VOL. 5, No. 1, 2025 (111-119)
JIEE:
Jurnal Ilmiah Ekotrans & Erudisi
EISSN: 2777-0184
PISSN: 2797-2259

Personal Data Protection and Disclosure of Information on Public Officials' Diplomas: A Legal Review in Indonesia

Robi Syafwar[1*]
[1] *Department of Law, Universitas Dharma Andalas, Padang, Indonesia*
** Corresponding author: syafwarrobi@gmail.com*

ARTICLE INFO

Article history:
Received 23 June 2025
Received in revised form 25 June 2025
Accepted 30 June 2025

Keyword:
Diploma, Personal Data, Information Disclosure, Legal Protection, Public Officials.

ABSTRACT

The controversy surrounding the authenticity of President Joko Widodo's diploma has sparked a legal debate regarding the status of the diploma as personal data or public information. Diplomas contain identity information protected by Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). Still, as documents related to public office, diplomas can also be considered relevant information for the public interest under Law Number 14 of 2008 concerning Public Information Disclosure (KIP Law). This study examines the legal status of diplomas about personal data protection and public information disclosure, employing normative legal research methods. The results indicate that diplomas are considered general personal data under the PDP Law, so their dissemination requires the consent of the owner. However, the KIP Law regulates limited access to diploma information when it relates to public office. Therefore, a balance is needed between protecting individual privacy and ensuring transparency of information in state administration.

INTRODUCTION

In recent times, the controversy surrounding the authenticity and transparency of public figures' diplomas has resurfaced, evolving into a more fundamental legal debate: whether diplomas constitute public information that must be disclosed or, conversely, constitute personal data that must be protected (Fenster, 2006; Kirchhof, 2024). This tension demonstrates the tug-of-war between demands for transparency and protection of privacy rights in modern state practice.

A diploma is an official document issued by an educational institution as a recognition of academic achievement (Saleh et al., 2019). It contains personal identification details such as name, place and date of birth, identification number, and educational information, which inherently allow for individual identification (Yin, 2023). This inherent nature of the document makes diplomas

[1] *putiannisaa@gmail.com*

vulnerable to misuse if they are distributed without a proper legal basis or control (Hsu et al., 2022; Torres-Hernández & Gallego-Arrufat, 2023).

Normatively, Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) distinguishes specific personal data from general personal data. Based on the elements contained therein, diplomas are classified as general personal data, so their processing and dissemination, in principle, require the consent of the data subject and are subject to the procedural rights of the data owner. This framework emphasizes that access to diplomas cannot be treated as unrestricted free access.

On the other hand, the public's right to information is guaranteed by the constitution and operationalized through Law Number 14 of 2008 concerning Public Information Disclosure (UU KIP). In the practice of accountable governance, information on the educational background of public officials is often considered relevant for citizen oversight and accountability. However, the Law also recognizes exceptions for information concerning privacy, so public access is not absolute.

The intersection of these two legal regimes raises sharp research questions: first, can diplomas qualify as personal data under the PDP Law? and second, how does the information disclosure regime in the KIP Law regulate access to diplomas, especially when it comes to verifying public officials? These questions are crucial for mapping the boundaries of state obligations and citizens' rights within the context of transparency and accountability (Green, 2025; Sanz, 2017; Solove, 2024).

From a policy perspective, the urgency of this topic lies in the need to find a balance between protecting individual dignity and demands for official accountability (Skinner-Thompson, 2021; Trautendorfer et al., 2024). Failure to strike a balance could potentially lead to two consequences: excessive restrictions on information that is legitimately subject to public scrutiny, or, conversely, the exposure of personal data, which opens the door to abuse and a violation of privacy rights (Cristóbal, 2015; Rodríguez Sánchez, 2020). Therefore, formulating proportionate transparency criteria is in the public interest (Docksey & Propp, 2023; Jingbo, 2015).

This research positions diplomas as objects of cross-examination against two principles: data protection and information transparency. By placing public and private interests within the same framework, the analysis is expected to produce accountable guidelines for information service providers, information requesters, and data owners. This direction also addresses the practical debate that often arises in cases of verifying official qualifications.

The methodology employed is normative legal research, which involves examining norms in relevant laws, regulations, principles, and legal rules. This approach allows for both dogmatic and systematic argumentation regarding the legal status of diplomas, while simultaneously testing the coherence between regulatory regimes without relying on empirical findings. Thus, the resulting answers are based on the construction of positive norms and general principles of information law.

