KRTHA BHAYANGKARA, Vol. 19, No. 3 (2025), pp. 935-947
ISSN 1978-8991 (print) | ISSN 2721-5784 (online)
Available online at: http://ejurnal.ubharajaya.ac.id/index.php/KRTHA

Cross-Border Data Transfer: Notary Compliance for Foreign Deeds under PDP Law

Hilman Mufidi[1] Hera Marlaena Handaruwati[2] Iis Kurniawati[3] Tetti Samosir[4] Agus Surono[5]
Universitas Pancasila
Email: hilmanmufidii@gmail.com, Heramarlaena@gmail.com, iiskurniawati13.ik@gmail.com, tettisamosir@univpancasila.ac.id, surono.agus7030@gmail.com

Article info

Received: Sep 16, 2025	Revised: Nov 23, 2025	Accepted: Dec 29, 2025

DOI: https://doi.org/10.31599/krtha.v19i3.4742

Abstract : The globalization of economic activity has significantly increased the interaction of Indonesian Notaries with foreign clients, both individuals (Foreign Citizens) and corporations (Foreign Companies), especially in facilitating Foreign Investment (PMA). This practice inherently involves the cross-border processing and transfer of personal data. The enactment of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) transforms the legal status of Notaries, from being merely Public Officials regulated by the Notary Office Law (UUJN), to becoming Personal Data Controllers. This research uses a juridical-normative method to analyze the implications of this new status, focusing on compliance with the cross-border data transfer mechanisms regulated in Article 56 of the PDP Law. The main findings indicate a critical legal vacuum. The PDP Law mandates a hierarchical data transfer mechanism (Equivalence Decision, Adequate Protection such as Standard Contractual Clauses/SCCs, and Explicit Consent). However, as of 2025, the implementing regulations (RPP) that authorize SCCs and establish the list of equivalent countries have not been issued. This creates a paradox of normative compliance: Notaries who attempt to comply with the due diligence principle of the UUJN by verifying client data with the country of origin are technically unable to comply with the data transfer standards of the UU PDP. Notaries are forced to rely on the mechanism of explicit consent as the sole legal basis, which in practice is weak and inadequate to protect Notaries from the risk of administrative and criminal sanctions under the PDP Law in the event of data protection failure in the destination country. This article recommends the urgency of the government's approval of the RPP, the interim adoption of international SCCs, and the issuance of proactive compliance guidelines by the Indonesian Notary Association (INI).

Keywords : Cross-Border Data Transfer, Personal Data Protection, Notary, Standard Contractual Clauses (SCCs), Legal Vacuum

I. INTRODUCTION

The development of global law and economics in the 21st century is characterized by the accelerated flow of capital, investment, and human mobility across national jurisdictional boundaries. Indonesia, as one of the economic powerhouses in Southeast Asia, continues to strive to attract foreign investment, one of which is thru the Foreign Direct Investment

(FDI) scheme. In this context, the profession of Notary holds a central role as a public official granted authority by the state to create authentic deeds.
The increase in transactions involving foreign legal entities—both foreign nationals (WNA) performing legal acts in Indonesia and foreign corporations establishing business entities in the form of Foreign Investment Limited Liability Companies (PT PMA)—has become a daily reality in notary offices. The creation of a deed of establishment for a foreign-owned limited liability company (PT PMA), a syndicated loan agreement with cross-border collateral, or even a will for a foreign national, requires a Notary to receive, verify, and process personal data originating from foreign jurisdictions.

Along with this globalization, there is also a digital revolution in notarial practice. Although the concept of a cyber notary in Indonesia is still under discussion and has not been fully implemented regulatively, the use of information technology is not new. Notaries now commonly use cloud-based storage, encrypted email, and digital document management systems to store protocols and client data. This digitalization, while increasing efficiency, also exponentially increases the volume, processing speed, and risks to the security of personal data managed by Notaries.

