Nusantara: Journal of Law and Islamic Law
Published by Yayasan Cerdas Pedia Indonesia
Volume 1 Issue 3, 2026 ISSN (Online) ***3110-8415***
Journal Homepage: **https://jurnal.smartpedia.co.id/index.php/nusantara**

Strengthening Data Security Systems in the Cyber Notary to Ensure Legal Certainty

Penguatan Sistem Keamanan Data dalam Cyber Notary untuk Menjamin Kepastian Hukum

Alisya Rahma Saebani
Faculty of Law, Doctoral Program in Law, Universitas Pembangunan Nasional 'Veteran' Jakarta, Indonesia

Article Info

Corresponding Author:
Alisya Rahma Saebani
✉alisyarahma51@gmail.com

History:
Submitted: 25-02-2026
Revised: 01-05-2026
Accepted: 17-05-2026

Keyword:
Cyber Notary; Personal Data Protection; Legal Certainty; Privacy by Design; Regulatory Harmonization.

Kata Kunci:
Cyber Notary; Perlindungan Data Pribadi; Kepastian Hukum; *Privacy by Design*; Harmonisasi Regulasi.

https://doi.org/10.65101/nusantara.v1i3.291

Abstract

The implementation of cyber notary practices in Indonesia currently encounters profound regulatory fragmentation among the Law on Notary Public Office, Electronic Information and Transactions Law, and Personal Data Protection Law. This fundamental normative vacuum triggers significant legal uncertainty in securing clients' electronic data. This normative legal research aims to comprehensively analyze the interconnection of positive legal instruments regarding privacy protection within the digital notarial ecosystem. Utilizing statutory, conceptual, and comparative approaches, this study critically evaluates the obligations of notaries who now transform into personal data controllers bearing absolute liability. The research findings demonstrate that the absence of uniform information security standards substantially elevates the risks of system hacking and digital identity breaches. Therefore, this research concludes the urgency for regulatory harmonization that strictly mandates the implementation of privacy by design principles alongside the standardization of encrypted information security systems. This legal measure constitutes an imperative directive to mitigate cybercrime threats.

Abstrak

Pelaksanaan *cyber notary* di Indonesia saat ini masih dihadapkan pada tantangan fragmentasi regulasi antara Undang-Undang Jabatan Notaris, Undang-Undang Informasi dan Transaksi Elektronik, serta Undang-Undang Perlindungan Data Pribadi. Kekosongan norma fundamental tersebut memicu ketidakpastian hukum yang signifikan dalam proses pengamanan data elektronik klien. Penelitian hukum normatif ini bertujuan untuk menganalisis interkoneksi instrumen hukum positif secara komprehensif terkait perlindungan privasi dalam ekosistem digital kenotariatan. Menggunakan pendekatan perundang-undangan, konseptual, dan perbandingan hukum, studi ini mengevaluasi secara kritis kewajiban notaris yang kini bertransformasi menjadi pengendali data pribadi dengan tanggung jawab mutlak. Hasil penelitian mendemonstrasikan bahwa ketiadaan standar keamanan informasi yang seragam sangat meningkatkan risiko peretasan sistem dan kebocoran identitas digital. Oleh karena itu, penelitian ini menyimpulkan urgensi harmonisasi peraturan yang secara tegas mewajibkan implementasi prinsip *privacy by design* serta standardisasi sistem keamanan informasi terenkripsi. Langkah hukum ini merupakan instruksi imperatif untuk memitigasi kejahatan siber, menjamin kepastian hukum, dan melindungi hak asasi privasi warga negara.

A. INTRODUCTION

1. Background

The rapid advancement of information technology has catalyzed profound transformations within the delivery of legal services, notably encompassing notarial practices. The conceptual framework of the *cyber notary* has emerged as a strategic adaptation by notaries public in response to the growing societal demand for expedited, digitally-driven legal services. Consequently, the procedural mechanisms for the execution, retention, and transmission of legal instruments are no longer tethered to physical embodiments, having comprehensively transitioned toward electronic systems.[1] Notwithstanding these developments, the regulatory framework governing *cyber notary* practices in Indonesia remains fragmented and lacks comprehensive codification. This regulatory vacuum engenders ambiguity in practical application and poses a substantial threat to the fundamental principle of legal certainty.[2] Consequently, legal protection for the parties involved in electronic transactions remains inadequately secured. This exigency underscores the imperative for formulating a more coherent and targeted regulatory framework to ensure that the legal validity of electronic documents is definitively recognized, thereby bolstering public trust and rendering the national legal system capable of seamlessly adapting to rapid digital advancements.[3]

Legal certainty plays a pivotal role in the execution of authentic deeds by notaries public. Absent such certainty, contracting parties are susceptible to potential liabilities due to the deficiency of adequate legal protection. Furthermore, this precarious condition exposes the notary to substantial legal risks, particularly when deeds are executed electronically in the absence of a well-defined statutory basis. In practice, notaries require definitive guidelines when executing electronic deeds; these guidelines serve as a normative benchmark to ensure that all operational actions remain strictly within legal parameters. Such benchmarks must emanate from regulations promulgated by competent authorities. Ultimately, the establishment of clear legal norms equips notaries

