INFOKUM
Volume 13, Number 04, 2025, DOI 10.58471/infokum.v13i04
ESSN 2722-4635 (Online)
https://infor.seaninstitute.org/index.php/infokum

Digital Notarial Archives in Indonesia: Regulatory Challenges vs. the EU's GDPR Data Protection Standards

Zakiah Noer[1], Rizki Kurniawan[2]
Arif Rahman Hakim Street No. 2B, Kramatandap, Gapurosukolilo, Gresik District, Gresik Regency, East Java

Article Info
Keywords:
Digital Notarial Archives,
Data Protection Compliance,
GDPR

ABSTRACT
This study examines the regulatory and operational challenges faced by Indonesian notarial institutions in complying with digital data protection standards. Using a qualitative approach through legal analysis and interviews with notaries in Jakarta, Surabaya, and Bandung, the research identifies major issues, including limited understanding of data governance, lack of sector-specific regulations, and weak cybersecurity infrastructure. Although Law No. 27/2022 on Personal Data Protection provides a legal foundation, it lacks clarity and enforcement tailored to notarial functions. A comparison with the European Union's General Data Protection Regulation (GDPR) reveals significant gaps, particularly in accountability, transparency, and risk-based mechanisms. The absence of roles such as Data Protection Officers and mandatory data impact assessments highlights the institutional unpreparedness in Indonesia. These shortcomings expose sensitive legal data to potential breaches, reducing public trust and legal reliability. The study recommends the adoption of a sector-specific regulatory model aligned with GDPR principles, supported by standardized protocols, professional training, and oversight mechanisms. These efforts are essential to ensure data security, improve institutional credibility, and support Indonesia's transition toward secure and professional digital legal services.

Corresponding Author:
Zakiah Noer
Arif Rahman Hakim Street No. 2B, Kramatandap, Gapurosukolilo, Gresik District, Gresik Regency, East Java
zakiahnoer12@gmail.com

INTRODUCTION

Compliance with data protection regulations among Indonesian notarial institutions is increasingly being questioned as digital technologies transform the landscape of legal document management. Notarial archives, once exclusively maintained in physical formats, are now being digitized, raising significant concerns regarding confidentiality, integrity, and lawful processing of sensitive legal data [1]. The ability of notaries to comply with digital data protection standards is essential to maintaining legal certainty, especially given the fiduciary role of notaries in safeguarding personal and transactional information.

This phenomenon reflects broader challenges within Indonesia's regulatory and technological ecosystem. Despite the momentum toward digitalization driven by government initiatives and industry pressure, many notarial institutions face a lack of clear technical standards, insufficient guidance on digital governance, and inadequate enforcement of data

INFOKUM
Volume 13, Number 04, 2025, DOI 10.58471/infokum.v13i04
ESSN 2722-4635 (Online)
https://infor.seaninstitute.org/index.php/infokum

privacy principles [2], [3]. The absence of sector-specific digital compliance protocols has resulted in fragmented practices, exposing both notaries and their clients to potential data breaches and regulatory risks [4].

Key contributing factors to this compliance gap include the limitations in Indonesia's legal framework on personal data protection, infrastructural disparities in digital readiness across regions, and a lack of comprehensive training for notaries regarding digital privacy and cybersecurity standards [5]. Although the enactment of Indonesia's Personal Data Protection Law (Law No. 27/2022) marked a legislative milestone, implementation remains inconsistent and lacks specificity for professional sectors such as notarial services [6].

To address these gaps, this study introduces the European Union's General Data Protection Regulation (GDPR) as a comparative standard. The GDPR offers a comprehensive legal framework built upon principles such as lawfulness, fairness, transparency, data minimization, and accountability [7], [8]. These principles serve as a benchmark for evaluating the robustness and completeness of national data protection regimes, particularly in sectors handling sensitive and high-risk data such as notarial archives [9].

