

Protection of Notaries as Controllers and Processors of Personal Data of Litigants

Stefanie Hartanto, Prisilia Permata Putri

Faculty of Law, Universitas Pelita Harapan, Tangerang, Indonesia

stefanie.hartanto@lecturer.uph.edu

Abstract

This research examines the prevention and protection measures that can be taken by notaries in their dual role as controllers and processors of personal data. This research is motivated by the limited awareness of some notaries regarding their legal obligations to protect the personal data of witnesses, as mandated by the Personal Data Protection Law (UUPDP). This research contributes new insights by framing notaries as Controllers and Processors under the UUPDP, an aspect that has rarely been emphasized in previous legal literature. The novelty of this study lies in its specific focus on notaries' dual capacity as both Controllers and Processors of personal data under Indonesian law, particularly in the context of witness data handling an area that has not been thoroughly examined in existing scholarship. Using normative juridical methods with statutory and conceptual approaches, this study found that notaries have dual responsibilities in managing witness data and must proactively comply with the UUPDP to prevent legal risks. These responsibilities include obtaining approvals, establishing internal data protection policies, and implementing secure technologies such as encryption and regular audits. Strengthening the role of notaries in personal data protection will foster greater legal certainty and public trust in the notary profession. The integration of these findings with practical recommendations emphasizes the need for regulatory guidance and professional capacity building to support compliance with personal data protection standards.

Keywords: *Controller and Processor; Data Protection; Litigants; Notary; Personal Data*

1. INTRODUCTION

In the current era of Globalization, the digitization of legal services is growing along with the increasing use of technology in legal profession activities, including by notaries. This digital transformation makes access easier and more efficient, but also presents new challenges, especially related to personal data protection. As electronic data processing increases, the risk of data breach by the legal profession also increases. Several cases of leakage of client information and witness data handled by legal actors indicate that professional awareness and capacity in protecting personal data still needs to be strengthened.

Indonesia is a country of law (Article 1 Paragraph 3 of the 1945 Constitution), which emphasizes that the administration of the state must be based on law. The law aims to ensure fair legal protection and certainty for every individual (Article 28D of the 1945 Constitution). Legal certainty is realized if the apparatus and legal professionals carry out their duties according to the rules. Law No. 2 of 2014 concerning the Notary Position regulates the authority of Notaries as public officials in the preparation of authentic deeds, which have perfect evidentiary power for

the parties according to the contents of the deed.¹ An authentic deed is a legal document made by or before an authorized official and has perfect evidentiary force for the parties and other parties who derive rights from it, in accordance with the contents contained in the deed.²

Then in Article 15 paragraph (2) of the UUJN gives the notary additional authority, including notarizing the signature and determining the certainty of the date of the letter under hand by recording it in a special book. The notary can also write the letter under hand in the book, as well as make a copy of the document in accordance with the original.³ In addition, the notary is authorized to certify the conformity of the photocopy with the original document. Not only that, notaries also play a role in providing legal counseling related to making deeds, compiling deeds related to land, and making auction minutes deeds.⁴ In the context of collecting and processing data provided in connection with the process of making deeds and/or other documents under their authority, notaries are required to pay attention to Law Number 27 of 2022 concerning Personal Data Protection (UUPDP).⁵

There is a gap between *das sollen (ideal law)* and *das sein (legal practice)* in the protection of personal data by Notaries. Normatively, the UUJN and UUPDP require Notaries to maintain the security of personal data with technical steps to prevent leakage. Notaries must also act honestly, fairly, and protect the interests of all parties.⁶ However, many Notaries do not understand their responsibilities in the UUPDP, still store client data conventionally without adequate protection,⁷ and the lack of socialization and supervision make the implementation of this rule not optimal.⁸

Based on this, this research is different from previous studies. Previous studies on personal data protection have largely focused on sectoral contexts. Simbolon et al. (2024)⁹ examined data protection in online lending, emphasizing data leakage risks and the right to be forgotten, but did

¹ Rifandika Naufal Afif, Andi Muh Ihsan, and Dita Elvia Kusuma Putri, "Akibat Hukum Bagi Notaris Terhadap Penyalahgunaan Keadaan Dalam Pembuatan Akta Autentik," *Jurnal Ilmu Kenotariatan* 5, no. 1 (2024): 45–61, <https://doi.org/10.19184/JIK.v5i1.47761>.

² Sedy Melinda and Gunawan Djajaputra, "Pembuatan Akta Notaris Di Luar Wilayah Jabatannya Berdasarkan Undang-Undang Nomor 2 Tahun 2014 Tentang Perubahan Atas Undang-Undang Nomor 30 Tahun 2004 Tentang Jabatan Notaris," *Syntax Literate; Jurnal Ilmiah Indonesia* 6, no. 7 (2021): 3521–41, <https://doi.org/10.36418/syntax-literate.v6i7>.

³ Komang Octaviani Dewi, "Penyuluhan Hukum Tentang Pembuatan Akta Oleh Notaris," *University Of Bengkulu Law Journal* 4, no. 1 (2019): 59–70, <https://doi.org/10.33369/ubelaj.4.1.59-70>.

⁴ Brilian Pratama, Happy Warsito, and Herman Adriansyah, "Prinsip Kehati-Hatian Dalam Membuat Akta Oleh Notaris," *Repertorium: Jurnal Ilmiah Hukum Kenotariatan* 11, no. 1 (2022): 24–33, <https://doi.org/10.28946/rpt.v11i1.1640>.

⁵ Aulia Gumilang Rosadi, "Tanggung Jawab Notaris Dalam Sengketa Para Pihak Terkait Akta Perjanjian Pengikatan Jual Beli (PPJB) Yang Dibuatnya," *JCH (Jurnal Cendekia Hukum)* 5, no. 2 (2020): 243–59, <https://doi.org/http://doi.org/10.33760/jch.v5i2.228>.

⁶ Intan Permata Mipon and Mohamad Fajri Mekka Putra, "Penyelenggaraan Pelindungan Data Pribadi Oleh Notaris Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi," *Jurnal Hukum & Pembangunan* 53, no. 3 (2024): 6, <https://doi.org/10.21143/jhp.vol53.no3.1576>.

