Electronic Integrated Computer Algorithm Journal
Vol. 4, No. 1, October 2026, pp 8~17

ISSN: 3031-0350, DOI: 10.62123/enigma.v4i1.188

Privacy and Data Protection Governance for Implementing Indonesia's Personal Data Protection Law (Law No. 27/2022): A Structured Literature Review

Deni Sulaeman[1*], Ferri Fatra[1] , M. Galih Fikran Syah[1], Ilman Manarul Qori[1], Muharman Lubis[1]

[1] *Information System, School of Industrial and System Engineering, Telkom University*, Indonesia.

DOI : 10.62123/enigma.v4i1.188

Received : June 20, 2026
Revised : July 06, 2026
Accepted : August 08, 2026

Keywords:
Data Governance, Personal Data Protection, Privacy Compliance, Privacy Governance, Regulatory Compliance

ABSTRACT

Indonesia's Law No. 27 of 2022 on Personal Data Protection (PDP Law) imposes extensive duties on controllers and processors, yet organizational governance for implementation remains unevenly documented. This structured literature review, informed by PRISMA reporting principles, synthesizes 23 governance-focused peer-reviewed publications (2022–2026) identified through a transparent purposive corpus strategy. No multi-database search was conducted in this study. Implementation is influenced by legal certainty, institutional accountability (including supervisory officer models), sector capacity, third-party ecosystem risk, rights interoperability, measurable compliance tools, and automated decision-making challenges. Privacy governance (74%), audit and compliance assessment (48%), and integrated data governance (39%) are the most frequent components; data protection impact assessment is rarely explicit. Governance structures are portrayed as prerequisites for compliance where accountability, assessment instruments, and platform intermediaries align. A seven-layer implementation framework for the PDP Law is proposed. Limitations include the purposive corpus, limited Indonesian empirical evidence, and the absence of exhaustive database screening.

1. INTRODUCTION

1.1 Background

Digital economic growth has increased the scale and sensitivity of personal data processing across Indonesia's public and private sectors. In response, the state enacted Law No. 27 of 2022 on Personal Data Protection (PDP Law) [1], which establishes rights of data subjects, duties of personal data controllers and processors, breach notification, accountability mechanisms, and institutional oversight including supervisory officers for certain organizations. Unlike a symbolic policy statement, the PDP Law imposes operational expectations organizational policies, security measures, governance roles, and documented compliance that require privacy and data protection governance rather than ad hoc technical fixes alone.

Parallel international experience, particularly under the European General Data Protection Regulation (GDPR), demonstrates that legal text alone does not guarantee effective protection; implementation depends on governance arrangements, institutional capacity, ecosystem coordination, and tools that make compliance observable. As Indonesian organizations move from legal awareness to operational maturity, a structured understanding of what the scholarly literature already recommends and where evidence remains thin is needed.

1.2 Problem Statement and Research Gap

Primary studies on Indonesian PDP implementation are emerging but remain fragmented: normative legal analyses dominate, sectoral studies (e-commerce, fintech, zakat platforms, digital government) use incompatible frames, and international literature rarely maps findings onto Indonesia's institutional vocabulary (e.g., *pengendali data*, *pejabat supervisi*, *pembaharuan* hak subjek data). Existing systematic or bibliometric reviews in adjacent fields were deliberately excluded from this synthesis to avoid reviewing "reviews about reviews." The gap addressed here is the absence of a transparent structured consolidation of primary governance-focused studies that can inform a national implementation framework.

1.3 Objectives and Research Questions

This structured review pursues four objectives aligned with four research questions (RQs) in table 1:

*Corresponding Author Email: denisulaeman@student.telkomuniversity.ac.id

Table 1. This structured review pursues four objectives aligned

Objective	RQ
Identify implementation factors	**RQ1:** What are the main factors influencing personal data protection implementation in organizations?
Map governance components	**RQ2:** What privacy/data protection governance components appear most frequently?
Explain governance–compliance linkage	**RQ3:** How is governance associated with regulatory compliance?
Propose implementation framework	**RQ4:** What framework can support PDP Law implementation?

1.4 Contribution

Contributions are threefold: (1) a transparent structured map of 23 governance-focused publications (2022–2026); (2) a quantified thematic profile of governance components with explicit identification of under-researched data protection impact assessment (DPIA) practice; and (3) a layered implementation framework integrating Indonesian scholarship with comparative evidence from GDPR, Thailand PDPA, and EU AI governance discourse.

1.5 Contribution

Section 2 situates core concepts. Section 3 describes the structured review method. Section 4 presents results and integrated discussion by RQ. Section 5 concludes with implications, limitations, and future research.

2. LITERATURE REVIEW

2.1 Privacy Governance and Data Governance

Privacy governance refers to the structures, policies, roles, and accountability mechanisms that steer how personal data are collected, used, shared, and retained. Data governance is broader covering data quality, stewardship, architecture, and lifecycle management but recent scholarship increasingly integrates PDP obligations into enterprise data governance rather than treating privacy as a downstream legal checklist [2][3]. In public–private regulatory environments, governance may combine state enforcement with industry self-regulation and cross-border regimes such as GDPR and APEC Cross Border Privacy Rules [4].