[1] Stefan Koos, "The Digitization of Notarial Tasks - A Comparative Overview and Outlook of 'Cyber Notary' In Indonesia and Germany," *The Indonesian Journal of Socio-Legal Studies* 2, no. 2 (March 25, 2023): 1–16, https://doi.org/10.54828/ijsls.2023v2n2.1.
[2] Ikhsan Lubis et al., "Cyber Notary as A Mean of Indonesian Economic Law Development," *Sriwijaya Law Review* 7, no. 1 (January 26, 2023): 62–72, https://doi.org/10.28946/slrev.Vol7.Iss1.1972.pp62-72.
[3] Henry Aspan et al., "Cyber Notary Issues Authority Certificate to Provide Legal Protection in Online Selling," *Journal of Law and Sustainable Development* 11, no. 10 (October 26, 2023): e1801, https://doi.org/10.55908/sdgs.v11i10.1801.

with a definitive mandate to exercise their authority while simultaneously guaranteeing legal certainty and robust protection for all stakeholders involved.[4]

In Indonesia, the statutory framework governing *cyber notary* practices is currently predicated on several distinct legislative acts, specifically the Law on Notary Public Office, the Electronic Information and Transactions Law, and the Personal Data Protection Law. Although these three statutes establish a foundational baseline, they remain inadequately harmonized. This fragmentation engenders a regulatory vacuum, particularly concerning the safeguarding of personal data entrusted to notarial stewardship. Operationally, notaries process a myriad of highly sensitive client information, rendering such data intrinsically susceptible to acute risks of data breaches and unauthorized exploitation. Notwithstanding the existence of data protection regulations, their enforcement within electronically mediated notarial services remains profoundly inconsistent. This inconsistency is further exacerbated by regional disparities in technological readiness. Consequently, information security systems, electronic authentication methodologies, and certification mechanisms conspicuously lack uniform standardization.[5]

Cross-jurisdictional comparative analyses confirm a fundamental disparity in both the codification and implementation of the *cyber notary* doctrine. Civil law jurisdictions, such as Germany, rigidly position the protection of the right to privacy and structured data security as the paramount constitutional priority within the digitization of the notarial profession. Conversely, common law jurisdictions, such as the United States, adopt a market-driven, pragmatic approach through the acceleration of remote online notarization (RON) to satisfy demands for institutional efficiency and accessible, inclusive legal services. This comparative exploration is widely utilized as a formal benchmark to map the projected trajectory of notarial digitization in Indonesia, as elaborated in prior scholarship focusing on the opportunities and generalized challenges of information

[4] Deny Fernaldi Chastra, "Kepastian Hukum Cyber Notary Dalam Kaidah Pembuatan Akta Autentik Oleh Notaris Berdasarkan Undang-Undang Jabatan Notaris," *Indonesian Notary* 3, no. 2 (2021): 248–67, https://scholarhub.ui.ac.id/notary/vol3/iss2/17/.
[5] Asriannor et al., "Tantangan Dan Peluang Profesi Notaris Diera Digital," *Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory* 3, no. 2 (June 24, 2025): 2040–46, https://doi.org/10.62976/ijijel.v3i2.1205.

technology adoption within the national notarial institution.[6,7,8,9]

On the domestic front, the enactment of Law No. 27 of 2022 on Personal Data Protection (the PDP Law) marks a paradigm shift in reinforcing the constitutional guarantees of the public's right to privacy. Nevertheless, the operationalization of the PDP Law within the digital notarial ecosystem precipitates a complex antinomy of norms when juxtaposed with the Law on Notary Public Office (the Notary Law) and the Electronic Information and Transactions Law (the EIT Law). This normative dissonance engenders a dogmatic ambiguity concerning the determination of a notary's legal status—specifically, whether a notary should be classified as a data controller bearing absolute liability or merely as a data processor. To resolve this doctrinal dilemma, prior scholarship has attempted to employ the analytical framework of responsive law to integrate privacy protections in the post-PDP Law era. Such studies underscore the imperative of internalizing the principles of *privacy by design* and *privacy by default*, ensuring that the mitigation of data breach risks is not reduced to a mere administrative formality but is instead inherently embedded within the architectural framework of the notarial information system.[10,11,12,13]

Although the discourse on regulatory harmonization and cyber data protection has been initiated by prior scholarship, a significant research gap persists concerning the resolution of concrete conflicts of norms between the obligation of notarial secrecy under

---

[6] Maria Debora Alamanda and Sri Laksmi Anindita, "Tantangan Dan Prospek Cyber Notary Di Indonesia," *Syntax Literate ; Jurnal Ilmiah Indonesia* 10, no. 5 (May 22, 2025): 4751–66, https://doi.org/10.36418/syntax-literate.v10i5.58183.