⁷ Elsa Daniella Simbolon, Mahmul Siregar, and Joiverdia Arifiyanto, "Pelindungan Korban Pemalsuan Data Diri Dalam Transaksi Pinjaman Online Melalui Penegakan Hak Untuk Dilupakan," *Neoclassical Legal Review: Journal of Law and Contemporary Issues* 3, no. 2 (2024): 77–88, <https://doi.org/10.32734/nlrjolci.v3i2.18351>.

⁸ Rifa, F., & Hidayati, M. N. (2024). Kebijakan Penal Dalam Perlindungan Data Pribadi Nasabah Fintech Lending Di Indonesia. *Binamulia Hukum*, 13(2), 461–481. <https://doi.org/10.37893/Jbh.V13i2.964>

⁹ Simbolon, Siregar, and Arifiyanto, "Pelindungan Korban Pemalsuan Data Diri Dalam Transaksi Pinjaman Online Melalui Penegakan Hak Untuk Dilupakan."

not explore the role of professional actors. Jasmine et al. (2024)¹⁰ analyzed the responsibilities of notaries based on Law No. 27 of 2022 using fault and strict liability approaches, yet lacked a discussion of concrete preventive actions and relevant technological safeguards. Meanwhile, Yudha et al. (2025)¹¹ focused on personal data misuse in e-commerce and proposed arbitration for dispute resolution, without addressing the formal legal role of notaries. Based on this, it needs to be emphasized that legal risks as well as administrative and criminal sanctions due to inappropriate personal data processing practices are an urgent issue that needs to be responded to immediately through legal research, in order to encourage stronger compliance and protection among the legal profession.

This study fills an important gap by specifically analyzing notaries as both Controllers and Processors of personal data in their capacity as public officials authorized to draft authentic deeds. Unlike previous research, it integrates the duties of notaries with the principles of personal data protection under the PDP Law and related regulations (ITE Law, PP 71/2019), and proposes practical, preventive measures—such as consent forms, internal data policies, and secure technology use—to ensure compliance and mitigate legal risk. The contribution of this study lies in offering a concrete, operational framework for notaries to implement personal data protection, a perspective that has been largely overlooked in existing legal literature.

The purpose of this study is to juridically analyze the responsibility of notaries as Controllers and Processors of Personal Data and to formulate preventive measures that can be operationalized within the scope of notarial duties. Unlike previous studies that focus either on general data protection or notary liability without offering practical guidance, this research provides a specific and novel contribution by constructing an integrated framework that aligns notarial responsibilities with the principles of the Personal Data Protection Law (UUPDP). This study explicitly addresses the gap between *das sollen* (legal norms) and *das sein* (practical implementation) by offering concrete preventive steps such as consent procedures, internal data policies, and secure technologies that notaries can adopt to ensure compliance. The findings are expected to offer practical value for notaries in performing their public functions, particularly in enhancing awareness, preventing data misuse, and reducing exposure to legal sanctions.

2. METHOD

This research employs a normative juridical method to examine the legal responsibilities and protections granted to notaries in their role as Controllers and Processors of Personal Data of witnesses. The analysis is conducted through a statute approach, by examining relevant legal provisions such as Law No. 27 of 2022 on Personal Data Protection (UUPDP), the Electronic

¹⁰ Alifia Jasmine, Benny Djaja, and Maman Sudirman, “Tanggung Jawab Notaris Dalam Perlindungan Data Pribadi Klien Berdasarkan UU No. 27 Tahun 2022 Tentang Perlindungan Data Pribadi,” *Jurnal Ilmu Hukum, Humaniora Dan Politik (JIHHP)* 5, no. 1 (2024), <https://doi.org/https://doi.org/10.38035/jihhp>.

¹¹ Iran Sahril and Dhody A R Widjaja Atmadja, “Perlindungan Data Pribadi Konsumen, Dokumen Dan Tanda Tangan Elektronik Yang Dipergunakan Oleh Pihak Ketiga Dalam Transaksi E-Commerce,” *CENDEKIA: Jurnal Penelitian Dan Pengkajian Ilmiah* 2, no. 2 (2025): 173–89, <https://doi.org/https://doi.org/10.62335/cendekia.v2i2.897>.

Information and Transactions Law (ITE Law), and Government Regulation No. 71 of 2019 concerning Electronic Systems and Transactions. Additionally, a conceptual approach is used to explore legal doctrines related to data protection, liability, and the role of notaries as public officials. The study relies on secondary data sources, which consist of: primary legal materials (statutory regulations and court decisions), secondary legal materials (doctrine from legal literature, such as academic books and peer-reviewed journals discussing notarial law and data protection), and tertiary legal materials (legal dictionaries and Indonesian dictionary). Data were collected through library research and analyzed qualitatively to construct descriptive legal arguments without the use of statistical or quantitative tools. This methodological approach aims to provide a normative justification for the legal position and responsibilities of notaries in processing and protecting personal data, by aligning their professional duties with existing regulatory standards and legal principles. It also seeks to offer a comprehensive understanding of notarial authority and responsibility in securing and maintaining the confidentiality of personal data in accordance with applicable legal standards.¹²

3. RESULTS AND DISCUSSION

The subject of Personal Data in Article 1 number 6 of the UUPDP provides is an individual to whom Personal Data is attached. Personal Data consists of specific Personal Data and general Personal Data based on Article 4 paragraph 1 of the UUPDP. General Data refers to Data that is likely not to have a significant impact on the relevant Subject in its processing, but can still be used to identify the Subject in question.¹³ The types of Personal Data that are generally regulated in Article 4 paragraph (3) of the UUPDP as seen in the *mind map* are as follows:



Figure 1. General Data Mind Map

The image shows the general categories of personal data, which refers to the type of information that can be used to identify an individual, even though it is not classified as sensitive data such as biometric data or health information. General personal data includes full name, gender,

¹² Kornelius Benuf and Muhamad Azhar, "Metodologi Penelitian Hukum Sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer," *Gema Keadilan* 7, no. 1 (2020): 20–33, <https://doi.org/https://doi.org/10.51749/JPHI.V2I1.14>.