For organizations, recurring elements include leadership commitment, documented privacy policies, role clarity (controller/processor), third-party management, and auditability. Empirical education-sector research demonstrates that absence of explicit privacy governance in vendor chains creates compliance vulnerability even when institutions believe they are GDPR-aligned [5].

2.2 Regulatory Compliance and Rights-Enabling Infrastructure

Compliance is not merely symbolic adherence to statutes; it requires observable practices: privacy notices, scoring, maturity assessment, and interoperability of data subject rights [6][7]. Comparative Indonesian scholarship emphasizes data portability and interoperability as legal rights requiring technical and organizational infrastructure, learning from EU/UK experience [8]. Intermediaries and voluntary standards can materially enable or obstruct portability compliance in platform ecosystems [9][10]. Accountability principles tie governance to compliance through institutional roles. Indonesia's supervisory officer (*pejabat supervisi*) regime, compared with Swedish data protection officer practice, illustrates how accountability is operationalized through dedicated oversight functions [10].

2.3 AI Governance and Automated Decision-Making

Automated and AI-mediated processing introduces layered compliance. EU scholarship analyzes generative AI under interacting liability, privacy, and cybersecurity rules [11], while the EU AI Act is discussed as adding compliance pathways that must remain consistent with GDPR data protection duties [12]. In Indonesia's digital state context, constitutional due process and explanation/correction rights become governance constraints on algorithmic public decision-making [13] a concern adjacent to DPIA-style risk governance, which remains rarely named in the current corpus.

2.4 Sectoral Implementation Contexts

Sector studies show that governance models must be contextualized: e-KYC in digital finance [14], consumer marketplaces and sanctions [5], zakat institutions adopting PDP-based organizational reform [15], and metaverse-related co-regulation proposals [2]. These works collectively signal that implementation factors are sector-mediated even when statutory duties are uniform.

2.5 Literature Gap Motivating This Review

Prior work establishes conceptual richness but lacks an integrated, transparent structured synthesis mapping governance components to Indonesia's PDP Law implementation priorities, especially DPIA, breach governance, and empirical compliance measurement. The present review addresses that gap. Table 2 summarizes how regulatory foci differ across Indonesia, the EU, and Thailand within the included scholarship.

Table 2. Comparative regulatory focus in included scholarship (illustrative, not exhaustive statutory mapping)

Dimension	Indonesia (UU PDP Law 27/2022)	EU (GDPR)	Thailand (PDPA)
Primary anchor in corpus	[8], [10], [13], [14], [15], [16], [17], [18], [19]	[3], [4], [5], [6], [7], [9], [11], [12], [20], [21], [22], [23], [24] (subset)	[2], [6]
Accountability mechanism	Supervisory officer (pejabat supervisi)	Data protection officer	Organizational accountability
Rights emphasis in literature	Portability, interoperability [8]	Ecosystem, platforms [6], [21], [24]	Compliance scoring SMEs [6]
Governance integration	Sector normative (e-commerce, fintech)	Empirical spillover, tools	Management system framework [2]
Emerging tech	Algorithmic state [13]	AI Act layering [11], [12]	Limited in corpus

3. RESEARH METHODS

3.1 Review Design and Scope

This study adopts a structured **literature review** informed by **PRISMA 2020 reporting principles** [25]. It does **not** claim to be a fully exhaustive PRISMA-based systematic literature review, because scholarship on PDP Law implementation especially empirical governance studies in Indonesia remains limited and emerging. PRISMA is used as a **reporting guide** to make identification, screening, eligibility, and synthesis transparent.

Publication years **2022–2026** and languages **English and Indonesian** were applied. The unit of analysis is the peer-reviewed journal article (or, where screened, reputable conference proceedings) addressing privacy or data protection governance, accountability, compliance, or institutional implementation mechanisms.

3.2 Literature Identification Strategy

Literature was identified through a purposive corpus **strategy** only. **No automated multi-database search** (e.g., Scopus, Web of Science) was executed for this study. The corpus was built by **systematic curation** of 25 candidate publications judged relevant to PDP governance, GDPR/PDPA comparators, and AI-related data protection (2022–2026). Curation applied the indexing thresholds in Table 2: **SINTA 3+** or **Scopus Q3+**, with a documented exception for Indonesia-core law journals at **SINTA 1–2** when publications directly addressed UU PDP implementation. Sources included peer-reviewed journals and reputable international outlets identified through prior domain mapping of Indonesia PDP scholarship and comparative governance literature.

This approach is appropriate because PDP Law implementation research especially empirical governance studies in Indonesia remains limited. A structured review based on a transparent purposive corpus is preferable to claiming exhaustive database coverage that was not performed. To make identification auditable and reproducible, the purposive corpus was assembled through six explicit steps. Step 1: the review scope was fixed to four concept clusters aligned with the research questions — privacy/data protection governance, regulatory compliance, GDPR/PDPA comparators, and AI-related data protection (2022–2026). Step 2: candidate venues were mapped from prior domain knowledge of Indonesian PDP scholarship and comparative governance literature, prioritizing SINTA- and Scopus-indexed journals. Step 3: the indexing thresholds in Table 2 (SINTA 3+ or Scopus Q3+, with the documented I4b exception for Indonesia-core law journals) were applied. Step 4: English- and Indonesian-language items within the 2022–2026 window were retained. Step 5: each candidate was checked for topical relevance against RQ1–RQ4 and for a discernible governance, legal, or organizational analytic layer. Step 6: all decisions, indexing tiers, and inclusion/exclusion codes were recorded in a screening log so that the corpus can be reconstructed and independently scrutinized.

