

Reconstructing legal protection against the risk of data misuse in the issuance of electronic land documents

Johamran Pransisto, Sakinah Putri Rahayu

Faculty of Law, Institut Ilmu Sosial dan Bisnis Andi Sapada, Indonesia

DOI: <https://doi.org/10.66856/ijl.2026.12.3.12295>

Corresponding Author: Johamran Pransisto

Abstract

The digitization of land registration through the issuance of electronic land documents has brought changes in the management of physical data, juridical data, and personal data of land rights holders. These changes support service efficiency and administrative order, but at the same time raise issues regarding data security, information access limits, and accountability for data misuse in electronic systems. This study aims to analyze the problems of personal data protection in the issuance of electronic land documents and formulate a reconstruction of legal protection that can maintain a balance between the principle of land registration publicity, legal certainty of land rights, and the privacy rights of data holders. This research uses normative legal methods with a statutory approach and a conceptual approach. Primary legal materials in the form of regulations in the field of agrarian law, land registration, electronic systems, and personal data protection are analyzed qualitatively-prescriptively through grammatical, systematic, and teleological interpretations. Research shows that existing arrangements have provided a basis for the issuance of electronic land documents and personal data protection, but have not adequately regulated the classification of land data, access procedures based on legal interests, and institutional accountability mechanisms for data misuse incidents. Legal protection reconstruction needs to be directed at proportional access arrangements, strengthening data change control, recording audit trails, assessing the impact of data protection, and redressing for aggrieved rights holders.

Keywords: Electronic land documents, personal data protection, land registration, data misuse, electronic certificates

Introduction

Land registration plays an important role in ensuring legal certainty over land ownership and ownership. Through land registration, the state records data on land parcels, rights holders, changes in rights, and burdens attached to land.^[1] The recording does not only meet administrative needs, but is the basis for the community to prove their legal relationship with a piece of land. Therefore, the accuracy of data and the security of land documents are an inseparable part of the protection of land rights. Government Regulation Number 24 of 1997 concerning Land Registration places land registration as an instrument to provide legal certainty and protection to land rights holders, apartment units, and other registered rights.^[2]

The development of information technology has driven changes in the way the state organizes land services. Documents that were previously managed in the form of land books, deeds, deeds, and physical certificates began to be integrated into electronic systems.^[3] These policies are regulated, among others, in the Regulation of the Minister of Agrarian and Spatial Planning/Head of the National Land Agency Number 3 of 2023 concerning the Issuance of Electronic Documents in Land Registration Activities. The implementation of electronic documents is directed to support more orderly, fast, and integrated services. In practice, digitization can also reduce dependence on physical archives that are prone to damage, loss, or difficulty in tracing. However, moving documents into an electronic system does not necessarily eliminate legal problems. The form of risk actually changes, from the risk of damage to physical documents to the risk of illegal

access, leakage, unauthorized data changes, and misuse of information.^[4]

The data managed in the land registration system has a different character than ordinary administrative data. Physical data describes the location, boundaries, area, and conditions of land parcels. Juridical data describes the legal status of land parcels, the identity of rights holders, the rights of other parties, and the various burdens attached to them. Both types of data determine the clarity of the relationship between a person and the land they control or own. When physical data and juridical data are managed electronically, they are not only of important value to land administration, but also have high economic and strategic value. Errors or changes in data regarding land area, name of rights holder, status of rights, or records of encumbrances can raise problems that are much larger than administrative errors, including disputes, economic losses, and uncertainty over the status of rights.^[5]

In this context, land data is closely related to the protection of personal data. The land registration process requires the applicant to submit various identity information, such as name, address, identity number, and documents that show the basis of land tenure or ownership. The information is then processed, stored, updated, and displayed through the land service.^[6] This series of activities is included in the definition of personal data processing as regulated in Law Number 27 of 2022 concerning Personal Data Protection. This law stipulates that the processing of personal data includes activities ranging from the acquisition and collection to the deletion or destruction of data. Therefore, the implementation of electronic land documents is not

enough only based on the need for service efficiency, but must also fulfill the obligation to maintain security, confidentiality, and the use of data in accordance with legitimate purposes

The issue of data protection in electronic land documents is becoming increasingly important because the data can be used for various purposes outside of land registration services. Information regarding the identity of the rights holder, the location of the land, the area of the field, the status of the right, and the history of the transfer of rights has the potential to be misused for fraud, identity forgery, asset mapping, or other actions that can harm the rights holder.^[7] Risks can also arise from parties outside the institution through cyberattacks, but they are not limited to the possibility of occurring from within the institution through the use of access that exceeds authority. Unauthorized data leaks or alterations not only violate the right to privacy, but can also disrupt legal certainty over the land. In the event of a failure to protect personal data, the data controller is required to provide written notice to the personal data subject and the authorized institution. This obligation indicates that data security is the legal responsibility of the system operator, not just an internal technical issue.^[8]

