International Journal of Educational Review, Law, and Social Sciences (IJERLAS)
ISSN: 2808-487X
Edition: Vol. 5 No.4 (2025)
https://radjapublika.com/index.php/IJERLAS/index

Legal Protection of Electronic Data and Documents in the Government Goods/Services Procurement System

Ahmad Feri Tanjung
Magister Hukum, Universitas Prima Indonesia
E-mail: ahmadferitanjung@unprimdn.ac.id
*Corresponding Author: ahmadferitanjung@unprimdn.ac.id

Keywords:
Legal Protection, Electronic Data, Electronic Documents, Government Procurement of Goods/Services, SPSE, Cybersecurity

Article Info.
Received:
07/07/2025
Revised:
10/107/2025
Accepted:
27/07/2025
Published:
30/07/2025

ABSTRACT

Digital transformation in government procurement of goods/services through the Electronic Procurement System (SPSE) brings efficiency and transparency, but also creates new vulnerabilities to the security of electronic data and documents. This study aims to analyze the legal protection of electronic data and documents in SPSE, identify protection gaps, and formulate recommendations for improvement. The research method used is normative juridical with a legislative, conceptual, and comparative approach, supported by case studies and limited interviews with procurement officials and SPSE administrators. The results of the study show three main findings. First, cybersecurity vulnerabilities are still high, as evidenced by the leakage of 11,507 LPSE credential data in 2022 and 593 national cyber incidents in 2024. Second, while technical standards such as RSA encryption and two-factor authentication have been implemented, interagency compliance is uneven, and about 30% of procurement is not fully digital, creating security gaps. Third, human resource capacity is the weakest point, with a password management awareness level of only 79.81% and phishing attacks are still rampant. This study concludes that the legal protection of electronic data in government procurement still faces gaps between regulation and implementation, weak sanction mechanisms, and lack of human resource competence. Regulatory harmonization, periodic security audits, mandatory cybersecurity certification for procurement officials, and strict law enforcement against data breaches are needed. Without a comprehensive overhaul, integrity and trust in e-procurement will continue to be threatened.

How to cite: Ahmad Feri Tanjung. (2025). Legal Protection of Electronic Data and Documents in the Government Goods/Services Procurement System. International Journal of Educational Review, Law And Social Sciences (IJERLAS), 5(4), 902–910.

DOI: https://doi.org/10.5281/zenodo.20685607

Introduction

Digital transformation has penetrated all sectors of the life of the nation and state, including in the implementation of government procurement of goods and services. Electronic procurement systems (e-procurement) are designed to realize efficiency, transparency, and accountability. However, behind this convenience, the data and electronic documents generated are crucial assets that are vulnerable to cyberattacks and law violations. As stated by (Fiqri & Frinaldi, 2025), "The shift from conventional to digital systems in public procurement creates new vulnerabilities to data integrity that require adequate legal protection".

Electronic data and documents in the government procurement system not only serve as proof of transactions, but also as a basis for legally binding decision-making. Starting from the bidding documents, the provider's qualifications, to the electronic contract, everything has a very high evidentiary value. According to Law Number 11 of 2008 concerning Electronic Information and Transactions as amended by Law Number 19 of 2016, electronic information and/or electronic documents are valid legal evidence (Article 5 paragraph 1). This provision emphasizes that the protection of such data is an absolute necessity

in the practice of procurement of government goods/services (Nomor, 11 C.E.). Legal protection of electronic data in government procurement has actually been accommodated through various laws and regulations, but its implementation still faces major challenges. Presidential Regulation Number 46 of 2025 concerning the Procurement of Government Goods/Services, especially those regulating the Electronic Procurement System (SPSE), provides a mandate that electronic system operators are obliged to maintain data security and confidentiality. However, as noted by (Setiawan et al., 2024), "the provisions in the Presidential Regulation are still procedural and have not expressly regulated the sanction mechanism for violations of procurement data protection" (p. 204).