Because no automated multi-database search was performed, this identification strategy carries three acknowledged limitations. First, coverage: relevant studies indexed only in databases not manually surveyed may have been missed, so the corpus is illustrative rather than exhaustive. Second, bias: purposive curation guided by prior domain mapping can favour already-visible or author-familiar work, introducing a risk of selection bias toward normative Indonesian and GDPR-oriented scholarship. Third, reproducibility: although the screening log makes the present selection transparent and repeatable, a different reviewer applying a full database protocol could assemble a partially different corpus. These constraints are revisited in Section 5, and they are the reason the framework proposed in Section 4.5 is presented as a provisional, analytically grounded proposal rather than an exhaustive or definitive model.

3.3 Inclusion and Exclusion Criteria

Table 3 summarizes eligibility rules applied during screening.

Table 3. Inclusion and exclusion criteria for the structured literature review

Code	Criterion Type	Criteria Description	Operational Rule
I1	Inclusion	Peer-reviewed publication	Journal article or reputable conference proceedings

I2	Inclusion	Publication year 2022–2026	Metadata year filter
I3	Inclusion	Topical relevance	Privacy/data protection governance, compliance, DPO/supervisory officer, PbD, DPIA, breach, rights, AI governance
I4	Inclusion	Indexing quality	SINTA 3+ or Scopus Q3+ minimum
I4b	Inclusion	Indonesia-core exception	SINTA 1–2 Indonesian law journals if directly on UU PDP (documented in screening log)
I5	Inclusion	Full text available	Publisher, repository, or legal open access
E1	Exclusion	Duplicate record	Same DOI or title
E2	Exclusion	Review-type paper	Systematic review, bibliometric review, pure narrative review
E3	Exclusion	Non peer-reviewed	Blog, news, industry white paper
E4	Exclusion	Unavailable full text	After reasonable retrieval effort
E5	Exclusion	Cybersecurity-only	No privacy governance dimension
E6	Exclusion	Technical-only	Engineering/crypto without governance linkage (technical-artefact-only; technical themes analysed at the governance or legal interface are retained)
E7	Exclusion	Opinion without method	No discernible research method

3.4 Screening and Selection Procedure

All 25 candidate publications underwent title/abstract and full-text screening using Table 2. Twenty-three publications entered the core thematic synthesis and frequency analysis. Two publications were excluded from core coding because full-text assessment showed predominantly technical content without sufficient standalone governance synthesis:

- Karisma and Tehrani (2023), blockchain governance proceedings [excluded under E6];
- Hussein et al. (2022), digital health GDPR toolkit chapter [excluded under E6].

These two exclusions concern the analytic level of a contribution, not its subject matter. Criterion E6 removes publications whose contribution is a technical artefact or engineering/cryptographic implementation with no standalone governance, legal, or organizational analysis; it does not remove technical themes as such. Interoperability and portability, discussed in Section 4.2 as legal-technical implementation factors, are therefore retained wherever the reviewed publications examine them at the governance or rights-infrastructure interface (e.g., [7][8][9][22]). The excluded proceedings — Karisma and Tehrani (2023) and Hussein et al. (2022) — were engineering- and toolkit-oriented and lacked such a governance layer at full-text assessment. This boundary is nonetheless a source of potential selection bias: excluding technical-only work may omit socio-technical evidence relevant to interoperability and secure data-sharing, and future reviews using a full database protocol should incorporate such sources. This limitation is revisited in Section 5. Figure 1 summarizes the selection flow for the purposive corpus. No additional records from electronic databases were included in this version of the review.

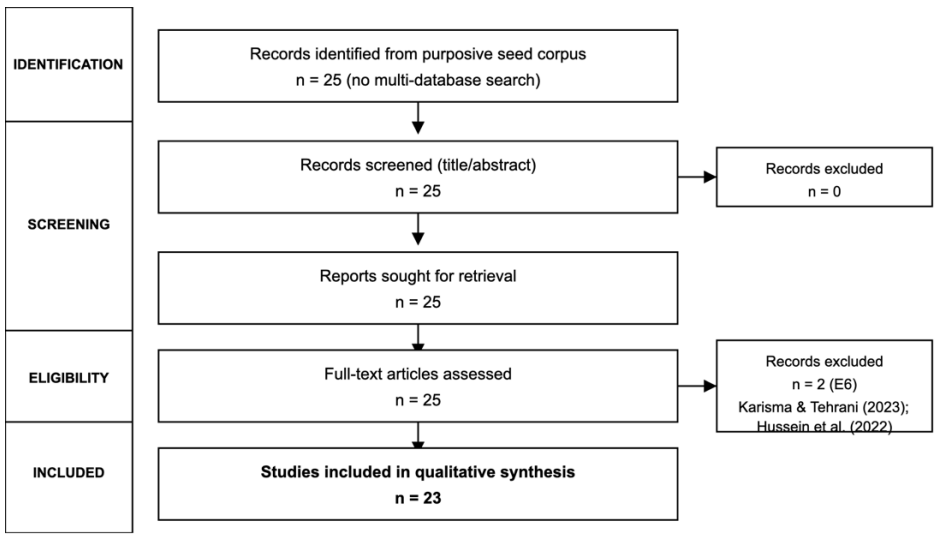


Figure 1. Literature selection flow for the structured review based on a purposive corpus (candidates n = 25; core synthesis n = 23)

