Policy Brief No. 1

From Rules to Protection: Closing the Implementation Gap in Indonesia's Personal Data Protection Law

by Kirana Aisyah and Audy Maharani Sagita



Executive Summary

Indonesia has established a relatively comprehensive legal framework for personal data protection through Law No. 27 of 2022 on Personal Data Protection (the PDP Law). The law regulates data subject rights, the obligations of controllers and processors, sanctions, cross-border data transfers, and the establishment of a supervisory authority. Its transition period ended on 17 October 2024. Indonesia's main personal data protection challenge has therefore shifted from establishing a legal framework to ensuring that the rules are implemented and enforced effectively.

This policy brief integrates a comparative legal and policy analysis of the Personal Data Protection Law (PDP Law) and the General Data Protection Regulation (GDPR), a Safe Nusa survey of 209 respondents, and seven semi-structured interviews with regulators, academics, and practitioners. These three sources of evidence are triangulated to compare what the law formally provides, what respondents know and experience, and how experts explain implementation challenges.

"**83.3%** of the respondents did not correctly know the status of the PDP supervisory authority; only **33.5%** said they trusted government institutions to protect their personal data; **73.2%** supported PDP supervision by **an independent authority**; and **96.2%** wanted **stronger enforcement**." The interviews also indicate that, in some cases, compliance remains confined to documents or exists only "on paper," while the survey identifies a gap between perceived understanding of the PDP Law and actual knowledge.

The comparison with the GDPR shows that Indonesia's gap does not lie solely in the substance of the rights granted. The PDP Law already contains many elements that are aligned in principle with the GDPR. The more relevant differences concern the implementation architecture linking legal norms to supervisory institutions, enforcement, organizational compliance, remedies, and the ability of the public to exercise its rights.

This policy brief therefore recommends **five priorities**:

1. Operationalize the PDP supervisory authority with functional independence, clear powers, adequate resources, and accountability mechanisms
2. Build an enforcement coordination architecture between the PDP authority and sectoral regulators
3. Provide complaint, investigation, and remedy mechanisms that are simple and accessible
4. Shift PDP literacy from awareness alone to measurable knowledge and practical ability to exercise rights
5. Promote risk-based compliance and privacy by design, including in the development of AI and new technologies

Indonesia's next agenda is therefore not simply to add more rules, but to close the implementation gap between rights available on paper and protection that people can genuinely experience.

Background: From Enacting the Law to the Challenge of Implementation

Digital transformation has increased the volume and intensity of personal data collection, processing, and exchange across many areas of public life, including financial services, e-commerce, social media, and public services. The expansion of digital activity brings economic and social benefits, but at the same time increases people's exposure to data misuse, privacy violations, and information leaks.

90.0%	**had experienced at least one digital security or privacy-related incident**
38.3%	**had received phishing messages containing personal data**
47.8%	**reported that one of their online accounts had been accessed without authorization**
47.4%	**had received an unsolicited one-time password (OTP)**

These findings do not mean that 90% of respondents experienced violations of the PDP Law or that all incidents resulted from data breaches. They are more appropriately read as an indication of respondents' broad exposure to risks involving accounts, identities, and personal data. This distinction matters because account-security risks, digital fraud, and breaches of personal data protection obligations are categories that may be related but are not legally identical. (Safe Nusa, 2026)

Indonesia Already Has a Legal Framework through the PDP Law

Indonesia took an important step by enacting Law No. 27 of 2022 on Personal Data Protection on 17 October 2022. Before the PDP Law, provisions concerning personal data were dispersed across various sectoral regulations. The PDP Law therefore marked an important shift toward a more comprehensive national legal framework for personal data processing and protection. In 2026, the government also issued Government Regulation No. 33 of 2026 as an implementing regulation for the PDP Law. It elaborates on several operational aspects of personal data protection and is scheduled to take effect on 16 January 2027. (Republic of Indonesia, 2022; Republic of Indonesia, 2026; Simbolon & Juwono, 2022; Razi et al., 2024)

The implementing regulation clarifies the implementation framework, but its issuance does not automatically resolve every issue. The increasingly important question is whether the established rights, obligations, compliance standards, supervision, and enforcement mechanisms can work in practice.