Paradigm Shift: The PDP Law and Its Impact on the Legal Profession

Responding to the challenges of the digital era and as a means of meeting international standards such as the General Data Protection Regulation (GDPR) in the European Union, Indonesia has enacted a major legislative milestone thru Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). The PDP Law marks a new era in data governance in Indonesia, providing a guaranty of protection for citizens' fundamental constitutional rights, as mandated in Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia.[1]

The implementation of the PDP Law will not only impact the technology and e-commerce sectors. This law applies horizontally to every person, public body, and international organization that processes Personal Data within the legal jurisdiction of Indonesia, whether electronically or non-electronically.[2] The implication is that legal professions, including notaries, who in their daily practice collect, process, and store clients' personal data, are now automatically subject to the PDP Law regime.

This triggered a fundamental paradigm shift. Previously, Notaries were "only" specifically regulated by Law Number 2 of 2014 concerning Amendments to Law Number 30 of 2004 concerning the Position of Notary (UUJN). Now, Notaries bear a dual status and responsibility. Based on the Notary Law, a Notary is a Public Official with an absolute obligation of professional secrecy. However, based on the PDP Law, a Notary is a "Personal Data Controller," a status that imposes a new set of obligations related to

[1]Fanisa Mayda Ayiliani and Elfia Farida, "Urgensi Pembentukan Lembaga Pengawas Data Pribadi sebagai Upaya Pelindungan Hukum terhadap Transfer Data Pribadi Lintas Negara", Semarang: Universitas Diponegoro, Vol. 6, No. 3, 2024. 437 – 440.
[2] Sophia Afifa Nasution and Siti Hajati Husein, "Pengaruh Teknologi Informasi Terhadap Kewajiban Kerahasiaan dan Perlindungan Data Pribadi Klien dalam Praktik Notaris", Depok: Universitas Indonesia, 2025.

transparency, accountability, data security, and fulfilling the rights of Personal Data Subjects.

II. RESEARCH METHODS

This research is a normative-juridical (normative-legal) study, also known as doctrinal research. The research focus is on analyzing positive legal norms, vertical and horizontal synchronization between regulations, and legal discovery (rechtsvinding) to fill identified legal gaps.

The research approach used includes:

1. **Statute Approach**: This approach is carried out by systematically examining and analyzing the hierarchy and relationships between relevant legal products, especially:
    - The 1945 Constitution of the Republic of Indonesia (specifically Article 28G regarding the right to personal protection).
    - Law Number 2 of 2014 concerning Amendments to Law Number 30 of 2004 concerning the Position of Notary (UUJN).
    - Law Number 27 of 2022 concerning Personal Data Protection (PDP Law).
2. **Conceptual Approach**: This approach is used to understand and elaborate on the legal concepts that are central to the research, such as the concepts of "Personal Data Controller," "Personal Data Processor," "Personal Data Processing," "Cross-Border Data Transfer," "Duty of Professional Secrecy," and "Legal Vacuum."
3. **Case Approach**: This approach is used by analyzing relevant legal jurisprudence and case studies to map the baseline risks faced by Notaries regarding breaches of professional confidentiality, even before the PDP Law came into effect. This analysis includes a review of court decisions, such as Palangkaraya High Court Decision Number 1/PDT/2018/PT PLK, and other decisions from the Supreme Court Directory related to violations of the oath of office or forgery of deeds involving Notaries.

Analysis of pre-PDP Law jurisprudence is essential. If a notary has been proven vulnerable to civil lawsuits (Unlawful Acts ex Article 1365 of the Civil Code) or criminal sanctions (ex Article 322 of the Criminal Code regarding disclosure of secrets) for failure to maintain the confidentiality of deeds, then the implementation of the PDP Law now adds a new layer of risk. The PDP Law introduces specific administrative sanctions (Article 57) and criminal sanctions (Articles 65-68) related to the failure to protect personal data. Thus, pre-PDP Law jurisprudence analysis is used to predict the occurrence of risk multiplication (doubled risks) faced by Notaries in the era of the PDP Law.

The legal materials used in this study consist of:

- **Primary Legal Materials**: The 1945 Constitution of the Republic of Indonesia, the Civil Code (KUHPerdata), the Notary Law (UUJN), and the Personal Data Protection Law (UU PDP).