The digitalization of legal documents in Indonesian notarial institutions has introduced serious challenges in data protection compliance, particularly in the absence of sector-specific digital governance standards. Although Indonesia has enacted the Personal Data Protection Law (Law No. 27/2022), its implementation remains broad and lacks specific guidelines for notarial practices, resulting in inconsistent and fragmented compliance [10], [11]. Prior studies tend to focus on general data protection or public-sector digitalization [10], [11], leaving a gap in the literature regarding how private legal professionals, especially notaries, navigate data confidentiality and cybersecurity in a digitized context [12], [13]. Furthermore, issues such as inadequate infrastructure, lack of cybersecurity training, and weak enforcement mechanisms contribute to a significant compliance gap [7], [8]. In contrast, the European Union's General Data Protection Regulation (GDPR) offers a comprehensive legal framework with actionable principles such as lawfulness, transparency, and accountability that could serve as a benchmark for improving Indonesia's regulatory design [9], [10]. However, little research exists that uses GDPR as a comparative tool to evaluate Indonesia's readiness and alignment, particularly in notarial institutions. This study fills that gap by examining how Indonesian notarial practices align with GDPR standards and introduces a tailored analysis of legal, technical, and institutional barriers, offering novel policy recommendations to strengthen digital data protection in the notarial sector.

The purpose of this study is to examine the extent of regulatory compliance among Indonesian notarial institutions, analyze the influence of legal and infrastructural factors on digital archiving practices, and evaluate Indonesia's alignment with GDPR standards. Through a comparative legal analysis, this research aims to highlight structural deficiencies, offer policy recommendations, and contribute to a more secure and rights-based framework for digital notarial data governance.

METHOD

This study adopts a qualitative approach, utilizing comparative legal analysis and literature

INFOKUM
Volume 13, Number 04, 2025, DOI 10.58471/infokum.v13i04
ESSN 2722-4635 (Online)
https://infor.seaninstitute.org/index.php/infokum

review methods to examine the extent of compliance among Indonesian notarial institutions with digital data protection regulations, particularly in relation to the European Union's General Data Protection Regulation (GDPR). The research aims to identify regulatory shortcomings, institutional obstacles, and technical challenges in the digitization of notarial archives. The primary object of the study is the digital document management practices of notaries in Indonesia, assessed under the Personal Data Protection Law (Law No. 27/2022).

Data were gathered through the examination of national legislation, EU regulations, sector-specific policies, and peer-reviewed academic journals that explore themes such as digital governance, privacy protection, and legal institutional readiness. This method is justified by Creswell and Poth, who state that qualitative research is suitable for analyzing intricate and underexplored phenomena that cannot be reduced to numerical analysis [1]. Furthermore, this study follows Yin's case-based research strategy to analyze normative and institutional frameworks systematically [2].

To deepen the analysis, semi-structured interviews were conducted with practicing notaries from Jakarta, Surabaya, and Bandung. These interviews aimed to extract insights into their awareness, application, and challenges regarding digital data protection standards. The qualitative data obtained were processed using thematic analysis, a method described by Braun and Clarke as effective for identifying, analyzing, and reporting patterns within data [3].

RESULTS AND DISCUSSION

The results of this study reveal a significant regulatory and operational gap in the compliance practices of Indonesian notarial institutions concerning digital data protection. Through semi-structured interviews conducted with practicing notaries in Jakarta, Surabaya, and Bandung, several critical issues were identified. These include limited understanding of digital data governance, lack of sector-specific guidelines, and an absence of secure digital infrastructure. The notaries interviewed expressed concerns over ambiguous interpretations of Indonesia's Personal Data Protection Law (Law No. 27/2022), particularly due to its broad and generalized nature. While the law provides a foundational framework for personal data protection, it fails to address the unique nature of notarial responsibilities, which involve handling highly sensitive and legally binding information. Respondents also indicated that, in practice, digital document management systems are either rudimentary or outsourced to third-party providers without standardized protocols for encryption, authentication, or secure storage. Consequently, the absence of a unified compliance protocol has led to highly fragmented practices across regions and institutions.

Furthermore, the study's comparative legal analysis demonstrates a pronounced divergence between Indonesia's data protection implementation and the stringent provisions of the European Union's General Data Protection Regulation (GDPR). The GDPR outlines a comprehensive legal structure grounded in fundamental principles such as lawfulness, fairness, transparency, data minimization, and accountability principles that remain inconsistently applied in Indonesia's notarial sector. For example, GDPR mandates the presence of a Data Protection Officer (DPO) in institutions handling large-scale or sensitive

INFOKUM
Volume 13, Number 04, 2025, DOI 10.58471/infokum.v13i04
ESSN 2722-4635 (Online)
https://infor.seaninstitute.org/index.php/infokum

data processing, yet such roles are virtually non-existent in Indonesian notarial institutions. In addition, GDPR requires data impact assessments for high-risk processing activities and includes robust enforcement mechanisms such as administrative fines and mandatory breach notification protocols. These provisions are either missing or poorly defined under Indonesian law, particularly in the context of private legal professionals. The lack of training and institutional capacity in cybersecurity, coupled with regional disparities in digital infrastructure, further exacerbates the compliance gap. As a result, the integrity and confidentiality of digitized notarial records are at substantial risk, undermining public trust and legal certainty.