¹³ Muhammad Fikri and Shelvi Rusdiana, "Ruang Lingkup Perlindungan Data Pribadi: Kajian Hukum Positif Indonesia," *Ganesha Law Review* 5, no. 1 (2023): 39–57, <https://ejournal2.undiksha.ac.id/index.php/GLR>.

nationality, marital status, religion, as well as combined data such as IP address and mobile phone number. Although categorized as general data, this type of data still requires protection in accordance with the provisions of Law No. 27 of 2022 on Personal Data Protection (UUPDP), as misuse of such data can lead to privacy violations and potential losses. As shown in Figure , general personal data, although not inherently sensitive, can become an entry point for profiling or identity theft when combined with other data sets. This highlights the responsibility of notaries to ensure that even general data is managed with adequate security, especially during the collection, storage, and deletion stages. The explanation of Article 4 paragraph (1) letter a of the UUPDP provides a specific definition of Personal Data, namely Personal Data which, if processed, can result in a greater impact on the Personal Data Subject, including acts of discrimination and greater losses for the Personal Data Subject. Article 4 paragraph (2) of the UUPDP stipulates several types of Personal Data that are specific as seen in the mind map below:

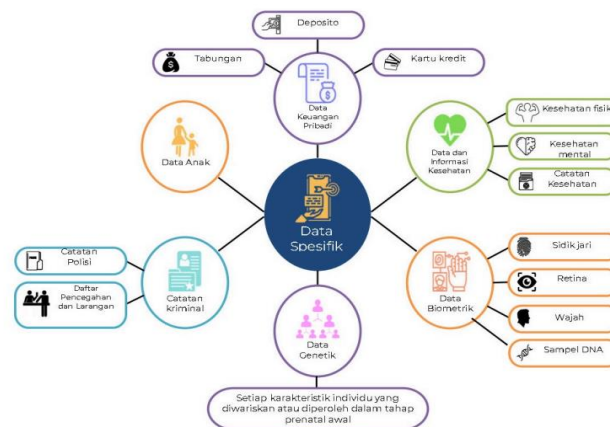


Figure 2. Types of Personal Data

The image illustrates the types of sensitive personal data that require strict protection in accordance with Law No. 27 of 2022 on Personal Data Protection (UUPDP). This category of data includes personal financial information such as savings, deposits, and credit card details; health data encompassing physical, mental, and medical records; and biometric data such as fingerprints, retina scans, facial recognition, and DNA samples that can uniquely identify an individual. Additionally, genetic information, criminal history, and police records are also included, as well as data related to children, who are considered vulnerable and therefore entitled to special protection. As shown in the figure, certain personal data is directly related to an individual's dignity, identity, and security, and its misuse can lead to serious consequences such as discrimination, fraud, or psychological harm. This requires notaries, in their role as data controllers and processors, to exercise heightened caution when handling such information. They must ensure that access to certain personal data is restricted, consent is given explicitly and informed, and technical safeguards such as encryption and secure storage are implemented. Additionally, notaries must be aware that the UUPDP imposes stricter obligations and heavier

penalties for violations involving certain personal data. Violations may result not only in administrative sanctions but also potential criminal liability. However, there are still regulatory gaps, as the Notary Public Act (UUJN) has not provided detailed guidelines on procedures for storing, retaining, or destroying sensitive personal data. This highlights the urgent need for harmonization between sectoral regulations and the UUPDP to ensure legal certainty and accountability in notary practices. Due to its highly sensitive nature, this data must be managed carefully according to data protection principles so as not to be misused and detrimental to the data owner. Based on this, the Notary as the Controller and Processor of Personal Data as referred to in Article 16 paragraph (1) of the UUPDP, carries out personal data processing activities which include:



Figure 3. Personal Data Processing Activities

This image illustrates the stages in the personal data management cycle that must be carried out carefully and in accordance with data protection principles. These stages include: data collection and acquisition, processing and analysis, storage, correction and updating, transmission or dissemination of data, and deletion or destruction of data. Each of these stages reflects the comprehensive process of personal data management aimed at safeguarding the confidentiality, accuracy, and security of personal information from misuse. As shown in the figure, the data management cycle represents a series of responsibilities that notaries must uphold when handling personal data, especially data belonging to clients, witnesses, or other related parties. At each stage, notaries must ensure that their practices comply with the principles set out in the UUPDP, including validity, fairness, purpose limitation, and data minimization.

Special attention should be given to the final stage of data deletion or destruction, which is often overlooked in legal practice. As shown in the figure, this stage requires notaries to implement clear internal policies to determine data retention periods and secure deletion methods. However, this remains a challenge, as the Notary Public Act (UUJN) does not regulate data storage or

destruction, leading to uncertainty about how long data can be stored and how it should be disposed of. Without clear guidance, notaries risk violating the UUPDP, especially if personal data is stored beyond its legal purpose or not destroyed properly.

Based on this, Article 16 paragraph (2) of the UUPDP regulates the principles that must be complied with in the Processing of Personal Data. Data collection must be carried out in a limited, specific, legal and transparent manner. The processing of data is mandatory in accordance with the purposes for which it was collected and guarantees the rights of the Personal Data Subject. In addition, the data processed must be accurate, complete, not misleading, always updated, and accountable. The security of Personal Data must also be maintained to avoid unauthorized access, disclosure, alteration, misuse, destruction, or deletion. In the process, there must be a notification regarding the purpose of the processing, the activities carried out, and in the event of a data protection failure. Personal Data that has passed the retention period or is requested to be deleted by the Personal Data Subject must be destroyed, unless there are other provisions in laws and regulations. Overall, the Processing of Personal Data must be carried out responsibly and clearly proven. In Personal Data Processing activities, there are various parties involved in processing activities as illustrated in the following diagram:



Figure 4. Parties Involved in Data Processing Activities

The image explains the main roles in the personal data protection system according to the Personal Data Protection Law (PDP Law). The controller is the party that determines the basic purpose of data processing and is responsible for its management. The processor is the party that processes the data on the Controller's command and name. Data subjects are individuals whose data is processed and have rights protected by the PDP Law. Meanwhile, the DPO (Data Protection Officer) is the party who carries out data protection functions, including supervision of compliance with personal data protection provisions. This image briefly describes the structure and responsibilities of each actor in the personal data management cycle.