3.5 Data Extraction and Thematic Coding

A structured extraction matrix recorded bibliographic metadata, country/regulatory context, research design, sector, objectives, methods, findings, and binary indicators (Y/N) for ten governance themes: leadership commitment; privacy governance; data governance; data protection officer/supervisory officer; privacy by design; DPIA; data breach management; third-party management; data subject rights; and audit/monitoring.

3.6 Quality Appraisal

Each core publication was appraised on five criteria scored 0–2 (indexing tier, methodological clarity, RQ relevance, explicit governance framing, compliance linkage; maximum 10). All 23 core publications scored ≥ 6. Scores ranged from 6 to 9, with a median of 8. Indonesian normative studies scored strongly on relevance but lower on empirical method clarity; international empirical studies scored highest on governance–compliance linkage.

3.7 Synthesis Approach

Narrative synthesis answered RQs 1, 3, and 4. Frequency counts across the 23 core publications supported RQ2. Because included studies comprise normative legal analysis, comparative law, conceptual frameworks, and empirical compliance research, meta-analysis was not appropriate.

4. RESULT AND DISCUSSIONS

4.1 Overview of Included Evidence

Table 4 summarizes the 23 core publications. Methodologically, normative and legal analyses predominate in Indonesian scholarship [8][10][13][14][15][16][17][18][19], while international contributions more frequently employ empirical, framework, or policy-ecosystem methods [3][4][5][6][7][9][11][12][20][21][22][23][24]. Regulatory anchors split into three clusters: Indonesia PDP Law (9 publications), GDPR/EU (12), and Thailand PDPA (2), with several explicit comparators [2][8][10].

Table 4. Characteristics of governance-focused core publications (n = 23)

Ref.	Author(s)	Year	Journal	Design	Context / sector	Primary regulation	Index
[16]	Ayunda	2022	Law Reform	Normative legal	E-commerce consumers	UU PDP	SINTA 1
[17]	Sulistyaningsih et al.	2023	Masalah-Masalah Hukum	Conceptual	Metaverse / digital industry	UU PDP	SINTA 2*
[18]	Firdaus	2024	Masalah-Masalah Hukum	Normative legal	Data controllers	UU PDP	SINTA 2*
[8]	Wiwoho et al.	2024	Masalah-Masalah Hukum	Comparative legal	Portability / interoperability	UU PDP, EU/UK	SINTA 2*
[19]	Priliasari	2023	Jurnal Rechts Vinding	Normative legal	E-commerce consumers	UU PDP	SINTA 2*
[14]	Fitriyanti et al.	2024	Diponegoro Law Review	Sectoral legal	Fintech / e-KYC	UU PDP	Scopus
[15]	Rahmatullah et al.	2024	Mazahib	Organizational legal	Zakat institutions	UU PDP	SINTA 1
[10]	Yuspin et al.	2024	Bestuur	Comparative institutional	Supervisory officer / DPO	UU PDP, Sweden	SINTA 1
[13]	Hariansah and Qhistina	2026	JPHI	Constitutional legal	Digital state / AI	UU PDP	SINTA 2*
[2]	Ketmaneechairat et al.	2024	IJTech	Framework	PDP + data governance	Thailand PDPA	Scopus
[3]	Guay and Birch	2022	Big Data & Society	Theoretical	USA–EU policy	GDPR context	Scopus
[4]	Peng	2022	Laws	Policy legal	Public–private regulation	GDPR, CBPR	Scopus
[9]	Nebbiai	2022	Internet Policy Review	Policy	Intermediaries	GDPR	Scopus
[20]	Duncan	2023	Internet Policy Review	Conceptual	Collective data actors	EU framework	Scopus
[21]	Peukert et al.	2022	Marketing Science	Empirical	Web ecosystem	GDPR	Scopus
[6]	Chatsuwan et al.	2023	Heliyon	Empirical	Thai SMEs	Thailand PDPA	Scopus
[22]	Pandit	2023	Information	Conceptual	Decentralized web	GDPR	Scopus
[5]	Sanfilippo et al.	2023	Inf. and Learning Sciences	Empirical	LMS vendors	GDPR	Scopus
[7]	Di Iorio et al.	2025	Front. Digital Health	Survey PoC	Digital health	EU DP law	Scopus

[11]	Novelli et al.	2024	Comput. Law & Sec. Rev.	Legal doctrinal	Generative AI	EU law	Scopus
[12]	Hohmann and Kollár	2025	Cogent Social Sciences	Legal policy	AI systems	EU AI Act, GDPR	Scopus
[23]	Breuer et al.	2022	Front. Sustainable Cities	Qualitative empirical	Vulnerable groups	GDPR	Scopus
[24]	Krämer	2024	Internet Policy Review	Empirical legal	App stores / apps	GDPR	Scopus

4.2 RQ1 Implementation Factors

Synthesis across publications yields ten implementation factor categories (Table 5). These are not mutually exclusive; mature implementations require bundles .