The scope of this study is limited to the Indonesian legal system, particularly the PDP Law and the KIP Law, along with their derivative regulations that directly impact data management and information services. The discussion does not cover the technical forensic aspects of document authenticity or internal university administrative practices beyond those defined by general norms; this limitation is intended to keep the analysis focused on normative questions about what should and should not be disclosed to the public.

Conceptually, this study adopts a balancing approach to examine whether, when, and to what extent diplomas can be accessed. In principle, maximum access is allowed as long as it does not violate the boundaries of privacy protection; meanwhile, restrictions must be justified through clear, relevant, and proportionate reasons to the risks faced by the data subject. This framework aligns with the construction of the Public Information Disclosure Law, which positions diplomas as conditionally open information, not closed.

Ultimately, this introduction lays the groundwork for further discussion on the legal classification of diplomas under the Personal Data Protection Law, the filtering of the boundaries of transparency under the Public Information Disclosure Law, and the formulation of practical guidelines for public bodies when receiving requests for information related to diplomas. With a clear normative basis and measurable balancing criteria, this study is expected to provide both conceptual and operational contributions to information disclosure practices that respect the right to personal data.

RESEARCH METHODS

This research employs a normative legal approach, focusing on norms specifically statutory regulations, principles, and legal rules, to address questions about the position of diplomas at the intersection of the Personal Data Protection (PDP) and Public Information Disclosure (PID) regimes. This choice aligns with the research objective of questioning the normative status of the object (diploma) and the limits of its accessibility, rather than assessing the empirical behavior of actors.

As a consequence of this approach, primary legal materials are the primary focus, including Law Number 27 of 2022 concerning the Personal Data Protection (PDP), Law Number 14 of 2008 concerning the Public Information Access (KIP), Government Regulation Number 61 of 2010 (implementation of KIP), and Regulation of the Minister of Education, Culture, Research, and Technology Number 50 of 2024 concerning Diplomas and Certification in Higher Education. These primary materials are read as a hierarchical and complementary system, with particular attention to definitions, scope, procedures, exceptions, and sanctions.

To enrich the argument and ensure the adequacy of the perspective, the research links secondary legal materials (books, journal articles, and institutional publications) and tertiary legal materials (e.g., legal dictionaries/encyclopedias for terminology clarification). Secondary materials are primarily used to map relevant principles (such as privacy, transparency, and proportionality) and best practices for balancing information disputes.

The material search strategy was conducted through a systematic inventory, starting from the research issue and the formulation of questions: (i) whether diplomas are classified as personal data according to the PDP Law; and (ii) how access to diplomas is regulated by the KIP Law in the context of public interest. Each document was selected based on the criteria of relevance (direct link to the definition/exception/procedure), authority (level of norm/authority of the issuer), and recency (the latest regulatory changes that impact the object).

All collected materials were processed through mapping of issues and norms: first, classification of norms according to regime (PDP vs KIP) and level (UU, PP, Permen); second, identification of tension points (conflict of norms) on the object of "diploma" (e.g., the definition of general personal data vs. exceptions to public information); third, formulation of

normative hypotheses regarding the degree of accountable openness. The analysis technique uses grammatical, systematic, and teleological interpretations of regulatory provisions, combined with balancing arguments and proportionality tests (suitability/legitimacy of purpose, necessity, and stricto sensu balance) to assess whether restricting access to or disclosure of information on diplomas is in line with the objectives of data protection and public accountability. The results of the analysis are presented as the construction of operational norms (rules of thumb) that PPID, applicants, and data subjects can apply.

As an internal validation step, preliminary findings were tested through source triangulation (matching interpretations between articles and regulations), consistency checks (to ensure that conclusions do not conflict with higher norms), and rationality tests (to determine whether the risk-benefit rationalization of information disclosure is justifiable). Where ambiguity existed, re-reading was conducted with a preference for the principles of fundamental rights protection and transparency, which are expressly limited by law. The research was limited to the Indonesian legal framework and the object of higher education diplomas associated with public office. The research did not conduct forensic verification of document authenticity or survey administrative behavior; its scope was limited to legal dogmatics, focusing on the formation and assessment of applicable rules and their implications for access to and protection of diplomas. This framework is consistent with the normative nature of the research, as stated by the author in the summary and body of the manuscript.

Procedurally, the analysis was conducted in four stages: (1) identification and comparative reading of key PDP–KIP norms and their implementing regulations; (2) binding normative facts regarding the content/content of diplomas according to the Minister of Education, Culture, Research, and Technology Regulation; (3) construction of a matrix of conflicts and exceptions (what is essentially personal data vs. what is appropriate to be disclosed for verification of public interest); and (4) formulation of operational guidelines (standards for selective disclosure, approval, and consequence testing) as normative research outputs. Finally, the quality of this method is measured by its ability to produce answers that are internally consistent, supported by authoritative sources. It can be replicated by readers when facing similar cases. Based on the above method, the discussion in the following section is expected to provide a clear framework for assessing diplomas as general personal data under the PDP Law, as well as conditional public information under the KIP Law.