In Article 1 number 4 of the UUPDP defines a Personal Data Controller as an individual, public body, or international organization that independently or jointly sets the purpose and controls the

processing of Personal Data. Meanwhile, Article 1 number 5 of the UUPDP defines a Personal Data Processor as an individual, public body, or international organization that, either alone or jointly, processes Personal Data on behalf of the Personal Data Controller.¹⁴ The main difference between a Personal Data Controller and a Personal Data Processor lies in the authority to determine the purpose of data processing. The Personal Data Controller has the authority to set the purpose of the data processing, while the Personal Data Processor is only responsible for carrying out the processing without specifying the purpose. To determine whether a person or entity is acting as a Controller, Processor, or both, there are several indicators that can be used to identify their role in the Personal Data Processing activities.¹⁵

The Personal Data Controller has a major role in determining the purposes, objectives, and methods of data processing. The Controller has a direct interest in the data processing, including in designating individuals who are categorized as data subjects. In addition, the processing carried out must be closely related to the controller and can be directly associated with it. The Controller also has full authority in determining the processing procedures and can give authority to other parties to carry out processing on behalf of an entity. On the other hand, the Personal Data Processor acts on behalf of the controller and only carries out the processing in accordance with the instructions given. The processor has no interest in data processing and only performs tasks according to the objectives set by the controller. In carrying out its role, the processor is under the supervision of another party and is bound by contractual obligations that legally govern the relationship with the controller.¹⁶

From the indicators mentioned above, it is clear that notaries are the Controllers and Processors of Personal Data because notaries are involved in all stages of Personal Data Processing,¹⁷ among others, the stage of data acquisition and collection is carried out by the Notary by collecting general data of the opposing parties for identification purposes. The data collected includes full name, gender, residential address, marital status, and ID card number, which is used to ensure the validity of the identity of the parties involved in a deed or agreement. In addition, the Notary also collects information related to the transaction, such as land certificates in the Sale and Purchase Agreement, as well as company data if the transaction involves a business entity. Data collection is carried out through physical and digital documents to ensure the completeness of information

¹⁴ Rizqi Akbar Kurniawan and Rosalinda Elsina Latumahina, "Tanggung Jawab Notaris Terhadap Penyimpanan Akta Notariil Secara Elektronik Ditinjau Dalam Perspektif Perundang-Undangan Di Indonesia," *Transparansi Hukum* 8, no. 1 (2025): 214–37.

¹⁵ Florianus Yudhi Priyo Amboro and Viona Puspita, "Perlindungan Hukum Atas Data Pribadi (Studi Perbandingan Hukum Indonesia Dan Norwegia)," in *CoMBInES-Conference on Management, Business, Innovation, Education and Social Sciences*, vol. 1, 2021, 415–27, <https://journal.uib.ac.id/index.php/combines>.

¹⁶ Gio Arjuna Putra, "Reformulasi Ketentuan Pengelolaan Data Pribadi Sebagai Ius Constituendum Dalam Menjamin Perlindungan Data Pribadi Pengguna Layanan Media Sosial," *Jurnal Hukum Lex Generalis* 2, no. 8 (2021): 684–700, <https://doi.org/https://doi.org/10.56370/jhlg.v2i8.105>.

¹⁷ Satrio Abdillah and Tessa Shasrini, "Peran Notaris Dalam Perlindungan Data Pribadi: Studi Kasus Implementasi UU Perlindungan Data Di Indonesia," *Sang Pencerah: Jurnal Ilmiah Universitas Muhammadiyah Buton* 11, no. 1 (2025): 281–94, <https://doi.org/https://doi.org/10.35326/pencerah.v11i1>.

Preventing personal data breaches in notary practice requires not only normative compliance with Law No. 27 of 2022 on Personal Data Protection (UUPDP), but also the implementation of technical measures and comprehensive internal policies. Notaries have the responsibility as controllers and processors of personal data, so the implementation of internal policies related to data processing is crucial. This internal policy should cover the entire cycle of personal data processing, from data collection, processing, storage, to data destruction. One of the concrete forms that must be prepared is a written consent form given to the client before the data is collected. In addition, notaries are required to develop and implement structured and documented internal personal data protection procedures..¹⁸

From a technical perspective, the protection of personal data must be implemented through the use of digital security protocols, such as data encryption, up-to-date firewalls and antivirus, as well as layered authorization systems such as the use of complex passwords and two-factor authentication (2FA). The main objective is to prevent unauthorized access, leakage or misuse of data by internal or external parties. It is also important for notaries to organize regular education and training for all employees, including apprentices. Training materials should include an understanding of the provisions of the UUPDP, data security procedures, and the importance of maintaining the confidentiality of client information. In contrast to Jasmine Yudha's research, which emphasizes the urgency of normative compliance with the UUPDP by notaries, and Simbolon's research, which highlights the need to strengthen ethical regulations in the notary position, this study seeks to integrate the legal and technical dimensions holistically. With this approach, preventive measures are not only normative, but also functional in practice, to ensure more effective and sustainable personal data protection..¹⁹

In addition to the notary itself, the Personal Data Processor can also be a notary employee who is assigned to process the personal data of the person by entering the data into the deed. So that to avoid potential lawsuits due to misuse of Personal Data or violations of the UUPDP, notaries need to implement comprehensive preventive measures in data processing activities. Some preventive steps that can be taken by notaries include providing an approval form for the provision of Personal Data to the witnesses for the witnesses to study and sign before the witnesses provide Personal Data..²⁰ The consent form should contain the rights of the Personal Data Subject as stipulated in Chapter IV of the UUPDP, including the following:

Consent Form to parties Consent forms from the parties regarding the provision and use of Personal Data need to include explicit consent to prevent future disputes. Clauses that can be used for example, "By submitting Personal Data to us, you consent to the collection, use, and

¹⁸ Nindi Wulandari, "Tanggung Jawab Hukum Notaris Dalam Pembuatan Akta," *PUTAT: Jurnal Pelita Pendidikan, Hukum, Ekonomi Dan Teknologi* 1, no. 1 (2025): 20–26, <https://jurnalpelitanegribelantaraya.com/index.php/putat>.