Table 5. Synthesis of implementation factors addressing RQ1.

Factor	Description	Representative refs.	Implication for UU PDP
F1. Regulatory clarity and legal certainty	Ambiguity in controller duties delays compliance	[16], [18], [19]	Sector guidelines and implementing regulations
F2. Institutional accountability	Supervisory officer / DPO-like roles anchor accountability	[2], [10], [18]	Formalize supervisory officer mandate
F3. Organizational and sector capacity	Sector-specific models needed (fintech, zakat, LMS)	[5], [6], [14], [15]	Sector playbooks beyond generic legal text
F4. Interoperability and rights infrastructure	Portability requires standards and intermediaries	[7], [8], [9], [22]	National interoperability roadmap
F5. Ecosystem and third-party chains	Platforms and vendors multiply compliance risk	[5], [19], [21], [24]	Processor registry and vendor audit
F6. Measurable compliance tools	Scoring and assessment make governance observable	[6], [7], [24]	National assessment instruments
F7. Data subject empowerment	Literacy affects rights effectiveness	[8], [13], [23]	Education and accessible redress
F8. AI and automated decision-making	Layered duties in algorithmic processing	[11], [12], [13]	DPIA-like governance for high-risk AI
F9. Multi-stakeholder governance	Co-regulation complements enforcement	[4], [17], [20]	Industry codes with government oversight
F10. Sanctions and enforcement credibility	Administrative sanctions drive compliance	[16], [19]	Visible enforcement to deter breach

Discussion (RQ1). Indonesian literature emphasizes regulatory clarity and controller obligations in digital commerce [16][18] [19], reflecting an early-stage implementation environment. Institutional accountability crystallizes in supervisory officer analysis [8], suggesting Indonesia's pathway parallels but does not identically mirror EU DPO institutions. International empirical work adds that ecosystem structure (third-party tags, app store rules, LMS vendors) can dominate outcomes even when formal policies exist [5][21][24]. Interoperability and portability emerge as dual legal-technical factors [8][9][22], implying that rights chapters in the PDP Law require infrastructure investments, not only procedural forms. A notable tension appears between normative prescriptions and measurement tools showing what organizations actually do [6][7]. Indonesia currently lacks the latter in the core corpus, signaling a priority for domestic empirical research.

4.3 RQ2 Governance Components

Frequency analysis (Table 6) shows privacy governance in 17/23 publications (74%), followed by audit, monitoring and compliance assessment (48%), data governance (39%), third-party management (30%), and data subject rights (30%). Leadership commitment appears in 26% of publications. DPIA is not explicitly surfaced in any core publication — a critical evidence gap given PDP Law risk-assessment expectations.

Table 6. Frequency of governance components addressing RQ2 (n = 23 core publications)

Governance component	n	%	Representative refs.
Privacy governance	17	74	[2], [8], [10], [13], [14], [15], [17], [18], [19], [4],[5], [6], [7], [11], [12], [21], [24]
Audit, monitoring and compliance assessment	11	48	[2], [5], [6], [10], [11], [12], [18], [21], [22], [24]

Data governance	9	39	[2], [3], [7], [8], [14], [16], [20], [21], [22]
Third-party / platform management	7	30	[5], [9], [16], [19], [20], [21], [24]
Data subject rights	7	30	[8], [9], [13], [16], [20], [22], [23]
Leadership and organizational commitment	6	26	[4], [6], [10], [13], [15], [17]
Data breach management and sanctions	1	4	[19]
Privacy by design	1	4	[14]
DPO / supervisory officer	1	4	[10]
DPIA	0	0	-

Discussion (RQ2). The dominance of privacy governance confirms the topical focus but reveals component imbalance: breach management appears only in [19]; privacy by design only in [14]; DPO/supervisory officer depth is concentrated in [10]. The strongest transferable model is the Thailand management system framework merging PDP and data governance [2]. Where privacy governance and assessment tools co-occur [6][7][24], literature supports measurable compliance. Where third-party governance is neglected, compliance fails despite policy formality [5].

4.4 RQ3 Relationship Between Governance and Compliance

Three mechanisms link governance to compliance:

Mechanism 1 : Accountability institutionalization. Supervisory officer and accountability principles translate legal duties into assigned oversight roles [10][18].

Mechanism 2 : Observability and metrics. Privacy policy scoring for SMEs [16] and governance assessment tools in digital health [7] shift governance from declarative to diagnostic.

Mechanism 3 : Ecosystem and platform enforcement. GDPR spillover evidence [21], app store governance [24], and intermediary-enabled portability [13] show that external governance nodes shape controller behavior as strongly as internal policies.

AI governance overlay. EU analyses argue that AI regulation layers additional compliance pathways atop GDPR [11]12]. Indonesia's algorithmic due process discourse [9] suggests a similar layering risk for public-sector automated decisions.

