Scientific Journal of Informatics
Vol. 13, No. 2, May 2026
p-ISSN 2407-7658 https://journal.unnes.ac.id/journals/sji/index e-ISSN 2460-0040

A Cross-Platform Assessment of Personal Data Protection Compliance among Electronic System Providers Under Indonesia's PDP Law

Rindy[1]*, Wahyu Catur Wibowo[2]
[1,2]Master of Information Technology, Universitas Indonesia, Indonesia

Abstract.
Purpose: This study evaluates the level of Personal Data Protection (PDP) compliance among Electronic System Providers (ESPs) in Indonesia based on the Personal Data Protection Law (PDP Law) and the Government Regulation concerning the Implementation of Electronic Systems and Transactions.
Methods: A descriptive-evaluative approach was conducted through observations of website and mobile application interfaces from 20 ESPs registered with the Ministry of Communication and Digital Affairs. Compliance was assessed using a binary scoring system based on six PDP indicators: consent mechanisms, privacy notices, TLS/SSL implementation, data disclosure, malicious libraries, and device data access. Descriptive statistical analysis was used to evaluate compliance levels. Instrument validity was established through content validity and expert judgment.
Result: Most ESPs were classified within the moderate compliance category, covering 90% of websites and 80% of mobile applications. Governance-related indicators showed the lowest compliance levels, particularly website consent mechanisms (15%) and website privacy notices (40%) and mobile consent and privacy notice compliance (20%). In contrast, all ESPs complied with technical indicators, including TLS/SSL, malicious library, and device data access requirements.
Novelty: Unlike previous studies that focused on single sectors or platforms, this study provides a cross-platform PDP compliance assessment integrating both technical and governance indicators within a single framework. The findings indicate that governance practices remain the primary challenge in PDP implementation, providing practical recommendations for regulators and ESPs in strengthening personal data protection implementation in Indonesia.

Keywords: Personal data protection, Electronic system providers, Personal data processing, Compliance
Received April 2026 / **Revised** May 2026 / **Accepted** May 2026

INTRODUCTION

According to a survey conducted by the Indonesian Internet Service Providers Association in 2025, the number of internet users in Indonesia has reached 229.4 million, representing approximately 80.66% of the total population. This number indicates that digital technology has become deeply integrated into various aspects of society. In the context of digital transformation, the availability and accessibility of the internet serve as fundamental prerequisites for shifting conventional activities into the digital space.

The use of the internet is no longer limited to communication activities but has expanded across multiple sectors, including education, healthcare, civil administration, and taxation [1]. Data shows that 14.95% of users utilize the internet for online commerce, 8.61% for public services, and 5.84% for financial services. This indicates that digital transformation acts as a key enabler in reshaping interaction patterns, economic activity, and digital service delivery.

However, alongside this advancement, the risk of personal data breaches in Indonesia has also increased. According to the 2024 Indonesian Cybersecurity Landscape report, the National Cyber and Crypto Agency recorded a total of 330,527,636 traffic anomalies during that year alone. These anomalies pose serious risks, and the continued occurrence of data breaches indicates the existence of vulnerabilities in systems processing personal data against both internal and external threats [2]. This condition suggests that both platform implementation and regulatory oversight have not yet been operated optimally [3], [4].

[1]*Corresponding author.
Email addresses: rindy@ui.ac.id (Rindy)*, wibowo@cs.ui.ac.id (Wibowo)
DOI: 10.15294/sji.v13i2.47516

Since the enactment of PDP Law, Indonesia has established a comprehensive legal framework governing of personal data processing activities [4]. This regulation clearly defines the rights of data subject, establishes obligations for data controllers, and provides stricter enforcement mechanisms [5]. The PDP Law outlines comprehensive provisions regarding the responsibilities of data controllers and processors, the implementation of core PDP principles, cross border data transfer, and other related aspects [6]. This law represents a significant milestone for Indonesia and is expected to strengthen the legal framework for personal data protection in response to the evolving digital landscape [7].

Despite the enactment of the PDP regulation, various studies indicate the compliance with the personal data protection requirements remains challenging [8]. Previous research shows that more than 60% of organizations have not fully complied with personal data protection standards [9]. Key challenges include limitations in technological infrastructure, low organizational awareness, and the complexity of policy integration [10].

Several prior studies have examined Personal Data Protection (PDP) compliance using different approaches. Research in the education-sector applications reveals variations in compliance across platforms [11]. A study on job search platforms found that most services do not adequately explain data subject rights in their privacy policies [12]. Meanwhile, research in banking sector identified non-compliance in consent mechanisms and transparency of data processing [13]. Other studies in the e-commerce sector applied GDPR-based audit checklists to assess compliance with data protection principles [14].

However, these studies share common limitations. Most of them focus on a single sector, a single type of platform, or a limited set of compliance indicators. Therefore, it can be concluded that there is still a lack of comprehensive research that evaluates personal data protection compliance across multiple platforms, including both websites and mobile applications, while incorporating both technical and governance-related indicators. To clarify the position of this study in comparison with previous research. Table 1 present a comparison of research objects, platform and indicator used.

