Al-Zayn: Jurnal Ilmu Sosial & Hukum e-ISSN 3026-2917
https://ejournal.yayasanpendidikandzurriyatulquran.id/index.php/AlZyn p-ISSN 3026-2925
Volume 4 Number 2, 2026
DOI: https://doi.org/10.61104/alz.v4i2.4653

Personal Data Protection In The Digitization Of Notary Services And PPAT: An Analysis Of The Legal Responsibility Of Notaries/PPAT On The Security Of Client Data

Wirda Ningsih Octavia
Doctoral Study Program in Law, University of Lampung, Indonesia
Email Korespondensi: wirdaningsih872@gmail.com

Article received: 01 Januari 2026, Review process: 12 Januari 2026
Article Accepted: 22 Februari 2026, Article published: 01 Maret 2026

ABSTRACT
The digitization of notary services and Land Deed Making Officials (PPAT) has brought significant transformation in public services in the legal sector, but at the same time has raised new challenges related to the protection of clients' personal data. This study analyzes the legal responsibilities of notaries and PPAT in securing clients' personal data in the digital era based on Law Number 27 of 2022 concerning Personal Data Protection. Using normative legal research methods with the approach of laws and regulations, cases, comparison, and theory, this study examines three main problem formulations: (1) how to regulate the legal responsibility of notaries/PPAT in protecting clients' personal data according to the PDP Law; (2) how to implement personal data protection in the practice of digitizing notary/PPAT services in Indonesia; and (3) how is the ideal concept of legal responsibility of notaries/PPAT that is balanced between digitization efficiency and personal data protection. The results of the study show that although the PDP Law provides a comprehensive legal framework, its implementation in the practice of notaries and PPAT still faces various technical, administrative, and legal understanding obstacles. This study recommends the need for harmonization of sectoral regulations, improvement of digital security infrastructure, and strengthening of supervisory mechanisms to ensure effective protection of personal data.
Keywords: *Personal Data Protection, Digitalization, Notary, PPAT, Legal Responsibility, Data Security*

ABSTRAK
Digitalisasi layanan notaris dan Pejabat Pembuat Akta Tanah (PPAT) telah membawa transformasi signifikan dalam pelayanan publik di sektor hukum, namun pada saat yang sama menimbulkan tantangan baru terkait perlindungan data pribadi klien. Penelitian ini menganalisis tanggung jawab hukum notaris dan PPAT dalam mengamankan data pribadi klien di era digital berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Dengan menggunakan metode penelitian hukum normatif melalui pendekatan peraturan perundang-undangan, kasus, perbandingan, dan teori, penelitian ini mengkaji tiga rumusan masalah utama: (1) bagaimana pengaturan tanggung jawab hukum notaris/PPAT dalam melindungi data pribadi klien menurut UU PDP; (2) bagaimana implementasi perlindungan data pribadi dalam praktik digitalisasi layanan notaris/PPAT di Indonesia; dan (3) bagaimana konsep ideal tanggung jawab hukum notaris/PPAT yang seimbang antara efisiensi digitalisasi dan perlindungan data pribadi. Hasil penelitian menunjukkan bahwa meskipun UU PDP telah memberikan kerangka

hukum yang komprehensif, implementasinya dalam praktik notaris dan PPAT masih menghadapi berbagai kendala teknis, administratif, serta pemahaman hukum. Penelitian ini merekomendasikan perlunya harmonisasi regulasi sektoral, peningkatan infrastruktur keamanan digital, serta penguatan mekanisme pengawasan guna menjamin perlindungan data pribadi yang efektif.
Kata Kunci: *Perlindungan Data Pribadi, Digitalisasi, Notaris, PPAT, Tanggung Jawab Hukum, Keamanan Data.*

INTRODUCTION

The era of digitalization has changed the landscape of public services in Indonesia, including in the legal services sector organized by notaries and Land Deed Making Officials (PPAT). This digital transformation is characterized by the use of electronic information systems in the creation, storage, and management of legal documents containing clients' personal data. The Ministry of Agrarian and Spatial Planning/National Land Agency (ATR/BPN) has launched various digital applications such as an electronic land registration system, which requires notaries and PPATs to adapt their conventional practices into digital platforms. The digitization of notary services and PPAT brings various significant benefits, including the efficiency of deed making time, ease of access to documents, reduced paper use, and increased transparency of the administrative process. However, on the other hand, digitalization also poses serious data security risks. Personal data managed by notaries and PPATs includes sensitive information such as personal identity, financial data, property information, and confidential legal documents. Such data leakage or misuse can cause significant material and immaterial losses to the client. (Greenleaf, 2021: 167)

