JURNAL AKTA
Volume 11 No. 3, September 2024
SINTA 2 by Nationally Accredited Journal,
Decree No. 164/E/KPT/2021

The Urgency of Regulation of Data Protection for the Parties in Cyber Notary

Nynda Fatmawati Octarina[1)], **Fadila Fernanda**[2)]**; Fironika Tri Asni Dewi**[3)] **& Habib Adjie**[4)]
[1)] Master of Notary Program, Faculty of Law, Narotama University, E-mail: nynda_f@yahoo.com
[2)] Master of Notary Program, Faculty of Law, Narotama University, E-mail: fadilafernanda10@gmail.com
[3)] Master of Notary Program, Faculty of Law, Narotama University, E-mail: virovir17@gmail.com
[4)] Master of Notary Program, Faculty of Law, Narotama University, E-mail: adjieku61@gmail.com

Abstract. *Notary is a public official authorized to make authentic deeds and have other authorities. In carrying out his duties and authority, the Notary must be able to maintain the confidentiality of every data of the parties in the deed he makes. parties in the deed he makes. The principle of confidentiality that has been regulated in UUJN Article 16 paragraph (1) letter f has the potential to clash with the concept of Cyber Notary, which has also been contained in notary concept which has also been contained in UUJN Article 15 paragraph (3) which in its explanation states explanation states that one of the other powers of Notary referred to is the authority to certify transactions conducted electronically (Cyber Notary). The authority of Notary in Cyber Notary has drawn pros and cons in various circles. various circles. The problem arises when in the implementation of Cyber Notary uses the services of third parties to build up to the maintenance of the Cyber Notary electronic system. Thus, there will be a third party. Thus, there will be a third party who can access all deeds in the system. This means that the data parties are no longer a secret of the notary and are no longer in accordance with the principle of confidentiality that requires the notary to in accordance with the principle of confidentiality that requires the Notary to maintain its confidentiality as it has been applied so far. This research will examine the implementation of the principle of Notary confidentiality and the urgency of regulating the protection of parties' data in Cyber Notary to prevent notaries from being sued in the future. This research uses a normative legal research method with a statue approach and conceptual approach. The results showed that the need for Cyber Notary must be in line with the regulation of data protection of the parties in the Cyber Notary because UUJN has provided rules that*

the Notary is obliged to keep confidential everything about the Deed he makes and all information obtained to protect the parties' data.

Keywords: *Confidentiality; Cyber; Data; Personal; Protection.*

1. INTRODUCTION

Digitalization efforts in various fields continue to be carried out as an effort to encourage the creation of efficient and easily accessible services for the public. The presence of increasingly developing technology plays a role in the success of improving the quality of services to the public in the digital era. Technological developments will certainly disrupt the order of people's lives in various fields, including the legal field. Now digitalization has spread to the notary realm. This digitalization is none other than a challenge and a demand for the legal field to be able to carry out reforms by following Society 5.0. The main aspect contained in society 5.0 is a human-centered technology obtained through artificial intelligence analysis of big data that includes thousands of pieces of information including real-time data.

Based on a report from the Law Society, increasingly advanced technological developments will influence the growth of the legal workforce in terms of the adoption of new technology and work methods, including:

a. *The Cloud*, changes in file storage needs that were originally conventional will change to digital. This change makes document archiving efficient and practical because it can reduce the need for physical office space.

b. *Digitizing routine legal tasks*, digitalization of legal documents through software enhancements that support practitioners to work more efficiently and are able to reduce costs related to secretarial matters.

c. *Document production*, acts as a program that can produce drafts digitally. Reducing physical and traditional duplication activities so that time efficiency is greatly increased.

d. *Legal research (due diligence)*, the technology that is present offers efficient features in collecting various sources of information and filtering relevant information in conducting legal research to be given to clients. Of course, with this technology, it will cut research time while increasing the accuracy of the data obtained.(Wicaksono 2023).

Cyber Notary as one of the forms of technological development in the legal field is predicted to be a new breakthrough for the notary world to provide convenience in services. Cyber Notary is a concept born from technological developments to create an authentic deed in the cyber space area and can help notaries carry out daily activities(Wicaksono 2023). Cyber Notary is here to

introduce an information technology aimed at notaries in carrying out their duties and authorities, such as in the efforts to digitize documents, signing authentic deeds electronically, using teleconferencing in the running of the company's General Meeting of Shareholders (GMS).(Princess 2017)

The implementation of Cyber Notary in Indonesia is based on Article 15 paragraph (3) of the Notary Law (UUJN) which provides an opportunity to implement the Cyber Notary concept, which states that "In addition to the authority as referred to in paragraph (1) and paragraph (2), Notaries have other authorities regulated in laws and regulations", which in its explanation explains that what is meant by other authorities regulated in laws and regulations include the authority to certify transactions carried out electronically (Cyber Notary), make deeds of waqf pledges, and airplane mortgages. The Cyber Notary concept contained in the amendment to the UUJN has caused pros and cons in various circles. For those in favor, Cyber Notary is viewed as a new breakthrough that is very efficient in terms of time which is shortened and in terms of costs which are reduced because there is no need to spend money to come face to face with a Notary in making a Deed. In addition, the Cyber Notary system also benefits notaries because it saves storage space for deeds at the notary's office. However, if examined more deeply, Cyber Notary in its implementation in Indonesia often causes cons in various circles.

The application of Cyber Notary in notary practice is contrary to the principle of Tabellionis Officium Fideliter Exercebo which states that a Notary must work in a traditional manner.(H. Utomo 2021). This principle requires the Notary to be present, see and hear in every deed being made and signed by the Notary himself and the respective parties as well as witnesses directly at the place where the deed is read by the Notary.(Ocean 2021). This principle requires that a Notary in carrying out his duties in making an authentic deed must make the deed directly face to face with the parties, in other words it cannot be made via electronic media such as the internet, audio visual, video conference or using an electronic signature.(Isnaini and Utomo 2019). This principle is in line with the provisions of the UUJN regulated in Article 16 paragraph (1) letter m that the Notary is obliged to read the Deed in front of the parties appearing in the presence of at least 2 (two) witnesses, or 4 (four) witnesses specifically for making a Deed of Will privately, and signed at that time by the parties appearing, witnesses and the Notary.