Table 1. Comparison of previous studies

Study	Sector	Platform	Indicators	Limitations
[11]	Education	Application	Multi aspect	Limited to a single sector
[12]	Job platforms	Website	Data subject rights	Limited indicators
[13]	Banking	Application	Consent	Limited to a single sector and a single indicators
[14]	Ecommerce	Website	GDPR checklist	Limited to single platform
This Study	Multi sector	Website & Mobile	Six aspects	Cross platform and six indicators

Based on identified research gap, this study aims to assess the level of compliance of ESPs with PDP regulations in Indonesia, including both the Government Regulation concerning the Implementation of Electronic Systems and Transactions and PDP Law. The assessment is conducted using six key indicators, namely:

- SSL/TLS validity
- Consent mechanisms
- Availability of privacy notices
- Potential data exposure
- Presence of malicious library, and
- Appropriateness of device data access

Based on this background and objective, the study formulates the following key research questions:

1. What is the level of ESPs compliance with the PDP Law based on monthly monitoring of websites and mobile applications?
2. Which compliance aspects exhibit the highest and lowest performance?
3. What recommendations can be provided to improve ESPs compliance in the future?

METHODS

In conducting this study, the authors proposed an assessment approach based on compliance with the PDP Law and Government Regulation concerning the Implementation of Electronic Systems and Transactions. This compliance assessment aims to identify gaps in the implementation of personal data protection by

ESPs in relation to the applicable regulatory requirements[15]. The overall workflow of this approach is illustrated in Figure 1.

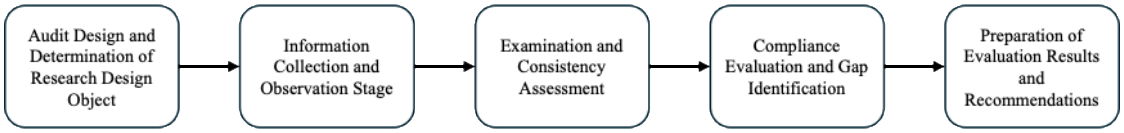

Figure 1. Research methodology flow diagram

This study adopts a descriptive-evaluative approach, which aligns with the nature of compliance assessment by combining empirical observation with analysis based on applicable legal provisions. This approach is consistent with prior studies that examine the alignment between regulatory requirements and their practical implementation at both national and international levels.

Audit Design and Research Object Definition
The audit design was developed by formulating the objective of the evaluation, namely to assess the level of compliance with personal data processing principles under the PDP Law, particularly the principles of transparency, lawful consent, data security and data minimization.

The research subject consists of 20 ESPs selected using purposive sampling based on specific criteria, namely being registered with Ministry of Communication and Digital Affairs. Compliance (KOMDIGI), having a significant number of users, engaging in personal data processing activities, and providing both website-based and mobile application services in Indonesia. A total of 20 ESPs were selected based on data from KOMDIGI. The website and mobile application evaluated in this study originated from the same ESP entities, enabling direct cross-platform comparison of compliance practices within each organization. These ESPs represent various sectors, including finance, retail, education, ICT, and social services. This classification ensures that the study covers diverse sectors with different characteristics, particularly in terms of data sensitivity and regulatory intensity, thereby providing a more comprehensive overview of PDP implementation in Indonesia. The identities of the ESPs were anonymized to protect their reputations.

Data Collection and Observation Stage
Data collection was conducted through document analysis and direct observation. Document analysis involved a literature review of relevant laws and regulations, books, journal articles, official reports from the KOMDIGI, as well as other relevant sources.

The observation aimed to examine the alignment between organizational and technical practices, which are often inconsistent in implementation. Observation was conducted by evaluating the interfaces of websites and mobile applications using a set of compliance indicators, including consent forms, the completeness of privacy notice, data access mechanisms, and personal data security aspects.

Compliance Assessment and Consistency Verification
Compliance assessment was conducted by comparing ESPs implementation on both website and mobile platforms with the evaluation instrument. The instrument consists of a checklist derived from PDP regulatory principles that can be assessed through user interfaces, including lawful and limited data collection, transparency of data purposes and activities, and the implementation of data security measures. In addition to compliance assessment, verification was conducted to evaluate consistency between the statement presented in privacy notices and their actual implementation.

The validity of the instrument was established through content validity. All assessment indictors were developed based on PDP regulatory provisions and aligned with established supervisory practices. To ensure relevance, clarity and the representativeness, the instrument was reviewed through expert judgment in the field of personal data protection. Based on expert evaluation, all indicators were deemed to adequately represent PDP compliance aspects and were therefore considered appropriate for use in this study.

Descriptive statistical analysis was employed, including frequency and proportion-based measures, to evaluate compliance levels across indicators and platforms. This stage represents the core of the study, as it provides a practical overview of PDP implementation across both platforms.