Another problem lies in the relationship between the principle of publicity in land registration and the right to confidentiality of personal data. Land registration requires information disclosure so that interested parties can know the physical and juridical state of a land parcel before taking legal action, such as buying and selling, encumbering of dependent rights, or applying for financing. However, such disclosure cannot be interpreted as unlimited access to all rights holders' information.^[9] Government Regulation No. 24 of 1997 concerning Land Registration distinguishes between physical data and juridical data that is open to interested parties with a list of names that can only be accessed by certain government agencies for the implementation of their duties. This regulation shows that land law has recognized the need to limit information that can reveal a person's personal relationship with his or her land assets

In electronic systems, the problem becomes more complicated because a single access can result in a copy of data that is easy to move, distribute, and reuse. The boundary between information that needs to be disclosed to ensure the certainty of transactions and information that must be kept confidential needs to be formulated more clearly.^[10] If the principle of publicity is applied too broadly, electronic systems can open up space for the collection of personal data and the mapping of assets disproportionately. On the other hand, restrictions that are too strict can also hinder parties with legal interests from obtaining the necessary information.^[11] Therefore, regulations regarding access to electronic land data must be able to distinguish the type of data, the purpose of use, the identity of the user, and the level of legal interest underlying the access request.

Based on these issues, this study examines the legal protection against the risk of data misuse in the issuance of electronic land documents. This study is important to assess whether the applicable legal arrangements are sufficient to protect land rights holders from the risk of unauthorized access, data leakage, information manipulation, and data use

outside the purpose of land services. The research is also directed to find a common ground between the need for digitization of land services, the principle of openness in land registration, and the obligation to protect personal data. The results of the research are expected to provide an argumentative basis for strengthening the regulation and governance of electronic land documents that are not only efficient, but also safe, accountable, and in favor of the protection of data holders' rights.

Method

This study uses a normative legal method by placing the issue of data misuse in the issuance of electronic land documents as an issue regarding the adequacy and integration of norms.^[12] The analysis is directed at the relationship between the principle of publicity in land registration, the obligation to protect personal data, and the responsibility of electronic system operators. The legislative approach is used to test the suitability and possible regulatory vacancies in Law Number 5 of 1960 concerning Basic Regulations on Agrarian Principles, Government Regulation Number 24 of 1997 concerning Land Registration, Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, Law Number 27 of 2022 concerning Personal Data Protection, and Regulation of the Minister of Agrarian and Spatial Planning/Head of the National Land Agency Number 3 of 2023 concerning the Issuance of Electronic Documents in Land Registration Activities. This research also uses a conceptual approach to examine the principles of publicity, limitation of data processing purposes, proportionality of access, data security, and accountability of data controllers as a basis for building a legal protection model. The legislative approach allows an assessment of the consistency between rules, while the conceptual approach is used to build arguments when positive arrangements have not provided operational answers to the legal issues faced.

The primary legal material in the form of laws and regulations is analyzed together with secondary legal materials, which include journal articles, books, doctrines, and previous research on electronic land registration, personal data protection, and electronic system governance. Legal materials are collected through literature studies and documentation on official sources and relevant scientific publications. The analysis is carried out qualitative-prescriptive through grammatical, systematic, and teleological interpretations. Grammatical interpretation is used to understand the scope of norms regarding data access and processing; systematic interpretation is used to read the relationship between land law, the PDP Law, and electronic system law; while teleological interpretation is used to assess whether the applicable norms are still in line with the purpose of land registration, which is to ensure legal certainty without ignoring the privacy rights of rights holders. From this process, the research identified weaknesses in the regulation of electronic land data access and formulated a verifiable legal interest-based multi-level access model, as a form of strengthening protection against the risk of data misuse.