The principle of Tabellionis Officium Fideliter Exercebo is based on maintaining the confidentiality of the authentic deeds of the parties because the Notary only deals with the parties directly without any interference from third parties considering that the position of Notary is equipped with the obligation to always maintain the confidentiality of all matters or information related to the authentic deeds he makes as a form of protection of the personal data of the parties. This provision is stated in Article 16 paragraph (1) letter f UUJN which states that "Notaries are required to keep confidential everything regarding the Deed he

makes and all information obtained for the purpose of making the deed in accordance with the oath/promise of office, unless the law determines otherwise". Notaries are required to keep confidential everything regarding the Deed he makes and all information obtained because it is a deed belonging to the parties. In this case, the Notary is only limited to making/validating the Deed(Isnaini and Wanda 2017). This obligation applies without a time limit, meaning that the notary is bound by the obligation to keep this deed confidential as long as the deed is still valid, not only as long as the notary is still actively carrying out his duties.

Problems arise when in the implementation of Cyber Notary using the services of a third party to build and maintain the Cyber Notary electronic system. When the deed has been uploaded to the system, in this case Cyber Notary, then at that time the third party has the opportunity to see and access the data of the parties contained in the deed. Indirectly, the Notary has given access to the third party to the data of the parties contained in the deed in the system. This means that the data of the parties contained in it is no longer confidential, which means it is not in accordance with the principle of confidentiality. In fact, a Notary who holds a position of trust, it is his obligation to maintain the confidentiality of his position, because if the Notary is unable to maintain the confidentiality of his position, then it cannot be called a position that is trusted(Adjie, 2011a). Legal protection of the confidentiality of data contained in the deeds of the parties is questionable and there is no certainty as to who is responsible for the leaking of the parties' data in the deeds uploaded to the Cyber Notary system.

The definition of information technology according to Law No. 1 of 2024 concerning the Second Amendment to Law No. 11 of 2008 concerning Electronic Information and Transactions (UU ITE) is a technique for collecting, preparing, storing, processing, announcing, analyzing, and/or disseminating information. Meanwhile, information technology itself according to the ITE Law is defined as one or a set of electronic data, including but not limited to writing, sound, images, maps, designs, photos, electronic data interchange (EDI), electronic mail, telegrams, telex, telecopy or the like, letters, signs, numbers, Access Codes, symbols, or perforations that have been processed that have meaning or can be understood by people who are able to understand them. The deed contained in the Cyber Notary is included in electronic information. The ITE Law specifically regulates electronic information concerning other people's personal data which must have the permission of the person concerned. In its explanation, it is stated that everyone has personal rights that must be respected, including in the cyber realm. This means that protecting other people's data binds all parties, including notaries.(The Great Resurrection of Christ 2024). This is in line with the principle of confidentiality of the parties that must be upheld by notaries.(Shodhiq 2022). In the ITE Law, Electronic Systems are also known, namely a series of electronic devices and procedures that function to prepare, collect, process, analyze, store, display, announce,

send, and/or distribute Electronic Information organized by Electronic System Organizers, namely parties that utilize Electronic Systems, including state administrators, Persons, Business Entities, and/or the community. Likewise in Cyber Notary, notaries do not work alone, there is one party that is the organizer of the electronic system. This party will be able to access data contained in the network or electronic means that are under its 'authority'. This party is certainly not bound by the UUJN as a notary.

This is detrimental to Notaries, because if Notaries do not maintain confidentiality as stated in Article 16 paragraph (1) letter f UUJN, they will be subject to sanctions in the form of written warnings, temporary dismissal, honorable dismissal or dishonorable dismissal as stipulated in Article 16 paragraph (11) UUJN. This shows that there is no legal protection for Notaries when Cyber Notary is carried out considering that with the entry of a third party, data leaks in the Deed can clearly occur. Legal protection is closely related to the sense of trust and security of users towards a digital system, therefore adequate legal protection is needed to protect the data of the parties in the deed.

In fact, digitalization in client services is not only happening to notaries, banks are doing it too.(Isa Anshari Arif 2021). Online banking services have been owned by almost all general banks in Indonesia, both government-owned and private banks. There is no closed opportunity for banks to cooperate with third parties in the IT field to build and maintain the operation of the online banking system. However, Law No. 10 of 1998 concerning Amendments to Law No. 7 of 1992 concerning Banking (Banking Law) has included regulations on parties affiliated with the Bank where affiliated parties in running a banking business can be held criminally responsible for banking crimes that involve them either directly or indirectly in carrying out their activities related to the existence of banking crimes within the scope of banking which is their authority(Maryogi 2023). According to Article 47 paragraph (2) of the Banking Law, those who are obliged to uphold bank secrecy are Members of the Bank's Board of Commissioners, Members of the Bank's Board of Directors, Bank Employees and other affiliated parties of the Bank. Based on Article 1 paragraph (22) of the Banking Law, the affiliated parties are:

a. Members of the Board of Commissioners, supervisors, Directors or their proxies, officers or employees of the bank;

b. members of the management, supervisors, managers or their proxies, officials or employees of the bank, specifically for banks in the legal form of cooperatives in accordance with applicable laws and regulations;

c. parties who provide services to banks, including public accountants, appraisers, legal consultants and other consultants;

d. parties who, according to Bank Indonesia's assessment, are involved in influencing bank management, including shareholders and their families, families of commissioners, families of supervisors, families of directors, families of managers

The Banking Law has bound third parties related to banking service activities to be jointly responsible if there are violations committed by the bank caused by the third party. One of them is related to banking confidentiality(Hendrik Handoyo Lugito 2021). The legal consequences for violations of bank secrecy have been regulated in the Banking Law, namely in the form of criminal threats or administrative fines. Criminal sanctions in the form of imprisonment and fines are imposed on affiliated parties who intentionally provide information that must be kept confidential as regulated in Article 47 paragraph (2) of the Banking Law and intentionally do not carry out the steps necessary to ensure the bank's compliance with the provisions of this Law and other laws and regulations applicable to banks as regulated in Article 50 of the Banking Law. Therefore, when there is cooperation between the Bank and an affiliated party and later on the affiliated party experiences a leak of customer data caused by the affiliated party, the affiliated party can be sued because the affiliated party is bound by the obligation to maintain bank secrecy.(HIW Utomo 2020).