- **Secondary Legal Materials**: Draft Government Regulation (RPP) Implementing the PDP Law, legal scientific journals, theses, legal articles, and textbooks related to notarial law and data protection.
- **Tertiary Legal Materials**: Legal dictionaries and encyclopedias to provide explanations of technical terminology.

All legal materials were analyzed qualitatively. The analytical technique used is a systematic and grammatical interpretation of legal norms, as well as legal synchronization to identify antinomies and harmonies between regulations. To address the issue of legal vacuum, this research employs the method of legal discovery (rechtsvinding) to formulate prescriptive recommendations.

III. DISCUSSION

Qualifications of a Notary as a Personal Data Controller

The legal status of notaries after the Personal Data Protection Law has undergone a fundamental transformation. To understand the implications, it is first necessary to affirm the Notary's qualification as a Personal Data Controller. Article 1, paragraph 4 of the PDP Law defines a Personal Data Controller as "any person, public body, and international organization that, acting alone or jointly, determines the purpose and controls the processing of Personal Data." If this definition is projected onto the activities of a Notary, these qualifications are clearly evident.[3] The process of creating an authentic deed, such as the Deed of Establishment of a Foreign Investment Company (PT PMA), involves a series of personal data processing activities that are entirely under the control of the Notary:

1. **Acquisition and Collection**: The notary collects personal data of foreign founders or directors (passport copies, KITAS, NPWP) and foreign corporate data (Certificate of Incorporation, Articles of Association of the parent company).
2. **Processing and Analysis**: The notary determines the purpose of the data, which is "for the preparation of a comparison of the Articles of Association of PT X" and "for verifying the validity of legal subjects". The notary exercises control by analyzing this data to ensure the legal capacity and authority of the parties present.
3. **Storage**: The personal data is then attached to the deed minutes and becomes part of the Notary Protocol, which the Notary is required to keep for the period specified by law. This storage can be physical or digital (electronic).
4. **Appearance, Announcement, Transfer, or Disclosure**: Notaries transfer data when registering deeds with the Legal Entity Administration System (SABH), or when providing copies of deeds to interested parties.

It is important to distinguish between a Notary (as Data Controller) and the staff or employes in the Notary's office. Internship staff or notaries acting on the notary's instructions to input data or archive documents are more accurately classified as "Personal Data Processors." The Data Processor only processes data on behalf of the Data

[3] Undang-Undang Republik Indonesia RI, Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi (UU No. 27 Tahun 2022).

Controller, while the ultimate legal responsibility for PDP Law compliance remains with the Notary as the Data Controller.[4]

The notary's status as a Personal Data Controller is ex officio—inherent automatically due to the performance of their duties—and is not a matter of choice. The notary cannot refuse this status. The implication is that notaries are no longer subject only to the UUJN. It is now mandatory to comply with all the rules and principles of Personal Data processing in the PDP Law, including the principles of legality, transparency, accountability, data security, as well as the obligation to report data protection failures (data breaches) to supervisory bodies and Personal Data Subjects.[5]

Antinomies and Harmonization: The Duty of Confidentiality in the UUJN vs. Compliance with the PDP Law

The implementation of the PDP Law on the established foundation of the JSN Law raises questions about potential antinomies or conflicts of norms, particularly between the obligation of confidentiality and the right to transparency.

Dogmatic Study of the Notary Law (Absolute Confidentiality): The foundation of the notary profession is trust, which is maintained thru confidentiality. Article 16 paragraph (1) letter f of the Notary Law explicitly requires Notaries to "keep confidential everything concerning the Deeds they make and all information obtained for the preparation of the Deeds in accordance with their oath/promise of office, unless otherwise provided by law."[6] This obligation is very fundamental; its violation is punishable by ethical and criminal sanctions (Article 322 of the Criminal Code).

This obligation is reinforced by Article 66 of the Law on Judicial Review, which grants procedural "Right to Refuse." For the purpose of judicial proceedings (investigation, prosecution, or trial), law enforcement agencies cannot simply summon a Notary or seize their protocols.[7] The summoning and collection of certified copies of deeds must first obtain approval from the Notary Honor Council (MKN). Jurisprudence and legal doctrine have affirmed that this procedure is lex specialis and must be followed.