Methodology

This policy brief uses a mixed-methods approach, integrating quantitative and qualitative evidence to develop a more comprehensive understanding of the implementation of personal data protection in Indonesia. Triangulation draws on three sources of evidence: comparative legal and policy analysis; a public survey* of 209 respondents; and semi-structured interviews with seven experts and practitioners.

1. **Comparative legal and policy analysis**

   Compares the PDP Law and GDPR to identify similarities, differences, implementation gaps, and institutional practices from which Indonesia may learn.

2. **Public survey**

   The Safe Nusa Personal Data Protection Awareness and Perceptions Survey was conducted on 13–21 July 2026 and received 209 responses from participants aged 15–30. The instrument covered risk experiences, knowledge, trust, behavior, institutional design, and policy preferences.

3. **Expert interviews**

   Seven semi-structured interviews were conducted in August–September 2026, covering perspectives from regulators/government, legal academia, law and technology, digital governance, and governance, risk, and compliance (GRC).

Policy recommendations are not derived from a single survey indicator or an isolated statement by one interviewee. They are developed by considering the relationships among the legal framework, empirical survey patterns, expert perspectives, and comparative lessons.

Expert Interview Participants

Participants represented regulators/government, legal academia, law and technology, digital governance, and governance, risk, and compliance (GRC). This diversity was used to compare how the same issues are understood from the perspectives of regulators, academics, and implementation practitioners.

Participant	Institution and Background	Perspective
Syahraki Syahrir, S.E., Ak., M.M., CA, CISA, CISM, CDPSE, GRCP, GRCA	CEO of Veda Praxis; more than 20 years in governance, risk management, and compliance consulting; former President of ISACA Indonesia.	Digital governance, GRC, organizational maturity, PDP Law's implementation, and trust.
Imelda Cardiana Sirait, GRCP, IRMP, IDPP, IAAP, ITGRC	Partner and Head of the PDP Center of Excellence at Veda Praxis; background in audit, risk management, and supporting PDP implementation across industries.	Organizational compliance, privacy maturity, Data Protection Officer (DPO), privacy by design, and PDP's implementation.
Rindy, S.Kom., M.T.I., JNCIS, CEH, ECSA, LA/A ISO 27001, DPO	Ministry of Communication and Digital Affairs; Head of the Digital Space Compliance Supervision Team; experience in information security, data security, and PDP.	Regulatory perspective, compliance supervision, enforcement, complaints, and literacy.
Prof. Dr. Sinta Dewi Rosadi, S.H., LL.M.	Legal academic at Padjadjaran University, specializing in personal data protection.	PDP legal framework, independence and design of the supervisory authority, data subject rights, and enforcement.
Dr. Wahyu Yun Santoso, S.H., M.Hum., LL.M.	Academic at the Faculty of Law, Gadjah Mada University; Center for Law and Technology Studies.	Law and technology, implementing regulations, institutional design, and implementation.

*The survey used a voluntary, non-probability sample. Because the probability of each population member being included in the sample is unknown, the survey percentages should be interpreted as patterns among the 209 respondents, not as prevalence estimates for the entire Indonesian population.

Participant	Institution and Background	Perspective
Faiz Rahman, S.H., LL.M.	Constitutional law academic at the Faculty of Law, Gadjah Mada University; researches the public interest in personal data protection.	Public interest, state interests, privacy, data subject rights, and institutional design.
Dr. Bambang Pratama, S.H., M.H.	Academic and cyberlaw researcher examining technology law, AI, and personal data protection.	Cyberlaw, AI, technological developments, regulatory design, and institutional response.

Source: Safe Nusa (2026), Expert Interview Transcripts, August–September 2026.