Reflecting on the Banking Law, the UUJN does not yet include rules on the obligations of third parties or affiliates or sanctions in Cyber Notary. The limited regulation on Cyber Notary in the UUJN creates no legal certainty in the protection of data of the parties in the deed and the blurring of the Notary's limitations in being responsible for his/her obligations in maintaining the principle of confidentiality when the deed he/she made is uploaded in the Cyber Notary system which has the potential to violate the principle of confidentiality because it indirectly provides an opportunity for third parties to be able to access it. For this reason, it is quite crucial to conduct this research considering that the Cyber Notary regulations in Indonesia are still very small in scope so that this research will examine the implementation of the Notary's confidentiality principle, the urgency of regulating data protection of the parties in Cyber Notary and solutions to Data Protection of the Parties.

2. RESEARCH METHODS

The research method used is the normative legal research method. Normative Law is a procedure and method of scientific research to find the truth based on the logic of legal science from a normative perspective by using a statutory approach, a conceptual approach and a historical approach.(Marzuki, 2010a).

The research approach used in this study is first, the statute approach, this approach is used to answer legal issues with the statutory regulations of the 1945 Constitution of the Republic of Indonesia (UUD NRI 1945), UUJN, Banking Law, Law No. 27 of 2022 concerning Protection of Personal Data. Second, the

conceptual approach, an approach using legal concepts or theories relevant to Cyber Notary, the principle of Notary confidentiality, the limitations of Notaries in Cyber Notary and the protection of personal data of the parties.

The legal materials used in this study are primary legal materials and secondary legal materials. Primary legal materials are legal materials obtained through legislation. Secondary legal materials are in the form of legal research results (thesis, dissertation, and legal journals), books on law, and discussion results in various forums related to the legal issues raised.

3. RESULTS AND DISCUSSION

3.1. Implementation of the Notary Confidentiality Principle in Cyber Notary in Indonesia

In the Notary's oath of office and the Notary's code of ethics, it contains the secret of the position held by the Notary. The Notary is obliged to keep the secret entrusted to the parties as a secret of office granted by law as regulated in Article 4, Article 16 letter f UUJN. Violation of this secret of office is regulated in Article 322 of the Criminal Code(Adjie 2022). As a holder of office, a Notary has sworn to keep confidential the contents of the deed and information obtained in the implementation of the office as stated in Article 4 paragraph (2) of the UUJN. Then the principle of confidentiality of the Notary's office which is based on Article 16 paragraph (1) letter f of the UUJN regulates the obligation of the Notary to maintain confidentiality not only regarding the deeds he makes but also including all information needed in the process of making the deed. Meanwhile, the regulation of the principle of confidentiality in a position in general has been regulated in Article 322 of the Criminal Code (KUHP) which states that "Anyone who intentionally reveals a secret that he must keep because of his position or profession, whether present or former, is threatened with a maximum imprisonment of nine months or a maximum fine of six hundred rupiah."

From the provisions above, it is clear that the principle of confidentiality is not just a theory but a very important obligation as well as an oath that has been taken by a Notary when serving. However, this principle will be a big question for the Cyber Notary system where the confidentiality of authentic electronic-based deeds uploaded to the Cyber Notary system can involve third parties. According to Emma Nurita, the concept of Cyber Notary can temporarily be interpreted as a notary who carries out his duties or authority based on information technology, which is related to the duties and functions of a notary, especially in making deeds(Makarim, 2013a).

A deed made before a notary is in fact a deed belonging to the parties, so the notary is obliged to keep confidential everything contained in the deed to protect the interests of the parties, as explained in the explanation of Article 16

paragraph (1) letter f UUJN that the obligation to keep confidential everything related to the deed and other documents is to protect the interests of all parties related to the deed.(Setiawan and Octarina 2022). Likewise, the contents of the deed are private, because they include the personal data of the parties. Even if there are other parties outside who are interested in the deed, there must be written approval from the parties (parties) to the interested party. As regulated by UUJN in Article 54 Paragraph (1) UUJN that "Notaries can only provide, show, or notify the contents of the Deed, Grosse Deed, Copy of Deed or Excerpt of Deed, to people who are directly interested in the Deed, heirs, or people who obtain rights, unless otherwise determined by statutory regulations."

Notaries in making deeds cannot be separated from the inclusion of personal data of the parties in the deed. In relation to personal data, the government is the authority given authority by the state to protect personal data in accordance with Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia (UUD NRI 1945) which states that "Everyone has the right to protection of themselves, their families, honor, dignity, and property under their control, and has the right to a sense of security and protection from the threat of fear to do or not do something that is a basic human right". The right to data which is the right of the parties is also regulated in the ITE Law, Article 26 paragraph (1), which requires all parties to ask for permission if they wish to enter someone's data into electronic media. And a Notary is a public official who is authorized to make authentic deeds and has other authorities. In the deeds made by a notary, the personal data of the parties who appear before him must be written.

Law No. 27 of 2022 concerning Personal Data Protection (UU PDP) explains that personal data is data about an individual who is identified or can be identified individually or combined with other information either directly or indirectly through an electronic or non-electronic system. The part of the notarial deed that describes personal data is called a comparison. In the case where the person facing the notary is an individual, the things that must be mentioned in the comparison include:

a. Full name
b. Place and date of birth
c. Citizenship
d. Job/Position/Position
e. Residence
f. Self-identity (Electronic KTP stating the Population Identification Number)

In addition to the comparison, in the notarial deed there is another part of the notarial deed that describes a person's personal data. This part is located at the end of the deed, which describes the witness's personal data with the same provisions as the parties as mentioned above.(Alwesius, 2018a). Moreover, regarding the deed of establishment of a company, there will be data containing

the composition of the value of shares from the shareholders, in this case the data is included in a person's financial data and is included in a person's personal data. Article 4 paragraph (3) of the UUPDP explains that general personal data includes: full name, gender, nationality, religion, marital status, and/or personal data that is combined to identify a person such as a mobile phone number and IP Address.