[7] Koos, "The Digitization of Notarial Tasks - A Comparative Overview and Outlook of 'Cyber Notary' In Indonesia and Germany."

[8] Satrio Abdillah, Norhasliza Ghapa, and Maheran Makhtar, "Regulatory Challenges and Social Dynamics of Online Notary Practices: A Comparative Legal Study of Indonesia and Malaysia," *Mawaddah: Jurnal Hukum Keluarga Islam* 4, no. 1 (2026): 376–409, https://doi.org/10.52496/mjhki.v4i1.46.

[9] Ikhsan Lubis et al., "Comparison of Civil Law Regarding The Implementation of Cyber Notary in Countries With Common Law and Civil Law Traditions," *Jurnal IUS Kajian Hukum Dan Keadilan* 10, no. 1 (April 23, 2022): 1–11, https://doi.org/10.29303/ius.v10i1.981.

[10] Emerentia Nathawira, M. Sudirman, and Benny Djaja, "Implementasi Cyber Notary Di Indonesia: Harmonisasi Regulasi Dan Perlindungan Data Pribadi Pasca Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi Dalam Kerangka Teori Hukum Responsif Dan Hak Privasi," *Jurnal Sosial Dan Sains* 5, no. 12 (December 8, 2025): 759–770, https://doi.org/10.59188/jurnalsosains.v5i12.32612.

[11] Naurah Humam Alkatiri, Mohamad Fajri Mekka Putra, and Kyle Ongko, "A Legal Perspective: Implementing an Electronic Notarization System in Indonesia in the Post-Pandemic Era," *Jambura Law Review* 5, no. 2 (June 30, 2023): 332–55, https://doi.org/10.33756/jlr.v5i2.19221.

[12] Satrio Abdillah, Norhasliza Ghapa, and Maheran Makhtar, "Cyber Notary: Adaptation to Changes in Notary Practices in Indonesia," *Jambura Law Review* 8, no. 1 (January 19, 2026): 76–96, https://doi.org/10.33756/jlr.v1i1.32490.

[13] Dwi Suryahartati and Jefri Mahardika, "Reforming the Legal Framework of Notary Supervision in Indonesia: Towards a Digital Governance Model," *Supremasi Hukum: Jurnal Kajian Ilmu Hukum* 14, no. 1 (June 30, 2025): 89–110, https://doi.org/10.14421/2xx8sn14.

the Notary Law and the principle of data processing accountability under the EIT and PDP Laws. The majority of previous studies remain confined to a macro-descriptive analysis of broad technological challenges and general privacy protections, failing to address the specific reconstruction of a notary's civil and administrative liability when electronic systems suffer from illegal interception (hacking). Consequently, the novelty of this research lies in the formulation of a doctrinal liability model that unequivocally designates the notary as a data controller subject to absolute liability, integrated within an internationally standardized, encrypted *privacy by design* operational framework. The primary problem identified—legal uncertainty stemming from this operational normative vacuum—demands urgent resolution, as it threatens to prejudice citizens' constitutional rights to privacy and erode the inherent legitimacy of authentic deeds. In light of these premises, this article aims to reconstruct the jurisdictional boundaries, rights, and legal obligations of notaries to establish a robust prescriptive foundation for the *cyber notary* ecosystem in Indonesia.

2. Research Questions

In light of the aforementioned background, the research questions of this study are formulated as follows:

a. How does the current statutory framework govern data protection and information security within the operationalization of *cyber notary* practices in Indonesia?
b. What is the doctrinal construction of notarial liability concerning potential data breaches and unauthorized data exploitation in *cyber notary* practices?

3. Research Methods

This study employs a normative (doctrinal) legal research methodology, centering on an analysis of the interconnectivity and coherence of positive legal instruments. The adoption of a doctrinal approach is predicated on the fundamental premise that the core exigency surrounding the operationalization of *cyber notary* practices in Indonesia does not stem from empirical or sociological phenomena. Rather, it is rooted in a normative vacuum and regulatory fragmentation among the Law on Notary Public Office, the Electronic Information and Transactions Law, and the Personal Data Protection Law. Through this methodological lens, the research is directed toward establishing a prescriptive foundation to guarantee legal certainty and formulating a robust doctrinal

model of notarial liability concerning the stewardship of electronic data.[14]

To achieve a comprehensive and profound analysis, this study employs three primary methodological approaches, justified as follows:

a. Statutory Approach: This approach serves as the primary analytical instrument selected to dissect the national legal architecture hierarchically and systematically. It is indispensable for examining the synchronization or conflict of norms between the obligation of notarial secrecy under the Law on Notary Public Office and the mandate for electronic system security under both the Electronic Information and Transactions (EIT) Law and the Personal Data Protection (PDP) Law.
b. Conceptual Approach: This approach is utilized to construct a theoretical framework by examining the paradigms of *privacy by design*, *privacy by default*, and the doctrine of data controller liability. The robust justification for this approach lies in the fact that data protection terminology within the *cyber notary* sphere is a contemporary issue necessitating a novel philosophical interpretation of the notary's legal standing—no longer merely as a public official, but concurrently as an entity processing highly sensitive data.
c. Comparative Approach: To introduce a globally standardized element of novelty, this study conducts a macro-level comparison between civil law jurisdictions (such as Germany, which prioritizes structured privacy protections) and common law jurisdictions (such as the United States, characterized by its pragmatic *remote online notarization*). This cross-jurisdictional comparison is strongly justified by the imperative to identify best practices that serve as an optimal middle ground, ensuring seamless compatibility and adaptation within the Indonesian legal system without compromising data security.