The PDP Law and GDPR: Similar in Principle, Different in Implementation

The enactment of the PDP Law brought Indonesia's data protection framework closer to the principles developed under the European Union's General Data Protection Regulation (GDPR). Similarities include recognition of data subject rights, obligations for controllers and processors, the use of lawful bases for processing, the principle of accountability, notification requirements for personal data breaches, and rules on cross-border data transfers. These similarities do not mean that the two regimes are identical. Important differences emerge when regulation is viewed as a governance system rather than merely a collection of rights and obligations. (Republic of Indonesia, 2022; European Parliament & Council of the European Union, 2016; Simbolon & Juwono, 2022)

Dimension	Comparison of the PDP Law and GDPR	Implication for Indonesia
Rights and lawful bases for processing	Both recognize data subject rights and provide several lawful bases for processing, not consent alone. The PDP Law provides for rights such as access, correction, erasure, withdrawal of consent, objection to automated decisions, compensation, and portability.	The main gap is no longer the list of rights, but individuals' ability to exercise those rights and organizations' ability to determine and document the appropriate lawful basis for processing.
Organizational accountability	Both the PDP Law and GDPR impose obligations on controllers and processors and apply the principle of accountability.	Compliance must be visible in practice—for example, through data mapping, risk assessments, access controls, DPOs, incident response, and privacy by design—not confined to documentation.
Personal data breach notification	Both use a timeframe of around 72 hours, although the triggers and recipients of notifications differ. The PDP Law requires notification to data subjects and the authority; the GDPR primarily requires notification to the supervisory authority and, in certain circumstances, the data subject.	Effectiveness depends on clear procedures: when an incident must be reported, to whom, what information is required, and how follow-up is handled.
Supervisory authority	The PDP Law mandates a supervisory institution appointed by the President; the GDPR requires one or more supervisory authorities to perform their tasks independently.	Indonesia's priority is to ensure functional independence, clear powers, resources, accountability, and working relationships with sectoral regulators.
Enforcement and remedies	Both provide sanctions and enforcement mechanisms. The GDPR grants supervisory authorities broad investigative and corrective powers, alongside administrative and judicial mechanisms.	The central issue is not merely whether sanctions exist, but whether complaints, investigations, corrective measures, and remedies can be implemented consistently and accessibly.
Cross-border data transfers	Both use concepts of adequate protection, safeguards, and certain derogations for cross-border data transfers.	Indonesia already has a substantive framework; the next challenge is to make assessments, safeguards, and oversight mechanisms genuinely operational.
Literacy and exercise of rights	The PDP Law identifies increased awareness as a data protection objective; the GDPR also tasks supervisory authorities with promoting public awareness and understanding.	Literacy should be measured by actual knowledge and the ability to exercise rights—including knowing how to submit a complaint—not merely exposure or the number of people attending outreach sessions.

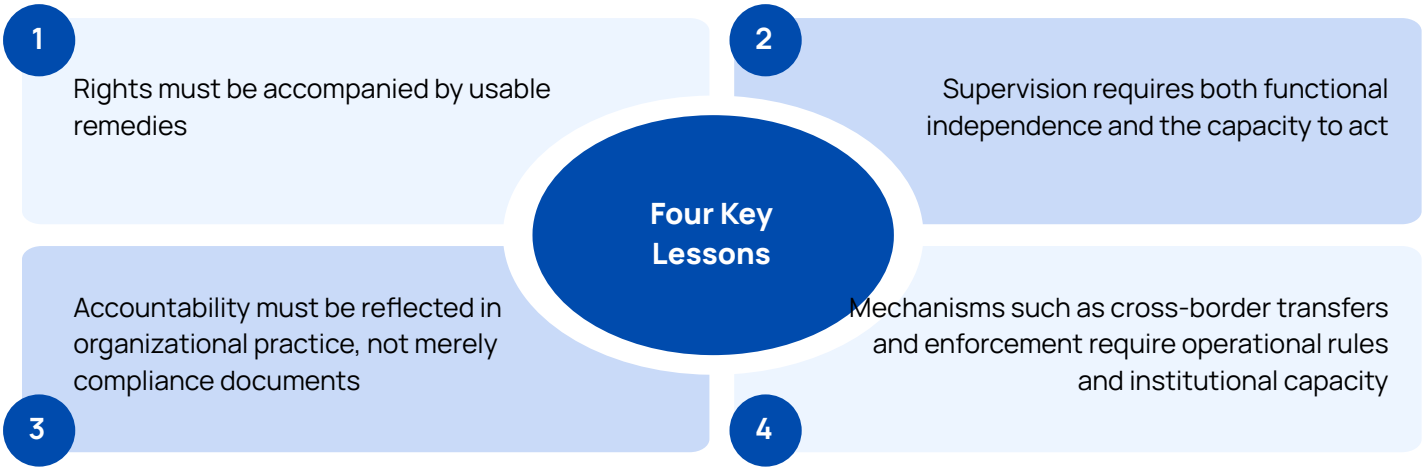
Source: Prepared by Safe Nusa based on Law No. 27 of 2022, the GDPR, comparative literature, and expert interviews.