Discussion (RQ3). Governance is a necessary condition for compliance, not a substitute: rules without organizational governance fail in vendor chains [5]; rights without interoperability infrastructure remain ineffective [8]; laws without assessment tools leave compliance opaque [6]. Regulators and controllers should invest simultaneously in roles, policies, ecosystem contracts, and metrics.

4.5 RQ4 Proposed Implementation Framework for the PDP Law

Based on RQ1–RQ3 synthesis, Figure 2 proposes a seven-layer implementation framework mapped to PDP Law logic and international evidence. Layer 1 (leadership and regulatory commitment) establishes executive accountability and alignment with Law No. 27/2022. Layer 2 institutionalizes governance structure and the supervisory officer (*pejabat supervisi*) through the accountability principle, defined organizational roles, and privacy policy oversight [2][10][18]. Layer 3 integrates data governance and privacy governance at policy and lifecycle level [2][7]. Layer 4 covers privacy by design and DPIA-style risk controls. Consistent with the frequency results, DPIA is included in this layer as a normative, statute-derived component rather than an evidence-derived one: it received zero explicit coverage in the reviewed corpus (Table 5, DPIA = 0%) and is retained only because the PDP Law — notably its Article 34 obligation to conduct a data protection impact assessment for high-risk processing — requires it. Its presence in Layer 4 therefore flags a statutory duty and a priority gap for future primary research, not a pattern observed in the literature; the layer's empirical support is confined to privacy-by-design (PbD) proxy evidence from e-KYC scholarship [6]. Layer 5 addresses processors, vendors, and platform intermediaries [5][21][24]. Layer 6 operationalizes data subject rights, portability, and interoperability [8], [9], [13]. Layer 7 closes the loop through breach notification, sanctions, and continuous audit/scoring [6][7][21]. Organizations should adapt layer depth to scale (SME, platform, or public sector).

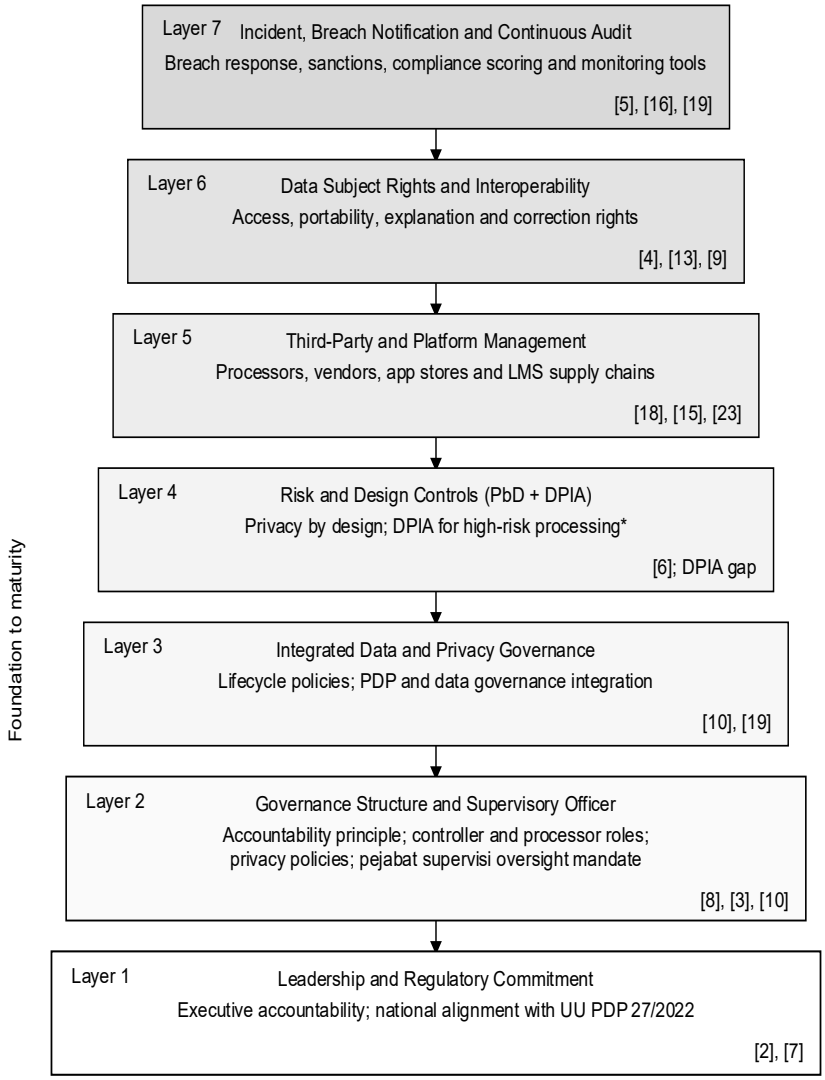


Figure 2. Layered implementation framework for Indonesia's Personal Data Protection Law (Law No. 27/2022), synthesized from the structured review corpus (2022–2026).