RESULTS AND DISCUSSION

The position of diplomas as personal data from the perspective of Law Number 27 of 2022 concerning Personal Data Protection

The rapid development of technology and the dissemination of information have had a significant impact on various aspects of human life, including the management and protection of personal data. In today's digital era, the issue of personal data protection has become crucial, given the increasing ease with which individuals' personal information is widely disseminated through various digital platforms. The concept of personal data protection is rooted in the recognition that every individual has the right to determine whether they wish to share or exchange their data. Furthermore, individuals also have the right to set specific conditions for the transfer and use of their data. This demonstrates that data protection is closely linked to the concept of the right to

privacy. The right to privacy has evolved to the point where it can serve as a basis for formulating the right to the protection of personal data. In this context, every citizen's activity in the digital realm almost always involves the use and processing of personal data. Therefore, the right to privacy through data protection mechanisms is a crucial element in ensuring freedom and upholding individual dignity.

Personal data protection is not merely a technical issue, but rather the foundation for upholding various fundamental freedoms, political, spiritual, religious, and even sexual, as well as the right to self-determination, freedom of expression, and the right to privacy that make humans whole and independent. To provide legal certainty for this protection, the state has enacted Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), which, in Article 1, number 1, defines personal data as data about an identified or identifiable natural person, either alone or through combination with other information, directly or indirectly, through electronic or non-electronic systems. The PDP Law also distinguishes between two groups of data: specific personal data including health data and information, biometric data, genetic data, criminal records, child data, personal information, and other data stipulated by law and general personal data including full name, gender, citizenship, religion, marital status, and personal data that, when combined, can identify an individual. Under this framework, information is categorized as personal data if, alone or when combined with other data, it can be used to identify an individual.

A college diploma is more than just a piece of paper; it is a formal representation of one's academic accomplishments. The process of obtaining it reflects a student's long journey completing the curriculum, facing educational challenges, and passing various assessments. As such, a diploma holds significant symbolic and administrative value. Accurate verification of the data contained within it is crucial to ensure the document's validity. Several elements of information are mandatory on a college diploma as part of validating the holder's academic identity. In general, a diploma is an official document issued by an educational institution as proof of a person's academic achievement. This document typically contains several vital pieces of information, including the holder's full name, place and date of birth, student ID number, degree or level of education, name of the educational institution, year of graduation, diploma serial number, signature of an authorized official, and institutional stamp.

By the provisions of Article 3 paragraph (3) of the Regulation of the Minister of Education, Culture, Research, and Technology Number 50 of 2024 concerning Diplomas, Competency Certificates, and Professional Certificates of Higher Education Level, diplomas must contain at least several important information. This information includes the national diploma number, the symbol and name of the higher education institution, the main number of the higher education institution, the higher education program, the name and main number of the study program, as well as the personal data of the diploma holder such as full name, place and date of birth, and student registration number. In addition, diplomas must also include the academic degree or vocational degree awarded, along with its abbreviation, the date of graduation, the place and date of issuance of the diploma, as well as the name, position, and signature of the head of the higher education institution authorized to sign the diploma. These provisions serve as the legal and formal basis for preparing diplomas, aiming to ensure the validity,

authenticity, and protection of the personal data of the diploma holder. Several elements of the diploma, including the name, place of birth, date of birth, student ID number, and educational history, constitute personal identification information that can be used to directly identify an individual. As an official document containing a person's identity and academic achievements, the diploma is also a concern in the context of personal data protection. Therefore, it is essential to determine whether a diploma can be classified as personal data under applicable laws and regulations, particularly Law Number 27 of 2022 concerning Personal Data Protection (PDP Law).

Judging from the elements commonly included in a diploma, including full name, place and date of birth, ID number, study program, year of graduation, and diploma serial number, this document inherently contains an identity that is included in general personal data as referred to in Article 4 paragraph (2) letter a of the PDP Law. This basic identity, whether standing alone or combined, enables a person to be directly identified, thereby fulfilling the elements of the definition of "personal data" in Article 1, paragraph 1, of the PDP Law, which emphasizes the identifiability of individuals, both directly and indirectly, through electronic or non-electronic systems. Therefore, a diploma cannot be treated as neutral information without consequences; it is a document that attaches identity and is thus subject to the principles of data protection purpose limitation, data minimization, accuracy, security, and access limitation. Consequently, any processing, use, or broadcast of copies of diplomas must be based on a lawful basis for processing, carried out in proportion to the legitimate purpose, and where necessary, accompanied by mitigation measures such as redaction of irrelevant items.