The GDPR as a Benchmark, not a Blueprint

The overall analysis shows that the PDP Law and GDPR share more similarities at the level of principle than is often assumed. Data subject rights, lawful bases for processing, controller and processor obligations, accountability, personal data breach notifications, sanctions, and cross-border data transfers all have a foundation in the PDP Law.

Findings from Safe Nusa's seven interviews reinforce and complicate this picture. There is broad agreement that having a law is not enough. However, experts do not always propose the same institutional design. Some emphasize structural independence, others functional independence; some highlight relationships with sectoral regulators, while others stress the importance of speed of execution.

The main lesson from the GDPR is therefore not that Indonesia should replicate European institutions. Widiatedja and Mishra (2023) emphasize the importance of organizational and functional independence for Indonesia's PDP authority, but the national context remains decisive in determining how that independence is translated into institutional structures.



The main gap between the PDP Law and GDPR is therefore not simply the number of rights or the strictness of legal norms. The more important difference lies in the implementation architecture connecting norms, institutions, enforcement, organizational compliance, and the public's ability to exercise its rights.

Key Findings: The PDP Law Implementation Gap

Analysis of the Safe Nusa survey, seven semi-structured interviews, also legal and policy literature indicates that Indonesia's main personal data protection challenge is no longer simply the existence of regulation. Law No. 27 of 2022 provides a substantive framework for data subject rights, controller and processor obligations, sanctions, and institutional arrangements. However, a gap remains between the protection provided in law and the governance system's ability to make that protection work in practice.

Finding 1: Institutional Gaps Are a Critical Bottleneck in PDP Law Implementation

The PDP Law gives the institution responsible for personal data protection a broad mandate to supervise, enforce administrative law, impose sanctions, handle complaints, conduct examinations, and cooperate with data protection authorities in other countries. However, the institutional dimension has not yet been fully operationalized. (Republic of Indonesia, 2022; Ministry of Communication and Digital Affairs, 2026)

Only 16.7% of Safe Nusa respondents correctly knew the status of the PDP supervisory authority. A total of 41.6% thought the institution already existed, while 41.6% said they did not know. Thus, 83.3% did not know the actual institutional status. The interviews did not reveal a consensus on one specific organizational form; the more consistent themes were the need for independent decision-making, clear powers, technical capacity and resources, and the ability to execute decisions effectively. (Safe Nusa, 2026)

Finding 2: Enforcement Matters More Than the Mere Existence of Rules

The PDP Law already provides enforcement instruments, including administrative sanctions. The existence of sanction provisions and the existence of an institution capable of imposing them are therefore interdependent. From the regulator's perspective, public complaints also reveal practical problems: people do not always know where to report, what evidence is required, or how a case will be processed.

The Safe Nusa survey found very strong support for stronger enforcement: 96.2% of respondents said Indonesia needs stronger enforcement against personal data protection violations. GDPR experience also shows that independence alone is insufficient without resources and enforcement capacity. (Safe Nusa, 2026; European Union Agency for Fundamental Rights, 2024; Baquero et al., 2025)

Finding 3: Compliance Is Uneven and Must Not Stop at Compliance on Paper

The interview analysis found organizational compliance to be one of the most prominent themes, but also one that varies considerably by sector and organizational maturity. Imelda Cardiana Sirait, describing her experience supporting nearly 50 companies across sectors, summarized one pattern of compliance: "But sometimes it's only on paper; it hasn't been implemented."

This statement distinguishes formal compliance from substantive compliance. An organization may have a privacy policy, consent forms, standard operating procedures, or PDP documentation, but the existence of documents does not prove that PDP principles are embedded in organizational processes. Across the interview coding, substantive compliance arose in discussions of data mapping, risk assessment, DPOs, incident procedures, privacy by design, internal controls, leadership involvement, and governance maturity.