Result and Discussion

1. Problems of Personal Data Protection in the Issuance of Electronic Land Documents

The electronic issuance of land documents is one of the consequences of changes in public service patterns that

increasingly rely on digital technology.^[13] In the field of land, this change is important because land documents not only function as administrative archives, but also as a basis for proving the legal relationship between a person and a specific piece of land. Digitization through the Regulation of the Minister of Agrarian and Spatial Planning/Head of the National Land Agency Number 3 of 2023 concerning the Issuance of Electronic Documents in Land Registration Activities is basically intended to speed up services, improve administrative order, and improve the security of document storage. However, the convenience generated by electronic systems also brings new problems, especially when land data can be accessed, moved, and processed much faster than in physical archive-based systems.^[14]

Before the implementation of electronic systems, the management of land documents relied more on land books, surveys, warkahs, and certificates in physical form. The system was not completely free from risks, such as loss, damage, forgery, or disorderly storage of archives. However, access to data at that time was relatively more limited because one had to visit the land office, follow administrative procedures, and face it directly with the authorized officers. In electronic systems, these physical restrictions were reduced.^[15] Data can be accessed through a network and processed in a single connected system. Therefore, the problem no longer lies only in the security of documents, but also in who can access the data, the extent to which the data can be used, and how the state ensures that such access does not exceed the interests of land services.

This change actually has a normative basis in Government Regulation Number 24 of 1997 concerning Land Registration. Article 35 paragraph^[5] opens up the possibility of storing and presenting land registration data using electronic equipment in stages. This provision shows that the use of technology in land administration is not completely new in the Indonesian legal system. However, when electronic technology functions not only as a storage medium, but as the basis for document issuance and data management in an integrated manner, the need for legal protection becomes greater.^[16] Electronic documents must still be able to ensure the integrity of the data, clarity of its origin, and the accountability of the officials or institutions that issue it. If this aspect is not maintained, the purpose of land registration to provide legal certainty can be disrupted.

In land registration, physical data and juridical data have a very decisive position.^[17] Physical data describes the location, boundaries, and area of land plots, including the existence of buildings on it. Meanwhile, juridical data explains the legal status of land, rights holders, rights of other parties, and the burdens attached to the land. These two types of data are the basis for determining land objects and parties who legally own or control land rights.^[18] Therefore, when the data is stored in an electronic system, its protection cannot be understood as limited to the protection of files or databases. Land data protection is directly related to the protection of a person's civil rights. Changes in one data regarding the name of the right holder, the area of the land plot, or the status of the encumbrance can cause serious legal consequences, including ownership disputes and economic losses.^[19]

Land data also cannot be separated from the personal data of rights holders. In the land registration process, a person submits identity, address, population documents, grounds of

rights, and other information that connects him or her with a piece of land. When such data is collected, stored, updated, or displayed through an electronic system, the entire process falls into the category of personal data processing. Law Number 27 of 2022 concerning Personal Data Protection includes the acquisition, collection, processing, storage, repair, update, appearance, transfer, disclosure, deletion, and destruction as a form of personal data processing. Thus, the issuance of electronic land documents cannot be viewed solely as a public service in the agrarian sector; it is also a personal data processing activity that must comply with the principles of prudence, security, and accountability.

The first risk that needs to be considered is access to data by parties who do not have authority. In electronic systems, access does not always mean intrusion by outside parties. Abuse can also occur from within the institution, for example when employees or parties who obtain technical access use data for purposes unrelated to their duties. Information about land owners, asset locations, land area, rights status, and transition history has high economic value.^[20] If this information is obtained by an unauthorized party, it can be used to map a person's assets, look for unhealthy transaction opportunities, or even build a fraud plan. Therefore, it is the duty of the data controller not only to provide a system that can be used, but also to ensure that any access is justified based on clear legal duties, authority, and interests

The next problem is data leakage. In the context of electronic land documents, data leaks do not always have to be understood as large-scale hacking. Leaks can arise from seemingly simple actions, such as the use of a shared account, sending documents through insecure communication media, storing copies of documents on personal devices, or disclosing data to parties who do not have a legal relationship with the parcel of land. Once the data is dispersed, control of the data becomes very difficult to do because copies can be made and moved indefinitely. This is in contrast to physical documents, which usually have space and quantity limits. Law Number 27 of 2022 concerning Personal Data Protection places data protection failures as events that give rise to a legal obligation for data controllers to deliver written notices to data subjects and authorized institutions no later than 3×24 hours. These provisions indicate that data protection does not stop at prevention, but also demands openness and remedial measures when failures occur.^[21]

In addition to leakage, data changes or manipulation are also problems that cannot be ignored. In land administration, data changes can be legally made in the event of a transfer of rights, division of land parcels, merger of fields, imposition of dependent rights, or other legal events. However, these changes must go through clear procedures, verification, and authority. In electronic systems, data changes can occur quickly and are not always easily recognized by rights holders if the system does not provide an adequate mechanism for notification or record of changes. This risk becomes serious because certificates serve as a powerful means of proof regarding the physical data and juridical data contained in them. If the source data is changed illegally, then the reliability of electronic certificates as evidence can be questioned. Therefore, any changes in data should be traceable, tested for legal basis, and attributed to the officials or users who carried out the action.