The data utilized in this study is predicated upon secondary data, comprising primary, secondary, and tertiary legal materials. Primary legal materials encompass relevant statutory regulations. Secondary legal materials are acquired through a rigorous systematic literature review of reputable international journal articles (Scopus-indexed) and accredited national

[14] Tunggul Ansari Setia Negara, "Normative Legal Research in Indonesia: Its Originis and Approaches," *Audito Comparative Law Journal (ACLJ)* 4, no. 1 (February 2, 2023): 1–9, https://doi.org/10.22219/aclj.v4i1.24855.

journals, thereby ensuring the currency and validity of the academic discourse surrounding cybercrime and *cyber notary* practices.

The collection of legal materials is executed through comprehensive documentary research. All amassed legal materials are subsequently analyzed using a qualitative methodology, specifically employing systematic and teleological interpretation techniques. The rationale for selecting these analytical techniques is to preclude a rigid, textualist reading of statutory provisions. Through systematic interpretation, the researcher aims to reconstruct the interpretive nexus among various statutory regulations to yield a prescriptive and measurable conclusion—one that furnishes viable solutions to the vulnerabilities of personal data security within the digital notarial ecosystem in Indonesia.

B. DISCUSSION

1. Data Protection and Information Security within the Operationalization of Cyber Notary Practices in Indonesia

The rapid proliferation of technological advancements presents a myriad of novel challenges, most notably the emergence of cybercrime, which poses a significant threat to security at both national and global levels. Within this landscape, the notary occupies a pivotal role in upholding legal certainty while fostering societal security. Cybercrime is defined as an unlawful act perpetrated through electronic systems, fundamentally characterized by the absence of direct physical interaction with the victim. Perpetrators are capable of executing their actions from virtually any location by exploiting vulnerabilities inherent in digital systems, typically driven by motives of economic gain. A prominent manifestation of such criminal activity is the targeted assault on personal data; acts of system hacking or unauthorized access represent quintessential examples that inflict substantial injury upon data subjects.[15]

Cybercrime encompasses unlawful acts perpetrated through the utilization of computers and internet networks, including, but not limited to, hacking, malware dissemination, identity theft, online harassment, and skimming practices.[16] Currently, a vast majority of personal activities and information are stored within digital systems, thereby creating significant opportunities for malicious actors to illicitly access and exploit such data. The

[15] Russel Butarbutar, "Kejahatan Siber Terhadap Individu: Jenis, Analisis, Dan Perkembangannya," *Technology and Economics Law Journal* 2, no. 2 (August 24, 2023): 299–317, https://doi.org/10.21143/TELJ.vol2.no2.1043.
[16] Venny Febriyanti Puspita, Ningrum, and Ufran, "Perlindungan Hukum Terhadap Korban Cyber Sexual Harassment Dalam Media Sosial," *Iuris Notitia: Jurnal Ilmu Hukum* 1, no. 2 (October 25, 2023): 51–55, https://doi.org/10.69916/iuris.v1i2.65.

unauthorized acquisition of personal data constitutes an unlawful act. Although a comprehensive regulatory framework specifically governing *cyber law* remains absent, data protection provisions have been accommodated within several regulations, most notably the Electronic Information and Transactions (EIT) Law. This statute explicitly affirms that any violation of Article 26 may give rise to legal liability, including claims for damages sustained by the aggrieved party.

Technological and information advancements offer not only convenience but also facilitate the commission of crimes in a more accelerated and organized manner. This paradigm impacts data and information management, particularly regarding personal data that necessitates specialized protection. The progress in communication technology has rendered the boundaries of privacy increasingly nebulous, thereby increasing the vulnerability of personal data to unauthorized access and dissemination. The escalation of data protection cases underscores the critical nature of this issue. The misuse of personal data poses diverse risks, including information breaches that inflict harm upon individuals. Sensitive data, such as National Identification Numbers (NIK), names, email addresses, and telephone numbers, possess significant economic value and frequently serve as targets for various illicit activities.