Awareness of the importance of personal data protection in Indonesia is increasing along with various cases of data breaches that have occurred in recent years. In response to this need, the Indonesian government has passed Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) which will come into full effect in October 2024. The PDP Law comprehensively regulates the rights of data subjects, the obligations of data controllers and processors, as well as sanctions for violations of personal data protection. In the context of the notary profession and PPAT, the PDP Law presents complex legal implications. Notaries and PPATs have a dual obligation: on the one hand they must maintain the confidentiality of their positions as stipulated in Law Number 2 of 2014 concerning Amendments to Law Number 30 of 2004 concerning Notary Positions (UUJN) and Government Regulation Number 18 of 2021 concerning Management Rights, Land Rights, Flats Units, and Land Registration (for PPAT), on the other hand they are now also subject to the provisions of the PDP Law as controllers or processors of personal data. (Hasibuan Otto, 2022: 189)

The problem becomes more complex when considering the technological infrastructure used by notaries and PPATs. Many notary offices and PPATs, especially in the regions, still have limitations in terms of digital security systems, competent human resources in the field of information technology, and an understanding of data security standards. This situation creates a gap between the

legal obligations regulated in the PDP Law and the actual capacity in its implementation. Furthermore, there is no clear harmonization between the confidentiality provisions in the UUJN and the PPAT regulations with the provisions in the PDP Law. Questions regarding the limits of data protection obligations, data processing consent mechanisms, the rights of data subjects to access or delete data in the context of notarial documents and PPAT, and legal responsibilities in the event of a data breach are still gray areas that require legal clarification.

From an academic perspective, studies on personal data protection in the digitization of notary services and PPAT are still limited. Most previous research has focused on the digitalization or data protection aspects separately, but has not integrated these two dimensions in the specific context of the notary profession and PPAT. In fact, this profession has unique characteristics as a public official who performs part of the state's functions in the creation of authentic deeds, which distinguishes it from other personal data controllers. (Dewi et al., 2019: 57)

The urgency of this research is also driven by the fact that the transition period of implementation of the PDP Law provides an opportunity to build an effective data protection system from the beginning. Without an adequate understanding of legal responsibilities and the protection mechanisms that should be in place, there is a risk that the digitization of notary services and PPAT will create new vulnerabilities to the privacy and security of client data. Therefore, this study seeks to fill the literature gap and provide a comprehensive analytical framework on the legal responsibilities of notaries and PPATs in protecting clients' personal data in the digital age, in the hope of contributing to the development of better regulation, professional practice, and law enforcement in the future.

Based on the background that has been described, this study focuses on the following three problem formulations: How is the regulation of the legal responsibilities of notaries and PPAT in protecting clients' personal data based on Law Number 27 of 2022 concerning Personal Data Protection?, How are the implementation and obstacles in the implementation of personal data protection in the practice of digitizing notary services and PPAT in Indonesia?, How is the ideal construction of notary and PPAT legal responsibilities that can balance the efficiency of digitizing services with the guarantee of client personal data protection?

METHODS

This research uses a normative legal research method that examines and analyzes law from an internal perspective with a focus on the consistency and coherence of legal norms. Normative legal research was chosen because the main focus of the research is to analyze laws and regulations related to personal data protection and its relation to the legal responsibilities of notaries and PPAT in the era of digitalization. (Sulistyowati et al., 2020: 34) The research approaches used in this study include: First, the Statute Approach, which is an approach that is carried out by examining all laws and regulations related to the legal issues being studied. In this study, the laws and regulations studied include: Law Number 27 of 2022 concerning Personal Data Protection, Law Number 2 of 2014 concerning

Amendments to Law Number 30 of 2004 concerning Notary Positions, Government Regulation Number 18 of 2021 concerning Management Rights, Land Rights, Flats Units, and Land Registration, as well as other related regulations such as the ITE Law and its implementing regulations.