Compliance Evaluation and Gap Identification

The study employed a structured compliance assessment instrument with predefined criteria to ensure consistency across all research objects. The evaluator in this study is the author, acting as independent assessor. The author has no direct involvement or professional relationship with the ESPs under study, ensuring objectivity in the evaluation process. All assessment were conducted independently based on publicly available information. To maintain consistency the evolution process utilized a structured instrument with clearly defined criteria.

The following two indicators were applied to both platforms:

- The existence and compliance of form consent provided to users in accordance with PDP regulations, including explicit consent statements indicating consent for their personal data to be processed for specific purposes.
- The availability and completeness of privacy notice regarding personal data processing activities. The assessment was conducted based on the provisions of PDP Law concerning the minimum requirement for a privacy notice, namely that the notice must be available and at least contain the legality of personal data processing, the purposes of processing, the type and the relevance of personal data being processed, the retention period of personal data, details regarding the information collected, and the right of personal data subject.

For website applications, the specific indicators include:

- The presence and validity of TLS/SSL certificates to ensure secure data transmission (TLS/SSL). This reflects compliance with personal data security guarantees under the Electronic System and Transaction Regulation and the PDP Law. The existence of a TLS/SSL certificate is indicated using an HTTPS domain on the website application. However, the implementation of TLS/SSL does not necessarily reflect comprehensive personal data protection.
- The absence of personal data disclosure on the website interface (without disclosure), namely the absence of publicly displayed personal data on the website application. This indicator also reflects compliance with Government Regulation concerning the Implementation of Electronic Systems and Transactions and the PDP Law. In this study, the focus is limited to the potential exposure of personal data through the interface, excluding other forms of disclosure within broader data processing practices.

For mobile applications, the specific indicators include:

- The appropriateness of device data access requests in accordance with the principle of data minimization (data access). This is important to ensure that collected data is limited to what is necessary for the purposes of personal data processing. This assessment is based on the provisions of Government Regulation concerning the Implementation of Electronic Systems and Transactions and the PDP Law. Mobile applications have characteristics that allow direct access to personal data stored on the device. The examination was conducted using the Yaahzini application by Veganird by uploading the APK file of the mobile application. After the parsing process was completed, the permission analysis output was compared with the information presented in the privacy notice.
- Application security in relation to malicious libraries (malicious library). This indicator evaluates one aspect of mobile application security related to the use of third-party components in application development. This indicator is also in accordance with the provisions of Government Regulation concerning the Implementation of Electronic Systems and Transactions and the PDP Law. Malicious libraries may potentially perform unwanted activities, such as accessing data, running background processes without adequate control, and other harmful actions. The examination was conducted by downloading the APK file of the mobile application to VirusTotal in order to display the detection results of libraries suspected to be malicious.

The differentiation of indicators between website and mobile applications is based on the distinct characteristics of data processing on each platform. Mobile applications do not rely on web-based protocols and do not directly expose potential data disclosure through user interfaces in the same manner as websites. Instead, indicators such as data access appropriateness and protection against malicious libraries are considered more relevant for identifying data processing practices on user devices as well as potential security risks arising from application components.

This study employs a binary scoring system, as presented in Table 2.

Table 2. Scoring criteria for compliance indicators

Score	Criteria
0	Does not comply with PDP requirements
1	Complies with PDP requirements

The use of a binary scoring system is common in prior studies due to its simplicity in distinguishing between two opposing conditions, which are compliance and non-compliance, thereby providing a clear boundary for assessing compliance[16] .

To classify the level of compliance based on the binary scoring results, this study categorizes compliance into three levels as follows:

- High: total binary score > 80%
- Moderate: total binary score between 40–79%
- Low: total binary score < 40%

The result of this stage identifies gaps between regulatory requirements and actual implementation. These gaps form the basis for recommendations discussed in result and discussion.

RESULTS AND DISCUSSIONS

This study examines the compliance of website and mobile applications operated by ESPs registered under the Ministry of Communication and Digital with the applicable PDP regulations in Indonesia, including provisions stipulated in both the Government Regulation concerning the Implementation of Electronic Systems and Transactions and the PDP Law.

The assessment focuses on key aspects as outlined in the research methodology.

Website Application Compliance Results

Based on observations of the website interfaces of the selected ESPs, an evaluation was conducted using predefined indicators that reflect compliance with the relevant provisions under the Government Regulation concerning the Implementation of Electronic Systems and Transactions and the PDP Law. A binary scoring system was applied to each indicator, allowing the overall compliance score to be calculated and subsequently classified into predefined compliance levels. The results of this assessment are presented in Table 3.