This research underscores the need for Indonesia to adopt a sector-specific regulatory framework that translates the core principles of the GDPR into actionable policies tailored for notarial practices. Such a framework should include mandatory certification programs for notaries on data privacy and cybersecurity, standardization of digital archiving practices, and the establishment of a supervisory authority dedicated to monitoring compliance in the legal sector. Additionally, pilot projects and regional capacity-building initiatives could serve as transitional models to align local practices with international standards. By integrating GDPR-aligned mechanisms into its regulatory landscape, Indonesia has the potential to enhance the credibility, security, and professionalism of its notarial institutions in the digital age. These findings contribute not only to the scholarly discourse on data protection in emerging economies but also offer practical policy recommendations to bridge the gap between legal norms and technological realities.

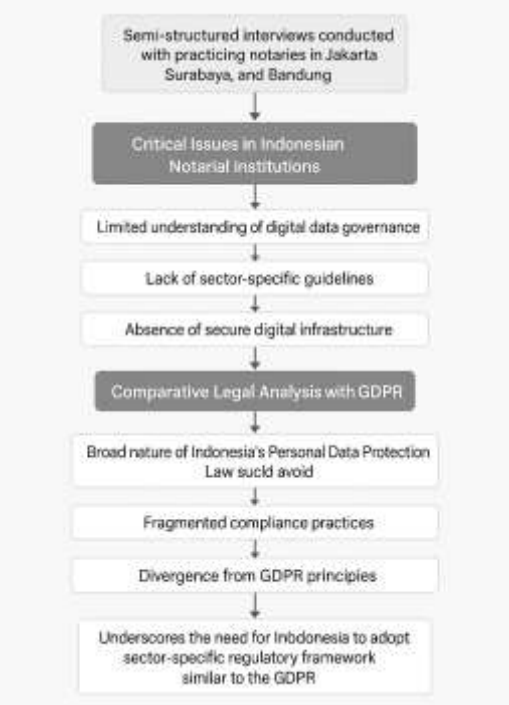

Figure 1. Structured Flowchart

Figure 1 presents a structured flowchart that visually summarizes the key findings and analytical trajectory of this study concerning the compliance of Indonesian notarial institutions

INFOKUM
Volume 13, Number 04, 2025, DOI 10.58471/infokum.v13i04
ESSN 2722-4635 (Online)
https://infor.seaninstitute.org/index.php/infokum

with digital data protection standards. The diagram begins with the data collection method semi-structured interviews with notaries from Jakarta, Surabaya, and Bandung which serve as the empirical foundation of the study. These interviews revealed several critical issues within Indonesian notarial institutions, which are depicted in a sequential manner: a limited understanding of digital data governance, the absence of sector-specific regulatory guidelines, and the lack of secure digital infrastructure. These points reflect systemic weaknesses in the institutional capacity to manage sensitive data under digital transformation.

The flowchart proceeds with a comparative legal analysis between the Indonesian framework and the European Union's General Data Protection Regulation (GDPR). The analysis identifies that the Indonesian Personal Data Protection Law (Law No. 27/2022) is too broad and generalized, making it difficult to implement effectively in specialized professions such as notarial services. As a result, compliance practices are fragmented across institutions, and there is a clear divergence from internationally accepted GDPR principles like lawfulness, accountability, and risk-based governance. The chart culminates in a policy-oriented conclusion: Indonesia must develop a sector-specific regulatory framework for notarial institutions that aligns with GDPR principles. Such a framework should address both legal and technical gaps to enhance institutional preparedness and public trust in digital notarial services. This visual representation reinforces the argument that policy development in data protection must be tailored and evidence-based, grounded in both legal analysis and real-world institutional practices.