¹⁹ Caesar Faturahman Hadju, "Tanggung Jawab Notaris Werda Terhadap Hilangnya Minuta Akta," *Officium Notarium* 1, no. 2 (2021): 270–83, <https://doi.org/https://doi.org/10.32816/paramarta.v21i1.171>.

²⁰ Triami Arie Vanensa, Fitra Deni, and B F Sihombing, "Perlindungan Hukum Bagi Penghadap Penyandang Disabilitas Dalam Pembuatan Akta Notaris," *Jurnal Hukum Dan Bisnis (Selisik)* 10, no. 1 (2024): 44–62, <https://journal.univpancasila.ac.id/>.

disclosure of such data in accordance with the Transaction Purpose." Additionally, it is important for the notary to explain the purpose for which personal data is collected, which should be limited to legitimate and clear uses. For example, "We use your Personal Data for certain purposes, such as creating a deed of agreement and to improve your experience of using our services." Data usage restrictions also need to be emphasized, by ensuring that data is only used for its original purpose and is not disseminated without permission or legal orders. The corresponding clause could read, "We are committed to maintaining the confidentiality of your Personal Data and only using it for the purposes that have been identified. The data can also be provided to third parties if necessary, such as to comply with government requests or to execute court orders."

Furthermore, implement internal policies related to the Processing of Personal Data. In addition to providing the consent form for the provision of Personal Data to the client, the notary also needs to implement strict internal policies to protect the personal data of the client.²¹ This policy must cover all aspects of the Processing of personal data, from data collection, processing, and storage. Notary's internal policy regarding the processing of personal data Notaries should implement strong security protocols to protect Personal Data from unauthorized access, leakage, or misuse. One of the main methods is encryption, which converts data into an illegible form for unauthorized parties. In addition, network security with an always-up-to-date firewall and antivirus, as well as access restrictions through strict authorization, including the use of complex passwords and two-factor authentication, are essential for keeping data safe.²² Then the existence of education and training for employees, including internships, is also a crucial step. This training must include an understanding of the UUPDP, internal privacy policies, and data security procedures so that all parties understand the importance of maintaining the confidentiality of Personal Data.²³

Furthermore, implement internal policies related to the Processing of Personal Data. In addition to providing the consent form for the provision of Personal Data to the client, the notary also needs to implement strict internal policies to protect the personal data of the client.²⁴ This policy must cover all aspects of the Processing of personal data, from data collection, processing, and storage. Notary's internal policy regarding the processing of personal data Notaries should implement strong security protocols to protect Personal Data from unauthorized access, leakage, or misuse. One of the main methods is encryption, which converts data into an illegible form for

²¹ Matthew Bias Ferari, Hasim Purba, and Suprayitno Suprayitno, "Penegakan Hukum Terhadap Pelanggaran Kode Etik Notaris Dalam Pembuatan Akta Otentik.," *Journal Of Science And Social Research* 8, no. 1 (2025): 914–21, <https://doi.org/https://doi.org/10.54314/jssr.v8i1.2799>.

²² Prado Dian Firmansyah et al., "Manajemen Sekuriti Dalam Era-Digital Untuk Mengoptimalisasi Perlindungan Data Dengan Teknologi Lanjutan," *Jurnal Kewirausahaan Dan Multi Talenta* 2, no. 2 (2024): 112–25, <https://doi.org/https://doi.org/10.38035/jkmt.v2i2.160>.

²³ Nurul Inayah Muchlisa Syarifudin, "Bentuk Perlindungan Da Pertanggung-Jawaban Notaris Terhadap Kerahasiaan Isi Akta," *SINERGI: Jurnal Riset Ilmiah* 1, no. 11 (2024): 1095–1105, <https://doi.org/https://doi.org/10.62335/9t8h2565>.

²⁴ Matthew Bias Ferari, Hasim Purba, and Suprayitno Suprayitno, "Penegakan Hukum Terhadap Pelanggaran Kode Etik Notaris Dalam Pembuatan Akta Otentik.," *Journal Of Science And Social Research* 8, no. 1 (2025): 914–21, <https://doi.org/https://doi.org/10.54314/jssr.v8i1.2799>.

unauthorized parties. In addition, network security with an always-up-to-date firewall and antivirus, as well as access restrictions through strict authorization, including the use of complex passwords and two-factor authentication, are essential for keeping data safe.²⁵ Then the existence of education and training for employees, including internships, is also a crucial step. This training must include an understanding of the UUPDP, internal privacy policies, and data security procedures so that all parties understand the importance of maintaining the confidentiality of Personal Data.²⁶

The legal protection of personal data is regulated in various regulations, including the ITE Law, the PDP Law, as well as government regulations and related agencies.²⁷ In this context, the Notary has an important role as the Controller and Processor of the Facing Data, especially in ensuring the security and confidentiality of personal data contained in the authentic deed. In the event of a violation of personal data, criminal and administrative sanctions can be imposed, as stipulated in the PDP Law. However, in practice, there are still challenges in the implementation of data protection, such as the lack of understanding of notaries of personal data protection obligations and the lack of optimal supervision. The PDP Law, which was passed in 2022, provides a clearer legal basis for personal data protection, including restrictions, rights, and obligations of parties involved in data management.²⁸ However, challenges in personal data protection still arise, especially related to the low level of legal awareness, the use of standard clauses in agreements, and the absence of a special institution that oversees the effective implementation of data protection.²⁹ In the context of Notary, this challenge has the potential to pose a risk of leakage or misuse of consumer data, so more decisive preventive measures are needed, both from regulatory and supervisory aspects.³⁰

As an official who makes an authentic deed, Notaries are obliged to integrate personal data protection into their professional practices. The absence of special regulations that regulate the data protection mechanism in the process of making authentic deeds can cause an imbalance between the rights and obligations of Notaries and Witnesses. Therefore, it is necessary to strengthen regulations and more specific policies related to the responsibility of Notaries as

²⁵ Firmansyah et al., “Manajemen Sekuriti Dalam Era-Digital Untuk Mengoptimisasi Perlindungan Data Dengan Teknologi Lanjutan.”