Second, the Case Approach, which is an approach that is carried out by examining cases related to the legal issues faced and has become a court decision with permanent legal force. This approach is used to analyze law enforcement practices related to personal data breaches and notary/PPAT's professional responsibilities. Third, the Comparative Approach, which is an approach that is carried out by comparing legal arrangements or implementations in various jurisdictions. This study compares the personal data protection system in Indonesia with several countries that have already implemented comprehensive data protection regulations, such as the European Union's General Data Protection Regulation (GDPR) and regulations in Southeast Asian countries. Fourth, the Theoretical Approach, which is an approach that moves from the views and doctrines that develop in law. (kuner et al., 2020: 47) This study uses legal responsibility theory, legal protection theory, and privacy theory to analyze the construction of notary legal responsibility and PPAT in protecting personal data.

RESULTS AND DISCUSSION

Regulation of Legal Responsibilities of Notaries and PPAT in Protecting Clients' Personal Data Based on the PDP Law

Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) is present as a new milestone in the Indonesian legal order. As the first comprehensive legal foundation governing data privacy, this law adopts international principles such as the European Union's General Data Protection Regulation (GDPR). Although referring to global standards, the PDP Law is still adjusted to the social, cultural, and national legal needs so that it can be implemented effectively for all data operators in the country. (Voigt et al., 2017) One of the fundamental points in the PDP Law is the definition of personal data formulated in Article 1 number 1. Personal data is understood as data about an identified natural person, either independently or through a combination of other information. This broad definition directly touches the scope of work of Notaries and PPATs, as the documents they manage range from basic identities to information that is very private and strategic to clients. (Schwatzet al., 2017: 115)

Furthermore, the PDP Law divides personal data into two categories, namely general data and specific data. Specific data, which includes health information, biometrics, to crime records and financial data, demands much higher security standards. Given that Notaries and PPATs often handle financial data and children's data in the making of deeds, they are required to implement strict security protocols and ensure explicit consent from the data owner. In the operational structure of the PDP Law, role determination is very crucial for legal compliance. Notaries and PPATs are in practice more appropriately categorized as "Personal Data Controllers" than just processors. This is because they have the independent authority to determine the purpose of making the deed and how the data processing

is carried out. This position carries the consequence of great responsibility in maintaining the integrity of the information they receive. (Sari et al., 2022: 789)

As data controllers, Notaries and PPAT are bound by legal obligations regulated in Article 27 of the PDP Law. These obligations include transparency in data acquisition, ensuring accuracy, and preventing unauthorized access. These new tasks are not only administrative, but also become a new dimension in professional responsibilities that must be integrated into daily practice in the Notary and PPAT offices. The harmonization between the PDP Law and the Law on the Notary Position (UUJN) is a crucial meeting point for legal practitioners. Article 16 of the Law has long required Notaries to keep secret all contents of deeds and information obtained. However, confidentiality in the Law on Confidentiality is passive, focusing only on the prohibition of disclosing information to third parties, while the PDP Law demands a much more dynamic role. Data protection in the PDP Law regime is active, which means Notaries and PPAT must take adequate technical and organizational measures. If the Law focuses on the aspect of professional ethics, then the PDP Law adds digital security standards and measurable accountability. Thus, these two legal regimes strengthen each other in creating a safe and trusted public service ecosystem. (Hartanto et al., 2023: 45)

The principles of data processing are a compass for Notaries and PPAT in carrying out their duties. The principles of lawfulness, fairness, and transparency require practitioners to inform clients honestly about the purpose of data use. Clients should not be in the dark about how their identity data is processed or who has access to such sensitive documents. The principle of purpose limitation is also an important limitation in the practice of notary. The data collected for the creation of a particular deed must not be misused for purposes outside of that transaction, such as marketing. This ensures that the trust given by the client to the Notary is not harmed by the use of data that deviates from the original intention of providing the document.

In addition, the principle of data minimization requires efficiency in information collection. Notaries and PPAT may only request data that is really relevant and necessary for the legality of making the deed. Excessive data collection is not only unethical, but it also increases security risks for data controllers in the event of a leak or cyberattack on their storage systems. The accuracy of data or the principle of accuracy is also an inherent responsibility. (Arifin Ridwan, 2022: 612) As the official who issues the authentic deed, Notaries and PPATs are obliged to verify the validity of the information provided by the client. This obligation is in line with the principle of the PDP Law which requires that data must be up-to-date and accountable, in order to avoid legal errors that can harm data subjects in the future.