Misuse of the identity of rights holders also needs to be placed as a real risk. Identity data matched with land parcel data allows a person to know not only who the rights holder is, but also what assets he owns and where those assets are located.^[22] If such information falls into the hands of irresponsible parties, it can be used to create false documents, apply for services using the identities of others, or arrange transactions that appear to be carried out by legitimate rights holders. In such circumstances, the impact of a personal data breach is no longer limited to the disruption of a person's privacy. Such violations can develop into threats to the possession, ownership, and economic value of land rights. Therefore, identity protection in electronic land systems must be placed as part of preventive protection against possible land crimes.

Another issue that needs to be studied is the use of land data outside the purpose of land registration. Land data has high value for various interests, such as property marketing, business analysis, asset valuation, or community economic mapping. However, this economic value cannot be used as an excuse to expand access and use of data without limits.^[23] The data provided by the community in the land registration process is essentially submitted to meet the needs of services and legal certainty on land. Therefore, the use of data for other purposes must have a clear legal basis and should not be carried out secretly. The principle of limited, specific, lawful, and transparent data processing requires that any use of data is associated with the original purpose for which it was collected. In this way, the right holder still has protection against the possibility that his or her data is used for purposes that have never been approved or never notified before.

It is at this point that the problem arises regarding the relationship between the principle of publicity in land registration and the obligation to maintain the confidentiality of personal data. The land registration system requires openness so that interested parties can know the physical and juridical state of a plot of land. Openness is necessary, for example, to avoid transactions on problematic land, to ascertain the status of rights before buying and selling, or to know the imposition of dependent rights. However, openness should not be interpreted as the freedom to disclose all data about rights holders to anyone. Government Regulation No. 24 of 1997 concerning Land Registration provides space for interested parties to know physical data and juridical data, but at the same time restricts access to the list of names only to certain government agencies in the context of carrying out their duties.^[24]

The restriction on the list of names shows that land law has since its inception distinguished between information that needs to be disclosed to ensure the certainty of transactions and information that has the potential to reveal the personal circumstances of the rights holder. In electronic systems, this distinction must be applied more carefully. If digital access is granted too broadly, the data originally obtained to check the status of a plot of land can be collected, copied, or used to profile a person's assets. This is clearly not in line with the spirit of personal data protection. Therefore, the phrase "interested party" must be interpreted in a limited way, i.e. parties who actually have a legal relationship or a demonstrable need to the land data requested. Access should also be provided as needed, so that the applicant only

obtains information that is relevant to the purpose of his examination, not the entire data of the right holder.

Based on this description, the main problem in the issuance of electronic land documents is not the choice between digitization or data protection. Digitalization is still needed to improve land services and reduce various administrative problems that have arisen in the management of physical documents. The problem is to ensure that the digitization is built with adequate legal protection. Regulatory frameworks are already available through the land registration law, regulations on electronic land documents, and the Personal Data Protection Law. However, all three still need to be translated into more operational arrangements, especially regarding access restrictions, user verification, recording of activities in the system, data storage security, notification in the event of a leak, and recovery for aggrieved rights holders. Without these steps, digitization can improve service efficiency, but at the same time open up new space for the misuse of land data.

2. Reconstruction of Legal Protection against the Risk of Data Misuse in the Issuance of Electronic Land Documents

The issuance of electronic land documents cannot be understood simply as replacing paper certificates with certificates in digital form. This change moves the trust center from physical documents to systems that manage data.^[25] In physical certificates, people can check the authenticity of documents through their forms, signatures, stamps, and accompanying administrative procedures. In electronic certificates, the trust depends on the accuracy of the data in the database, the security of access, the validity of the data change process, and the system's ability to prove that the document was issued by an authorized official. Therefore, the issue of data protection is not on the fringes of the electronic certificate policy. Instead, it determines whether digitization is able to strengthen or otherwise weaken legal certainty over land.