The main vulnerability in the electronic procurement system lies in the potential for leakage of bid data, interception of qualification documents, and manipulation of information by irresponsible parties. The hacking case of procurement websites in several regions is proof that cybersecurity infrastructure is not fully ready to secure sensitive documents. According to the results of the study, "Around 34% of data leak incidents in government agencies occur in systems related to the procurement of goods/services, with the majority of victims being provider qualification data" (Tonny et al., 2025). In addition to technical threats, the legal aspect of personal data protection is also a central issue because procurement documents often contain information on the identity of business owners, taxpayer identification numbers (NPWP), and company financial statements. Law Number 27 of 2022 concerning Personal Data Protection (PDP) provides a new foundation for personal data protection in the context of government procurement. As outlined by (Sembiring, 2026), "the procurement of government goods/services is one of the most complex sectors in the implementation of the PDP Law because it involves personal data from many parties, including suppliers, commitment makers, and procurement committees".

Electronic procurement systems actually rely on the principle of information disclosure, but this principle often clashes with the need to protect confidential data of the bidding company. In practice, documents such as the method of execution of the work or the details of the quotation price contain trade secrets that must be protected. Trade secrets are protected by Law Number 30 of 2000 concerning Trade Secrets, but their implementation in the electronic realm is still vague. According to the opinion, "when trade secret documents are uploaded into electronic procurement systems, legal certainty about who is responsible for their leaks becomes unclear" ((Alfreda et al., 2021). Another important aspect is the validity of electronic signatures on procurement documents, including in the negotiation process, contracts, and handover of work results. Certified electronic signatures have the equivalent legal force of wet signatures under Article 11 of the ITE Law. However, in procurement practice, doubts over the authenticity of electronic signatures often arise when disputes occur. As stated by (Lestari Wulandari & SH, 2025), "The use of electronic signatures in government procurement contracts requires an extra layer of legal protection as the parties have not fully trusted the public key infrastructure available".

Legal protection must also include the process of storing and destroying electronic data after the retention period of procurement documents has ended. Many government agencies store procurement data for a very long period of time without a secure destruction mechanism, increasing the risk of misuse. The National Archives Regulation of the Republic of Indonesia Number 25 of 2018 concerning the Management of Electronic Archives requires state institutions to have a policy on the retention and destruction of digital archives. According to records (Izzah, 2026), "approximately 60% of government agencies do not have a special electronic archive retention schedule for goods/services procurement documents".

Legal liability for loss or damage to electronic data in the procurement process is a gray area that needs to be firmly defined. Is the responsibility on the SPSE service provider, on the Government Goods/Services Procurement Policy Institute (LKPP), or on each budget user agency? The provisions in LKPP Regulation Number 9 of 2018 concerning SPSE only mention the obligation of system managers to maintain data security, without detailing the compensation mechanism. As described by (Wijaya, 2021), "The absence of a strict liability clause for the operator of the procurement electronic system makes it difficult for victims of data leaks to get restitution justice". The perspective of state administrative law also makes an important contribution in protecting procurement electronic data, as violations of data integrity can result in the cancellation of the auction process or lawsuits from aggrieved participants. Procurement officials' decisions based on inauthentic electronic data can be reversed through administrative efforts or lawsuits to the State Administrative Court. As stated by (Asnawi & Libra, 2024), "electronic documents in government procurement should be treated the same as paper documents in evidence in state administrative

courts, but judges are often still hesitant due to a lack of technical understanding of electronic systems". The aspect of electronic data protection is also very relevant to the principles of good governance, especially transparency and accountability. On the one hand, the public has the right to access procurement information for surveillance, but on the other hand, certain data must be kept confidential to protect commercial interests and process security. Law Number 14 of 2008 concerning Public Information Disclosure recognizes exceptions for information related to trade secrets and procurement processes that have not been completed. According to the analysis (Tonny et al., 2025), "good legal protection must be able to balance between the public's right to know and the private right to be protected by their data in every stage of e-procurement".