Dogmatic Study of the PDP Law (Conditional Transparency): On the other hand, the PDP Law grants a series of rights to Personal Data Subjects (in this case, the Notary's clients). One of its key rights is the right to transparency and access. Article 21 of the PDP Law, for example, requires the Data Controller (Notary) to provide information regarding the legality, purpose, type of data, and retention period of the processed data. Data subjects also have the right to access and obtain a copy of their personal data.[8]

---

[4] Intan Permata Mipon and Mohamad Fajri Putra, "Penyelenggaraan Pelindungan Data Pribadi Oleh Notaris Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi", Depok: Universitas Indonesia, Vol. 53, No. 3, 2023. 483 – 487

[5] Undang-Undang Nomor 30 Tahun 2004 Tentang Jabatan Notariis (UU No. 30 Tahun 2004), 2004.

[6] Biro Hukum Dan Humas Badan Urusan Administrasi Mahkamah Agung-RI, " Batas-batas Berlakunya Aturan dan Pidana", Jakarta: Humas Badan Urusan Administrasi Mahkamah Agung RI, 2023.

[7] 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", Jakarta: Dinasti Review, Vol. 5, No. 1, 2024. 656 – 660

[8] Mislaini and Habib Adjie, "Tanggung Jawab Notaris Dalam Pengamanan Data Pribadi Dalam Perjanjian Notariil Pada Era Digital", Surabaya: Universitas Narotama, Vol. 6, No. 2, 2024. 7487 – 7489

Identifying and Resolving the Antinomy: At first glance, these two regimes appear to be in conflict.

- **Conflict 1 (Transparency vs. Secret):** If a foreign client (Data Subject) asks their Notary, "Where did you send my passport data for verification?", is the Notary obligated to answer (to comply with the PDP Law) or obligated to remain silent (to comply with the Notary Law)?
- **Conflict 2 (Third-Party Access):** If law enforcement agencies request data on foreign clients from a Notary for "law enforcement" purposes as stipulated in the exceptions to the PDP Law, does this negate the Notary's obligation to seek the MKN's approval in accordance with Article 66 of the Notary Law?

A deeper analysis shows that this antinomy can be harmonized. This conflict is more philosophical than normative-applied, if its purpose is understood:

- **Conflict Solution 1:** Official Secrets Obligation (Article 16 of the Law on Legal Aid) is essentially designed to protect the client's interests from third parties. Meanwhile, the Transparency Obligation (Article 21 of the PDP Law) is designed to protect Data Subjects (the clients themselves) from unfair practices by Data Controllers (Notaries). The two do not conflict. Notaries are required to be transparent with their clients (Data Subjects) regarding how their data is processed. However, notaries are still obliged to maintain confidentiality regarding their clients toward third parties.
- **Conflict Solution 2:** The PDP Law is lex generalis in the context of data processing, but the JN Law (specifically Article 66) is lex specialis that regulates the procedure for summoning public officials. The legal principle of lex specialis derogat legi generali applies. The "law enforcement interest" exception in the PDP Law governs the legal basis for processing, but does not regulate how (the procedure for) obtaining data from public officials who are protected by the right to refuse to testify. Therefore, law enforcement agencies wishing to access client data from a Notary must still comply with the procedures of Article 66 of the Notary Law (through the Notary Ethics Council).[9]

To visualize this analysis, here is a table comparing liabilities:

Table 1: Analysis of Harmonization of Notary Obligations (UUJN vs. Personal Data Protection Law (PDP Law)

[9] Undang-Undang Nomor 2 Tahun 2014 Tentang Jabatan Notariis (UU No. 2 Tahun 2014)