The principle of utility (*asas kemanfaatan*) is evident in the implementation of the *cyber notary* concept within the certification process, which assists notaries in executing their functions with greater practicality. This system enhances efficiency, as various processes can be executed digitally. In practice, electronically mediated services require public documents in digital formats, including the utilization of electronic signatures by notaries. For the verification of parties, notaries typically rely on identities such as National ID cards (KTP), driver's licenses (SIM), or passports. With the emergence of *cyber notary* practices, these methodologies have evolved to leverage Electronic Identity (e-ID) as a primary means of verification. e-ID constitutes a component of *e-government* implementation—the utilization of information technology by the government to enhance the quality of public services and information dissemination. Given that these identities contain highly sensitive personal data, their management must be conducted with rigorous scrutiny. Unrestricted access potentially facilitates misuse, particularly by perpetrators of cybercrime. Consequently, every data subject must be afforded legal protection, including for biometric data stored within digital systems.[17]

[17] Litha Nabilla Mallolongan and Hendry Julian Noor, "Peluang Penerapan Penyimpanan Minuta Akta Secara Elektronik Menuju Era E-Notary Berdasarkan Undang- Undang No. 2 Tahun 2014 Tentang Jabatan Notaris," *Notary Law Journal* 2, no. 1 (January 23, 2023): 54–81, https://doi.org/10.32801/nolaj.v2i1.39.

In the discourse surrounding the *cyber notary* concept, a critical aspect requiring substantive attention is the legal protection of the identities of the parties involved. Such identity serves as an elemental feature, functioning as a unique identifier for individuals. Prior to addressing electronic identity (e-ID), it is essential to establish that identity is fundamentally a marker intrinsically linked to an individual. Conversely, e-ID denotes an identity presented through electronic media, encompassing an individual's personal data. The exigency for personal data in the digital era is increasingly pronounced, as such data is utilized to facilitate diverse activities, including the mitigation of technology-based criminal activities.

Threats within the digital domain are in a state of constant evolution, with computer system hacking representing a significant concern. Hacking is defined as an unauthorized access to devices or networks for specific objectives, typically aimed at illicit gain. Within the context of *cyber notary* practices, this risk becomes acute when the systems or devices utilized by the notary are compromised. Documents such as draft deeds stored digitally are susceptible to exposure. Such a breach potentially engenders severe repercussions, including the unauthorized utilization of parties' personal data, the disclosure of confidential information, and the unauthorized alteration of data, all of which pose substantial harm to both the parties and the notary.[18]

The regulation of hacking activities is encapsulated within the Electronic Information and Transactions (EIT) Law, which characterizes hacking as a form of cybercrime involving the unlawful infringement upon electronic systems. Specifically, Article 30 of the EIT Law stipulates the following:

(1) "Any Person who intentionally and without authorization or unlawfully accesses any Computer and/or Electronic System belonging to another in any manner whatsoever;

(2) Any Person who intentionally and without authorization or unlawfully accesses any Computer and/or Electronic System in any manner whatsoever with the intent to obtain Electronic Information and/or Electronic Documents;

(3) Any Person who intentionally and without authorization or unlawfully accesses any Computer and/or Electronic System in any manner whatsoever by

[18] Jenny Divia Fitcanisa and Busyra Azheri, "Keabsahan Tanda Tangan Elektronik Pada Akta Notaris," *SIBATIK JOURNAL: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, Dan Pendidikan* 2, no. 5 (April 30, 2023): 1449–58, https://doi.org/10.54443/sibatik.v2i5.809.

breaching, bypassing, exceeding, or penetrating security systems."

The penal provisions for such violations are prescribed in Article 46 of the EIT Law. An individual found guilty of illegal access, as stipulated in Article 30, paragraph (1), is subject to imprisonment of up to six years and/or a maximum fine of IDR 600,000,000. If the unauthorized access is executed with the intent to obtain electronic information or documents, as outlined in paragraph (2), the penalty is enhanced to a maximum imprisonment of seven years and/or a maximum fine of IDR 700,000,000. Furthermore, where the act is committed by breaching or damaging security systems, as described in paragraph (3), the perpetrator may be sentenced to imprisonment of up to eight years and/or a maximum fine of IDR 800,000,000.

The threat to personal data within *cyber notary* practices constitutes a matter of grave concern. The evolution of digitally-mediated notarial services has engendered an increasingly diverse array of threats to information security. Notaries occupy a vulnerable position, given their role in managing highly sensitive client data. Absent robust protective systems, the risk of data exploitation or unauthorized disclosure is substantial. A frequent threat is unauthorized access via cyberattacks. Hacking of systems or storage media enables third parties to illicitly obtain critical information, such as identity data, legal instruments, and financial information. Such breaches not only inflict harm upon aggrieved clients but also diminish public trust in the notarial profession.

Although the Personal Data Protection Law, the Notary Law, and the EIT Law provide a foundational regulatory basis, comprehensive harmonization among these statutes remains unachieved. This regulatory discordance precipitates practical uncertainty, particularly as notaries adapt to the digitalization of services through the *cyber notary* paradigm. While the Notary Law mandates that notaries uphold the confidentiality of deeds as a professional obligation, this provision lacks granular detail regarding the protection of data in electronic form. Conversely, the transition to digital systems necessitates clear standards governing data storage, security, and access control to ensure the preservation of confidentiality.[19]

[19] Nathawira, Sudirman, and Djaja, "Implementasi Cyber Notary Di Indonesia: Harmonisasi Regulasi Dan Perlindungan Data Pribadi Pasca Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi Dalam Kerangka Teori Hukum Responsif Dan Hak Privasi."