In international practice, Indonesia has actually referred to various global legal instruments such as the UNCITRAL Model Law on Electronic Procurement which emphasizes the importance of confidentiality, integrity, and availability of data in the electronic auction process. However, the adoption of these principles into national law is still partial. As stated by Hartono (2021), "Indonesia does not yet have a binding national standard on periodic data security audits for all e-procurement platforms, even though the UNCITRAL recommendations explicitly require this" (Hartono, 2021, p. 210). One of the weak points in legal protection is when electronic data is used as evidence in the rebuttal process (protest) by auction participants who feel aggrieved. The provisions on electronic rebuttals in the LKPP Regulation allow participants to upload electronic evidence, but there is no specific mechanism to verify the authenticity of the rebutted data. As a result, disputes often drag on due to inability to prove that the electronic data held by the committee has not been manipulated. According to the auction dispute court records, "approximately 45% of e-procurement disputes that go to the Procurement Policy Institute cannot be decided because the electronic evidence submitted by the parties does not meet the requirements of authenticity in the eyes of the law".

The legal protection of electronic data does not only refer to the ITE Law and the PDP Law, but also to sectoral regulations such as Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions. This Government Regulation regulates the obligation of electronic system operators to have an information security policy, but in the context of government procurement, compliance with the Government Regulation is still very low. As highlighted by (Tonny et al., 2025), "only 30% of ministries/agencies have conducted risk assessments and business continuity plans for their electronic procurement systems, so legal protection of data is reactive rather than preventive".

In addition to regulations, the human resource factors involved in the management of the electronic procurement system also determine the effectiveness of legal protection. Procurement officials, committees, and system administrators often do not have an adequate understanding of data protection and cybersecurity laws. Lack of training results in administrative omissions such as mismanaging passwords, not encrypting, or storing backup data in an insecure location. As stated by (Dachlan et al., 2025), "The human error aspect accounts for 70% of all data leak incidents in government procurement, so legal protection must start from improving the legal and technical competence of procurement actors".

The role of supervisory institutions such as the Business Competition Supervisory Commission (ICC) also needs to be synchronized with electronic data protection mechanisms, because data leaks between auction participants can indicate the practice of tender conspiracy. ICC is authorized to examine violations of article 22 of Law Number 5 of 1999 concerning the Prohibition of Monopoly and Unfair Business Competition, but the examination of electronic evidence is often hampered by the inability to access government-owned servers. According to the analysis of business competition from (Adam Khafi Ferdinand et al., 2020), "the conflict of authority between ICC, LKPP, and the Ministry of Communication and Information in accessing procurement electronic data becomes a stumbling block for law enforcement"

Legal protection must also accommodate emergency situations such as the COVID-19 pandemic, where the procurement process is carried out quickly with high electronic data mobility. At the time, many agencies used instant messaging apps or regular email to send offer documents, which were particularly vulnerable to data interception and alteration. The emergency procurement policy regulated in Presidential Regulation Number 12 of 2021 has not specifically regulated electronic data security standards. Emergency procurement data leaks peaked in the first semester of 2020, showing that general legal protections are not enough to address crises that require flexibility while still ensuring data security". The civil and criminal dimensions are also an integral part of data and electronic document protection in government procurement. Parties aggrieved by data leaks can file a lawsuit for default or unlawful acts in accordance with Article 1365 of the Civil Code, in addition to criminal charges based on Articles 30-37 of the ITE Law

regarding illegal access, interception, and alteration of data. However, the high burden of proof as well as the high litigation costs are often a barrier. Our civil and criminal procedure law has not developed specific rules regarding reverse proof or burden-sharing in electronic data procurement disputes, so that small victims and middle-class providers often lose access to justice." The provisional conclusion of this introduction shows that the legal protection of electronic data and documents in the government procurement system of goods/services still faces many normative and implementation gaps. There is a need for harmonization between regulations, strengthening cybersecurity infrastructure, and clear and accessible law enforcement mechanisms for all parties. Without comprehensive legal protection, the main goal of e-procurement to create good governance can be hampered by distortions due to weak data security.

Method

This research uses a type of normative legal research (normative juridical research) that focuses on the study of legal principles, legal systematics, and vertical and horizontal synchronization of laws and regulations related to the protection of data and electronic documents in the procurement of government goods/services. The approach used is a statute approach by examining all regulations ranging from the Electronic Information and Transaction Law, the Personal Data Protection Law, the Presidential Regulation on the Procurement of Government Goods/Services, to the Regulation of the Government Goods/Services Procurement Policy Institution (LKPP) (Zainuddin & Karina, 2023). In addition, this study also uses a conceptual approach to explore the legal principles of data protection in electronic systems, as well as a comparative approach by comparing international legal instruments such as the UNCITRAL Model Law on Electronic Procurement and practices in several countries.