In the perspective of the PDP Law, a Notary is required to guarantee the security of the parties' personal data. This is because a Notary is a legal subject in the category of an individual who makes his own actions and can determine for himself where the processing of personal data contained in the authentic deed is intended.(Wicaksono 2023). This means that a Notary is a Personal Data Controller, namely every person, public body, and international organization that acts individually or together in determining the purpose and controlling the processing of Personal Data as explained in Article 1 number 4 of the UUPDP. Personal data that is used as an authentic deed by an interested party becomes the responsibility of a Notary in maintaining its security. Therefore, notaries must also directly comply with the provisions of the PDP Law.

In the case of Cyber Notary, in carrying out his/her official functions so far, the Notary is bound by the oath of office, UUJN, KUHP and UUPDP, all of which require him/her to maintain the principle of confidentiality of the contents of the deed which includes the personal data of the parties as well as the information he/she obtains as stated in Article 16 paragraph (1) letter f UUJN, both from the time the parties are received until the deed is processed electronically.

However, in its implementation, it is not impossible to involve a third party who in quotation marks has the authority in organizing the Cyber Notary electronic system, for example if the party responsible for implementing Cyber Notary uses the services of a third party to build and maintain its electronic system. This third party can certainly access the data contained in the Cyber Notary electronic system and of course this third party is not bound by the current UUJN. This results in the potential for the principle of confidentiality that has been regulated in the UUJN not to be guaranteed because the personal data of the parties contained in the deeds uploaded to the Cyber Notary system. And this problem will be a problem for the Notary concerned if there is data that is leaked because there is no clear limit of responsibility or implementing regulations regarding this.

3.2. The Urgency of Establishing a Law Regulating Cyber Notary

The development of increasingly sophisticated information and communication technology is able to make everything connected to the internet network. Until now, legal products are still continuing to adjust to these developments. Notaries are no exception, in carrying out their duties and authorities they have

also begun to be aligned through the Cyber Notary concept which is stated in the amendment to UUJN in 2014. The Cyber Notary concept is a new concept in Indonesia that provides a way for the authority of notaries to carry out their duties electronically, as an intermediary for the main media to make deeds. Where previously the deed was written in physical form (written on paper) and attended directly (face to face) it became an electronic deed and its creation does not have to come directly to the notary but can be done electronically where the parties and the notary are connected to a Cyber Notary system.(Merlyani, D., Yahanan, A., & Trisaka 2020).

In simple terms, the term Cyber Notary is used to refer to the authority of a Notary applied in electronic transactions.(Pangesti, Darmawan, and Limantara 2021). Based on the ITE Law Article 1 paragraph (2), it explains that electronic transactions are legal acts carried out using computers, computer networks, and/or other electronic media. Grammatically, electronic transaction certification means that a Notary records an activity or transaction carried out electronically and there is an output from the recording in the form of a certificate or document.(Pangesti, Darmawan, and Limantara 2021)

Meanwhile, an electronic certificate is an electronic certificate containing an electronic signature and identity indicating the legal subject status of the parties in an electronic transaction issued by an electronic certification organizer as regulated in Article 1 number 9 of the ITE Law. Following up on electronic certification, the Minister of Communication and Information of the Republic of Indonesia (Menkominfo) on August 27, 2018 stipulated the Regulation of the Minister of Communication and Information Number 11 of 2018 concerning the Implementation of Electronic Certification (Permenkominfo No. 11 of 2018) which stipulates that upon an application from the applicant for the issuance of an electronic certificate, the electronic certification organizer can appoint a Notary as a registration authority. This is reaffirmed in Article 25 in conjunction with Article 27 letter c of Permenkominfo No. 11 of 2018. Furthermore, Article 30 of Permenkominfo Permenkominfo No. 11 of 2018 stipulates that in the event that the examination conducted by a Notary is declared to meet the requirements, the Notary forwards the application to the electronic certification organizer to issue an electronic certificate.(Pangesti, Darmawan, and Limantara 2021). Electronic Certification Organizer (PSrE) is managed by the Directorate of Informatics Application Management, Ministry of Communication and Informatics (Ditjen Aptika Kominfo).It should be emphasized that when a deed has entered the electronic system, the deed becomes an electronic certificate which is included in electronic documents where its protection has been specifically regulated in the ITE Law. This means that all personal data in electronic deed documents must be protected by a Notary and the rights to the deed are attached to the parties.

The UUJN does not regulate Cyber Notary comprehensively, but only mentions Cyber Notary without providing a normative definition, so that with the inclusion

of the Explanation of Article 15 paragraph (3) of the UUJN, what is categorized as Cyber Notary is in a limited way the matter of certifying transactions carried out electronically.(Pangesti, Darmawan, and Limantara 2021). UUJN only regulates it by including Cyber Notary in other authorities. Even that is only mentioned in the explanation of the article. Article 15 paragraph (3) of the amendment to UUJN regulates that notaries have other authorities regulated in statutory regulations. In the explanation of the article, it is stated that one of the other authorities referred to is certifying transactions carried out electronically or Cyber Notary.(Fardhian, 2014).

Cyber Notary brings changes that have an impact on the legal aspects of the principle of confidentiality of deeds in the form of electronic information. In the Explanation of Article 16 paragraph (1) of the UUJN it is explained that Deeds and letters made by Notaries as official documents are authentic and require security for both the Deed itself and its contents to prevent irresponsible misuse. In cyberspace, the gap for data leaks to misuse of data by third parties is very high, so that a special legal regulation or lex specialist regarding Cyber Notary is needed, one of which is so that there is no violation of the principle of confidentiality.

In addition, the UUJN also does not specifically regulate the technical implementation or rules for third parties involved in the Cyber Notary electronic system. In fact, the regulation regarding the involvement of third parties is very crucial considering that notarial deeds are confidential and only the parties to the deed have full rights to see or access the contents of the deed. The obligation to keep confidential everything related to the deed and other letters is none other than to provide protection of personal data in the interests of all parties related to the deed. As in the UUJN there is a similar regulation contained in Article 54 which states that "Notaries can only provide, appoint, or notify the contents of the deed, Grosse Deed, Copy of Deed and Citation of Deed to people who have a direct interest in the deed, heirs or people who have rights, unless otherwise stipulated in the laws and regulations. " This means that notaries have been ordered by law not to provide, appoint, or notify the contents of the deed except to people who have a direct interest until there are other rules that are exceptions.