The principle of storage limitation brings its own challenges to the world of notary. The PDP Law stipulates that data should not be stored for longer than necessary, but the Law requires the retention of deed minutes forever. The synchronization of these two rules requires a data separation policy, where data that is not essential to the deed can be destroyed after a certain retention period has been met. The security aspect, which includes integrity and confidentiality, places technology as a key element. Notaries and PPATs must ensure that their data

storage systems are protected from accidental damage or external sabotage. Data integrity ensures that the information in the deed is not altered or falsified, while confidentiality ensures that only authorized parties can access it.

The legal basis for the processing of client data by Notaries and PPATs generally relies on a combination of contractual obligations and legal obligations. As an official who performs a public function, data processing is often a statutory mandate to create legal certainty for the public. Therefore, as long as the processing is carried out within the corridor of the duties of the position, the Notary has a strong legal justification under the PDP Law. Despite having a public mandate, sanctions for data protection violations remain in the shadows of practitioners. Administrative responsibilities regulated in Article 57 of the PDP Law can be in the form of written warnings to large administrative fines. This sanction aims to ensure that every data controller, including public officials, is not negligent in managing sensitive information belonging to the public entrusted to them. (Pratama, 2023: 78) On the other hand, civil liability allows aggrieved clients to file a lawsuit for damages. Data leaks that result in material or immaterial losses can be grounds for data subjects to claim compensation. This adds to the risk of litigation for Notary and PPAT offices that do not implement adequate data security standards in their digital systems.

The most severe consequence is criminal liability as regulated in Articles 67-68 of the PDP Law. Illegal disclosure of personal data or the use of data that does not belong to them can lead to prison sentences and fines of billions of rupiah. This criminal provision shows how serious the state is in protecting citizens' privacy rights from all forms of abuse by any party. In the interaction of services, Notaries and PPAT are obliged to respect the rights of data subjects guaranteed by law. The Client has the right to obtain clear information, the right of access to their data, as well as the right to correction if inaccuracies are found. This transparency builds trust between the public and public officials who are in charge of providing authentic legal services.

The right to deletion of data is one of the points that requires special adjustments in the context of notary. Given the nature of authentic deeds as permanent evidence, requests for deletion of data by clients cannot be made haphazardly. A balanced legal interpretation is needed so that privacy protection does not compromise the state archival function and the legal certainty inherent in the minutes of the deed. In closing, the implementation of the PDP Law in the world of Notaries and PPAT is not just a matter of technical compliance, but a paradigm shift towards accountable data governance. By harmonizing office confidentiality obligations and personal data protection standards, Notaries and PPAT will be able to provide more modern, secure, and harmonious legal services in line with the times in the increasingly complex digital era.

Implementation and Obstacles in the Implementation of Personal Data Protection in the Practice of Digitizing Notary Services and PPAT

The process of digitizing Notary and PPAT services in Indonesia is currently running gradually, but shows an uneven distribution pattern. This effort was

triggered by a government initiative through the Ministry of ATR/BPN which has launched the Computerized Land Office (KKP) system and electronic land registration services. Although integration with the Online Single Submission (OSS) system continues to be strengthened, the reality on the ground shows that there is a fairly wide digital gap among practitioners. (Nurhaimah, 2022: 134) The rate of technology adoption is greatly influenced by the geographical location and readiness of the region's infrastructure. In big cities such as Jakarta, Surabaya, and Bandung, many Notary and PPAT offices have been modernized by adopting electronic document management systems. On the other hand, in areas with limited internet access, many practitioners still stick to conventional methods

with very minimal levels of digitalization. Digitalization in this sector actually covers a wide spectrum, from storing documents in digital format to using special applications for deed management. Communication with clients has also shifted from just physical meetings to digital interactions through email and messaging apps. The integration of data with government systems, such as e-KTP and tax systems, is clear evidence that digitalization is no longer an option, but a functional necessity. (Danusaputro, 2020)

However, behind this convenience, there are major challenges related to the implementation of digital data security standards. The use of cloud storage for data backup and encryption implementation are two crucial aspects that are difficult to implement uniformly. Without robust security systems such as firewalls and strong password protocols, the digitization process can actually open the door to the risk of client personal data leakage. Technical obstacles are the main obstacle in meeting the security standards set by the PDP Law. Many offices in the area do not have adequate technological infrastructure to support secure data processing. The use of outdated computer systems and unstable internet networks often make digital operations vulnerable and inefficient. In addition to infrastructure, the lack of a reliable data backup system poses a serious threat to the continuity of client documents. (Salove, 2021: 154) In the digital ecosystem, the risk of data loss due to hardware damage or system failure is very real. Without a proven recovery procedure, Notaries and PPATs risk violating their obligations to maintain the availability and integrity of the data entrusted to them.