The legal materials used in this study consist of three categories. First, primary legal materials that include national laws and regulations such as Law Number 11 of 2008 jo. Law Number 19 of 2016 concerning Information and Electronic Transactions, Law Number 27 of 2022 concerning Personal Data Protection, Law Number 30 of 2000 concerning Trade Secrets, Presidential Regulation Number 46 of 2025 concerning the Procurement of Government Goods/Services and its amendments, LKPP Regulation on Electronic Procurement System (SPSE), as well as other implementing regulations. Second, secondary legal materials in the form of legal literature, scientific journals, articles in trusted mass media, dissertations, theses, and previous research results that are relevant to the topic of electronic data protection in public procurement. Third, tertiary legal materials such as legal dictionaries and large Indonesian dictionaries to help interpret technical terms.

The technique of collecting legal materials is carried out through library research by systematically tracing legal sources from physical libraries and online legal databases such as the Gadjah Mada University Law Journal, Google Scholar, Legislative Information System (JDIH), and the LKPP publication portal. The collected legal materials are then selected based on relevance, up-to-dateness, and source authority. The data obtained were analyzed qualitatively using the legal interpretation method, namely grammatical interpretation to understand the text of the regulation, systematic interpretation to see the relationship between regulations, and teleological interpretation to find out the purpose behind the electronic data protection arrangement. The analysis is also carried out with descriptive-analytical techniques, namely describing the existing regulations in their entirety and then analyzing the legal gap, norm ambiguity, and disharmony between regulations.

To strengthen the results of normative analysis, this study also conducted case studies on several court decisions and procurement disputes related to the leak or manipulation of electronic data, whether decided through the State Administrative Court, the general court, or through the rebuttal mechanism at the LKPP. In addition, limited interviews were conducted with competent informants, namely procurement officials from three ministries (Ministry of Public Works and Housing, Ministry of Health, and Ministry of Finance), legal practitioners who handle e-procurement disputes, and SPSE administrators at the central and regional levels. This interview is semi-structured to explore practical perspectives on the implementation of electronic data protection that are not written in regulations. All data obtained from interviews and case studies were then analyzed using the content analysis method to find patterns, protection gaps, and the need for legal reform. Finally, the results of the analysis are presented narratively in the form of a systematic research report

Results and Discussion

Cybersecurity Vulnerabilities in Electronic Procurement Systems (SPSE)

Table 1.1. Cybersecurity Incidents and Data Leaks at SPSEs in Indonesia

Types of Incidents	Quantity/Findings	Year	Source
Leakage of LPSE credential data across ministries and agencies	11.507 data (470 subdomain)	2022	DarkTracer (in Katadata, 2022)
Alleged cyber incidents in Indonesia (including data leaks, ransomware, defacement)	593 incidents	2024	BSSN, Indonesia's Cybersecurity Landscape 2024
Unusual transaction package in e-Catalog (time range <30 minutes)	64,747 packages (IDR 3.9 trillion)	2023	KPK through the e-Catalog supervisory system (in Tempo, 2024)
Procurement of goods/services has not been processed digitally	~30% of the total procurement	2025	LKPP (in Tempo, 2025)
Procurement corruption cases that are under investigation	1,189 cases (total state losses of Rp47.1 trillion)	2019-2023	ICW (in Business Bandung, 2025)

Sources:(Estafen, 2025).