Through the Notary Honorary Council, the state provides legal protection for the Notary's right to refuse regarding the obligation to keep the contents of the deed confidential. The Notary Honorary Council is a body that has the authority to carry out Notary guidance and the obligation to provide approval or rejection for the purposes of investigations and judicial processes, for taking photocopies of deed minutes and summoning Notaries to attend examinations related to deeds or Notary Protocols that are in the Notary's storage as explained in the Regulation of the Minister of Law and Human Rights of the Republic of Indonesia Number 17 of 2021 concerning the Duties and Functions, Requirements and Procedures for Appointment and Dismissal, Organizational

Structure, Work Procedures, and Budget of the Notary Honorary Council (Permenkumham No. 17 of 2021). One of the duties of the Notary Honorary Council as regulated in Permenkumham No. 17 of 2021 is to provide approval or rejection of requests for taking photocopies of deed minutes and summoning Notaries to attend investigations, prosecutions, and judicial processes. To open the contents of a deed or to request a copy of a deed made by a notary, permission from the Notary Honorary Council is required. Thus, the only ministerial institution that is related to and authorizes investigations and examinations involving Notaries and Notary products is the Ministry of Law and Human Rights. If this product has entered the electronic realm, then as mandated by law, the Ministry of Communication and Information has the authority to make policies and impose sanctions for all actions and documents or information in the cyber realm.

The limitation of the Notary's obligation to maintain the confidentiality of the deed including the personal data of the parties in relation to the notary's right to deny which is based on the UUJN. In the position of being a witness in a civil case as regulated in Article 1909 paragraph (3) of the Civil Code (KUHPerdata), a Notary can submit a request to be exempted from the obligation to provide testimony because the UUJN regulates Notaries to always maintain the confidentiality of the processes and products they make. A Notary has an obligation to deny not in the notary's own interests but in the interests of the party who has given his trust when making the Deed to the Notary. This is also regulated in Article 1909 paragraph (2) letter 3e of the Civil Code which states that "Anyone who, due to his position, job or position from the Law, is given the obligation to maintain confidentiality, but only with regard to matters whose knowledge is entrusted to him". The authorities cannot force a Notary, among other things, because the minutes of the deed are under the authority and protection of the Notary at the Notary's place concerned. This is different when the notary product is moved into electronic media, which can be accessed by anyone even though it requires permission from the related party. At least the Notary is not the only party who can (in quotation marks) control the product.

Based on the perspective of the UUPDP, the regulation regarding the mechanism for protecting personal data contained in electronic deeds uploaded in the Cyber Notary electronic system is very essential. This is because the essence of the purpose of imposing the Notary's obligation is to maintain the confidentiality of all information including personal data contained in the deed. The legal vacuum governing the protection of personal data in the Cyber Notary electronic system will cause uncertainty in the protection of personal data of the parties contained in the deed and has the potential to be misused by third parties. This means that if there is a third party in the Cyber Notary system, it is included in the violation of the principle of confidentiality because the Notary directly provides access to the deed to a third party in Cyber Notary which has not been regulated/determined in the UUJN as a lex specialist regulating the Notary Position. If there is data misuse or data leakage due to the actions of a

third party, then because only the notary is bound by the obligation to maintain confidentiality, the notary is placed in the position of being blamed because in the UUJN only the notary is regulated in imposing sanctions for violating the principle of confidentiality. The existing legal relationship is only between the parties and the notary.

From the explanation above, it proves that the state has actually regulated the protection of personal data including regulating its obligations, sanctions and other related regulations. However, of the many regulations ranging from UUJN, Criminal Code, Civil Code, UUPDP, ITE Law to Permenkumham No. 17 of 2021, none of these regulations regulate Cyber Notary, either Notaries in maintaining the principle of confidentiality in relation to Cyber Notary or the involvement of third parties who act as organizers of the Cyber Notary electronic system.

Based on the explanation above, it can be said that UUJN only provides another authority for Notaries, namely to certify transactions carried out electronically, namely Cyber Notary, without further regulating the extent of the notary's authority and how the form of implementation of a Cyber Notary concept. Notaries as public officials who are obliged to keep the contents of the deed confidential must obtain legal protection when the Notary concerned must upload the deed he made into an electronic system. The unclear regulations regarding Cyber Notary have caused many problems in implementing the Cyber Notary regulation concept. Including the issue of protecting the personal data of the parties listed in the uploaded deed. Therefore, there needs to be a law on Cyber Notary that provides legal certainty regarding the limitations of the confidentiality principle required of notaries before Cyber Notary is implemented further.

3.3. Solutions for Data Protection of the Parties

Following the current era of Society 5.0 with all the needs of bureaucratic and legal services to the community, requires the position of Notary to be more able to adapt to the existing system. Openness to technology is needed so that Society 5.0 becomes an opportunity, namely helping it to accelerate in the fields of administration, archiving and sending data.(Talita & S, 2023).

Of course, in the rapid development of technology, there is a relationship between the notary profession and the development. Until then a concept of Cyber Notary emerged. The applicable concept and cyber space must be utilized in creating optimal services. The use of technology in notary services can increase effectiveness and efficiency, to reduce existing operational costs so that it can increase the competitiveness and quality of notaries in the digitalization era. The focus of the concept can be divided into at least two parts. First, is the authority section and the second part is technology. In addition, there are factors that influence it, namely developments in the economic sector. Aspects of the dynamic economic situation demand that

notaries be able to process agreements, so to support the speed of these needs, information technology facilities are used.(Syamsir; Rahmi 2019). In the aspect of authority, "Notaries have the authority to make authentic Deeds regarding all acts, agreements and stipulations which are required by statutory regulations and/or which are desired by interested parties to be stated in authentic Deeds, guarantee the certainty of the date of making the Deed, store the Deed, give grosse, copy and quotation of the Deed, all of this as long as the making of the Deed is not also assigned or excluded to another official or other person as determined by law."

One of the main challenges in implementing cyber notary in Indonesia is the lack of legal certainty that regulates in detail the mechanism for implementing Cyber Notary, including data protection rules for the parties contained in notarial deeds made electronically that are uploaded to the Cyber Notary electronic system. This makes the application of Cyber Notary in terms of making authentic deeds with electronic media still very difficult to implement in Indonesia because there is no legal certainty for notaries and parties involved in electronic transactions. UUJN, whose status is lex specialis that regulates the Notary Position, in reality does not regulate Cyber Notary. UUJN only mentions Cyber Notary as another authority held by a Notary.