Table 3. ESPs compliance in website applications

ESPs	Form Consent	Privacy Notice	TLS/ SSL	No Disclosure	Total	Compliance Level
1	1	1	1	1	4	High
2	1	1	1	1	4	High
3	1	0	1	1	3	Moderate
4	0	0	1	1	2	Moderate
5	0	0	1	1	2	Moderate
6	0	1	1	1	3	Moderate
7	0	0	1	1	2	Moderate
8	0	0	1	1	2	Moderate
9	0	0	1	1	2	Moderate
10	0	0	1	1	2	Moderate
11	0	1	1	1	3	Moderate
12	0	1	1	1	3	Moderate
13	0	0	1	1	2	Moderate
14	0	1	1	1	3	Moderate
15	0	1	1	1	3	Moderate
16	0	0	1	1	2	Moderate
17	0	0	1	1	2	Moderate
18	0	0	1	1	2	Moderate
19	0	1	1	1	3	Moderate

20	0	0	1	1	2	Moderate
Total	15%	40%	100%	100%		

Table 3 shows that 90% of ESPs fall under the moderate level of compliance, indicating that most of them have not fully complied with key indicators, particularly privacy notice or form consent. Meanwhile, only 10% of ESPs demonstrate a high level of compliance, and none are categorized as having low compliance.

The findings also indicate that form consent represents the primary issue in PDP compliance within website applications. Only 15% of ESPs comply with the form consent indicator. This suggests that the majority of ESPs either do not provide a consent mechanism or that the existing consent format does not align with regulatory requirements.

In comparison, 40% of ESPs comply with the privacy notice indicator. Although this figure is higher than that of form consent, it remains relatively low. This indicates that most ESPs have not yet achieved sufficient transparency in informing users about their personal data processing activities.

On the other hand, the indicators related to TLS/SSL implementation and the absence of data disclosure on website interfaces show that all ESPs have fulfilled these technical aspects. This suggests that technical security measures have been relatively well implemented and tend to be prioritized in achieving compliance within electronic systems.

Results of Mobile Application Compliance Monitoring

The assessment results of the indicators based on interface observation of mobile applications are presented in Table 4.

Table 4. ESPs compliance in mobile applications

ESPs	Form Consent	Privacy Notice	Data Access	Malicious Library	Total	Compliance Level
1	1	1	1	1	4	High
2	1	1	1	1	4	High
3	1	1	1	1	4	High
4	0	0	1	1	2	Moderate
5	0	0	1	1	2	Moderate
6	0	0	1	1	2	Moderate
7	0	0	1	1	2	Moderate
8	0	0	1	1	2	Moderate
9	0	0	1	1	2	Moderate
10	0	0	1	1	2	Moderate
11	0	0	1	1	2	Moderate
12	1	1	1	1	4	High
13	0	0	1	1	2	Moderate
14	0	0	1	1	2	Moderate
15	0	0	1	1	2	Moderate
16	0	0	1	1	2	Moderate
17	0	0	1	1	2	Moderate
18	0	0	1	1	2	Moderate
19	0	0	1	1	2	Moderate
20	0	0	1	1	2	Moderate
Total	20%	20%	100%	100%		

Table 4 shows that the majority of ESPs in mobile applications remain at a Medium level of compliance, accounting for 80%. This indicates that most ESPs have not yet fulfilled the consent form and privacy notice indicators. Meanwhile, 20% of ESPs have achieved a High level of compliance. No ESPs was categorized as Low compliance, indicating that all ESPs have at least partially met the compliance indicators.

In terms of technical implementation, the Data Access and Malicious Library indicators have been fully implemented by all ESPs. This indicates that ESPs place strong emphasis on data minimization practices and application security.

Comparative Results of Website and Mobile Application Compliance Monitoring
Based on Tables 2 and 3, it can be observed that the two platform-specific technical indicators, namely TLS/SSL and disclosure absence for websites, as well as Data Access and Malicious Library for mobile applications, have been fully fulfilled by all ESPs across both platforms. This finding indicates that ESPs do not encounter significant challenges in meeting technical and operational aspects of electronic system management.

However, the two shared indicators across both website and mobile applications, namely the consent form and privacy notice, remain the primary issues in PDP compliance.

Consent form
An interesting finding emerged in the consent form indicator, where one ESPs did not meet the requirement on the website platform but fulfilled it on the mobile application. This may be attributed to the generally more controlled ecosystem of mobile applications, such as digital application distribution platforms that require permission requests prior to accessing personal data.

The consent form is regulated under Articles 20–22 of PDP Law, which stipulate several requirements for obtaining data subject consent, including that consent must be explicit, must include information regarding data processing activities, and must be provided in written and recorded form. Previous studies have shown that the design of consent forms must comply with applicable personal data protection regulations [17].

Although this study does not explicitly distinguish whether non-compliance with the consent form indicator is due to the absence of the mechanism or due to misalignment with regulatory requirements, the findings in mobile applications allow for further interpretation.

Identified PDP non-compliance in mobile applications may reflect issues of implementation quality and regulatory conformity rather than the complete absence of mechanisms. In the context of this study, such interpretation should be regarded as an initial indication requiring further verification.

Privacy notice
Another notable finding emerged in the privacy notice indicator, where some ESPs only provided a privacy notice on one platform, either the website or the mobile application. This indicates variations in implementation practices regarding the provision of information on personal data processing.

Such a condition may occur when ESPs provide a privacy notice on only one platform and consider it sufficient to represent all data processing activities. However, the PDP regulations do not explicitly state that compliance with privacy notice requirements may be limited to a single platform.