CONCLUSION

This study underscores the urgent need for Indonesia to modernize and harmonize its data protection practices within the notarial sector by adopting a more nuanced, sector-specific regulatory approach. The analysis of qualitative data gathered from notaries in major urban centers revealed systemic weaknesses in both institutional awareness and digital infrastructure readiness. While the enactment of Law No. 27/2022 represents a critical legal milestone, its current form lacks the specificity and enforcement mechanisms required for effective application in high-risk professional domains such as notarial services. These shortcomings result in inconsistent practices and heightened vulnerability to data breaches, ultimately compromising public trust and the integrity of legal transactions. By drawing upon the European Union's General Data Protection Regulation (GDPR) as a comparative benchmark, this study identifies concrete legal and procedural principles that Indonesia could adapt to its national context. These include the establishment of mandatory training programs, appointment of Data Protection Officers, standardized encryption protocols, and independent supervisory bodies to enforce compliance. Without such reforms, the digitization of notarial records will continue to outpace the legal and institutional capacity to manage them securely. Therefore, this study calls for a comprehensive re-evaluation of Indonesia's digital data governance in the legal profession, aiming to ensure both legal certainty and the protection of fundamental rights in the digital era.

REFERENCE

[1] C. Bennett and C. Raab, The Governance of Privacy: Policy Instruments in Global Perspective, 2nd ed., Cambridge, MA: MIT Press, 2006. [Online]. Available: https://mitpress.mit.edu/books/governance-privacy

[2] V. Braun and V. Clarke, Thematic Analysis: A Practical Guide, London: SAGE Publications, 2021. [Online]. Available: https://books.google.com/books/about/Thematic_Analysis.html?id=mToqEAAAQBAJ

[3] J. W. Creswell and C. N. Poth, Qualitative Inquiry and Research Design: Choosing Among Five Approaches, 4th ed., Thousand Oaks, CA: SAGE Publications, 2018. [Online]. Available:https://books.google.com/books/about/Qualitative_Inquiry_and_Research_Design.html?id=DLbBDQAAQBAJ

[4] European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), Official Journal of the European Union, L 119, 4 May 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[5] L. Edwards, "Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective," European Data Protection Law Review, vol. 2, no. 1, pp. 28–58, 2016. [Online]. Available: https://doi.org/10.21552/EDPL/2016/1/6

[6] S. Gutwirth, R. Leenes, and P. de Hert, Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges, Dordrecht: Springer, 2014. [Online]. Available: https://doi.org/10.1007/978-94-017-9980-3

[7] M. Hildebrandt, Smart Technologies and the End(s) of Law, Cheltenham: Edward Elgar Publishing, 2015. [Online]. Available: https://doi.org/10.4337/9781781954044

[8] Republic of Indonesia, Law No. 27 of 2022 on Personal Data Protection, Jakarta: Ministry of Communication and Information Technology, 2022. [Online]. Available: https://peraturan.bpk.go.id/Home/Details/200200/uu-no-27-tahun-2022

[9] J. Smith, Y. Zhang, and A. Renshaw, "Strengthening cybersecurity in digital public services: A comparative study," Journal of Information Policy, vol. 11, pp. 35–58, 2021. [Online]. Available: https://doi.org/10.5325/jinfopoli.11.2021.0035

[10] N. van Dijk, B. van der Sloot, and C. Prins, "The New Privacy Regime for Biometric Data: A Critical Evaluation of the GDPR," Computer Law & Security Review, vol. 34, no. 1, pp. 1–12, 2018. [Online]. Available: https://doi.org/10.1016/j.clsr.2017.05.003

[11] P. Voigt and A. von dem Bussche, The EU General Data Protection Regulation (GDPR): A Practical Guide, Cham: Springer, 2017. [Online]. Available: https://doi.org/10.1007/978-3-319-57959-7

[12] D. Wright and P. De Hert, Privacy Impact Assessment, Dordrecht: Springer, 2012. [Online]. Available: https://doi.org/10.1007/978-94-007-2543-0

[13] R. K. Yin, Case Study Research and Applications: Design and Methods, 6th ed., Thousand Oaks, CA: SAGE Publications, 2018. [Online]. Available: https://books.google.com/books/about/Case_Study_Research_and_Applications.html?id=6DwmDwAAQBAJ