A study conducted by Juliyanti, Dharsana, and Ujianti (2023) shows that digital certificates and analog certificates basically have an equal legal standing, as long as their issuance meets the required elements of authenticity and security. However, this equality of status does not automatically eliminate the problem of protecting rights holders. Electronic certificates store the identity of the rights holder and information about land parcels in a system that can be accessed and processed digitally. When the access mechanism is not carefully designed, the ease of service can turn into the ease of obtaining data about other people's assets. This is where the problem that is often overlooked in the discussion of land digitization lies: the security of certificates is not enough to judge the existence of QR codes or electronic signatures, but also from the system's ability to limit the use of data only for legitimate purposes.^[26]

The reconstruction of legal protection needs to start from a firm distinction between data that is necessary for the sake of publicity and data that must be protected because it relates to the identity of the rights holder. Land registration does require disclosure. Prospective buyers, creditors, or parties who want to take legal action on land need information about the status of the land parcel, the type of rights, the area, and the possibility of imposition of dependent rights. However, this need does not necessarily

mean that the party also needs to know the identity number, residential address, copy of identity documents, or personal history of the rights holder. In this case, the principle of publicity needs to be placed as a principle of functional openness, not total disclosure. Restrictions on access are not an obstacle to legal certainty, but rather a way to ensure that information is provided proportionately according to the purpose for which it is used.

This distinction is in line with the provisions in Government Regulation Number 24 of 1997 concerning Land Registration. Article 34 paragraph ^[1] provides an opportunity for interested parties to find out the physical data and juridical data stored in registration maps, land registers, survey letters, and land books. However, Article 34 paragraph ^[2] limits access to the list of names only to certain government agencies in the context of carrying out their duties. The restriction is important because the list of names can show a person's relationship with the land he or she owns. In the electronic system, the meaning of this provision needs to be further developed. Physical data and juridical data presented to interested parties need to be sorted based on the level of need, while identity data and supporting documents of rights holders must be placed in the category of limited access. ^[27]

Anugrah and Susanti's (2023) research on electronic certificates from the perspective of personal data protection reminds that the digitization of land services expands personal data processing activities by the state. The research places rights holders not only as service users, but also as data subjects who have an interest in the security of their personal information. This perspective is important because the relationship between the community and the Ministry of Agrarian Affairs and Spatial Planning/National Land Agency is not completely equal. The community needs land registration services and at the same time is obliged to submit data to obtain these services. In such a situation, the state cannot only demand that the public trust the system. The state must demonstrate that the system is designed to limit data collection, prevent use outside the purpose of the service, and provide space for rights holders to know how their data is processed. ^[28]

On that basis, authority-based access restrictions need to be a major part of the reconstruction of legal protection. Each user of the system must obtain access in accordance with the functions and needs of his or her duties. The officer receiving the file does not need to have the authority to change the judicial data; the notifying official does not need to access all supporting documents that are not related to the act to be ratified; and the outside party should not obtain more data than is necessary to check the status of the land. ^[29] In practice, this model requires separation of user roles, access level regulation, identity verification, and proof of legal interest for the party requesting information. Such restrictions do not reduce the quality of service. Rather, it prevents access based on curiosity, economic interests, or the use of positions that are not in line with the purpose of land registration.

The next aspect is strengthening authentication and supervision of any data changes. The biggest risk in electronic land documents is not only the possibility of data being stolen, but also the possibility of data being changed without a valid legal basis. Changes in the name of the rights holder, the area of the land plot, the record of

encumbrance, or the history of the transfer of rights can have far greater legal consequences than ordinary data leaks. Therefore, data changes should not be completed through just one administrative stage in the system. Changes that have an impact on the status of rights must go through document checks, verification by different officials, and attestation through traceable electronic signatures. This is in line with the regulation on the use of electronic systems and electronic documents in the Regulation of the Minister of Agrarian and Spatial Planning/Head of the National Land Agency Number 3 of 2023 concerning the Issuance of Electronic Documents in Land Registration Activities (2023).

The existence of an audit trail must also be placed as an element of proof, not solely a technical facility. An audit trail is needed to show who opened the data, when the data was accessed, what part of the data was viewed or changed, and the basis for the action. In land disputes, information like this can determine whether the data changes occurred through legitimate procedures or due to abuse of authority. Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions requires electronic system operators to provide an audit track record of all electronic system implementation activities. This provision provides a strong enough basis to place trail audits as an obligation in the electronic land system, especially since the data managed is related to the assets and civil rights of the community. ^[30]

In addition, data protection must be built from the system design stage. This approach is commonly called privacy by design, which is a perspective that requires privacy protection to be included in the design of services and technology from the beginning, rather than just added when an incident has occurred. In electronic land systems, its application can be seen from the use of limited data displays, partial identity number disguise, restrictions on document downloads, sending notifications when data is accessed or altered, and separation between information that is public and information that is only available to authorized officials. This approach is related to the obligation of personal data controllers to ensure data security through proper technical and operational steps as referred to in Law Number 27 of 2022 concerning Personal Data Protection.