A privacy notice is information that explains what personal data is collected, the purposes of processing, the parties that may receive the data, and the rights of personal data subjects [18]. From a regulatory perspective, Article 5 of PDP Law and Article 14 paragraph (1) letter f of Government Regulation concerning the Implementation of Electronic Systems and Transactions stipulate the obligation of data controllers to provide clear information regarding identity, legal basis, processing purposes, and accountability in personal data management. Thus, transparency obligations are inherently attached to every data processing activity, regardless of the media or platform used.

Accordingly, the practice of providing a privacy notice on only one platform by ESPs operating multiple platforms can be viewed as a minimal interpretation of regulatory compliance. Although it may be considered practically sufficient in certain contexts, this approach has the potential to create information asymmetry for users accessing services through other platforms.

Analysis of Compliance Patterns and Implementation Gaps
Overall compliance levels across website and mobile applications are illustrated in Figure 2.

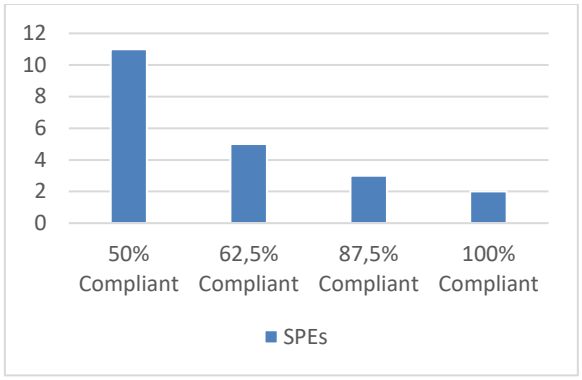

Figure 2. Overall compliance percentage across all ESPs

Based on Figure 2, it can be observed that 11 ESPs achieved an overall compliance percentage of 50%, followed by five ESPs with a compliance percentage of 62,5%, three ESPs with a compliance percentage of 87,5%, and two ESPs that achieved 100% compliance. These findings indicate that the overall compliance level of ESPs is predominantly categorized as moderate. This condition is largely caused by the imbalance between compliance fulfilment in technical and governance-related aspects. Figure 3 illustrates the gap in PDP compliance between technical and organizational aspects.

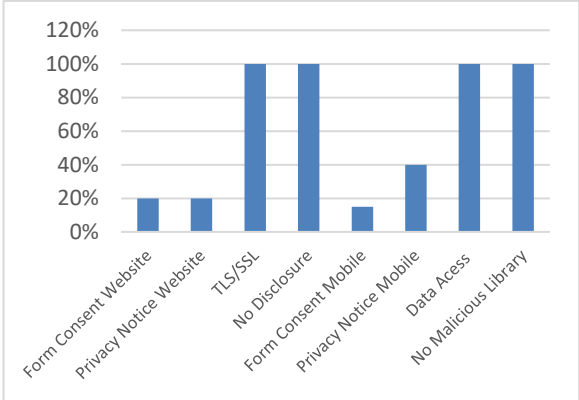

Figure 3. Gap between indicators

The finding presented in Figure 3 are consistent with previous studies indicating that the implementation of data protection compliance involves interactions between technical and organizational domains, which in practice are often fragmented and insufficiently integrated [19]. In addition, a technical control-based approach alone does not guarantee full compliance unless it supported by legal and organizational aspects [20]. Since regulations also require the simultaneous implementation of both technical and organizational measures, compliance inherently encompasses two distinct yet interconnected domains [21]. Therefore, the dominance of technical compliance observed in this study reflects a form of partial compliance resulting from the lack of optimal governance integration.

The dominance of technical aspects in this study can be explained by the characteristics of data protection regulation implementation. Previous studies indicate that regulatory requirements are complex and often require interpretation during implementation [22], particularly in governance-related aspects such as consent and transparency. Organizations also continue to face challenges in achieving compliance [23], especially in areas evolving organizational processes and structures. Several key factors pose challenges for organizations in implementing PDP) governance aspects, including a lack of PDP knowledge and expertise, the high costs associated with achieving PDP compliance, difficulties in modifying internal business processes to align with PDP regulations, and governance-related challenges such as transforming organizational culture and policies, employee resistance to change, as well as difficulties in monitoring and ensuring third-party compliance with PDP requirements [24].

Low compliance in governance aspects has significant implications for the effectiveness of personal data protection. This condition may increase the risk of violating the principle of lawful personal data collection. If ESPs fail to fulfill their obligations, they may be subject to administrative sanctions [25]. Beyond legal sanctions, organizations that fall to comply with personal data protection obligations may face various consequences, including low of customer trust, financial losses, legal penalties, service disruptions, contractual violations, operational disturbances with international regulations [26].

Therefore, personal data protection should be regarded not only as a legal obligation but also a critical factor in building customer trust and a strategic asset for the sustainability of digital businesses [27].