Vulnerability to cyberattacks is also a very urgent issue. Most Notary and PPAT offices do not have sophisticated cybersecurity systems to ward off various digital threats. The practice of using weak passwords and the absence of an intrusion detection system make sensitive client data an easy target for cybercriminals who use hacking and phishing techniques. The phenomenon of ransomware that locks data to demand ransom is now a real threat that can cripple the practice of a Notary. Without adequate cyber protection, a client's identity data and valuable property information can be held hostage or disseminated illegally. This not only damages professional reputation, but also brings very severe legal consequences in accordance with the provisions of the PDP Law. (Sitompul Joshua, 2021)

The issue of dependence on third parties also adds complexity in data protection. Many practitioners use public cloud storage services or software from

external vendors without understanding the legal aspects in depth. This raises critical questions about the division of responsibility in the event of a data breach: whether the burden falls on the Notary as the data controller or on the service provider. The implementation of data encryption, which is one of the key security standards in the PDP Act, is often difficult to realize at the small office level. Encryption requires specialized technical expertise and significant investment costs for reliable software licenses. (Edmon, 2023: 28) For individual practitioners, these financial and technical constraints are often the main reason they delay implementing stronger data protection measures. In addition to the technical aspect, human resource (HR) constraints are no less complicated. Based on surveys of professional organizations such as INI and IPPAT, the majority of Notaries and PPATs have limitations in understanding the basic principles of data security. This lack of digital literacy risks creating a security gap simply due to negligence in daily practice.

Many practitioners are not yet aware of how risky it is to send sensitive documents, such as photocopies of ID cards or draft deeds, via regular email without protection. The use of popular instant messaging apps for the exchange of confidential data is also often done without considering privacy standards. This ignorance shows that there is a wide gap between legal obligations in the PDP Law and work behavior in the field. The absence of dedicated IT staff at the Notary and PPAT offices exacerbates the digital security situation. The management of technology systems is usually carried out on an ad hoc basis by administrative staff who do not have a background in expertise in the field of information security. As a result, system updates (patching) and monitoring of suspicious activity on the network are often overlooked. (Warren et al., 1890: 193)

Cultural resistance is also a real barrier, especially among the older generation in this profession. There is a tendency to view digitalization as complicated, expensive, and actually adds legal risks rather than providing benefits. This conservative view hinders efforts to transform the actual work procedures needed to meet modern data protection standards. Changes in work procedures required by the PDP Law require adaptation of behavior that is not instantaneous. Practices such as "clear desk" policies and securing physical access to server computers are often taken for granted. In fact, information security must start from the smallest discipline in an office environment before moving on to more complex software protection.

To overcome this obstacle, professional organizations have a great responsibility in providing continuous education. Technical training on how to use password management tools and simple encryption methods should start to be massively socialized. Without the help of practical guidance, many Notaries will still have difficulty in translating the articles in the PDP Law into concrete action. The government also needs to consider providing incentives or providing shared infrastructure that is more guaranteed security for legal practitioners. The development of a centralized data exchange platform that is already encrypted automatically can be a solution for offices that have limited budgets. Synergy

between the government and professional organizations will accelerate the realization of secure digital services.

In the midst of all these obstacles, practitioners must begin to realize that data protection is a new form of office confidentiality in the 21st century. The integrity of a Notary is now not only judged by the validity of the deed on paper, but also by his ability to maintain the integrity of bits and bytes of his client's data. Avoiding digitalization is not a solution, because the demands of the times and regulations will still force these changes. The most realistic first step is to independently map the risk to the system currently in use. By identifying where personal data is stored and who has access, Notaries can begin to close the most crucial security gaps. The journey towards full compliance with the PDP Law is challenging, but it must start early to avoid future sanctions.

In the end, the digitization of Notary and PPAT services must go hand in hand with strengthening a privacy-conscious culture. Although technical and HR obstacles still loom, a commitment to continue learning and adapting will be the determinant of success. Data protection is not just an administrative burden, but an investment in trust which is the main foundation of the Notary and PPAT professions in the digital era.