Obligation Aspect	Notary Office Law (UUJN)	Personal Data Protection Law (UU PDP)	Harmonization/Antinomy Analysis
Nature of Main Obligation	Official Secrecy (Article 16). Absolute against third parties.	Processing Transparency (Article 21) and Data Security (Article 36).	**Harmonization:** Confidentiality applies "outward" (protecting the client from third parties). Transparency applies "inward" (Notaries are required to be transparent to clients/Data Subjects).
Protected Subject	Client's Interests (Appearing Party) and the Integrity of Authentic Deeds.	Constitutional Rights of Personal Data Subjects (Individuals).	**Harmonization:** Notary Clients are Data Subjects. The PDP Law strengthens the protection of clients in terms of their personal data.
Data Access Rights	Limited only to "parties directly concerned" with the deed (Article 54 of the Notary Law).	Widely granted to Data Subjects over all personal data processed about them (Chapter IV of the PDP Law).	**Potential Antinomy:** The PDP Law grants data subjects (clients) broader access rights than just a copy of the deed.
Access by Law Enforcement Agencies	Must be approved by the Notary Honor Council (MKN) (Article 66).	This is permissible on the basis of "the interests of the law enforcement process" (Article 10 of the PDP Law).	**Harmonization (UUJN Lex Specialis):** The legal basis of the PDP Law does not eliminate the special procedures in Article 66 of the UUJN. The MKN procedure remains in effect.
Data Breach Notification	Not explicitly regulated.	Mandatory (Article 46 of the PDP Law). The Notary (Data Controller) is required to notify	**New Obligations:** The PDP Law adds new obligations for Notaries that were not previously present in

Obligation Aspect	Notary Office Law (UUJN)	Personal Data Protection Law (UU PDP)	Harmonization/Antinomy Analysis
		the Supervisory Authority and the Data Subject (Client).	the Notary Law. This is the applicable lex posterior.

Critical Analysis of Cross-Border Data Transfer Standards (Article 56 of the PDP Law)

The core of the problems faced by Notaries in serving foreign clients lies in Chapter VII of the Personal Data Protection Law (PDP) regarding the Transfer of Personal Data, specifically Article 56 which regulates the transfer of data outside the jurisdiction of Indonesia.

The PDP Law (adopting global best practices) establishes a hierarchical or tiered mechanism that Data Controllers (Notaries) must meet before conducting cross-border data transfers.[10] The mechanism is:

1. **First-Level Mechanism: Adequacy Decision**
    - Article 56 paragraph (1) letter a states that a transfer can be made if "the recipient country has a level of Personal Data Protection that is equivalent to or higher" than the PDP Law.[11]
    - This level of equivalence is determined by the Agency (Article 56 paragraph (2)), which has not yet been established, and the list of equivalent countries (adequacy list) has also not been published.
2. **Second-Level Mechanism: Adequate and Binding Protection (Appropriate Safeguards)**
    - If the first mechanism is not met (e.g., the destination country is not on the adequacy list), Article 56(1)(b) states that the transfer can be made if "there is sufficient and binding protection."
    - This form of protection (as regulated in the draft RPP and global practices) is a legal instrument such as Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs). SCCs are standard contract clauses that have been pre-approved by the authorities and are signed between the data sender (Notary) and the data recipient (e.g., a foreign bank or law firm in the destination country).

[10] Della Fauziah, "Tantangan Penerapan Konsep Cyber Notary terhadap Kewenangan Pembuatan Akta Otentik oleh Notaris", Jakarta: Yayasan Pendidikan Dzurriyatul Quran, 2025.
[11] Fanisa Mayda Ayiliani and Elfia Farida, "Urgensi Pembentukan Lembaga Pengawas Data Pribadi sebagai Upaya Pelindungan Hukum terhadap Transfer Data Pribadi Lintas Negara", Semarang: Universitas Diponegoro, Vol. 6, No. 3, 2024. 437 – 440

3. **Third-Level Mechanism: Explicit Consent and Other Derogations**
    - If mechanisms 1 and 2 cannot be met, Article 56 paragraph (1) letter c opens the option of transfer if "explicit valid consent has been obtained from the Data Subject".
    - This consent must be specific to that transfer and the Data Subject must be informed of the risks of the transfer without adequate protection.[12]

Hypothetical Case Study (Application): This analysis is based on a realistic case study. Notary B in Jakarta was appointed to prepare the Articles of Association for the Foreign Investment Company (PT PMA) by two prospective shareholders:

- **Investor A:** A company (Legal Entity) from country X (e.g., a tax haven country with loose data regulations).
- **Investor B:** An individual (foreign national) from country Y (e.g., a European Union member state like Germany).