Practical Recommendations

Based on the main findings regarding the significant gap between technical and governance compliance, this study proposes several practical recommendations as follows:

- KOMDIGI as the regulator, is recommended to develop technical guidelines that provide standardized templates for privacy notice and consent form to promote consistent implementation across all ESPs sectors. Previous studies emphasize that the clear technical regulatory guidance is a key factor in improving organizational compliance with personal data protection regulation in Indonesia [28], [29].
- ESPs are encouraged to appoint a Data Protection Office (DPO) who can bridge technical information technology aspect with the legal obligations mandated under the PDP Law. The DPO play a crucial role in supporting the effectiveness implementation of personal data protection within organization [30], [31].
- ESPs should conduct periodic self-audit to ensure consistency between privacy policies implemented on website and mobile platforms, thereby minimizing information gaps experienced by users. Audit are considered essential in assessing whether platform complies with applicable standards and regulations [30], [32].
- ESPs are advised to adopt a Privacy by Design approach by integrating standardized security controls to ensure automated and sustainable compliance [21]. The implementation of privacy principle from the design phase has been shown to effectively align system functional requirement with organizational data protection governance obligation [23].

Research Limitation and Future Research

This study has several limitations, as it only focuses on observations of publicly accessible interfaces. Actual data processing activities on the server side could not be verified using this approach. In addition, the research sample was limited to 20 registered ESPs.

Future studies are expected to conduct more comprehensive assessments, including full-scale audits of personal data processing activities, to obtain deeper and more comprehensive findings regarding PDP compliance implementation.

CONCLUSION

This study evaluated the level of compliance of Electronic System Providers (ESPs) with personal data protection regulations in Indonesia by comparing the implementation of Personal Data Protection (PDP) principles across website and mobile application platforms using an integrated cross-platform assessment framework. The framework combines technical and governance-related indicators, enabling a more comprehensive evaluation of PDP implementation across different digital platforms.

The findings indicate the most ESPs fall within the medium compliance category, with 90% of website platforms and 80% of mobile applications classified at this level. Governance-related indicators demonstrated significantly lower compliance levels across both platforms. On website platforms, compliance with consent mechanisms and privacy notices reached only 15% and 40%, respectively. Similarly, on mobile applications, compliance with consent mechanisms and privacy notices was only 20% for both indicators. In contrast, technical indicators, including TLS/SSL implementation, device data access controls, and malicious library assessments, showed consistently high compliance across all evaluated ESPs.

These finding answer the research objective by demonstrating that PDP implementation among ESPs remains insufficient. The imbalance between technical and governance practices became the primary factor

contributing to the overall moderate compliance level. This condition indicates that current compliance practices are still partial rather than fully comprehensive.

The boarder implication of this study is that effective personal data governance cannot rely solely on technical safeguards. Stronger organizational accountability, transparency mechanisms, and governance integration are equally important to ensure sustainable PDP implementation. Weak governance practices may increase the risk of regulatory violations and reduce public trust in digital services.

Based on these findings, regulators are encouraged to provide more practical and implementable compliance guidelines, particularly regarding consent mechanisms and privacy notices. Meanwhile, ESPs need to ensure alignment between policies, organizational processes, and technical control through periodic audits, internal governance strengthening, and consistent cross-platform privacy practices.

This study is limited to observations of publicly acceessible interfaces and does not assess server-side data processing activities. Future research may adopt more in-depth and comprehensive approaches, including technical audits and organizational assessments, to obtain broader insights into PDP implementation practices.

Overall, this study highlight that the main challenge in PDP implementations lies not only in technical safeguards, but also in the ability of organizations to integrate governance and technical compliance practices in a balanced and sustainable manner.

REFERENCES

[1] C. Abdullah, N. Durand, and R. M. Moonti, "Transformasi Digital dan Hak atas Privasi: Tinjauan Kritis Pelaksanaan UU Perlindungan Data Pribadi (PDP) Tahun 2022 di Era Big Data," *Amandemen: Jurnal Ilmu pertahanan, Politik dan Hukum Indonesia*, vol. 2, no. 3, pp. 233–241, Jun. 2025, doi: 10.62383/amandemen.v2i3.1073.

[2] Tanti Kirana Utami, Kayla Andini Putri, Salsa Octaviani Suryanto, and Fina Asriani, "Personal Data Breach Cases in Indonesia: Perspective of Personal Data Protection Law," *Journal Customary Law*, vol. 2, no. 2, p. 21, Feb. 2025, doi: 10.47134/jcl.v2i2.3742.

[3] W. Koswara, "Implementasi Peraturan Perlindungan Data Pribadi oleh Penyelenggara Sistem Elektronik Dikaitkan dengan Teori Keadilan dan Kepastian Hukum," *Jurnal Paradigma Hukum Pembangunan*, vol. 7, no. 2, Aug. 2022, doi: 10.25170/paradigma.v7i2.3681.

[4] R. Sitorus, J. Zaman Felix Saragih, and R. Banke, "Kendala Pelaksanaan Perlindungan Data Pribadi," *Locus: Jurnal Konsep Ilmu Hukum*, vol. 5, no. 1, Mar. 2025, doi: 10.56128/jkih.v5i1.438.