In the UUJN which is related to regulating the data of the parties, it can refer to the obligation to maintain confidentiality. A notary is a party that plays a role in storing personal data, because in the deed he makes there is an obligation for the parties to include their personal data/identity.(Wijayanti and Ariawan 2021). The consequences that arise due to violations regarding the confidentiality of deeds and their contents are in the provisions of UUJN Article 16 paragraph (11) which states that a Notary who commits a violation (does not keep the deed and its contents confidential) will receive sanctions/punishments in the form of a written warning, temporary dismissal for a specified period of time, and finally honorable dismissal or dishonorable dismissal. As stipulated in the provisions of Article 16 paragraph (12) of UUJN which explains that in addition to administrative sanctions, there are also sanctions regulated by law in the form of compensation submitted by the parties to the Notary due to suffering losses.

In addition, Cyber Notary regulations that regulate personal data protection can refer to current regulations. First, refer to the UUPDP. That the procedure for implementing cyber notary follows the provisions for making deeds manually and follows the provisions for processing Personal Data as stated in Articles 16 to 18 of the UUPDP. Legal protection for the security of Cyber Notary data in the event of negligence on the part of the Notary is regulated in Article 46 and Article 47 of the UUPDP. Meanwhile, legal protection for the security of cyber notary data from cyber crime is regulated in Articles 67 and 68 of the UUPDP(Najib 2023).

Second, referring to the ITE Law, to be used as a legal basis for the implementation of Cyber Notary. Article 5 paragraph (1) of the ITE Law recognizes the validity of electronic documents and electronic signatures in which the use of technology in notary services can increase efficiency and reduce operational costs which can ultimately increase the competitiveness of notaries. Article 1 number 12 of the ITE Law explains "An electronic signature is a signature consisting of electronic information that is attached, associated or related to other electronic information used as a means of verification and authentication. An electronic signature is one of the personal data of the parties that is affixed to the deed.

Based on the Dynamic Integration Theory in Cyber Law, data security and privacy are important aspects in the implementation of Cyber Notary in Indonesia. Notaries must ensure that the electronic data they manage is protected from cyber security threats through the implementation of end-to-end encryption technology and adequate security infrastructure. This is in line with the principles of regulation and technology integration, where cyber law regulations must be drafted by adjusting to the latest technological developments and the needs of society to create a progressive and responsive legal framework.

In addition, the readiness of technological infrastructure is also an important factor in the implementation of Cyber Notary. The government through the Ministry of Communication and InformationTechnology (Kominfo) must work together to facilitate infrastructure and security systems, but further efforts are needed to ensure that all notaries have access and the ability to use this technology effectively by increasing the resources and quality of notaries in using technology.

This is in line with the principle of a multidisciplinary approach in the Dynamic Integration Theory as a form of collaboration between policy makers, technology experts, legal policies implemented by practitioners such as notaries, the creation of comprehensive regulations is needed. The implementation of Cyber Notary also requires a paradigm shift among notaries and the community. The sociological constraint is that many notaries are still accustomed to conventional working methods and do not want to switch to a digital system. Therefore, efforts such as intensive socialization and training are needed to improve the understanding and skills of notaries in utilizing information technology. With adequate training, notaries can be better prepared to face challenges and take advantage of existing opportunities. This is in line with the principle of community participation in the Dynamic Integration Theory, where the active involvement of notaries and the community of technology users is essential.

Thus, the implementation of cyber notary in Indonesia requires close integration between regulation, technology, and community participation,

following the application of the principles of Dynamic Integration Theory in cyber law. Collaboration between stakeholders, namely between the government, notaries, and other related parties is very important to prioritize in order to realize the harmonization of the implementation of Cyber Notary. The parties or parties, as interested parties, together with notaries who provide services are expected to be able to overcome this problem with all the challenges that exist, and take advantage of the opportunities available because it can provide optimal benefits to the community. Akbar Panjang Syahril also emphasized the importance of understanding the rights and obligations of information technology users, as well as the sanctions that can be imposed if a violation occurs. This is relevant to the implementation of cyber notary which must also pay attention to aspects of data security and privacy. By understanding the regulations, notaries can be better at carrying out their duties and avoiding legal risks that may arise.

Information security risk management in the notary sector is an increasingly critical issue as global digitalization accelerates. Notaries handle a large amount of sensitive personal data, including identity documents, property records, wills, powers of attorney, and electronic signatures. Poor security makes this data vulnerable to leakage, theft, and misuse, thereby violating the right to privacy. In addition, notaries face increasing threats from hacking, viruses, and computer attacks that can paralyze operations, cause financial losses, and undermine trust. These growing challenges underscore the urgent need to reevaluate and strengthen the legal framework for information security risk management for notaries.

Existing regulations, such as UUJN and UU ITE, provide a starting point but still require more detailed and clear implementing regulations. In addition, the readiness of technological infrastructure and human resources are also key factors in the success of Cyber Notary implementation. With close cooperation between the government, notary associations, and other related parties, as well as increased socialization and training, it is hoped that cyber notaries can be implemented effectively and provide optimal benefits for the community and business world in Indonesia.

Some ways that can be done to ensure the security of data for the parties include:

Effortenforcement of strict civil penalties for non-compliance with security standards, commensurate with the severity of the violation, to effectively deter negligent handling of data. The EU's tiered sanctions approach sets a good precedent for imposing large fines for major violations, while avoiding excessive penalties for minor incidents.

Efforts to build transparency mechanisms, such as centralized public records, to track events in real time for notaries, thus requiring the feasibility of platforms to support such activities so that they are mandatory as implemented in the UK.

Furthermore, requiring independent third-party audits and regular integration testing to assess the notary information security summary. Checks on security and technical compliance must be carried out efficiently. The General Data Protection Regulation in the European Union requires data protection impact assessments for high-risk processing, such as the use of personal data by notaries.