Although a diploma is not specific personal data (because it does not contain biometric, health, or genetic data), its status as general personal data still provides the owner with the right to legal protection, as guaranteed in Article 58 paragraph (1) and Article 59 of the PDP Law, which regulates the safety and rights of data subjects. The PDP Law also emphasizes the position of individuals as Personal Data Subjects, namely natural persons to whom personal data is attached. As a data subject, every individual has special rights as regulated in Articles 5 to 15 of the PDP Law, including: the right to information, the right to correct data errors, the right to delete data, and the right to withdraw consent to the processing of their data. The protection of data subjects is a crucial foundation for ensuring that personal data management is carried out ethically, transparently, and by legal principles. By referring to the substance of Articles 1 and 4 of the PDP Law, diplomas can be categorized as general personal data, because they contain identity information that can lead to the identification of individuals. Therefore, diplomas are subject to the principles of personal data protection stipulated in the PDP Law, including provisions regarding the consent of the data owner before processing or dissemination.

Regulations on the disclosure of information regarding diplomas in Law Number 14 of 2008 concerning Public Information Disclosure

Transparency and freedom of information are two key pillars in guaranteeing citizens' rights in a democratic country. In this context, every public policy and decision must be transparent and accountable to the public. To achieve this, Indonesia enacted Law

Number 14 of 2008 concerning Public Information Disclosure (UU KIP), which serves as the legal basis for guaranteeing citizens' right to access public information. The UU KIP adopts the principle of maximum access limited exemption (MALE), meaning access to information must be as wide as possible, with minimal exceptions. This principle emphasizes the importance of transparency in state administration as a form of strengthening democracy and public participation. Thus, information disclosure becomes a means to realize clean, transparent, and accountable governance. The UU KIP ensures public access to information managed by public bodies. Article 7 of the UU KIP stipulates that every public body is obliged to provide, give, and/or publish public information under its authority to information applicants, except for information that is exempted. However, the UU KIP also stipulates limitations on information that is confidential or concerns private rights. One of them is stated in Article 17, letter h, which states that information that, if opened, could reveal personal secrets, including the results of evaluations of capabilities, intellectualism, and other personal records, can be excluded from public access.

In public information governance, diplomas are often requested by third parties for educational verification, recruitment processes, or legal purposes, as they are documents awarded to graduates of academic and vocational education, recognizing their learning achievements and/or completion of accredited study programs at universities. However, because they contain personal identity, access to them is subject to the Public Information Disclosure regime, which limits the disclosure of personal information only under certain circumstances. In principle, other parties can access diplomas if the owner provides written consent, or if the information is directly related to the fulfillment of requirements and verification of public office and therefore concerns the public interest (for example, in the nomination of officials or legislative members). Thus, the legal position of diplomas is not confidential information, but also not information that is entirely free to access. It is classified as conditional public information, which can be disclosed as long as the legal basis is met and only for legitimate purposes, while maintaining proportionality, including, if necessary, through limited disclosure or obscuring parts that are irrelevant to the purpose of the request.

Protection of personal information is also regulated in Government Regulation Number 61 of 2010 concerning the Implementation of the KIP Law. Article 8, paragraph (2) states that the retention period for personal information is set for as long as necessary to ensure the protection of said information. This means that public bodies are also responsible for maintaining the confidentiality of documents containing personal data, including diplomas, as long as the retention period remains relevant. One critical case that can serve as a reference is the Decision of the Central Information Commission (KIP) No. 153/V/KIP-PS-A/2011 in the case between LBH Medan, the Medan City Government, and the University of North Sumatra (USU). In this case, LBH Medan requested copies of the exam participant's answer documents to prove any discrepancies in the selection results. The KIP rejected the request because the requested documents contained personal information and the protection of other people's data, which cannot be freely disclosed. This case reinforces the principle that public information disclosure must be implemented while still considering the protection of an individual's right to privacy. Therefore, requests for copies of diplomas must also be examined based on

the purpose of the request, the legal context, and the status of the requesting party.

Based on the provisions of the Public Information Disclosure Law and its derivative regulations, it can be concluded that diplomas are public information that is conditionally open to disclosure. Access to diplomas is regulated by prioritizing the principle of balance between information transparency and personal data protection. In practice, diplomas can be accessed by other parties only with the owner's consent or if the information pertains to a public position that requires verification of the educational qualifications. Therefore, the regulation of information disclosure regarding diplomas in the Public Information Disclosure Law places diplomas as information that is not closed, but remains subject to the principle of protecting individual rights.