[5] M. Gustryan and Z. A. Hoesein, "Peran Undang-Undang ITE dan Undang-Undang Perlindungan Data Pribadi dalam Perlindungan Data dan Privasi di Era Ekonomi Digital," *Jurnal Minfo Polgan*, vol. 14, no. 2, pp. 3333–3343, Dec. 2025, doi: 10.33395/jmp.v14i2.15746.

[6] N. Afifah, "Tanggung Jawab Hukum Platform E-Commerce terhadap Keamanan Data Pribadi Pengguna: Analisis Berdasarkan UU PDP 2022," *Jurnal Legalitas*, vol. 2, no. 1, pp. 29–38, Jan. 2024, doi: 10.58819/jle.v2i1.165.

[7] F. Razi, H. tuasikal, and D. Pratiwi Markus, "Implementation and Challenges of the Personal Data Protection Law in Indonesia," *Indonesian Journal of Social Technology*, vol. 5, no. 12, pp. 6559–6565, Dec. 2024, doi: 10.59141/jist.v5i12.1285.

[8] M. A. Rinjani and R. Firmansyah, "Hambatan Implementasi UU 27/2022 dan Strategi Penguatan Perlindungan Data Pribadi di Indonesia," *Jurnal Analisis Hukum*, vol. 8, no. 1, pp. 70–83, Apr. 2025, doi: 10.38043/jah.v8i1.6793.

[9] S. Hukom, N. Humi, and I. Lukman, "The Urgency of Legal Regulation for Personal Data Protection in Indonesia in the Big Data Era," *Hakim: Jurnal Ilmu Hukum dan Sosial*, vol. 3, no. 1, pp. 974–992, Feb. 2025, doi: 10.51903/hakim.v3i1.2291.

[10] G. F. Hisyam and M. A. Rojabi, "Penerapan Undang-Undang Perlindungan Data Pribadi Nomor 27 Tahun 2022: Studi Kasus Pada Industri FMCG," *Nusantara Journal of Multidisciplinary*

Science, vol. 2, no. 7, pp. 1544–549, 2025, Accessed: May 03, 2026. [Online]. Available: https://jurnal.intekom.id/index.php/njms

[11] G. Ayu, W. P. Surya, S. N. Maharani, P. M. Yonata, and A. Eldrian, "Audit Kepatuhan Aplikasi Pendidikan di Indonesia terhadap UU Pelindungan Data Pribadi," 2025. doi: 10.5281/zenodo.17815941.

[12] G. Ghoniyyu Atha Akbar, F. Fadaukas Ahmad, and M. Ramdhan Zulfikri, "Audit Kepatuhan Platform Pencarian Kerja terhadap UU Perlindungan Data Pribadi," *Etika Teknologi Informasi*, vol. 1, no. 2, pp. 1–20, 2025, Accessed: Mar. 17, 2026. [Online]. Available: https://www.researchgate.net/publication/398328595_audit_kepatuhan_platform_pencarian_kerja_terhadap_uu_perlindungan_data_pribadi

[13] Nyimas Safira Septiana, Sinta Dewi, and Laina Rafianti, "Juridical Analysis of the Application of Data Minimization Principles in Mobile Banking According to the Personal Data Protection Law and EU GDPR 2018," *Justices: Journal of Law*, vol. 4, no. 3, pp. 154–168, Aug. 2025, doi: 10.58355/justices.v4i3.203.

[14] R. Muhammad Raissa Wirabuwana and F. Rizky Susanto, "Audit Kepatuhan Platform E-Commerce Terhadap UU Perlindungan Data Pribadi," *Etika Teknologi Informasi*, vol. 1, p. 2025, 2025, Accessed: May 03, 2026. [Online]. Available: https://www.researchgate.net/publication/398328875_Audit_Kepatuhan_Platform_E-Commerce_Terhadap_UU_Perlindungan_Data_Pribadi

[15] E. Fallatah, "Ensuring Compliance: Data Privacy Audits Under Global Privacy Regulations," *International Journal of Applied Economics, Finance and Accounting*, vol. 22, no. 2, pp. 133–144, Jun. 2025, doi: 10.33094/ijaefa.v22i2.2308.

[16] D. S. Guamán, D. Rodriguez, J. M. del Alamo, and J. Such, "Automated GDPR compliance assessment for cross-border personal data transfers in android applications," *Comput. Secur.*, vol. 130, Jul. 2023, doi: 10.1016/j.cose.2023.103262.

[17] P. F. A. van Erkel, D. N. Hopmann, M. Skovsgaard, and L. Terren, "The Role of Consent Form Design Under GDPR: A Survey Experiment," *Int. J. Public Opin. Res.*, vol. 36, no. 1, 2024, doi: 10.1093/ijpor/edad047.

[18] I. Wagner, "Privacy Policies across the Ages: Content of Privacy Policies 1996-2021," *ACM Transactions on Privacy and Security*, vol. 26, no. 3, May 2023, doi: 10.1145/3590152.