²⁶ Syarifudin, “Bentuk Perlindungan Dan Pertanggung-Jawaban Notaris Terhadap Kerahasiaan Isi Akta.”

²⁷ Dinda Pratiwi and Rianda Dirkareshza, “Pengelabuan Informasi Harga Di E-Commerce Terhadap Konsumen Melalui Flash Sale,” *Jurnal Ius Constituendum* 8, no. 3 (2023): 406–23, <https://doi.org/https://doi.org/10.26623/jic.v8i3.7344>.

²⁸ Husni Kurniawati and Yunanto Yunanto, “Perlindungan Hukum Terhadap Penyalahgunaan Data Pribadi Debitur Dalam Aktivitas Pinjaman Online,” *Jurnal Ius Constituendum* 7, no. 1 (2022): 102–14, <https://doi.org/https://doi.org/10.26623/jic.v7i1.4290>.

²⁹ Hasnati Hasnati and Puti Mayang Seruni, “Consumer’s Personal Data Protection in the Digital Era,” *Jurnal Ius Constituendum* 9, no. 1 (2024): 20–35, <https://doi.org/https://doi.org/10.26623/jic.v9i1.8061>.

³⁰ Muhammad Alhadi Murizqy and Rianda Dirkareshza, “Peninjauan Aspek Keamanan Dan Perlindungan Hukum Terhadap Investor Cryptocurrency,” *Jurnal Ius Constituendum* 7, no. 2 (2022): 277–92, <https://doi.org/https://doi.org/10.26623/jic.v7i2.4067>.

Controller and Processor of Facing Data, including technical obligations in maintaining data security as well as stricter supervision mechanisms to ensure legal compliance.³¹

As a preventive evaluative measure, notaries need to conduct regular internal audits to review the effectiveness of the data protection policies they have implemented. These audits aim to identify potential risks of violations, provide recommendations for improvement, and ensure compliance with applicable legal provisions, thereby maintaining public trust in the integrity of the notary profession. From a legal perspective, this obligation is in line with Article 14(b) and (f) of Law No. 27 of 2022 on Personal Data Protection (UUPDP), which stipulates that data controllers must maintain integrity, accuracy, and accountability at every stage of personal data processing.

The protection of notaries is not only seen from the juridical aspect and compliance with regulations, but also from the moral and ethical aspects of professionalism. Islamic principles such as justice, honesty, and transparency play an important role in shaping the integrity of notaries in managing the personal data of the parties to the case. The integration of these values encourages more responsible and ethical notary practices, so as to prevent abuse of authority and strengthen public trust in the notary profession. Thus, the protection of notaries as data controllers and processors not only relies on formal legal instruments, but is also supported by a solid moral foundation as part of ethical reform in the national legal system.³²

The implementation of strict internal policies in the processing of personal data by notaries is not only a manifestation of normative compliance with the UUPDP but also a legal protection instrument for data subjects. These policies must include strict access control mechanisms, granting access rights only to parties who are legally and professionally authorized based on their duties and responsibilities. To ensure transparency and oversight, notaries must also adopt a data access activity logging system that can be used to detect data breaches or misuse.³³ In the event of a data breach or violation, Article 46(2) of the UUPDP stipulates that the data controller must immediately notify the data subjects and, if necessary, the data protection authority. Therefore, notaries must establish data security incident response procedures that include reporting, cause analysis, and corrective measures to prevent further impact.

Furthermore, the relationship between notaries and third parties, such as interns, administrative staff, or information technology service providers, must be understood as a legal relationship with liability implications. Pursuant to Article 51(1) of the UUPDP, data controllers are responsible for all processing of personal data carried out by parties acting on their behalf. This means that notaries remain fully liable if third parties commit violations in data processing,

³¹ Ruth Deta Louisa and Mohammad Fajri Mekka Putra, "Pendirian Persero Perorangan Tanpa Akta Notaris Berdasarkan Undang-Undang Cipta Kerja," *Jurnal Ius Constituendum* 8, no. 2 (2023): 185–206, <https://doi.org/https://doi.org/10.26623/jic.v8i2.6722>.

³² Afifi Lubis et al., "Strengthening The Integrity Of The Notary Position From The Perspective Of Islamic Ethics," *PETITA: Jurnal Kajian Ilmu Hukum Dan Syariah* 10, no. 1 (2025): 449–65.

³³ Veronika Christiana, Didik Suahriyanto, and Ismail Ismail, "Perlindungan Data Nasabah Perbankan Dengan Perjanjian Pembukaan Rekening," *Mutiara: Multidiciplinary Scientifict Journal* 3, no. 1 (2025): 1–16, <https://doi.org/https://doi.org/10.57185/mutiara.v3i1.329>.

including misuse, unauthorized access, or negligence. Therefore, it is crucial for notaries to establish legal relationships with third parties in writing through non-disclosure agreements (NDAs) and/or data processing agreements (DPAs) that include provisions on access limits, data protection standards, and legal sanctions for violations. In addition, notaries are also required to implement regular monitoring and control mechanisms to ensure that third parties act in accordance with applicable legal compliance standards.³⁴

Therefore, the implementation of strict internal policies on Personal Data Processing not only ensures compliance with regulations but also strengthens the protection of personal data. This policy must include strict access control mechanisms, including granting access rights only to authorized parties in accordance with their duties and responsibilities. Notaries also need to adopt a data access activity logging system to monitor potential violations or misuse. Additionally, to enhance accountability, notaries can establish procedures for reporting data security incidents. Any violations or data breaches must be reported, analyzed, and addressed promptly to prevent further impact. This mechanism should also include notification to affected parties and, if necessary, to the relevant authorities in accordance with applicable regulations.³⁵

4. CONCLUSION

In exercising his authority under the UUJN, the notary cannot deviate from his position as the Controller and Processor of Personal Data based on the UUPD. Notaries have an absolute responsibility to protect Personal Data from the risk of misuse and infringement. The application of the UUPDP must be used as a legal basis in every stage of personal data processing in notary practice. Notaries must expressly provide consent forms that must be studied and signed by witnesses before data is collected, to avoid potential misunderstandings in the future. In addition, notaries are required to develop and implement clear internal policies and conduct regular internal audits to ensure compliance and identify deficiencies. Therefore, by implementing these preventive measures, notaries can not only minimize the risk of lawsuits that may arise, but can also maintain the trust of witnesses. This trust is key in every transaction, which will ultimately strengthen the reputation of notaries as reliable professionals in managing personal data.