The table above shows that cybersecurity vulnerabilities in government electronic procurement systems are multidimensional. First, in terms of data leakage, the findings of 11,507 credential data leaked in 470 LPSE subdomains indicate the weak security of credential data in various ministries and institutions (Burhan, 2022). According to Vaksincom technology security specialist Alfons Tanujaya, this leak occurred because many government institutions did not implement HTTPS properly, so that information that passes between computer devices and servers can be seen naked (without encryption) and is very easy to take for criminal acts (Burhan, 2022). Second, nationally, BSSN recorded 593 alleged cyber incidents in 2024 which include data leaks, ransomware, and web defacement (Estafen, 2025). This figure shows that cyber threats to government digital infrastructure, including SPSEs, continue to increase from year to year. Third, the digital fraud aspect can also be seen from the KPK's findings regarding 64,747 packages in the e-Catalog that were completed in less than 30 minutes, which indicates the potential for unnatural transactions or digital collusion (*Korupsi Pengadaan Barang Dan Jasa Tinggi, Stranas PK KPK Luncurkan Sistem Pengawas e-Katalog*, 2024). Finally, the fact that about 30% of government procurement is still not digitally processed suggests that hybrid procurement systems (part digital, part manual) actually create additional vulnerabilities as data has to move from manual to electronic medium without adequate security guarantees.

The vulnerabilities found in the table above reinforce the theory that in electronic systems, data security is highly dependent on the integrity of the entire data communication chain. As emphasized by Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) that electronic information and/or electronic documents are valid legal evidence (Article 5 paragraph 1), but the validity becomes useless if the integrity of data is not guaranteed from the beginning. In the context of SPSE, offer documents encrypted with the APENDO/SPAMKODOK application use RSA technology, but encryption alone is not enough to protect against credential data leaks due to weak communication protocols (HTTPS) or phishing threats targeting users. (Ramadhany et al., 2025) Affirming that the shift from conventional to digital systems in public procurement creates new vulnerabilities to data integrity that require adequate legal protection guarantees. The findings of 1,189 procurement corruption cases that were investigated during 2019-2023 also show that digitalization does not automatically eliminate corrupt practices, but only changes its modus operandi to be more sophisticated, so an adaptive legal approach to cybercrime modes is needed.

System Operator's Level of Compliance with Data Security Standards

Table 2. Government Agency Compliance with Electronic Procurement Data Security Standards

Compliance Indicators	Findings
Compliance with information security standards (ISO 27001)	Referenced standard: ISO 27001 for Information Security Management System and LKPP guidelines
System security standards implemented by SPSE	Enkripsi RSA (APENDO/SPAMKODOK), SSL/TLS 256-bit, Two-Factor Authentication (2FA)
Implementation of centralized domain management for DNS and SSL	The SPSE domain is centrally managed by LKPP and PT Telkom Indonesia for efficiency and uniformity of security configuration
Implementation of two-step verification (2FA) features	All users are urged to improve system security and reduce unauthorized access
Periodic security audits and evaluations	There are standards for managing operational, server, network, and compliance security (16 standards)

Sources:(Estafen, 2025)

The table above shows that normatively and procedurally, SPSE has been equipped with fairly good security standards. RSA encryption through APENDO/SPAMKODOK developed with BSSN is a relatively strong standard to protect the confidentiality of bid documents. In addition, the implementation of 256-bit SSL/TLS and Two-Factor Authentication (2FA) also shows LKPP's serious efforts in meeting international security standards (LPSE Bogor Regency, 2025). Nevertheless, this compliance still leaves some critical loopholes. First, although SPSE domains are now centrally managed for security configuration efficiency, the fact that there were previously 470 different LPSE subdomains with uneven levels of HTTPS deployment (Burhan, 2022) It shows that technical centralization has not completely solved the problem of diversity of security standards between agencies. Second, the implementation of 2FA is only an appeal, not an absolute obligation for all SPSE users. This means that there are still security loopholes in terms of user authentication. Third, although there are 16 security management standards ranging from operational to (Santoso et al., 2025), there is no data to show the extent to which these standards are actually audited and complied with consistently by all LPSEs in Indonesia.

This inequality between existing standards and uneven implementation reflects what in administrative law theory is referred to as*implementation gap*. LKPP Regulation Number 9 of 2018 concerning SPSE has required system managers to maintain data security, but as noted by (Maulana et al., 2026), the provision is still procedural and has not expressly regulated the sanction mechanism for procurement data protection violations (p. 204). The finding that there are still 30% of procurement that has not been digitally processed exacerbates the situation, as data from manual processes must be integrated into electronic systems without equivalent security guarantees. In the perspective of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), every electronic system operator is required to implement adequate technical and organizational measures to protect personal data in the processing process. However, the implementation of the PDP Law in the procurement sector still faces major challenges due to the complexity of the data involved including the personal data of providers, commitment officials, and procurement committees as outlined by (Lestari et al., 2026). In other words, formal compliance with security standards is not enough; A supervisory mechanism, independent periodic audits, and strict

administrative sanctions are needed for agencies that are negligent in protecting procurement electronic data.