To comply with the principle of prudence and the verification obligation under the Notary Law, Notary B must conduct due diligence:

- Regarding Investor A (Company): Notary B needs to verify the existence and good standing status of Investor A by contacting the Company Registrar in country X.
- Regarding Investor B (Individual): Notary B needs to verify the validity of Investor B's passport, possibly by requesting confirmation from the embassy of country Y or thru the relevant authorities in country Y.

Notary B's actions of sending an email containing Investor A's Certificate of Incorporation to country X, or sending a copy of Investor B's passport to country Y, constitute cross-border data transfers subject to Article 56 of the PDP Law.

How can Notary B comply with this?

- **Mechanism 1 (Adequacy):** Notary B cannot use this. Indonesia has not yet published an adequacy list. Notary B does not have the legal authority to "assess" on their own whether country X or Y is "equivalent."
- **Mechanism 2 (SCCs):** Notary B cannot use this. The Indonesian government has not yet ratified and published the official Indonesian SCC format. Notary B cannot use EU or ASEAN SCCs because they are not necessarily recognized by Indonesian law.
- **Mechanism 3 (Consent):** Notary B has only one option left: to request explicit consent from Investor A and Investor B to transfer the data, explaining that countries X and Y may not have equivalent data protection and no SCCs are applicable.

Implications of Legal Vacuum for Notarial Practice

The PDP Law has been ratified since 2022. The two-year compliance transition period ended on October 17, 2024. However, as of 2025, the Draft Government Regulation

[12] Sindi Luchia Saldi, Rembrandt, and Edita Elda, "Tanggung Jawab Notaris Dalam Menjaga Kerahasiaan Data Penghadap Di Era Digital",Padang: Recital Review Vol. 6, No. 3, 2024. 2025. 437 – 440

(RPP) as the implementing regulation for the PDP Law—which is crucial for regulating technical matters such as data transfer mechanisms, the establishment of supervisory bodies, and the format of SCCs—is still under discussion and has not been ratified.[13]

The delay in ratifying this RPP creates a legal vacuum in the implementation of Article 56. Mechanism (1) Adequacy List and Mechanism (2) SCCs are de facto unusable by Notaries. As a result, all cross-border data transfer practices in Indonesia, including those by Notaries, are forced to rely entirely on Mechanism (3) Explicit Consent.

Sole reliance on this "consent" is highly problematic and carries significant risk:

1. **Heavy Burden of Proof:** For consent to be valid, it must be informed (the data subject understands the risks), specific (for that specific transfer), and explicit (clearly stated). Notaries now bear the additional administrative burden of designing, managing, and proving the existence of valid consent for each cross-border verification.
2. **Does Not Cover All Risks:** The consent of the clients (Investors A and B) protects Notary B from lawsuits by those clients. However, that agreement does not protect data from leaks in the destination country. If the data is leaked by the Company Register in country X, the PDP Law (as Data Controller) still holds Notary B accountable.
3. **Creating a Paradox of Normative Compliance:** Notaries are now trapped in an unsolvable paradox of compliance:
    - **Option A:** Notary B complies with the Notary Law (principle of due diligence) and verifies data with countries X and Y. To do this, he must perform a data transfer. Because Mechanisms 1 and 2 are not available, it operates under weak compliance with the PDP Law (consent only), making it vulnerable to PDP Law sanctions if data fails in the destination country.
    - **Option B:** Notary B complies with the GDPR (avoiding transfer risk) and refuses to conduct cross-border verification due to the absence of valid SCCs. As a result, Notary B violated the principle of caution under the UUJN, potentially accepted false data, and the deed he prepared risked being legally defective or could be canceled.