2. Notarial Liability for Potential Data Breaches and Unauthorized Data Exploitation within *Cyber Notary* Practices

With the enactment of Law No. 27 of 2022 on Personal Data Protection (the PDP Law), the professional liability of notaries in safeguarding client data confidentiality has become increasingly rigorous, particularly concerning the utilization of electronic systems. Pursuant to Article 1, point 1 of the PDP Law, personal data is defined as any information that identifies an individual, either directly or in combination with other data, processed through electronic or non-electronic systems. In notarial practice, the contents of a deed almost invariably incorporate the personal information of the parties involved. Such data encompasses identities, financial statuses, and legal documents pertaining to business entities. Furthermore, a portion of this data falls within the category of 'specific personal data,' as stipulated in Article 4, paragraph (2), letter b, which includes private financial information. This paradigm positions the notary in a capacity that transcends the traditional role of a deed-drafting official; rather, the notary is concurrently tasked with the stewardship and processing of personal data. This functional evolution aligns with the regulatory concepts of 'data controller' and 'data processor' established within the prevailing personal data protection regime.[20]

This provision is congruent with Article 16, paragraph (1), letter f of the Law on Notary Public Office, which mandates that notaries preserve the confidentiality of the entire content of deeds and any information obtained during the drafting process, in accordance with their official oath of office. This obligation has transitioned from being merely within the sphere of professional ethics and conduct to being reinforced by the personal data protection regime, which imposes legal consequences in the form of administrative and penal sanctions. Within the framework of the Personal Data Protection Law, parties involved in data processing are bifurcated into two categories: the *personal data controller* and the *personal data processor*. Pursuant to Article 1, points 4 and 5, a personal data controller is defined as the party that determines the objectives of and exercises control over the processing of personal data. Conversely, a personal data processor is the party that performs data processing on the basis of instructions from, or

[20] Intan Permata Mipon and Mohamad Fajri Putra, "Penyelenggaraan Pelindungan Data Pribadi Oleh Notaris Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi," *Jurnal Hukum & Pembangunan* 53, no. 3 (September 30, 2023): 479–92, https://doi.org/10.21143/jhp.vol53.no3.1576.

for the benefit of, the personal data controller.[21]

The role of a notary can be classified as a *personal data controller*, as notaries determine the objectives and modalities of data utilization in the process of drafting authentic deeds. Consequently, notaries bear direct responsibility for the security, confidentiality, and accountability of every stage of client data processing. This obligation is affirmed by Article 20, paragraph (1) of the Personal Data Protection (PDP) Law, which mandates that personal data controllers must process data in accordance with the principles of lawful basis, purpose limitation, transparency, accuracy, storage limitation, integrity and confidentiality, and accountability. In the practice of *cyber notary*, these provisions necessitate that notaries ensure every electronic deed executed, stored, and transmitted is protected through adequate information security systems, such as encryption, authentication, and audit mechanisms.

Conversely, the Electronic Information and Transactions (EIT) Law provides legitimacy for the utilization of electronic signatures within digital documents. Article 11, paragraph (1) affirms that electronic signatures possess valid legal force. Furthermore, Article 12, paragraph (1) stipulates that electronic signatures have evidentiary weight equivalent to conventional signatures, provided they meet specific requirements: they must be exclusively linked to the signatory, the creation data must be under the signatory's control, any alterations to the signature must be detectable, and any alterations to the associated electronic information must be discernible.

Such responsibility requires notaries to ensure that every electronic deed executed, stored, and transmitted has undergone an adequate security system. This system must encompass standard encryption, clear authentication processes, and audit mechanisms capable of tracking all data-related activities. Within the legal framework, the EIT Law provides the foundation for the use of electronic signatures in digital documents. Article 11, paragraph (1) reaffirms that electronic signatures carry legal force and generate valid legal consequences. Subsequently, Article 12, paragraph (1) states that electronic signatures possess evidentiary power equivalent to conventional ones, contingent upon meeting specified requirements. These requirements include direct linkage to the signatory, the signatory's control over the signature creation data, the capability to detect

[21] Pingkan Chandra Dewi Tamaka, "Prinsip Kepastian Hukum Profesi Notaris Terhadap Amanah Dalam Sumpah Atau Janji Jabatan Notaris," *Al Qodiri : Jurnal Pendidikan, Sosial Dan Keagamaan* 22, no. 1 (September 2024): 71–92, https://doi.org/10.53515/qodiri.2024.22.1.71-92.

modifications to the electronic signature, and the capability to detect modifications to the related electronic information.