Efforts to develop detailed and specific security regulations for the notary sector that translate common standards into practical protocols that are appropriate for the notary's general technology and data environment. The California precedent illustrates the importance of guidelines tailored to a universal approach. This requires adequate software and hardware, and subsidies can help support the development of such tools.

Implementation of public or private collaborations between policy makers, professionals, academics, technology experts, and information security experts to develop well-informed regulatory measures and cost-effective best practices tailored to notary risk precognition.

In addition, several complementary non-regulatory initiatives can support secure notary data management including issuing easy-to-use tools to improve notary quality on best practices, providing subsidized security consulting services and technology audits to enable notaries to identify and address vulnerabilities to the security of parties' data. Creating a secure digital platform for notaries to manage identity and records, rather than relying on stand-alone or public systems.

Research into technologies such as AI-enabled adaptive security systems that automatically respond to the evolving threat landscape. Development of standard methodologies for assessing information security risks in notarial practice to identify regulatory intervention priorities. In practice, in storing Notary protocols (archives), Notaries can utilize cloud computing services such as Google Drive and Cloud to store scanned protocols so that they are easy for Notaries to upload and download them again.

This proves that Notaries have used a system that stores large-scale data (big data), a development of the Industrial Revolution 4.0. However, on the other hand, with the use of cloud services that facilitate protocol storage, there are risks that Notaries must pay attention to regarding the protection of their protocol data in the event of a data leak or unauthorized access. In addition, society has now developed towards society 5.0, where society is faced with technology that accesses virtual space as well as physical space. In society 5.0,

technology relies on big data and AI to support human work. Therefore, along with the rapid development of technology, the Notary profession needs to keep up with this rapid development.

The legal certainty of storing Notary protocols digitally is currently still a grey area for Notaries because there are no implementing regulations for storing Notary protocols digitally. In terms of effectiveness, storing Notary protocols digitally will make it easier for Notaries in Indonesia and the public. It is necessary to examine whether the transition from conventional Notary protocols to digital/electronic Notary protocols has the same evidentiary power as the conventional style. In line with the development of current information technology, evidence in civil cases does not only include written evidence. The civil trial process has developed with the introduction of several pieces of evidence that are not regulated by law, such as photocopies, portraits, voice and image recordings, faxes, scans, flash disks, electronic mail (email), witness examination using video teleconferencing, short message service systems (SMS or short message service), and other electronic data/documents that can be included.

There is evidence in electronic form, Michael Chissick and Alistair Kelman stated that there are three types of evidence created by computers, namely: (Hasanah 2014):

1. Real Evidence is objective evidence that includes analysis or calculations performed by a device through software applications and the receipt of information from other devices.

2. Evidence in the form of evidence as output from a device in the form of documents or data produced by the device from documents or data inputted by humans.

3. Derived evidence. Derived evidence combines objective evidence with information provided by humans to the computer to form a composite data set, which contains the device's analysis with human-entered data.

In short, the Solutions combine the needs of notaries, facilities and infrastructure, and collaboration between the government and the private sector, showing the potential to strengthen cyber risk management in this sector, especially in the security of data for the parties. Continuous multi-stakeholder engagement can provide input for policy design.

Non-regulatory initiatives such as education, subsidies and public-private partnerships can complement the less well-developed legal measures. Further empirical research is needed to map the threat landscape facing notaries and measure the impact of policies to inform legal reforms related to the security of parties' data.

Thus, effective and efficient storage of data of the parties such as Notary Protocols and other Notary documents can be more easily accessed by storing deeds electronically, as one form of implementation of the Cyber Notary concept in the future. The use of computer devices and networks for Notaries is no longer a strange thing because Notaries currently make deeds and store records and data needed to support the efficiency of Notary performance in providing services to the Community, so the implementation of Cyber Notary with the concept of data security must be implemented. Regulations regarding the protection of personal data protect and guarantee the basic rights of citizens, provide legal certainty to citizens, and protect Notaries in carrying out their duties.

4. CONCLUSION

The solution to protecting the data of the parties is to carry out risk management planning related to information security as something that must be prepared carefully in the implementation of Cyber Notary. There are several efforts that can guarantee the security of the data of the parties, including efforts to develop detailed and specific security regulations in the notary sector that translate general standards into practical protocols that are in accordance with the technological environment and notary data in general, requiring independent third-party audits and routine integration testing and implementing public or private collaboration between policy makers, professionals, academics, technology experts, and information security experts to develop well-informed regulatory measures and cost-effective best practices that are tailored to the notary's risk precognition. The government in implementing Cyber Notary must carry out risk management planning and guarantee information security in the Cyber Notary electronic system in collaboration with academics, notary practitioners and external parties who can support the success of risk management planning.

5. REFERENCES

Journals:

Adjie, Habib; Sri Agustini. 2022. "Kode Etik Notaris Menjaga Isi Kerahasian Akta Yang Berkaitan Hak Ingkar Notaris (UUJN Pasal 4 Ayat 2)." *Hukum dan Kenotariatan* 6(1).

Hasanah, H. 2014. "Aspek Hukum Pidana Cybersquating Yang Menimbulkan Kerugian Terhadap Pemilik Nama Domain Asli Dalam E-Commerce." *Majalah Ilmiah Unikom* 12(2). https://ojs.unikom.ac.id/index.php/jurnal-unikom/article/download/24/24/ .

Hendrik Handoyo Lugito, & Nynda Fatmawati Octarina. 2021. "Independence of Notary PPAT As Bank Partner." *YURISDIKSI: Jurnal Wacana Hukum Dan Sains,* 16(1). https://yurisdiksi.unmerbaya.ac.id/index.php/yurisdiksi/article/view/87.

Hildatul Insyiroh, & Nynda Fatmawati Octarina. 2024. "Kekuatan Tanda Tangan Elektronik Dalam Konsep Cyber Notary Menurut Presfektif Permen Kominfo Nomor

11 Tahun 2022." *Doktrin:Jurnal Dunia Ilmu Hukum Dan Politik,* 2(2). https://journal.widyakarya.ac.id/index.php/Doktrin-widyakarya/article/view/2851.

Isa Anshari Arif, & Nynda Fatmawati Octarina. 2021. "Urgency of Cyber Notary Application In The Pandemic of Covid-19 For The Need of Authentic Deed." *YURISDIKSI : Jurnal Wacana Hukum Dan Sains,* 16(1). https://yurisdiksi.unmerbaya.ac.id/index.php/yurisdiksi/article/view/58.