The Ideal Construction of Notary and PPAT Legal Responsibilities: Balancing Digitalization and Data Protection

Efforts to overcome the conflict of norms between the Personal Data Protection Law (PDP Law) and sectoral regulations such as the Notary Position Law (UUJN) and PPAT regulations require a comprehensive harmonization approach. The crucial first step is to apply a harmonious interpretation of the storage limitation principle. In this case, the obligation of notaries to keep the minutes of the deed forever must be aligned with the obligation to delete data in the PDP Law through clear data categorization. (Rahamanto, 2023: 201) The practical solution lies in distinguishing between the data contained in the minutes of the deed and the supporting data or work data. Data in minuta must be stored indefinitely with maximum security standards due to its permanent legal value. (Hartanto et al., 2023: 45) On the other hand, supporting data such as photocopies of identities or draft documents that are not included in the minuta can be deleted after a certain retention period ends, so that the data efficiency principles in the PDP Law are still met.

In addition to interpretation, the application of the principle of Lex Specialis Derogat Legi Generali is the second pillar in this harmonization. Special provisions in the UUJN or PPAT regulations regarding the confidentiality of positions and document management must be seen as a law that overrides the general rules of the PDP Law. However, this exception only applies to the extent that the sectoral regulation is still able to provide adequate protection and does not injure the basic rights of the data subject. In the long run, amendments or revisions to sectoral regulations are inevitable to create absolute legal certainty. The revision of the UUJN and PPAT regulations needs to explicitly accommodate digital data security obligations, consent management, and response mechanisms for data leaks.

Without these updates, practitioners will continue to be in the gray zone between job title compliance and data protection compliance.

Along with legal harmonization, the establishment of minimum technical standards is an urgent need for Notaries and PPAT in managing digital data. Referring to international frameworks such as ISO/IEC 27001, this standard must be adapted to local capacity. The main focus includes strict access control, where each user is required to have an individual account with a strong password as well as the implementation of multi-factor authentication (MFA) for sensitive systems. The next technical aspect is data encryption, both when data is stored (at rest) using the minimum standard AES-256, and when data is being sent (in transit) via HTTPS or TLS protocols. Electronic communications containing confidential client information must also use end-to-end encryption. This ensures that even if the data is successfully intercepted by an unauthorized party, the information in it remains unreadable. Data resilience also depends on disciplined backup and recovery procedures . Notaries and PPATs are advised to back up data on a daily basis to a separate location, either through off-site backup or encrypted cloud storage. These data recovery procedures should be tested regularly to ensure that in an emergency, office operations can recover quickly without fatal loss of client data. (Wisnubroto, 2023: 56)

Network security also plays a vital role through the use of properly configured firewalls and network segmentation. Separation between systems containing sensitive data and public or guest networks can minimize the risk of cyberattacks. In addition, regular updates of the operating system and software through patching are essential to close the security gaps found by developers. Not only digital, but physical office security also remains a priority. Access to server space or document storage areas must be restricted, monitored with CCTV, and implement clear desk and clean screen policies. This simple step is effective in preventing direct information theft by outside parties or unauthorized staff, known as shoulder surfing.

All digital system activities must be documented in comprehensive logging and monitoring. Records of who accessed the data, when, and what was done should be kept for at least six months for audit or investigation purposes in the event of an incident. This technical transformation is planned in stages over three years, starting from basic policies to advanced automated monitoring systems in the third year. In terms of transparency, Notaries and PPAT are obliged to implement a privacy notice mechanism that is easy to understand. This privacy policy must honestly explain the type of data collected, the purpose of the processing, the legal basis, and the third parties involved such as BPN or tax offices. This information should not simply contain complex legal terms, but should be accessible and understandable to the client at the time of first contact.

Consent management must also be explicitly documented. The consent of the client must be given freely, specifically and without hesitation, whereby the client also has the right to withdraw such consent easily. To support accountability, each office must maintain Records of Processing Activities (RoPA) as concrete evidence that all data processing is carried out in accordance with applicable legal standards.

Another preventive measure is the implementation of Data Protection Impact Assessment (DPIA) for high-risk business processes, such as the use of new cloud storage systems or artificial intelligence in document processing. (Asyhadie, 2021) DPIA helps identify risks early and determine the necessary mitigation measures. This ensures that every technological innovation in the notary's office continues to prioritize the protection of data subject rights.