[19] O. Klymenko, S. Meisenbacher, and F. Matthes, "Identifying Practical Challenges in the Implementation of Technical Measures for Data Privacy Compliance," in *29th Americas Conference on Information Systems (AMCIS 2023)*, Jun. 2023. doi: 10.48550/arXiv.2306.15497.

[20] D. Granata, M. Mastroianni, M. Rak, P. Cantiello, and G. Salzillo, "GDPR compliance through standard security controls: An automated approach," *Journal of High Speed Networks*, vol. 30, no. 2, pp. 147–174, 2024, doi: 10.3233/JHS-230080.

[21] C. Koolen, K. Wuyts, W. Joosen, and P. Valcke, "From insight to compliance: Appropriate technical and organisational security measures through the lens of cybersecurity maturity models," *Computer Law & Security Review*, vol. 52, p. 105914, 2024, doi: 10.1016/j.clsr.2023.105914.

[22] C. Negri-Ribalta, M. Lombard-Platet, and C. Salinesi, "Understanding the GDPR from A Requirements Engineering Perspective—A Systematic Mapping Study on Regulatory Data Protection Requirements," *Requir. Eng.*, vol. 29, no. 4, pp. 523–549, Dec. 2024, doi: 10.1007/s00766-024-00423-4.

[23] Z. S. Li, C. Werner, N. Ernst, and D. Damian, "Towards privacy compliance: A design science study in a small organization," *Inf. Softw. Technol.*, vol. 146, no. C, Jun. 2022, doi: 10.1016/j.infsof.2022.106868.

[24] Y. Smirnova and V. Travieso-Morales, "Understanding challenges of GDPR implementation in business enterprises: a systematic literature review," *International Journal of Law and Management*, vol. 66, no. 3, pp. 326–344, Apr. 2024, doi: 10.1108/IJLMA-08-2023-0170.

[25] C. P. Ramadhan, E. Charlest, M. B. Ambarita, and S. A. Hutapea, "Analisis Kewajiban Penyelenggara Sistem Elektronik dalam Memberikan Perlindungan Bagi Anak: Konteks UU Nomor 1 Tahun 2024," *Demokrasi: Jurnal Riset Ilmu Hukum, Sosial dan Politik*, vol. 2, no. 2, pp. 21–27, Apr. 2025, doi: 10.62383/demokrasi.v2i2845.

[26] R. Maharani and A. L. Prakoso, "Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital," *Jurnal USM Law Review*, vol. 7, no. 1, pp. 333–347, Mar. 2024, doi: 10.26623/julr.v7i1.8705.

[27] M. Fitria, D. Iryani, and P. Aji Hari Setiawan, "Perlindungan dan Tanggung Jawab Hukum Kebocoran Informasi Data Pribadi pada Penyelenggara Sistem Elektronik Berdasarkan Perspektif Rahasia Dagang," *Jurnal Ilmiah Indonesia, Januari*, vol. 5, no. 1, pp. 1–8, Jan. 2025, doi: 10.36418/cerdika.v4i12.871.

[28] Wyanda Kinanti Syauqi Ramadhani and Sidi Ahyar Wiraguna, "Implementasi Pelindungan Data Pribadi dalam Sistem Informasi pada Perusahaan Jasa Keuangan," *Perspektif Administrasi Publik dan hukum*, vol. 2, no. 2, pp. 158–175, Apr. 2025, doi: 10.62383/perspektif.v2i2.248.

[29] A. P. Susanty and F. Bintarawati, "Tinjauan Hukum terhadap Implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dalam Layanan Finansial Digital Article Info ABSTRAK," *Sanskara Hukum dan HAM*, vol. 4, no. 02, pp. 164–172, Dec. 2025, doi: 10.58812/shh.v4.i02.

[30] Y. Wibowo, I. A. DPW, and Ismiyanto, "Tinjauan Yuridis Tentang Perlindungan Data Pribadi Masyarakat Pada Era Digitalisasi," *Jurnal Serambi Hukum*, vol. 18, no. 1, 2025, doi: 10.36418/serambihukum.v18i01.121.

[31] S. A. Wiraguna, "Strengthening the Functional Autonomy of Data Protection Officers Under Indonesia's PDP Law 2022: A Critical Legal and Institutional Review," *Jurnal Sosial Politik, Pemerintahan dan Hukum*, vol. 4, no. 3, Nov. 2025, doi: 10.59818/jps.v4i3.2317.

[32] F. H. Zannah, N. Dihniah, M. S. Agil, S. Informasi, S. Thaha, and S. Jambi, "Studi Explanatory tentang Pengaruh Sosialisasi Peran Audit dan Aspek Hukum terhadap Tingkat Kesadaran Keamanan Informasi Mahasiswa Baru," *Jurnal Penelitian Nusantara*, vol. 1, no. 12, pp. 381–388, Dec. 2025, doi: 10.59435/menulis.v1i12.791.