CONCLUSION

First, university diplomas can be categorized as general personal data as regulated in Law Number 27 of 2022 concerning Personal Data Protection (UU PDP). Information contained in diplomas, such as full name, place and date of birth, student ID number, and other academic data, constitutes information that can be used to directly identify an individual. Therefore, diplomas are subject to the principles of personal data protection, including the obligation to obtain the data subject's consent for any processing and dissemination. Second, from the perspective of Law Number 14 of 2008 concerning Public Information Disclosure (UU KIP), diplomas are classified as conditionally open public information. This means that information contained in diplomas can be accessed by third parties only under certain conditions, namely with the written consent of the diploma holder or if the information is required in the context of public interest, such as for the verification of candidates for public office. The Law on Public Information Disclosure expressly prioritizes the principle of openness while respecting the right to privacy, making the balance between the public's right to information and the individual's right to data protection a crucial element in its implementation. Thus, although diplomas are essentially public documents with both administrative and social relevance, their distribution must consider two legal aspects simultaneously: the principle of personal data protection and the principle of transparency in public information. The implementation of both principles must be balanced and proportional to ensure the safety of individual rights while supporting transparency in public governance.

REFERENCES

Cristóbal, R. S. (2015). The reduction of number of parliamentary members and the modification of remuneration schemes for deputies in autonomous community. *Revista de Derecho Politico*, *92*, 73–118.

Docksey, C., & Propp, K. (2023). Government Access to Personal Data and Transnational Interoperability: An Accountability Perspective. *Oslo Law Review*, *10*(1). https://doi.org/10.18261/olr.10.1.2

Fenster, M. (2006). The opacity of transparency. *Iowa Law Review*, *91*(3), 885–949.

Green, D. (2025). Strategic Indeterminacy and Online Privacy Policies: (Un)informed Consent and the General Data Protection Regulation. *International Journal for the Semiotics of Law*, *38*(2), 701–729. https://doi.org/10.1007/s11196-024-10132-4

Hsu, C.-S., Tu, S.-F., & Chiu, P.-C. (2022). Design of an e-diploma system based on consortium blockchain and facial recognition. *Education and Information Technologies*, *27*(4), 5495–5519. https://doi.org/10.1007/s10639-

021-10840-5

Jingbo, W. (2015). Weighing the Public Interest in the Disclosure of Government Information. *Social Sciences in China*, *36*(3), 37–55. https://doi.org/10.1080/02529203.2015.1062228

Kirchhof, F. (2024). Transparenz – Segen oder Fluch für den Rechtsstaat? *Zeitschrift Fur Die Gesamte Versicherungswissenschaft*, *113*(1), 1–9. https://doi.org/10.3790/zverswiss.2024.1430401

Rodríguez Sánchez, C. M. A. (2020). Two examples of claudican transparency: The protection of data and the secrets of state. *Revista Espanola de La Transparencia*, *10*, 129–150. https://doi.org/10.51915/RET.80

Saleh, O. S., Ghazali, O., & Al Maatouk, Q. (2019). Graduation certificate verification model: A preliminary study. *International Journal of Advanced Computer Science and Applications*, *10*(7), 575–582.

Sanz, R. M. (2017). Comparative analysis of public policies and best practices of transparency in Ecuador 2004-2014. *Reforma y Democracia*, *2017-Febru*(67), 197–226.

Skinner-Thompson, S. (2021). Agonistic privacy & equitable democracy. *Yale Law Journal*, *131*, 454–474.

Solove, D. J. (2024). Data Is What Data Does: Regulating Based on Harm and Risk Instead of Sensitive Data. *Northwestern University Law Review*, *118*(4), 1081–1138. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85183932494&partnerID=40&md5=dfe51da260c14635777d34093815f4d4

Torres-Hernández, N., & Gallego-Arrufat, M.-J. (2023). Pre-service teachers' perceptions of data protection in primary education. *Contemporary Educational Technology*, *15*(1). https://doi.org/10.30935/cedtech/12658

Trautendorfer, J., Schmidthuber, L., & Hilgers, D. (2024). Are the answers all out there? Investigating citizen information requests in the haze of bureaucratic responsiveness. *Governance*, *37*(3), 845–865. https://doi.org/10.1111/gove.12805

Yin, W. (2023). Zero-Knowledge Proof Intelligent Recommendation System to Protect Students' Data Privacy in the Digital Age. *Applied Artificial Intelligence*, *37*(1). https://doi.org/10.1080/08839514.2023.2222495