In the event of a security incident, the construction of an ideal liability requires an alert Incident Response Plan. The PDP Law requires notification to supervisory agencies and data subjects within 72 hours after the violation is discovered. This plan includes the detection stages, isolation of the affected system, impact scale assessment, and notification delivery using pre-prepared templates for speed of response. Given the complexity of this task, the appointment of a Data Protection Officer (DPO) becomes particularly relevant. For offices with large data volumes, the DPO is in charge of overseeing compliance, providing technical advice, and being the point of contact with regulators. For small offices, alternative solutions such as the use of a joint DPO or the services of an external consultant can be considered so that the cost burden does not hinder regulatory compliance.

Vendor management is also an integral part of the data protection chain. Notaries and PPATs must conduct due diligence on software or IT service providers before cooperating. The cooperation contract must contain a Data Processing Agreement (DPA) clause that affirms the responsibility of the vendor in maintaining data security and provides audit rights for notaries to ensure that the security promise is fulfilled. Increasing the capacity of human resources is the key to long-term success. A systematic education program is needed, ranging from basic awareness for administrative staff to technical training for IT managers. Professional organizations such as INI and IPPAT can take on the role of providers of special data protection certifications for their members, in order to provide a guarantee of professionalism to the wider community.

In terms of technology, the availability of affordable and scalable solutions is the main supporting factor. Strategies such as the collective purchase of software licenses by professional organizations or the utilization of trusted open source applications can help small-scale practitioners. The government is also expected to provide tax incentives or subsidies for cybersecurity investment in this legal services sector. Law enforcement against violations by Notaries and PPAT must be carried out proportionately and educationally. In the transition phase, regulators should adopt a phased approach, ranging from warnings to fines, taking into account the good faith of practitioners in efforts to comply. The main focus of law enforcement should be on system improvement and ongoing compliance, not just financial penalties.

In closing, this entire framework boils down to the principle of accountability where Notaries and PPATs are able to demonstrate their compliance through complete documentation. By maintaining valid audit records, privacy policies, and certifications, public trust in the integrity of Notary and PPAT positions in the digital era will be stronger. This harmonization is not only a matter of law, but also about building a safe and modern legal services ecosystem.

CONCLUSION

Based on the comprehensive analysis that has been carried out, this study produces several main conclusions: (1) The regulation of notary and PPAT's legal responsibilities in protecting clients' personal data based on Law Number 27 of 2022 concerning Personal Data Protection places them as personal data controllers with extensive legal obligations. These obligations include the obligation to provide transparent information, ensure data security, prevent data breaches, and respect the rights of data subjects. The PDP Law provides a comprehensive legal framework that adopts international best practices, but its application in the specific context of the notary profession and PPAT requires harmonization with pre-existing sectoral regulations, especially UUJN and PPAT regulations. This legal responsibility is multidimensional, encompassing administrative, civil, and criminal liability, with the threat of significant sanctions for violators. (2) The implementation of personal data protection in the practice of digitizing notary services and PPAT in Indonesia faces various substantive obstacles. These constraints include: (a) limited technological infrastructure and cybersecurity capacity, especially in the regions; (b) lack of digital literacy and understanding of data protection principles among notaries, PPATs, and their staff; (c) the unclarity of specific regulations and potential conflicts of norms between the PDP Law and sectoral regulations; (d) limited financial resources for investment in adequate data security systems; and (e) practical difficulties in implementing the rights of the data subject, especially the right to deletion of data that clashes with the obligation to keep the deed minutes forever. Surveys and case studies show that the majority of notaries and PPATs are not ready to meet the standards set by the PDP Law, creating a significant gap between legal norms and practice in the field. (3) The ideal construction of notary and PPAT legal responsibilities that can balance the efficiency of digitalization with the guarantee of personal data protection requires a multifaceted approach that includes: (a) the adoption of the principles of Privacy by Design and Privacy by Default in every aspect of digital services; (b) the implementation of a multi-layered responsibility model involving not only individual notaries/PPATs, but also professional organizations, regulators, and governments; (c) harmonization of regulations through coherent interpretation, application of the principle of lex specialis, and amendments to sectoral regulations; (d) the establishment of realistic and achievable minimum technical standards with a phased implementation roadmap; (e) strengthening transparency mechanisms, consent management, and incident response; (f) systematic education and capacity building programs; (g) the provision of affordable technology solutions through collective action and government support; (h) enforcement that is proportionate to the educational approach; and (i) an accountability framework that allows for measurable demonstration of compliance.