Table 7. Layer, component anda key refs

Layer	Component	Key refs.
1	Leadership and regulatory commitment	[15], [17]
2	Governance structure and supervisory officer	[2], [10], [18]
3	Integrated data and privacy governance	[2], [7], [14]
4	Risk and design controls (PbD + DPIA)*	[14]
5	Third-party and platform management	[5], [21], [24]
6	Data subject rights and interoperability	[8], [9], [13]
7	Incident, breach notification and continuous audit	[6], [7], [19]

** DPIA is retained in Layer 4 as a statutory (normative) requirement of the PDP Law (Article 34, data protection impact assessment for high-risk processing), even though it received no explicit coverage in the reviewed corpus (Table 5, DPIA = 0%). It is flagged as a priority for primary research rather than presented as an empirically frequent governance component.*

Discussion (RQ4). The framework is scale-sensitive: SMEs may begin at Layers 2, 3, and 7 with lightweight assessment [6], whereas digital platforms must prioritize Layer 5 early [24]. Public-sector automated decision systems should treat Layer 6 and constitutional rights as linked to Layer 4 risk controls [13]. Indonesia's nine domestic publications anchor Layers 1–2 and 6 legally, but Layer 4 (DPIA) requires primary research.

4.6 Comparative Insights: Indonesia Versus International Evidence

Indonesia is not behind in legal discourse but under-measured in empirical governance tooling. Thailand's integrated framework [10] and SME scoring [16] offer near-peer ASEAN templates.

Table 8. Comparative insights: Indonesia-focused versus international evidence in the review corpus.

Dimension	Category 1	Category 2
Dominant method	Normative / comparative legal	Empirical / policy ecosystem
Institutional focus	Supervisory officer, controllers	DPO analogues, platforms
Rights emphasis	Portability/interoperability legal analysis	Operational intermediaries and tech
Compliance proof	Legal-duty argument	Measurement and spillover studies
Emerging tech	Algorithmic state / AI constitutional	EU AI Act + GDPR layering

4.7 Comparative Insights: Indonesia Versus International Evidence

a. G1. DPIA practice under the PDP Law (0 explicit core publications).
b. G2. Empirical breach notification and enforcement outcomes in Indonesia.
c. G3. Privacy by design maturity models beyond fintech e-KYC.
d. G4. National compliance assessment instruments adapted from [6][7].
e. G5. AI governance operationalization linked to PDP supervisory officer mandates [12][13].

5. CONCLUSSION

This structured literature review analyzed **23 governance-focused peer-reviewed publications** (2022–2026) relevant to implementing Indonesia's PDP Law. Regarding **RQ1**, implementation is shaped by legal certainty, accountability institutions, sector capacity, ecosystem intermediaries, rights infrastructure, assessment tools, and AI-related governance challenges. **RQ2** shows privacy governance as the most frequently reported component (74%), followed by audit/compliance assessment (48%) and data governance (39%), while DPIA remains absent as an explicit theme. **RQ3** demonstrates that governance enables compliance through accountability roles, measurable practices, and platform/ecosystem enforcement rather than through legal text alone. **RQ4** delivers a seven-layer implementation framework from leadership and supervisory officer design through integrated governance, risk/design controls, third-party management, rights interoperability, and continuous audit/breach response. Because it is derived from a non-exhaustive purposive corpus rather than an exhaustive database search, the framework is offered as a provisional, analytically grounded proposal that should be empirically validated and refined before it informs binding implementation guidance.

Practical implications: Controllers should prioritize supervisory officer clarity, integrated data governance policies, vendor governance, and assessment tools; regulators should publish sector guidelines and interoperability roadmaps; sector associations should develop PbD/DPIA templates for high-risk processing including AI. **Limitations:** This review relies on a **purposive structured corpus** only; **no multi-database search was conducted**. Indonesian empirical studies are few; two technical publications were excluded from core coding; thematic synthesis should be refreshed after full-text re-verification and, in future work, after formal database screening. **Future research:** Longitudinal compliance studies post-2024 implementing regulations, validated Indonesian DPIA registries, cross-ASEAN comparative assessment tools, and a **follow-up systematic update** using formal Scopus/Web of Science search protocols to test whether the purposive corpus omitted relevant publications.

REFERENCES

[1] R. of Indonesia, *Law No. 27 of 2022 on Personal Data Protection*. State Gazette of the Republic of Indonesia, 2022.

[2] H. Ketmaneechairat, M. Maliyaem, and P. Pulawalanakul, "Towards a Management System Framework for the Integration of Personal Data Protection and Data Governance: A Case Study of Thai Laws and Practices," *International Journal of Technology*, vol. 15, no. 1, 2024, doi: 10.14716/ijtech.v15i1.5885.

[3] R. Guay and K. Birch, "A Comparative Analysis of Data Governance: Socio-Technical Imaginaries of Digital Personal Data in the USA and EU," *Big Data Soc.*, 2022, doi: 10.1177/20539517221112925.

[4] S. Peng, "Public-Private Interactions in Privacy Governance Laws," *Laws*, vol. 11, no. 6, p. 80, 2022, doi: 10.3390/laws11060080.

[5] M. R. Sanfilippo, N. Apthorpe, K. Brehm, and Y. Shvartzshnaider, "Privacy Governance Not Included: Analysis of Third Parties in Learning Management Systems," *Information and Learning Sciences*, vol. 124, no. 9–10, pp. 326–348, 2023, doi: 10.1108/ILS-04-2023-0033.