Strengthening preventive protection needs to be followed by a clear accountability mechanism in the event of data leakage or misuse. Law Number 27 of 2022 concerning Personal Data Protection requires personal data controllers to notify personal data protection subjects and authorized institutions no later than 3×24 hours. For electronic certificate holders, this provision is important because delays in information can increase the risk of data being used for adverse actions. The notification must be accompanied by an explanation of the affected data, the cause of the incident, the security measures that have been taken, and the recovery measures available. In the case of land data, remedial measures may include temporary access blocking, checking the history of data changes, correction of manipulated data, and providing administrative assistance to affected rights holders.

Ultimately, the Ministry of Agrarian and Spatial Planning/National Land Agency needs to be firmly positioned as the institution responsible for data

management in electronic land systems. This responsibility cannot stop at the obligation to provide applications or store data on servers. This institution must ensure that data is used according to the purpose of land registration, access is provided on a limited basis, third parties are bound by security obligations, and rights holders are entitled to recovery in the event of losses. A number of studies show that one of the main problems with electronic certificates is that public concerns about data leakage and digital land governance readiness have not been fully addressed. Therefore, it is not enough to reconstruct legal protection by adding security procedures. Reconstruction must clarify institutional responsibility, data holder rights, and legal consequences for any form of data misuse.

Conclusion

The issuance of electronic land documents has gained a legal basis in the Indonesian land registration system, but its regulation has not fully provided adequate protection for the personal data of rights holders. The main problem lies in the unclear boundary between land data that can be opened to meet the principle of publicity and data that must be limited because it contains identity and information about rights holders' assets. In electronic systems, access, copying, transferring, and using data can take place much faster than physical archive-based systems. Therefore, the risk of unauthorized access, leakage, data manipulation, unlawful use of identity, and the use of data outside the purpose of land registration can directly interfere with privacy as well as legal certainty on land rights. These findings reinforce the view that the protection of electronic certificates is not sufficiently measured by the recognition of the form of the document, but must be supported by guarantees of data security and accountable processing governance.

The reconstruction of legal protection needs to be directed at the establishment of land data governance that places ATR/BPN firmly as the controller of personal data. The reconstruction requires the classification of data based on the level of sensitivity, access based on verifiable legal authority and importance, authentication in any data changes, and audit trails that can be used for proof and supervision. This protection must be complemented by an assessment of the impact of data protection on the development of the system, incident notification obligations, easily accessible correction and recovery mechanisms, and administrative, civil, and criminal liability for data misuse. With such a framework, the principle of publicity can still be carried out to ensure the certainty of land transactions, without making the personal data of rights holders as open information that is open and vulnerable to misuse.