In *cyber notary* practice, the utilization of certified electronic signatures is mandatory for the legal recognition of electronic deeds. These signatures provide a guarantee of identity authenticity and document integrity in transactions. Moreover, Article 15, paragraph (1) of the EIT Law mandates that every electronic system provider must operate a reliable, secure, and responsible system. Such systems must be capable of ensuring the availability, integrity, confidentiality, and accessibility of personal data. In this context, systems employed in *cyber notary* practices must adhere to these standards. Consequently, notaries, as system users, are obligated to ensure that their information security management systems meet recognized national or international standards, such as ISO or other established information security frameworks. This is imperative to maintain stakeholder trust and ensure legal protection for the data managed.[22]

Ethically, the status of a notary as a public official entrusted by the public demands a standard of integrity that exceeds that of other legal professions. The notary's role transcends mere document attestation, as it simultaneously represents the public trust vested in the state. Should a notary fail to maintain the confidentiality of personal data, the repercussions extend beyond the immediate prejudice to the client; such failure undermines the state's legitimacy in guaranteeing legal certainty. From a legal philosophical perspective, this matter is inextricably linked to the protection of privacy as an inherent human right. Article 28G(1) of the 1945 Constitution of the Republic of Indonesia affirms that every individual has the right to protection of their personal self, family, honor, dignity, and the property under their control. Furthermore, every individual is entitled to a sense of security and protection against threats that restrict their freedom of action. Consequently, *cyber notary* cannot be reduced to a mere administrative or technical concern. Rather, it concerns the constitutional obligation of the state to guarantee and safeguard the privacy rights of its citizens.

[22] Dinda Cantik Senantya, Fany Rahmasari, and Intan Glarita Zodies Liusyadi, "Analisis Transformasi Pelayanan Notaris Di Era Digital : Studi Tentang Tanda Tangan Elektronik Dalam Akta Otentik," *Jurnal Ilmu Multidisiplin* 4, no. 2 (June 19, 2025): 823–31, https://doi.org/10.38035/jim.v4i2.959.

C. CONCLUSION

The implementation of *cyber notary* practices in Indonesia currently confronts regulatory fragmentation among the Law on Notary Public Office, the Electronic Information and Transactions Law, and the Personal Data Protection Law, which precipitates legal uncertainty in securing clients' electronic data. Within the legal construction of data protection, the notary has transitioned into the role of a personal data controller, bearing absolute liability for any breach or exploitation of digital identities throughout the execution of authentic deeds. Consequently, there is an urgent necessity for regulatory harmonization that strictly mandates the adoption of *privacy by design* principles and the standardization of encrypted information security systems across all phases of digital notarial services. This comprehensive measure serves as an imperative directive, not only to mitigate cybercrime threats but also to ensure legal certainty and the constitutional protection of the public's right to privacy.

REFERENCES

Abdillah, Satrio, Norhasliza Ghapa, and Maheran Makhtar. "Cyber Notary: Adaptation to Changes in Notary Practices in Indonesia." *Jambura Law Review* 8, no. 1 (January 19, 2026): 76–96. https://doi.org/10.33756/jlr.v1i1.32490.

———. "Regulatory Challenges and Social Dynamics of Online Notary Practices: A Comparative Legal Study of Indonesia and Malaysia." *Mawaddah: Jurnal Hukum Keluarga Islam* 4, no. 1 (2026): 376–409. https://doi.org/10.52496/mjhki.v4i1.46.

Alamanda, Maria Debora, and Sri Laksmi Anindita. "Tantangan Dan Prospek Cyber Notary Di Indonesia." *Syntax Literate ; Jurnal Ilmiah Indonesia* 10, no. 5 (May 22, 2025): 4751–66. https://doi.org/10.36418/syntax-literate.v10i5.58183.

Alkatiri, Naurah Humam, Mohamad Fajri Mekka Putra, and Kyle Ongko. "A Legal Perspective: Implementing an Electronic Notarization System in Indonesia in the Post-Pandemic Era." *Jambura Law Review* 5, no. 2 (June 30, 2023): 332–55. https://doi.org/10.33756/jlr.v5i2.19221.

Aspan, Henry, Abdi Setiawan, Irawan, Etty Sri Wahyuni, Ari Prabowo, and Ami Natuz Zahara. "Cyber Notary Issues Authority Certificate to Provide Legal Protection in Online Selling." *Journal of Law and Sustainable Development* 11, no. 10 (October 26, 2023): e1801. https://doi.org/10.55908/sdgs.v11i10.1801.

Asriannor, Muhammad Afdal Zikri, Muhammad Indra Gazali, and Riski Dwi Nugraha. "Tantangan Dan Peluang Profesi Notaris Diera Digital." *Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory* 3, no. 2 (June 24, 2025): 2040–46. https://doi.org/10.62976/ijijel.v3i2.1205.

Butarbutar, Russel. "Kejahatan Siber Terhadap Individu: Jenis, Analisis, Dan Perkembangannya." *Technology and Economics Law Journal* 2, no. 2 (August 24, 2023): 299–317. https://doi.org/10.21143/TELJ.vol2.no2.1043.