Human Resources Capacity in Electronic Data Protection

Table 3. The Level of Awareness and Competence of Human Resources towards Electronic Data Security

HR Indicators	Findings	Year	Source
Information security awareness level of government employees (national average)	81.67% (category baik)	2024	Dewi, Yudistira & Ruldeviyani, *Indonesian Journal of Computer Science*
Areas of awareness that need to be improved	Password management (79,81%), mobile computing (75,59%), incident reporting (79,81%)	2024	Dewi, Yudistira & Ruldeviyani, *IJCS*
Public perception of improving public service data security	33.2% of respondents stated that data security should be improved and protected	2024	Kompas R&D, in Databoks
Procurement officer certification obligations	PPK and members of the Working Group are required to have certification according to the type of work (Presidential Decree 46/2025)	2025	Presidential Regulation Number 46 of 2025
Human factors as the weakest point of cybersecurity	Phishing attacks posing as SPSE admins still often take victims	2026	School of Procurement, "Data Security in SPSE"
Cybersecurity training for SPSE HR	Training modules are available that include password policy, encryption, incident response	-	LPSE Bekasi City, LPSE SOPs & Regulations

Sources:(Dewi et al., 2024)**.**

The table above reveals that in general, the level of information security awareness of government employees is relatively good with a value of 81.67% (Dewi, Yudistira & Ruldeviyani, 2024). However, this figure still leaves about 18.33% of areas of unconsciousness that need to be corrected. More worrying is the specific finding that the*password management*(79,81%),*mobile computing*(75.59%), and*incident reporting*(79.81%) is the area with the lowest achievement (Dewi, Yudistira & Ruldeviyani, 2024). These areas are particularly relevant to SPSE security, as weak password practices, insecure use of mobile devices to access procurement systems, and low incident reporting can be major gateways for cyberattacks. On the other hand, the public perception that data security in public service applications must be improved (33.2% of respondents, Kompas R&D in Databoks, 2024) shows that the public who use government services, including goods/service providers, still has a low level of trust in their data protection. Affirmation of (Noval et al., 2023) That phishing attacks posing as SPSE admins still often take victims confirms that the human factor is the weakest point in the cybersecurity chain, regardless of how sophisticated the encryption system built by LKPP is. The good news is that Presidential Regulation Number 46 of 2025 has required certification for Commitment Making Officials (PPK) and members of the Election Working Group according to the type of work, which indirectly includes an understanding of electronic data security.

These findings are in line with the theory*human factor in cybersecurity*which states that no technology as advanced as it will be effective without the support of conscious and competent users. In the context of SPSE, bid documents encrypted with APENDO/SPAMKODOK can be easily compromised if the user becomes a victim*phishing*who are disguised as SPSE admins. This reinforces the importance of ongoing education and training, not just one-time certification. (Jannah, 2025) emphasizing that human resources play a role in creating information security risks for organizations, so awareness-raising interventions must be carried out systematically using the*Knowledge, Attitude, Behavior (KAB)*as used in their research. (Wahyudi, 2012) It also reminded that electronic documents in government procurement should be treated the same as paper documents in court evidence, but judges are often still hesitant due to a lack of technical understanding of electronic systems. This doubt can only be overcome if all stakeholders ranging from

procurement officials, committees, to law enforcement officials have an equal understanding of electronic data protection mechanisms. Therefore, the certification obligation in Presidential Regulation 46/2025 should not only focus on the procedural aspects of procurement, but also explicitly include cybersecurity competencies and personal data protection. This is in line with the recommendations (Ananta, 2026) that the*human error*account for 70% of all data leak incidents in government procurement, so legal protection must start from improving the legal and technical competence of procurement actors.