[6] P. Chatsuwan, T. Phromma, N. Surasvadi, and S. Thajchayapong, "Personal Data Protection Compliance Assessment: A Privacy Policy Scoring Approach and Empirical Evidence from Thailand's SMEs," *Heliyon*, vol. 9, no. 10, p. e20648, 2023, doi: 10.1016/j.heliyon.2023.e20648.

[7] C. T. Di Iorio, E. Ronchi, I. Pristas, T. Buble, N. Nicholson, and F. Carinci, "Data Protection, Interoperability and Governance Assessment Tool: Results from a Proof-of-Concept Survey," *Front. Digit. Health*, vol. 7, p. 1685774, 2025, doi: 10.3389/fdgth.2025.1685774.

[8] J. Wiwoho, U. K. Pati, and A. M. Pratama, "Enabling Data Portability and Interoperability under Indonesia's Data Protection Law," *Masalah-Masalah Hukum*, vol. 53, no. 3, pp. 271–282, 2024, doi: 10.14710/mmh.53.3.2024.271-282.

[9] M. Nebbiai, "Intermediaries Do Matter: Voluntary Standards and the Right to Data Portability," *Internet Policy Review*, vol. 11, no. 2, 2022, doi: 10.14763/2022.2.1639.
[10] W. Yuspin, T. Rajput, A. B. Bal, K. Wardiono, and Absori, "The Regulations of the Supervisory Officer Personal Data Protection-Based Accountability Principle," *Bestuur*, vol. 12, no. 1, 2024, doi: 10.20961/bestuur.v12i1.89742.
[11] C. Novelli, F. Casolari, P. Hacker, G. Spedicato, and L. Floridi, "Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity," *Computer Law and Security Review*, vol. 52, p. 106066, 2024, doi: 10.1016/j.clsr.2024.106066.
[12] B. Hohmann and G. Kollar, "Reflections on the Data Protection Compliance of AI Systems under the EU AI Act," *Cogent Soc. Sci.*, vol. 11, no. 1, 2025, doi: 10.1080/23311886.2025.2560654.
[13] S. Hariansah and L. Qhistina, "Toward Algorithmic Due Process: Constitutional Challenges and Human Rights Risks in Indonesia's Digital State," *Jurnal Pembangunan Hukum Indonesia*, vol. 8, no. 1, 2026, doi: 10.14710/jphi.v8i1.25-25.
[14] F. Fitriyanti, S. Devty, S. Putri, and R. E. Thora, "Securing Personal Data in E-KYC: Vital for Digital Economy Growth," *Diponegoro Law Review*, vol. 9, no. 1, pp. 104–120, 2024, doi: 10.14710/dilrev.9.1.2024.104-120.
[15] I. Rahmatullah, P. Suwadi, and H. Purwadi, "Legal Reform of Zakat Management Based on Personal Data Protection Law in Indonesia," *Mazahib*, vol. 23, no. 1, 2024, doi: 10.21093/mj.v23i1.5917.
[16] R. Ayunda, "Personal Data Protection to E-Commerce Consumer: What Are the Legal Challenges and Certainties?," *Law Reform*, vol. 18, no. 2, 2022, doi: 10.14710/lr.v18i2.43307.
[17] D. Sulistyaningsih, M. Ihwan, A. Setiawan, and M. S. Prabowo, "Tata Kelola Perlindungan Data Pribadi di Era Metaverse," *Masalah-Masalah Hukum*, vol. 52, no. 1, pp. 97–106, 2023, doi: 10.14710/mmh.52.1.2023.97-106.
[18] F. H. Firdaus, "Perlindungan dan Kepastian Hukum bagi Pengendali Data Pribadi di Masa Depan," *Masalah-Masalah Hukum*, vol. 53, no. 2, pp. 135–144, 2024, doi: 10.14710/mmh.53.2.2024.135-144.
[19] E. Priliasari, "Perlindungan Data Pribadi Konsumen dalam Transaksi E-Commerce," *Jurnal Rechts Vinding*, vol. 12, no. 2, 2023, doi: 10.33331/rechtsvinding.v12i2.1285.
[20] J. Duncan, "Data Protection beyond Data Rights: Governing Data Production through Collective Intermediaries," *Internet Policy Review*, vol. 12, no. 3, 2023, doi: 10.14763/2023.3.1722.
[21] C. Peukert, S. Bechtold, M. Battikas, and T. Kretschmer, "Regulatory Spillovers and Data Governance: Evidence from the GDPR," *Marketing Science*, 2022, doi: 10.1287/mksc.2021.1339.
[22] H. J. Pandit, "Making Sense of Solid for Data Governance and GDPR," *Information*, vol. 14, no. 2, p. 114, 2023, doi: 10.3390/info14020114.
[23] J. Breuer, R. Heyman, and R. van Brakel, "Data Protection as Privilege: Factors to Increase Meaning of GDPR in Vulnerable Groups," *Frontiers in Sustainable Cities*, vol. 4, p. 977623, 2022, doi: 10.3389/frsc.2022.977623.
[24] J. Kramer, "The Death of Privacy Policies: How App Stores Shape GDPR Compliance of Apps," *Internet Policy Review*, vol. 13, no. 2, 2024, doi: 10.14763/2024.2.1757.
[25] M. J. Page *et al.*, "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," *BMJ*, vol. 372, 2021, doi: 10.1136/bmj.n71.