Chastra, Deny Fernaldi. "Kepastian Hukum Cyber Notary Dalam Kaidah Pembuatan Akta Autentik Oleh Notaris Berdasarkan Undang-Undang Jabatan Notaris." *Indonesian Notary* 3, no. 2 (2021): 248–67. https://scholarhub.ui.ac.id/notary/vol3/iss2/17/.

Divia Fitcanisa, Jenny, and Busyra Azheri. "Keabsahan Tanda Tangan Elektronik Pada Akta Notaris." *SIBATIK JOURNAL: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, Dan Pendidikan* 2, no. 5 (April 30, 2023): 1449–58. https://doi.org/10.54443/sibatik.v2i5.809.

Koos, Stefan. "The Digitization of Notarial Tasks - A Comparative Overview and Outlook of 'Cyber Notary' In Indonesia and Germany." *The Indonesian Journal of Socio-Legal Studies* 2, no. 2 (March 25, 2023): 1–16. https://doi.org/10.54828/ijsls.2023v2n2.1.

Lubis, Ikhsan, Tarsisius Murwadji, Mahmul Siregar, Detania Sukarja, Robert Robert, Dedi Harianto, and Mariane Magda Ketaren. "Comparison of Civil Law Regarding The Implementation of Cyber Notary in Countries With Common Law and Civil Law Traditions." *Jurnal IUS Kajian Hukum Dan Keadilan* 10, no. 1 (April 23, 2022): 1–11. https://doi.org/10.29303/ius.v10i1.981.

Lubis, Ikhsan, Tarsisius Murwadji, Sunarmi Sunarmi, and Detania Sukarja. "Cyber Notary as A Mean of Indonesian Economic Law Development." *Sriwijaya Law Review* 7, no. 1 (January 26, 2023): 62–72. https://doi.org/10.28946/slrev.Vol7.Iss1.1972.pp62-72.

Mallolongan, Litha Nabilla, and Hendry Julian Noor. "Peluang Penerapan Penyimpanan Minuta Akta Secara Elektronik Menuju Era E-Notary Berdasarkan Undang- Undang No. 2 Tahun 2014 Tentang Jabatan Notaris." *Notary Law Journal* 2, no. 1 (January 23, 2023): 54–81. https://doi.org/10.32801/nolaj.v2i1.39.

Mipon, Intan Permata, and Mohamad Fajri Putra. "Penyelenggaraan Pelindungan Data Pribadi Oleh Notaris Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi." *Jurnal Hukum & Pembangunan* 53, no. 3 (September 30, 2023): 479–92. https://doi.org/10.21143/jhp.vol53.no3.1576.

Nathawira, Emerentia, M. Sudirman, and Benny Djaja. "Implementasi Cyber Notary Di Indonesia: Harmonisasi Regulasi Dan Perlindungan Data Pribadi Pasca Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi Dalam Kerangka Teori Hukum Responsif Dan Hak Privasi." *Jurnal Sosial Dan Sains* 5, no. 12 (December 8, 2025): 759–770. https://doi.org/10.59188/jurnalsosains.v5i12.32612.

Negara, Tunggul Ansari Setia. "Normative Legal Research in Indonesia: Its Originis and Approaches." *Audito Comparative Law Journal (ACLJ)* 4, no. 1 (February 2, 2023): 1–9. https://doi.org/10.22219/aclj.v4i1.24855.

Pingkan Chandra Dewi Tamaka. "Prinsip Kepastian Hukum Profesi Notaris Terhadap Amanah Dalam Sumpah Atau Janji Jabatan Notaris." *Al Qodiri : Jurnal Pendidikan, Sosial Dan Keagamaan* 22, no. 1 (September 2024): 71–92. https://doi.org/10.53515/qodiri.2024.22.1.71-92.

Puspita, Venny Febriyanti, Ningrum, and Ufran. "Perlindungan Hukum Terhadap Korban Cyber Sexual Harassment Dalam Media Sosial." *Iuris Notitia: Jurnal Ilmu Hukum* 1, no. 2 (October 25, 2023): 51–55. https://doi.org/10.69916/iuris.v1i2.65.

Senantya, Dinda Cantik, Fany Rahmasari, and Intan Glarita Zodies Liusyadi. "Analisis Transformasi Pelayanan Notaris Di Era Digital : Studi Tentang Tanda Tangan Elektronik Dalam Akta Otentik." *Jurnal Ilmu Multidisiplin* 4, no. 2 (June 19, 2025): 823–31.

https://doi.org/10.38035/jim.v4i2.959.

Suryahartati, Dwi, and Jefri Mahardika. "Reforming the Legal Framework of Notary Supervision in Indonesia: Towards a Digital Governance Model." *Supremasi Hukum: Jurnal Kajian Ilmu Hukum* 14, no. 1 (June 30, 2025): 89–110. https://doi.org/10.14421/2xx8sn14.