The implication is that a uniform approach for all organizations may be ineffective. Enforcement still requires common minimum standards for data subject rights, but the way organizations achieve and demonstrate compliance can take account of risk levels, processing scale, data sensitivity, and organizational maturity.

Finding 4: Feeling Knowledgeable Is Not the Same as Actually Knowing

One of the most important findings of the Safe Nusa survey is the mismatch between perceived knowledge and actual knowledge. Among respondents who said they felt they understood the PDP Law, 52.7% gave an incorrect answer about the status of the supervisory authority, compared with 29.3% among those who felt they understood it less well. This does not mean that people who feel they understand the PDP Law generally have poorer knowledge; rather, it shows that self-assessment is not sufficient as a proxy for actual knowledge. (Safe Nusa, 2026)

This finding is consistent with privacy literacy research showing that self-assessed privacy literacy does not always align with actual privacy literacy. Literacy programs should therefore move from



(Ma & Chen, 2023)

Finding 5: Public Trust Is Part of PDP Governance, Not Merely a Matter of Perception

The Safe Nusa survey found a substantial difference in respondents' trust in various institutions handling personal data. Some 60.3% said they trusted companies, 54.1% trusted digital platforms, but only 33.5% trusted government institutions. At the same time, 73.2% supported PDP supervision by an independent authority. (Safe Nusa, 2026)

Syahraki Syahrir described trust as something broader than digitalization: "Trust is the currency of the present era." He also emphasized that government, as the rule-maker, needs to set an example in data management. Trust should therefore not be treated merely as a communications target. Transparency when incidents occur, accountability of public bodies, consistent enforcement, credible complaint mechanisms, and independent oversight are themselves part of the infrastructure of trust.

Finding 6: AI and New Technologies Test the PDP Law's Ability to Adapt

Across the seven expert interviews, recurring themes included AI, emerging technologies, and privacy by design. The findings do not indicate that Indonesia needs an entirely new PDP regime every time a new technology emerges. Instead, the interviews tend to highlight the importance of translating existing PDP principles into a rapidly changing technological environment.

AI, big data, blockchain, profiling, and other data-dependent technologies increase the complexity of processing scale, data inference, transparency, purpose limitation, and data erasure. The concept of data protection by design provides a bridge between legal principles and technology design: data protection is incorporated into technical and organizational measures from the outset, rather than being assessed only after a system has been built. (Veale et al., 2018)

Institutions determine who supervises and enforces the rules; enforcement determines whether rights have real consequences; organizational compliance determines whether PDP principles enter everyday practice; literacy determines whether people can recognize and exercise their rights; trust affects the legitimacy of data governance; and AI and new technologies test whether the entire system can adapt.

Policy Recommendations

The findings indicate that stronger PDP Law implementation requires more than refinement of legal norms. Policy priorities should focus on institutional capacity, workable enforcement mechanisms, public access to remedies, measurable literacy, and organizational compliance that can keep pace with technological developments.

1 Operationalize the PDP Supervisory Authority with Functional Independence, Clear Powers, and Accountability Mechanisms

Establishing and operationalizing the PDP supervisory authority should be a priority because several important functions under the PDP Law depend on its existence. However, creating an institution alone is not enough. Institutional design must guarantee functional independence: the ability to investigate, make decisions, and impose corrective measures without interference in individual cases.

The interviews revealed differing views on whether independence must be achieved through full structural separation from government. Nevertheless, there was more substantive common ground: the authority needs clear powers, technical capacity, adequate resources, the ability to execute decisions, and accountability mechanisms that do not undermine its supervisory independence.

Policy success should not be assessed solely by whether the institution has been established, but by its operational readiness: adequate personnel and budget, examination procedures, publication of decisions, case-resolution times, and the ability to exercise its powers consistently.

2 Clarify Enforcement Coordination between the PDP Authority and Sectoral Regulators

Establishing a PDP authority does not make sectoral regulators irrelevant. Data processing takes place within ecosystems that already have their own supervisory structures. Problems arise when personal data violations also intersect with cybersecurity, consumer protection, sectoral regulation, criminal law, or obligations imposed on electronic system operators.