References

1. Santoso P. Tinjauan Yuridis Pendaftaran Status Tanah Sertipikat Hak Milik Pada Badan Hukum Yayasan Menurut Undang-Undang Nomor 28 Tahun 2004 Tentang Perubahan Atas Undang-Undang Nomor 16 Tahun 2001 Tentang Yayasan. Diss. Fakultas Sosial Sain, 2024.
2. Vide Pasal 3 Peraturan Pemerintah Nomor 24 Tahun 1997 tentang Pendaftaran Tanah, 1997.
3. Hafidz A, Kamal U. "Urgensi Sertifikasi Tanah Dalam Menjamin Kepastian Hukum Hak Atas Tanah Pasca Peniadaan Alat Bukti Tanah Tertulis Bekas Milik Adat Berdasarkan PP Nomor 18 Tahun 2021." Bookchapter Hukum Dan Lingkungan 1, 2025, 50-85.
4. Vide Peraturan Menteri Agraria dan Tata Ruang/Kepala Badan Pertanahan Nasional Nomor 3 Tahun 2023 tentang Penerbitan Dokumen Elektronik dalam Kegiatan Pendaftaran Tanah, 2023.
5. Vide Pasal 1 angka 6–7 Peraturan Pemerintah Nomor 24 Tahun 1997 tentang Pendaftaran Tanah, 1997.
6. Sormin CA, Masykur MH, Putri CC. "Perlindungan Data Pribadi dan Kaitannnya dengan Asas Publisitas pada Sertifikat Tanah Elektronik." *RechtJiva*, 2025, 86-105.
7. Dharma WS, Perdana S, Moertiono J. "Perlindungan hukum terhadap data pendaftaran tanah yang dilakukan secara elektronik." *Legalitas: Jurnal Hukum*, 2023;15(1):29-39.
8. Vide Pasal 46 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, 2022.
9. Sormin CA, Masykur MH, Putri CC. "Perlindungan Data Pribadi dan Kaitannnya dengan Asas Publisitas pada Sertifikat Tanah Elektronik." *RechtJiva*, 2025, 86-105.
10. Syahril MAF. "Hukum Informasi Dan Transaksi Elektronik." *Eureka Media Aksara*, 2023.
11. Sormin CA, Masykur MH, Putri CC. "Personal Data Protection and Its Relation to the Principle of Publicity on Electronic Land Certificates." *RechtJiva*, 2025, 86-105.
12. Juliardi B, *et al.* Metode penelitian hukum. CV. Gita Lentera, 2023.
13. Rosidin R, Indarti S, Adriadi R. "Analisis Penerapan E-Government Pada Penggunaan Aplikasi Sentuh Tanahku Dalam Meningkatkan Pelayanan Di Kantor Pertanahan (Kantah) Kota Bengkulu." *Innovative: Journal Of Social Science Research*, 2025;5(4):356-370.
14. Vide Peraturan Menteri Agraria dan Tata Ruang/Kepala Badan Pertanahan Nasional Nomor 3 Tahun 2023 tentang Penerbitan Dokumen Elektronik dalam Kegiatan Pendaftaran Tanah, 2023.
15. Yanti N, Wibawanti ES. "Pelaksanaan Perubahan Sertipikat Analog ke Sertifikat Elektronik di Kantor Pertanahan Kabupaten Sleman." *Journal of Syntax Literate*, 2026;11(3):2203.
16. Vide Pasal 35 ayat 5 Peraturan Pemerintah Nomor 24 Tahun 1997 tentang Pendaftaran Tanah, 1997.
17. Suyadi YSH. Menuntaskan pendaftaran tanah sistematis lengkap (PTSL). Sinar Grafika, 2024.
18. Suyadi YSH. Menuntaskan pendaftaran tanah sistematis lengkap (PTSL). Sinar Grafika, 2024.
19. Vide Pasal 1 angka 6–7 Peraturan Pemerintah Nomor 24 Tahun 1997 tentang Pendaftaran Tanah, 1997.
20. Pemuli R, Barkatullah AH. "Liability Of Business Actors For Breaches In Electronic Banking Systems." *Jurnal Hukum Sehasen*, 2024;10(2):535-550.
21. Vide Pasal 46 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, 2022.
22. Santini I, Rifla C, Siregar RML. Hukum Agraria: Sertipikat Tanah Menjadi Bukti Kepemilikan yang Sah atas Tanah. CV Eureka Media Aksara, 2025.
23. Chamdani MC, *et al.* "Tanah dan Ruang untuk Keadilan dan Kemakmuran Rakyat.", 2019.