Conclusion

Based on the results of the research and discussion, it can be concluded that the legal protection of electronic data and documents in the government procurement system of goods/services still faces three main challenges. First, cybersecurity vulnerabilities in SPSEs are proven to be high, as evidenced by the leakage of thousands of credential data and the findings of abnormal transactions in the e-Catalog. Second, although technical standards such as RSA encryption and 2FA have been implemented, interagency compliance is uneven and breach sanctions are still weak. Third, human resource capacity is the weakest point, with low awareness in password management and incident reporting. Therefore, it is necessary to harmonize strict regulations, supervise periodic audits, improve human resource competence through mandatory cybersecurity certification, and enforce administrative and criminal sanctions for violators. Without a comprehensive overhaul, the integrity and trust in e-procurement will continue to be threatened.

AI Usage Statement

This section is a statement from the author that the use of Artificial Intelligence (AI) tools in this work is strictly limited to supportive functions, and authors are only permitted to use AI for language editing, grammar checking, and improving clarity and readability. AI was not used to generate core ideas, conduct substantive analysis, interpret data, or draw scholarly conclusions. The author retains full responsibility for the originality, accuracy, and academic integrity of the content, and AI tools are not credited as authors or contributors, in accordance with ethical standards in academic publishing.

References

Adam Khafi Ferdinand, A., Sunarto DM, S., & Maya Shafira, M. S. (2020). Penegakan Hukum dalam Pengadaan Barang dan Jasa Pemerintah oleh Komisi Pengawas Persaingan Usaha (KPPU) dan Komisi Pemberantasan Korupsi (KPK). *Cepalo*, *4*(2), 95–110.

Alfreda, I. J., Permata, R. R., & Ramli, T. S. (2021). Pelindungan dan tanggung jawab kebocoran informasi pada penyedia platform digital berdasarkan perspektif rahasia dagang. *Jurnal Sains Sosio Humaniora*, *5*(1), 1–16.

Ananta, W. V. A. (2026). Keamanan siber pemerintah dan aspek hukum administrasi negara: Tanggung jawab administratif dalam perlindungan sistem informasi publik di era digital. *Jurnal Atribusi Hukum*, *1*(1), 1–15.

Asnawi, E., & Libra, R. (2024). Analisis Yuridis Mengenai Pembuktian Informasi Dan Dokumen Elektronik Pada Sengketa Proses Pemilihan Umum Di Pengadilan Tata Usaha Negara. *HUKMY: Jurnal Hukum*, *4*(1), 553–567.

Burhan, F. A. (2022). *Hampir 12 ribu data pengadaan barang kementerian RI dikabarkan bocor*. Katada.Co.Id. https://katadata.co.id/digital/teknologi/62679cbe74bc6/hampir-12-ribu-data-pengadaan-barang-kementerian-ri-dikabarkan-bocor

Dachlan, A. A., Nabila, A., Putri, N. A., & Nurmasitha, N. (2025). Pertanggungjawaban Hukum Pemerintah Dalam Kebocoran Data Pribadi Pada Penyelenggaraan Pusat Data Nasional. *Jurnal Hukum Samudra Keadilan*, *20*(1), 109–124.

Dewi, K. M. R., Yudistira, R. D., & Ruldeviyani, Y. (2024). Pengukuran Tingkat Kesadaran Keamanan Informasi Pegawai Pada Instansi Pemerintah. *The Indonesian Journal of Computer Science*, *13*(2).

Estafen, G. (2025). *PERENCANAAN PERCEPATAN DIGITALISASI MELALUI PELATIHAN KEAMANAN SIBER JUNIOR PENETRATION TESTER (JPT), DI BADAN SIBER DAN SANDI NEGARA (BSSN)*. Universitas Nasional.

Fiqri, I. N., & Frinaldi, A. (2025). Integrasi Prinsip Hukum Administrasi Negara dalam Transformasi Digital Governance untuk Pelayanan Publik Akuntabel dan Transparan. *Jurnal Ilmu Sosial Dan Humaniora*, *3*(3), 334–346.