LIST OF REFERENCES

Arifin, Ridwan. (2022). "Implementation of Personal Data Protection in Indonesia in the Era of Digitalization." Journal of Law and Development, Vol. 52, No. 3, pp. 612-635.

Asyhadie, Zaeni and Arief Rahman. (2021). Introduction to Law. Jakarta: PT RajaGrafindo Persada.

Danusaputro, Munadjat. (2020). Data Protection Law: Concept and Implementation. Bandung: PT Alumni.

Dewi, Shinta and Sudikno Mertokusumo. (2019). Personal Data Protection Law in the Digital Era. Yogyakarta: Genta Publishing.

Greenleaf, Graham. (2021). "Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance." Privacy Laws & Business International Report, Issue 167, pp. 1-5.

Hartanto, Junita and Michael Winata. (2023). "Notary Legal Responsibility in the Protection of Clients' Personal Data." Journal of Notariil, Vol. 8, No. 1, pp. 45-67.

Hasibuan, Otto. (2022). "Digitization of Notary Services: Opportunities and Challenges in the Indonesian Legal Perspective." Indonesian Business Law Journal, Vol. 15, No. 2, pp. 189-210.

Kuner, Christopher et al. (2020). "The Challenge of 'Big Data' for Data Protection." International Data Privacy Law, Vol. 2, Issue 2, pp. 47-49.

"Please, Edmon. (2022). Introduction to Telematics Law: A Compilation of Studies. Jakarta: PT RajaGrafindo Persada.

"Please, Edmon. (2023). "Harmonization of Personal Data Protection Law with Sectoral Regulations in Indonesia." Journal of Law and Technology, Vol. 5, No. 1, pp. 1-28.

Nurhalimah, Siti. (2022). "Privacy by Design: Implementation in Notary Information Systems and PPAT." Journal of Information Technology and Law, Vol. 4, No. 2, pp. 134-156.

Pratama, Yoga and Rani Aprilyani. (2023). "Obstacles to the Implementation of the PDP Law on the Notary Profession in Indonesia: A Case Study of Jakarta and Surrounding Areas." Journal of State Law, Vol. 12, No. 1, pp. 78-102.

Rahmanto, Tomy. (2023). "Data Breach and the Legal Responsibility of Personal Data Controllers: An Analysis of Court Decisions." Private Law Journal, Vol. 6, No. 2, pp. 201-225.

Sari, Dewi Kartika and Ahmad Junaidi. (2022). "The Balance of Interests in Personal Data Protection: A Human Rights Perspective." Constitutional Journal, Vol. 19, No. 4, pp. 789-815.

Schwartz, Paul M. and Karl-Nikolaus Peifer. (2017). "Transatlantic Data Privacy Law." Georgetown Law Journal, Vol. 106, pp. 115-179.

Sitompul, Joshua. (2021). Cyberspace, Cybercrimes, Cyberlaw: A Review of Criminal Law Aspects. Jakarta: Tatanusa.

Sitompul, Joshua. (2022). "Aspects of Criminal Law in Personal Data Protection Violations." Indonesian Journal of Criminal Law, Vol. 8, No. 3, pp. 301-328.

Solove, Daniel J. (2021). "A Taxonomy of Privacy." University of Pennsylvania Law Review, Vol. 154, pp. 477-564.

Sulistyowati, Irianto and Sidharta. (2020). Legal Research Methods: Constellations and Reflections. Jakarta: Yayasan Pustaka Obor Indonesia.

Voigt, Paul and Axel Von dem Bussche. (2017). The EU General Data Protection

Regulation (GDPR): A Practical Guide. Switzerland: Springer International Publishing.

Warren, Samuel D. and Louis D. Brandeis. (1890). "The Right to Privacy." Harvard Law Review, Vol. 4, No. 5, pp. 193-220.

Wisnubroto, Aloysius. (2023). "Notary Confidentiality Obligations in the Digital Era: Challenges and Solutions." Indonesian Journal of Notary, Vol. 10, No. 1, pp. 56-78

