia, Nusamedia, Bandung

Abdul Wahid dan Mohamad Labib, 2004, Kejahatan Mayantara (Cyber Crime), Refika Aditama, Bandung

Abubakar Eby Hara et al., 2023, Keamanan Insani (HUMAN SECURITY): Eksplorasi Berbagai Perspektif di Dunia, Pandiva Buku, Yogyakarta

Achmad Surya et. al., 2025, Perlindungan Hukum Di Indonesia, Penerbit Widina, Bandung

Aditya Ahmad Fauzi et al, 2023, Pemanfaatan Teknologi Informasi di Berbagai Sektor Pada Masa Society 5.0, PT. Sonpedia Publishing Indonesia, Jambi

Aep S. Hamidin, 2010, Tips & Trik Kartu Kredit Memaksimalkan dan Mengelola Resiko Kartu Kredit, MedPress, Yogyakarta

Agustinus Sihombing, 2023, Hukum Perlindungan Konsumen, CV. Azka Pustaka, Pasaman

Carl Joachim Friedrich, 2004, Filsafat Hukum Perspektif Historis, Nuansa dan Nusamedia. Bandung

I. Gede Iwan Sudipa, et al, 2023, Teknologi Informasi & SDGs, Sonpedia Publishing Indonesia, Jambi

I. Made Pasek Diantha, 2016, Metodologi Penelitian Hukum Normatif Dalam Justifikasi Teori Hukum, Prenada Media, Jakarta

L. J. Van Apeldoorn, 1996, Pengantar Ilmu Hukum, cetakan kedua puluh enam Pradnya Paramita, Jakarta

Nur Arifatus Sholihah et al., 2023, Metode Penelitian Kualitatif dan Kuantitatif, Selat Media, Yogyakarta

Nurul Irfan dan Masyrofah, 2013, Fiqih Jinayah, Amzah, Jakarta

Qadriani Arifuddin et al, 2025, Metodologi Penelitian Hukum, Sonpedia Publishing Indonesia, Jambi

Qodariah Barkah dan Andriyani, 2024, Perlindungan Hukum, CV. Doki Course and Training, Palembang

Ridha Ramadhany et al., 2025, Transformasi Digital Sektor Publik, Star Digital Publishing, Yogyakarta

Seva Maya Sari, 2023, Fiqih jinayah (Pengantar memahami hukum pidana Islam), PT. Sonpedia Publishing Indonesia, Jambi

Sigit Suseno, 2012, Yurisdiksi Tindak Pidana Siber, Refika Aditama, Bandung

Sinta Dewi Rosari, 2023, Pembahasan UU Pelindungan Data Pribadi (UU RI No. 27 Tahun 2022), Sinar Grafika, Jakarta

Soetandyo Wignjosoebroto, 2009, Penelitian Hukum dan Hakikatnya sebagai Penelitian Ilmiah, dalam Metode Penelitian Hukum: Konstelasi dan Refleksi, ed. Sulistyowati Irianto dan Shidarta, Yayasan Obor Indonesia, Jakarta

Taufik Firmanto et al., 2024, Metodologi Penelitian Hukum: Panduan Komprehensif Penulisan Ilmiah Bidang Hukum, PT. Sonpedia Publishing Indonesia, Jambi

Wahyudi Djafar dan M. Jodi Santoso, 2019, Perlindungan Data Pribadi, Konsep, Instrumen, dan Prinsipnya, Lembaga Studi dan Advokasi Masyarakat (ELSAM), Jakarta

Zainuddin, 2006, Hukum Islam: Pengantar Ilmu Hukum Islam di Indonesia, Sinar Grafika, Jakarta

Regulation:

Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions

Law Number 1 of 2023 concerning the Criminal Code (National Criminal Code)

Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions

Law Number 27 of 2022 concerning Personal Data Protection

Law Number 39 of 1999 concerning Human Rights

The 1945 Constitution of the Republic of Indonesia