REFERENCES

- Abdillah, Satrio, and Tessa Shasrini. "Peran Notaris Dalam Perlindungan Data Pribadi: Studi Kasus Implementasi UU Perlindungan Data Di Indonesia." *Sang Pencerah: Jurnal Ilmiah Universitas Muhammadiyah Buton* 11, no. 1 (2025): 281–94. <https://doi.org/https://doi.org/10.35326/pencerah.v11i1>.
- Afif, Rifandika Naufal, Andi Muh Ihsan, and Dita Elvia Kusuma Putri. "Akibat Hukum Bagi Notaris Terhadap Penyalahgunaan Keadaan Dalam Pembuatan Akta Autentik." *Jurnal Ilmu Kenotariatan* 5, no. 1 (2024): 45–61. <https://doi.org/10.19184/JIK.v5i1.47761>.

³⁴ Johannes Ibrahim Kosasih and Hassanain Haykal, *Kasus Hukum Notaris Di Bidang Kredit Perbankan* (Bumi Aksara, 2021), <https://books.google.co.id/books?hl=id&lr=&id=O-QhEAAQBAJ&oi>.

³⁵ Wahyu Hidayat and Anas Lutfi, "Implementasi Kode Etik Notaris Di Wilayah Tangerang Selatan," *Binamulia Hukum* 14, no. 1 (2025): 1–17, <https://doi.org/https://doi.org/10.37893/jbh.v14i1.974>.

- Amboro, Florianus Yudhi Priyo, and Viona Puspita. "Perlindungan Hukum Atas Data Pribadi (Studi Perbandingan Hukum Indonesia Dan Norwegia)." In *CoMBInES-Conference on Management, Business, Innovation, Education and Social Sciences*, 1:415–27, 2021. <https://journal.uib.ac.id/index.php/combines>.
- Benuf, Kornelius, and Muhamad Azhar. "Metodologi Penelitian Hukum Sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer." *Gema Keadilan* 7, no. 1 (2020): 20–33. <https://doi.org/https://doi.org/10.51749/JPHI.V2I1.14>.
- Christiana, Veronika, Didik Suahriyanto, and Ismail Ismail. "Perlindungan Data Nasabah Perbankan Dengan Perjanjian Pembukaan Rekening." *Mutiara: Multidisciplinary Scientific Journal* 3, no. 1 (2025): 1–16. <https://doi.org/https://doi.org/10.57185/mutiara.v3i1.329>.
- Dewi, Komang Octaviani. "Penyuluhan Hukum Tentang Pembuatan Akta Oleh Notaris." *University Of Bengkulu Law Journal* 4, no. 1 (2019): 59–70. <https://doi.org/https://doi.org/10.33369/ubelaj.4.1.59-70>.
- Ferari, Matthew Bias, Hasim Purba, and Suprayitno Suprayitno. "Penegakan Hukum Terhadap Pelanggaran Kode Etik Notaris Dalam Pembuatan Akta Otentik." *Journal Of Science And Social Research* 8, no. 1 (2025): 914–21. <https://doi.org/https://doi.org/10.54314/jssr.v8i1.2799>.
- Fikri, Muhammad, and Shelvi Rusdiana. "Ruang Lingkup Perlindungan Data Pribadi: Kajian Hukum Positif Indonesia." *Ganesha Law Review* 5, no. 1 (2023): 39–57. <https://ejournal2.undiksha.ac.id/index.php/GLR>.
- Firmansyah, Prado Dian, Achmad Fauzi, Riky Barja, Andrea Putra Mulyana, Theresia Naomi Putri, Adam Surachman, and Gilang Ramadhan. "Manajemen Sekuriti Dalam Era-Digital Untuk Mengoptimalkan Perlindungan Data Dengan Teknologi Lanjutan." *Jurnal Kewirausahaan Dan Multi Talenta* 2, no. 2 (2024): 112–25. <https://doi.org/https://doi.org/10.38035/jkmt.v2i2.160>.
- Hadju, Caesar Faturahman. "Tanggung Jawab Notaris Werda Terhadap Hilangnya Minuta Akta." *Officium Notarium* 1, no. 2 (2021): 270–83. <https://doi.org/https://doi.org/10.32816/paramarta.v2i1.171>.
- Hasnati, Hasnati, and Puti Mayang Seruni. "Consumer's Personal Data Protection in the Digital Era." *Jurnal Ius Constituendum* 9, no. 1 (2024): 20–35. <https://doi.org/https://doi.org/10.26623/jic.v9i1.8061>.
- Hidayat, Wahyu, and Anas Lutfi. "Implementasi Kode Etik Notaris Di Wilayah Tangerang Selatan." *Binamulia Hukum* 14, no. 1 (2025): 1–17. <https://doi.org/https://doi.org/10.37893/jbh.v14i1.974>.
- Jasmine, Alifia, Benny Djaja, and Maman Sudirman. "Tanggung Jawab Notaris Dalam Perlindungan Data Pribadi Klien Berdasarkan UU No. 27 Tahun 2022 Tentang Perlindungan Data Pribadi." *Jurnal Ilmu Hukum, Humaniora Dan Politik (JIHHP)* 5, no. 1 (2024). <https://doi.org/https://doi.org/10.38035/jihhp>.
- Kosasih, Johannes Ibrahim, and Hassanain Haykal. *Kasus Hukum Notaris Di Bidang Kredit Perbankan*. Bumi Aksara, 2021. <https://books.google.co.id/books?hl=id&lr=&id=O-QhEAAAQBAJ&oi>.
- Kurniawan, Rizqi Akbar, and Rosalinda Elsin Latumahina. "Tanggung Jawab Notaris Terhadap Penyimpanan Akta Notariil Secara Elektronik Ditinjau Dalam Perspektif Perundang-Undangan Di Indonesia." *Transparansi Hukum* 8, no. 1 (2025): 214–37.
- Kurniawati, Husni, and Yunanto Yunanto. "Perlindungan Hukum Terhadap Penyalahgunaan