24. Vide Pasal 4 ayat & Pasal 34 Peraturan Pemerintah Nomor 24 Tahun 1997 tentang Pendaftaran Tanah, 1997.
25. Rahmawati LW, Dewi N, Nurwanti YD. "Analisis Yuridis terhadap Pengaturan Sertipikat Elektronik (E-Sertipikat) atas Tanah Wakaf dalam Sistem Hukum Positif di Indonesia." *Jurnal Hukum Lex Generalis*, 2026, 7(9).
26. Juliyanti NKED, Dharsana IMP, Ujianti NMP. "Perlindungan Hukum Terhadap Pemegang Sertifikat Tanah Digital Dikaitkan Dengan Keamanan Data Pribadi." *Jurnal Preferensi Hukum*, 2023;4(1):91-96.
27. Vide Pasal 34 Peraturan Pemerintah Nomor 24 Tahun 1997 tentang Pendaftaran Tanah, 1997.
28. Shabranah AN, Maskun M, Aswan M. "Sertipikat Elektronik dalam Perspektif Perlindungan Data Pribadi." *UNES Law Review*, 2023;5(4):3648-3657.
29. Astuti D, Saepulloh A, Hafizd JZ. "Pengelolaan Arsip Dokumen Digital Dalam Sistem Informasi Penelusuran Perkara (SIPP) Di Pengadilan Agama Sumber." *PEPAKEM*, 2025;3(2):91-101.
30. Vide Pasal 22 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, 2019.
31. Astuti, Dwi, Asep Saepulloh, and Jefik Zulfikar Hafizd. "Pengelolaan Arsip Dokumen Digital Dalam Sistem Informasi Penelusuran Perkara (SIPP) Di Pengadilan Agama Sumber." *PEPAKEM 3.2* (2025): 91-101.
32. Chamdani, Muchammad Chanif, *et al.* "Tanah dan Ruang untuk Keadilan dan Kemakmuran Rakyat." (2019).
33. Dharma, Wahyu Surya, Surya Perdana, and Juli Moertiono. "Perlindungan hukum terhadap data pendaftaran tanah yang dilakukan secara elektronik." *Legalitas: Jurnal Hukum* 15.1 (2023): 29-39.
34. Hafidz, Ahmad, and Ubaidillah Kamal. "Urgensi Sertifikasi Tanah Dalam Menjamin Kepastian Hukum Hak Atas Tanah Pasca Peniadaan Alat Bukti Tanah Tertulis Bekas Milik Adat Berdasarkan PP Nomor 18 Tahun 2021." *Bookchapter Hukum Dan Lingkungan* 1 (2025): 50-85.
35. Juliardi, Budi, *et al.* *Metode penelitian hukum*. CV. Gita Lentera, 2023.
36. Juliyanti, Ni Kadek Erna Dwi, I. Made Pria Dharsana, and Ni Made Puspasutari Ujianti. "Perlindungan Hukum Terhadap Pemegang Sertifikat Tanah Digital Dikaitkan Dengan Keamanan Data Pribadi." *Jurnal Preferensi Hukum* 4.1 (2023): 91-96.
37. Pemuli, Reihana, and Abdul Halim Barkatullah. "Liability Of Business Actors For Breaches In Electronic Banking Systems." *Jurnal Hukum Sehasen* 10.2 (2024): 535-550.
38. Rahmawati, Lyta Wury, Nourma Dewi, and Yulian Dwi Nurwanti. "Analisis Yuridis terhadap Pengaturan Sertipikat Elektronik (E-Sertipikat) atas Tanah Wakaf dalam Sistem Hukum Positif di Indonesia." *Jurnal Hukum Lex Generalis* 7.9 (2026).
39. Rosidin, Rosidin, Sri Indarti, and Rekho Adriadi. "Analisis Penerapan E-Government Pada Penggunaan Aplikasi Sentuh Tanahku Dalam Meningkatkan Pelayanan Di Kantor Pertanahan (Kantah) Kota Bengkulu." *Innovative: Journal Of Social Science Research* 5.4 (2025): 356-370.
40. Santini, Inawati, Cici Rifla, and Risna Menda Lovinta Siregar. *Hukum Agraria: Sertipikat Tanah Menjadi Bukti Kepemilikan yang Sah atas Tanah*. CV Eureka Media Aksara, 2025.
41. Santoso, Priyo. *Tinjauan Yuridis Pendaftaran Status Tanah Sertipikat Hak Milik Pada Badan Hukum Yayasan Menurut Undang-Undang Nomor 28 Tahun 2004 Tentang Perubahan Atas Undang-Undang Nomor 16 Tahun 2001 Tentang Yayasan*. Diss. Fakultas Sosial Sain, 2024.
42. Shabranah, Andi Nur, Maskun Maskun, and Muhammad Aswan. "Sertipikat Elektronik dalam Perspektif Perlindungan Data Pribadi." *UNES Law Review* 5.4 (2023): 3648-3657.
43. Sormin, Carmenita Angelina, Mohammad Hamidi Masykur, and Cyndiarnis Cahyaning Putri. "Perlindungan Data Pribadi dan Kaitannnya dengan Asas Publisitas pada Sertifikat Tanah Elektronik." *RechtJiva* (2025): 86-105.
44. Syahril, Muh Akbar Fhad. "Hukum Informasi Dan Transaksi Elektronik." *Eureka Media Aksara* (2023).
45. Yagus Suyadi, S. H. *Menuntaskan pendaftaran tanah sistematis lengkap (PTSL)*. Sinar Grafika, 2024.
46. Yanti, Novi, and Erna Sri Wibawanti. "Pelaksanaan Perubahan Sertipikat Analog ke Sertifikat Elektronik di Kantor Pertanahan Kabupaten Sleman." *Journal of Syntax Literate* 11.3 (2026): 2203.
47. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi
48. Peraturan Pemerintah Nomor 24 Tahun 1997 tentang Pendaftaran Tanah
49. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik
50. Peraturan Menteri Agraria dan Tata Ruang/Kepala Badan Pertanahan Nasional Nomor 3 Tahun 2023 tentang Penerbitan Dokumen Elektronik dalam Kegiatan Pendaftaran Tanah