Izzah, F. (2026). *Pengelolaan Arsip Dinamis Inaktif Di Record Center Lembaga Ketahanan Nasional Republik Indonesia*. Politeknik STIA LAN Jakarta.

Jannah, M. Z. (2025). Strategi Manajemen Risiko Sumber Daya Manusia dalam Meningkatkan Kinerja Organisasi. *Jurnal Ilmu Manajemen Dan Pendidikan | E-ISSN: 3062-7788*, *2*(3), 820–824.

Korupsi pengadaan barang dan jasa tinggi, Stranas PK KPK luncurkan sistem pengawas e-Katalog. (2024). Tempo. https://www.tempo.co/hukum/korupsi-pengadaan-barang-dan-jasa-tinggi-stranas-pk-kpk-luncurkan-sistem-pengawas-e-katalog-80358

Lestari, C. R., Az'zahra, A. B., Octavia, N. M., Pandia, F. K. B. S., Wirdani, R., & Takhir, S. H. (2026). Analisis Tingkat Kepatuhan Pengelolaan Data Pribadi Pengguna Terhadap Undang-Undang Perlindungan Data Pribadi (UU PDP) Pada Platform Digital. *Adagium: Jurnal Ilmiah Hukum*, *4*(1), 146–168.

Lestari Wulandari, S., & SH, M. H. (2025). *Hukum Perjanjian Dalam Pembangunan Daerah Tertinggal (Kontrak Investasi, Infrastruktur, Dan Pemberdayaan Lokal)*. Penerbit: Kramantara JS.

Maulana, F. K., Purwani, S. P. M. E., & Satyawati, N. G. A. D. (2026). POLITIK HUKUM SANKSI ADMINISTRASI DALAM PERATURAN PRESIDEN TENTANG PENGADAAN BARANG DAN JASA PEMERINTAH. *Kertha Semaya: Journal Ilmu Hukum*, *14*(2), 88–108.

Nomor, U.-U. (11 C.E.). *tahun 2008 tentang Informasi dan Transaksi Elektronik*.

Noval, S. M. R., SH, M. H., Soecipto, S. T., & Ahmad Jamaludin, S. H. (2023). *Perlindungan Hak Digital: Ancaman Privasi di Tengah Serangan Social Engineering-Rajawali Pers*. PT. RajaGrafindo Persada.

Ramadhany, R., Rustiyana, R., Rianty, E., Baskoro, S. E., Hardini, I. R., & Anitasari, M. (2025). *Transformasi Digital Sektor Publik*. Star Digital Publishing,.

Santoso, S., Oktarino, A., Tugiman, T., & Wicaksono, A. D. A. (2025). *Buku Ajar Cyber Security*. PT. Sonpedia Publishing Indonesia.

Sembiring, M. W. (2026). *PERAN TRANSPARANSI DAN AKUNTABILITAS DALAM MENGURANGI RISIKO KORUPSI (Studi Kasus di Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah, Sumatera Utara)*. Magister Hukum, Universitas Islam Sumatera Utara.

Setiawan, D. B., Rokhman, A., & Kurniasih, D. (2024). Peningkatan Efisiensi Dan Transparansi Melalui Sistem Pengadaan Barang Dan Jasa Secara Elektronik Di Sektor Publik. *Journal of Social and Economics Research*, *6*(1), 1613–1623.

Tonny, F., Suhartono, R. M., & Nurcahyo, E. (2025). *TRANSFORMASI PENGADAAN BARANG DAN JASA DI INSTANSI PEMERINTAH*. Kamiya Jaya Aquatic.

Wahyudi, J. (2012). Dokumen elektronik sebagai alat bukti pada pembuktian di pengadilan. *PERSPEKTIF: Kajian Masalah Hukum Dan Pembangunan*, *17*(2), 118–126.

Wijaya, S. (2021). *Pertanggung jawaban pidana korporasi penyedia layanan teknologi informasi elektronik berbasis web dan aplikasi atas adanya kebocoran data pribadi pengguna*.

Zainuddin, M., & Karina, A. D. (2023). Penggunaan Metode Yuridis Normatif Dalam Membuktikan Kebenaran Pada Penelitian Hukum. *Smart Law Journal*, *2*(2), 114–123.