- Data Pribadi Debitur Dalam Aktivitas Pinjaman Online.” *Jurnal Ius Constituendum* 7, no. 1 (2022): 102–14. <https://doi.org/https://doi.org/10.26623/jic.v7i1.4290>.
- Louisa, Ruth Deta, and Mohammad Fajri Mekka Putra. “Pendirian Persero Perorangan Tanpa Akta Notaris Berdasarkan Undang-Undang Cipta Kerja.” *Jurnal Ius Constituendum* 8, no. 2 (2023): 185–206. <https://doi.org/https://doi.org/10.26623/jic.v8i2.6722>.
- Lubis, Afifi, Ikhsan Lubis, Nelly Azwarni Sinaga, Duma Indah Sari Lubis, and Andi Hakim Lubis. “Strengthening The Integrity Of The Notary Position From The Perspective Of Islamic Ethics.” *Petita: Jurnal Kajian Ilmu Hukum Dan Syariah* 10, no. 1 (2025): 449–65.
- Melinda, Sendy, and Gunawan Djajaputra. “Pembuatan Akta Notaris Di Luar Wilayah Jabatannya Berdasarkan Undang-Undang Nomor 2 Tahun 2014 Tentang Perubahan Atas Undang-Undang Nomor 30 Tahun 2004 Tentang Jabatan Notaris.” *Syntax Literate; Jurnal Ilmiah Indonesia* 6, no. 7 (2021): 3521–41. <https://doi.org/https://doi.org/10.36418/syntax-literate.v6i7>.
- Mipon, Intan Permata, and Mohamad Fajri Mekka Putra. “Penyelenggaraan Pelindungan Data Pribadi Oleh Notaris Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi.” *Jurnal Hukum & Pembangunan* 53, no. 3 (2024): 6. <https://doi.org/10.21143/jhp.vol53.no3.1576>.
- Murizqy, Muhammad Alhadi, and Rianda Dirkareshza. “Peninjauan Aspek Keamanan Dan Perlindungan Hukum Terhadap Investor Cryptocurrency.” *Jurnal Ius Constituendum* 7, no. 2 (2022): 277–92. <https://doi.org/https://doi.org/10.26623/jic.v7i2.4067>.
- Pratama, Brilian, Happy Warsito, and Herman Adriansyah. “Prinsip Kehati-Hatian Dalam Membuat Akta Oleh Notaris.” *Repertorium: Jurnal Ilmiah Hukum Kenotariatan* 11, no. 1 (2022): 24–33. <https://doi.org/10.28946/rpt.v11i1.1640>.
- Pratiwi, Dinda, and Rianda Dirkareshza. “Pengelabuan Informasi Harga Di E-Commerce Terhadap Konsumen Melalui Flash Sale.” *Jurnal Ius Constituendum* 8, no. 3 (2023): 406–23. <https://doi.org/https://doi.org/10.26623/jic.v8i3.7344>.
- Putra, Gio Arjuna. “Reformulasi Ketentuan Pengelolaan Data Pribadi Sebagai Ius Constituendum Dalam Menjamin Perlindungan Data Pribadi Pengguna Layanan Media Sosial.” *Jurnal Hukum Lex Generalis* 2, no. 8 (2021): 684–700. <https://doi.org/https://doi.org/10.56370/jhlg.v2i8.105>.
- Rosadi, Aulia Gumilang. “Tanggung Jawab Notaris Dalam Sengketa Para Pihak Terkait Akta Perjanjian Pengikatan Jual Beli (PPJB) Yang Dibuatnya.” *JCH (Jurnal Cendekia Hukum)* 5, no. 2 (2020): 243–59. <https://doi.org/http://doi.org/10.33760/jch.v5i2.228>.
- Sahril, Iran, and Dhody A R Widjaja Atmadja. “Perlindungan Data Pribadi Konsumen, Dokumen Dan Tanda Tangan Elektronik Yang Dipergunakan Oleh Pihak Ketiga Dalam Transaksi E-Commerce.” *CENDEKIA: Jurnal Penelitian Dan Pengkajian Ilmiah* 2, no. 2 (2025): 173–89. <https://doi.org/https://doi.org/10.62335/cendekia.v2i2.897>.
- Simbolon, Elsa Daniella, Mahmul Siregar, and Joiverdia Arifiyanto. “Pelindungan Korban Pemalsuan Data Diri Dalam Transaksi Pinjaman Online Melalui Penegakan Hak Untuk Dilupakan.” *Neoclassical Legal Review: Journal of Law and Contemporary Issues* 3, no. 2 (2024): 77–88. <https://doi.org/https://doi.org/10.32734/nlrjolci.v3i2.18351>.
- Syarifudin, Nurul Inayah Muchlisa. “Bentuk Perlindungan Dan Pertanggung-Jawaban Notaris Terhadap Kerahasiaan Isi Akta.” *SINERGI: Jurnal Riset Ilmiah* 1, no. 11 (2024): 1095–1105. <https://doi.org/https://doi.org/10.62335/9t8h2565>.
- Vanensa, Triami Arie, Fitra Deni, and B F Sihombing. “Perlindungan Hukum Bagi Penghadap

Penyandang Disabilitas Dalam Pembuatan Akta Notaris.” *Jurnal Hukum Dan Bisnis (Selisik)* 10, no. 1 (2024): 44–62. <https://journal.univpancasila.ac.id/>.

Wulandari, Nindi. “Tanggung Jawab Hukum Notaris Dalam Pembuatan Akta.” *PUTAT: Jurnal Pelita Pendidikan, Hukum, Ekonomi Dan Teknologi* 1, no. 1 (2025): 20–26. <https://jurnalpelitanegribelantaraya.com/index.php/putat>.