Once the PDP authority is operational, the government should establish inter-agency coordination protocols that define the division of responsibilities among the PDP authority, the Ministry of Communication and Digital Affairs (Komdigi), the Financial Services Authority (OJK), law enforcement agencies, and other sectoral regulators. The protocols should explain case-referral mechanisms, information sharing, joint investigations, designation of the lead authority, and handling of cases that fall under more than one legal regime.

3 Build Simple, Usable Complaint and Remedy Mechanisms for the Public

Recognition of rights under the PDP Law has practical value only if data subjects can exercise them when violations occur. Implementation should therefore establish a clear connection between



The issue is not simply whether people know they have rights, but whether they understand what to do when those rights are not respected.

The PDP authority should provide an accessible single-entry complaint channel, using plain language and procedures that can be understood without in-depth legal knowledge. Ideally, the system would help users identify the type of problem, the party allegedly responsible, the information or evidence to provide, the stages of case handling, and possible remedies. Where a case falls within the jurisdiction of another regulator or authority, the complaint system should have a clear referral mechanism.

Success indicators should include not only the number of complaint channels established, but also complaint resolution rates, handling times, procedural accessibility, remedies provided, and users' experiences with the mechanism.

4 Shift PDP Literacy from Awareness Alone to Measurable Knowledge and the Ability to Exercise Rights

PDP literacy programs need to go beyond outreach that merely ensures people have heard of the PDP Law. The Safe Nusa survey shows that self-reported awareness cannot, by itself, serve as a measure of actual knowledge.

The government, PDP authority, educational institutions, and civil society organizations should change how literacy programs are designed and evaluated. Educational materials should begin with concrete situations, such as what to do when an account is accessed without authorization, when a company refuses a data-erasure request, when a breach occurs, or when someone wants to know what data a platform stores about them.

Participant numbers, campaign reach, and the percentage of people who say they understand PDP may still be recorded, but they should be complemented by objective questions and simulations that measure whether participants genuinely know their rights and can identify appropriate actions.

5 Promote Risk-Based Compliance and Privacy by Design, Including for AI and New Technologies

PDP Law implementation should avoid a compliance approach that produces documents alone. Substantive compliance should be integrated into the organization's data-management lifecycle, from identifying what data is collected and for what purpose, determining the lawful basis for processing, conducting data mapping and risk assessments, restricting access, and preparing incident-response procedures, to ensuring that the DPO function operates where required and evaluating risks before new technologies or products are launched.

The same protection standards do not mean that every organization must follow identical compliance processes. Organizations have different risk profiles and capacities. The PDP authority and sectoral regulators should therefore develop risk-based supervision, prioritizing processing that has a greater scale, sensitivity, or potential impact on individual rights.

AI and new technologies should be addressed within the same framework. Because technology develops faster than legislation changes, the government and PDP authority need the capacity to issue adaptive technical guidance, conduct research, involve experts, and update regulatory interpretations in response to emerging risks. Privacy by design, data protection impact assessments, data minimization, transparency, and decision documentation can enable innovation without relegating privacy protection to a consideration only after technology has been launched.

Success should not be measured by the number of organizations with compliance documents, but by the maturity of their practices: conducting risk assessments and data mapping, readiness for incident response, use of privacy by design, impact assessments for high-risk processing, and the ability to demonstrate how PDP Law principles are applied in systems and everyday decisions.

Implementation Direction

The five recommendations should be understood as a connected sequence, not five independent agendas. A strong authority without complaint mechanisms limits public access to enforcement; complaints without regulatory coordination create confusion over jurisdiction; enforcement without compliance guidance increases organizational uncertainty; and rights without practical literacy are difficult for the public to exercise. At the same time, AI and new technologies require the entire system to adapt to changing risks.

Implementation Chain



The goal of PDP Law implementation should therefore move beyond mere regulatory compliance toward genuinely effective data protection governance: rights can be exercised, complaints can be acted upon, regulators can enforce the rules, organizations can demonstrate compliance, and people have the practical ability to protect and exercise their rights over their personal data.