Isnaini, Hatta, and Wahyu Utomo. 2019. "The Existence of the Notary and Notarial Deeds within Private Procedural Law in the Industrial Revolution Era 4.0." *International Journal of Innovation, Creativity and Change* 10(3): 128–39.

Isnaini, Hatta, and Hendry Dwicahyo Wanda. 2017. "Prinsip Kehati-Hatian Pejabat Pembuat Akta Tanah Dalam Peralihan Tanah Yang Belum Bersertifikat." *Jurnal Hukum Ius Quia Iustum* 24(3): 467–87. http://journal.uii.ac.id/IUSTUM/article/view/8218.

Maryogi, Maryogi. 2023. "Pertanggungjawaban Pidana Pihak Terafiliasi Pada Pidana Perbankan." *Jurnal Ilmiah Publika* 11(1): 188. https://jurnal.ugj.ac.id/index.php/Publika/article/view/8219.

Merlyani, D., Yahanan, A., & Trisaka, A. 2020. "Kewajiban Pembacaan Akta Otentik Oleh Notaris Di Hadapan Para Pihak Dengan Konsep Cyber Notary." *Repertorium: Jurnal Ilmiah Magister Kenotariatan* 9(1). http://journal.fh.unsri.ac.id/index.php/repertorium/article/view/358/244 .

Najib, A. 2023. "Perlindungan Hukum Keamanan Data Cyber Notary Berdasarkan Undang-Undang Perlindungan Data Pribadi." *Acta Diurnal Jurnal Ilmu Hukum Kenotariatan* 7(1). http://jurnal.fh.unpad.ac.id/index.php/acta/issue/archive .

Pangesti, Shinta, Grace I Darmawan, and Cynthia P. Limantara. 2021. "The Regulatory Concept of Cyber Notary in Indonesia." *Rechtsidee* 7. https://rechtsidee.umsida.ac.id/index.php/rechtsidee/article/view/701.

Putri, R. N. 2017. "Konsep Cyber Notary Dalam Perubahan Undang-Undang Jabatan Notaris Sebagai Hasil Program Legislasi Nasional." Universitas PAdjajaran. https://www.researchgate.net/publication/321994757_Konsep_Cyber_Notary_Dalam_Perubahan_Undang-Undang_Jabatan_Notaris_Sebagai_Hasil_Program_Legislasi_Nasional .

Samudera, Satrio Arung; Saidin; Saihaan Rudy Haposan. 2021. "Konsep Cyber Notary Dalam Perspektif Asas Tabellionis Officium Fideliter Exercebo Menurut Peraturan Perundang-Undangan Di Indonesia." *Jurnal Ilmu Sosial Dan Pendidikan (JISIP)* 1(2). https://jurnal.alazhar-university.ac.id/index.php/normatif/article/view/96.

Setiawan, Nurwanty, and Nynda Fatmawati Octarina. 2022. "Legal Uncertainty Over Notary Protocols in Law No. 43 of 2009." *Journal of Law and Legal Reform* 3(4): 543–66. https://journal.unnes.ac.id/sju/index.php/jllr/article/view/58654.

Shodiq, Achmad. 2022. "Problems of Law Enforcement of Notary Code of Ethics in the Digital Era." *Jurnal Justisia : Jurnal Ilmu Hukum, Perundang-undangan dan Pranata Sosial* 7(2): 537. https://jurnal.ar-raniry.ac.id/index.php/Justisia/article/view/15773.

Syamsir; Rahmi, Elita; Yetniwati. 2019. "Prospek Cyber Notary Sebagai Media Penyimpanan Pendukung Menuju Profesionalisme Notaris." *Recital Review* 2(1). https://online-journal.unja.ac.id/RR/article/view/7458.

Utomo, Hatta. 2021. "The Validity of A Notarial Deed Created Virtually as a Supporting Facility For Economic Activities During The Covid-19 Pandemic." In *Proceedings of the 1st Tidar International Conference on Advancing Local Wisdom Towards Global Megatrends, TIC 2020, 21-22 October 2020, Magelang, Jawa Tengah, Indonesia*, EAI. http://eudl.eu/doi/10.4108/eai.21-10-2020.2311904.

Wicaksono, R. Budi Prabowo. 2023. "Kewajiban Notaris Dalam Menjaga Data Pribadi Secara Digital Persepektif Undang-Undang Perlindungan Data Pribadi Indonesia." *Otentik's: Jurnal Hukum Kenotariatan* 5(2): 208–26. https://journal.univpancasila.ac.id/index.php/otentik/article/view/5015.

Wijayanti, Adinda Ari, and I Gusti Ketut Ariawan. 2021. "Upaya Perlindungan Terhadap Identitas Para Pihak Dalam Praktik Cyber Notary." *Acta Comitas* 6(03): 679. https://ojs.unud.ac.id/index.php/ActaComitas/article/view/73452.

Books:

Adjie, H. (2011). *Merajut Pemikiran Dalam Dunia Notaris & PPAT*. PT Citra Aditya Bakti.

Alwesius. (2018). *Dasar-Dasar Teknik Pembuatan Akta Notaris*. LP3H INP Jakarta.

Makarim, E. (2013). *Notaris dan Transaksi Elektronik, Kajian Hukum tentang Cybernotary atau Electronic Notary* (2nd ed.). Rajawali Press.

Marzuki, P. M. (2010). *Penelitian Hukum*. Kencana Prenada Media Group.

Utomo, Hatta Isnaini Wahyu. 2020. *Memahami Peraturan Jabatan Pejabat Pembuat Akta Tanah*. Jakarta: Kencana.

Internet:

Fardhian. (2014). *Legalisasi Dokumen Publik dan Transaksi Elektronik*. http://lkht.org/ diskusiterbuka-cybernotary-5-februari-2014/

Regulation:

The 1945 Constitution (UUD) and Amendment Number - concerning the 1945 Constitution

Criminal Code

Civil Code

Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Electronic Information and Transactions

Law No. 27 of 2022 concerning Protection of Personal Data

Law No. 2 of 2014 concerning Amendments to Law No. 30 of 2004 concerning the Position of Notary