The legal vacuum caused by the delay in the draft law has effectively punished careful Notaries (Option A) and incentivized negligent practices (Option B, from the perspective of the Notary Law). This is an acute regulatory disharmony situation that places Notaries at unacceptable legal, administrative, and criminal risk, simply for fulfilling their official duties.[14]

[13] Fanisa Mayda Ayiliani and Elfia Farida, "Urgensi Pembentukan Lembaga Pengawas Data Pribadi sebagai Upaya Pelindungan Hukum terhadap Transfer Data Pribadi Lintas Negara", Semarang: Universitas Diponegoro, Vol. 6, No. 3, 2024. 437 – 440

[14] Sophia Afifa Nasution and Siti Hajati Husein, "Pengaruh Teknologi Informasi Terhadap Kewajiban Kerahasiaan dan Perlindungan Data Pribadi Klien dalam Praktik Notaris", Depok: Universitas Indonesia, 2025.

IV. CONCLUSION

Based on the legal-normative analysis that has been outlined, this study draws three main conclusions:

1. **Transformation of Notary Legal Status:** Enactment of Law No. Law No. 27 of 2022 has fundamentally transformed the legal status of Notaries. Notaries are now not only public officials (based on the Notary Law), but also, by operation of law, are considered Personal Data Controllers. This new status adds to a series of legal obligations not previously regulated in the UUJN, particularly obligations regarding processing transparency, data security implementation, and data breach notification.
2. **Harmonizing the Antinomy between the UUJN and the PDP Law:** Although there appears to be an antinomy (norm conflict) at first glance between the absolute confidentiality obligation of the UUJN (Article 16) and the transparency right of the PDP Law (Article 21), these two regimes can be harmonized. The confidentiality obligation of the Notary Law applies externally (protecting clients from third parties), while the transparency obligation of the Personal Data Protection Law applies internally (the Notary's obligation to be transparent to clients/Data Subjects). Furthermore, the Notary's procedural right of refusal (Article 66 of the Notary Law) remains in effect as a lex specialis that must be adhered to by law enforcement officials, and is not superseded by the general law enforcement provisions in the PDP Law.
3. **Legal Vacuum and the Paradox of Data Transfer Compliance:** The main conclusion and most critical finding of this research is that Indonesian notaries currently serving foreign clients are in a position of systemic and unavoidable non-compliance regarding cross-border data transfers. This is due to a legal vacuum caused by the fact that the implementing regulations for the PDP Law have not yet been ratified. The absence of valid legal instruments for Mechanism 1 (Adequacy List) and Mechanism 2 (Standard Contractual Clauses/SCCs) in Article 56 of the PDP Law has forced Notaries to rely on the weak Mechanism 3 (Explicit Consent). This condition creates a paradox of normative compliance ("Catch-22"): Notaries who comply with the UUJN (by verifying data) automatically become vulnerable to violating the UU PDP, and vise versa.

Suggestions and Recommendations

Based on the above conclusions, immediate action is needed from stakeholders to provide legal certainty for Notaries. Here are the proposed prescriptive recommendations:

Recommendation 1: To the Government

1. **Urgent Priorities (Short-Term):** Immediately ratify the implementing regulations for the PDP Law, giving absolute priority to the chapter governing cross-border data transfer mechanisms (implementation of Article 56). Further delays will prolong legal uncertainty and increase risks for legal practitioners and business operators.

2. **Interim Solution (Regulatory Pragmatism):** While finalizing the Indonesian version of SCCs, the Government is advised to immediately issue a Ministerial Regulation (Permen) or Institutional Decision that recognizes or adopts internationally established Standard Contractual Clauses, such as the ASEAN Model Contractual Clauses (MCCs) or EU Standard Contractual Clauses (SCCs), as a legitimate instrument (appropriate safeguards) for the time being.
3. **Publication of the List of Equivalent Countries:** Immediately publish the List of Equivalent Countries (Adequacy List), even if in the initial phase it only includes countries that clearly have high standards (e.g., EU member states, Japan, Singapore) to provide initial legal certainty for Notaries.

Recommendation 2: To Professional Organizations (Indonesian Notary Association - INI)

- **Proactive (Don't Wait for the Lesson Plan):** This should not be passive, waiting for the lesson plan to be approved. Organizations must take proactive steps immediately to protect their members by issuing Organizational Regulations (OR) or at least a Circular Letter on Compliance Guidelines for the PDP Law for Notaries.
- **Document Compliance Standardization:** This INI guide must be practical and provide templates (standard drafts) that members are required to use, including:
    - **Explicit Consent Clause:** To be added to the client data form or at the beginning (comparison) of the deed. This clause must specifically (i) mention the type of data being transferred, (ii) the destination country for the transfer, (iii) the purpose of the transfer (e.g., "for corporate data verification..."), and (iv) a warning that the destination country may not yet be recognized by the Indonesian Government as having equivalent protection.
    - **Simple Data Processing Addendum (DPA):** A draft simple supplementary agreement between the Notary (Data Controller) and the Client (Data Subject) that governs rights and obligations related to personal data.

Recommendation 3: To Notaries (Practitioners)

1. **Internal Risk Mitigation:** Immediately conduct Data Mapping at each office. Identification: What personal data is collected, where is it stored (physical/digital), who can access it, and where is the data transferred?
2. **Enhanced Technical Security:** Improving cybersecurity standards (using encryption, firewalls, the latest antivirus software, and regular backups) to protect electronically stored Notary Protocols. The notary is fully responsible for data breaches, whether caused by staff or by malware attacks.
3. **Implementation of Administrative Compliance:** Until the RPP and this INI Guide are published, Notaries are required to use the Explicit Consent Clause for every foreign client involving potential cross-border data transfer, without exception. This is the main (though weak) legal defense available at the moment.

REFERENCES

Laws and Regulations

Undang-Undang Nomor 30 Tahun 2004 Tentang Jabatan Notariis (UU No. 30 Tahun 2004)

Undang-Undang Nomor 2 Tahun 2014 Tentang Jabatan Notariis (UU No. 2 Tahun 2014)

Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi (UU No. 27 Tahun 2022)

Books

Syailendra, Moody Rizqy, "Hukum Perlindungan Data Pribadi di Indonesia" Depok: Rajagrafindo Persada, 2025. 124 - 131

Indrajaya, Rudi and Yogastio, Esa Dimmarca, "Notaris dan PPAT" Bandung: Refika Aditama, 2020. 277 - 286

Articles from Journal

Mislaini and Habib Adjie, "Tanggung Jawab Notaris Dalam Pengamanan Data Pribadi Dalam Perjanjian Notariil Pada Era Digital", Surabaya: Universitas Narotama, Vol. 6, No. 2, 2024. 7487 – 7489

Ayiliani, Fanisa Mayda, Elfia Farida, "Urgensi Pembentukan Lembaga Pengawas Data Pribadi Sebagai Upaya Pelindungan Hukum Terhadap Transfer Data Pribadi Lintas", Semarang: Universitas Diponegoro, Vol. 6, No. 3, 2024. 437 – 440

Alifia Luchia Saldi, Rembrandt, and Edita Elda, "Tanggung Jawab Notaris Dalam Menjaga Kerahasiaan Data Penghadap Di Era Digital", Padang: Recital Review c, 2025. 55-58

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", Jakarta: Dinasti Review, Vol. 5, No. 1, 2024. 656 – 660

Intan Permata Mipon and Mohamad Fajri Putra, "Penyelenggaraan Pelindungan Data Pribadi Oleh Notaris Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi", Depok: Universitas Indonesia, Vol. 53, No. 3, 2023. 483 – 487

Websites

Batas-batas Berlakunya Pidana, "Biro Hukum Dan Humas Badan Urusan Administrasi Mahkamah Agung-RI", Jakarta: Humas Badan Urusan Admin istrasi Mahkamah Agung, 2023.https://jdih.mahkamahagung.go.id/storage/uploads/produk_hukum/PERMA%20NOMOR%208%20TAHUN%202022/1672035889_2022perma8