Five-Year Implementation Roadmap (2027–2031)

To translate the five recommendations into realistic stages, Safe Nusa proposes the following five-year implementation sequence. The stages build on one another: institutional and coordination foundations are established first, then strengthened through enforcement, access to remedies, measurable literacy, and risk-based governance that can adapt to technological developments.

1 2027 focus on institutional foundations and coordination

Priority Actions: Operationalize the PDP authority; define roles with sectoral regulators and law enforcement agencies; prepare standard operating procedures (SOPs) for complaints, examinations, and coordination; ensure a clear transition to implementation of Government Regulation No. 33 of 2026.

Progress Indicators: The authority is operational; its mandate and coordination SOPs are published; complaint channels and service standards are available.

2 2028 focus on risk-based supervision and sectoral guidance

Priority Actions: Issue implementation guidance for sectors and high-risk processing; prioritize sectors processing sensitive data or data at scale; strengthen DPO functions, impact assessments, data mapping, and privacy by design.

Progress Indicators: Sectoral guidance is available; risk-based supervision begins; priority organizations have substantive compliance mechanisms.

3 2029 focus on usable enforcement and remedies

Priority Actions: strengthen investigation capacity and complaint follow-up; transparently publish enforcement processes and outcomes; measure case-handling times and the effectiveness of remedies for data subjects.

Progress Indicators: complaint data, resolution times, corrective measures, and enforcement outcomes are published regularly.

4 2030 focus on measurable literacy and technological adaptation

Priority Actions: shift literacy programs from awareness to knowledge and practical ability to exercise rights; conduct repeated measurements; issue or update guidance on AI, big data, blockchain, cross-border data transfers, and other data-intensive technologies.

Progress Indicators: Improvements in objective knowledge can be measured; guidance on new technologies is updated based on risk and implementation evidence.

5 2031 focus on evaluation of effectiveness and governance maturity

Priority Actions: Conduct an independent evaluation of the authority's capacity, inter-agency coordination, enforcement patterns, organizational compliance maturity, public exercise of rights, and the need to revise policies or guidance.

Progress Indicators: A five-year evaluation report is available; recommendations for improving regulation, institutions, resources, and supervision are acted upon.

This roadmap is not intended as five separate agendas. Each stage depends on the foundations laid by the previous stage, while evaluation should be repeated so that supervision, compliance, literacy, and responses to new technologies develop as one governance system.

References

Baquero, P. M., Wang, A., & Amariles, D. R. (2025). Unveiling transparency in data protection enforcement across the EU: Assessing the level and quality of disclosure of GDPR fines by data protection authorities. *European Law Journal, 31*(3), 177–202. https://doi.org/10.1111/eulj.70008

European Union Agency for Fundamental Rights. (2024). *GDPR in practice: Experiences of data protection authorities*. Publications Office of the European Union. https://fra.europa.eu/en/publication/2024/gdpr-experiences-data-protection-authorities

Kementerian Komunikasi dan Digital. (2026, July 22). *Wamen Nezar Patria: Indonesia siapkan otoritas pelindungan data pribadi yang independen* [Deputy Minister Nezar Patria: Indonesia prepares an independent personal data protection authority]. https://portal.komdigi.go.id/kanal-publik/berita-kini/10412

Ma, S., & Chen, C. (2023). Are digital natives overconfident in their privacy literacy? Discrepancy between self-assessed and actual privacy literacy, and their impacts on privacy protection behavior. *Frontiers in Psychology, 14*, Article 1224168. https://doi.org/10.3389/fpsyg.2023.1224168

Peraturan Pemerintah Republik Indonesia Nomor 33 Tahun 2026 tentang Peraturan Pelaksanaan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi [Government Regulation of the Republic of Indonesia Number 33 of 2026 concerning the Implementation of Law Number 27 of 2022 on Personal Data Protection], Lembaran Negara Republik Indonesia Tahun 2026 Nomor 88 (2026).

Razi, F., Tuasikal, H., & Markus, D. P. (2024). Implementation and challenges of the Personal Data Protection Law in Indonesia. *Jurnal Indonesia Sosial Teknologi, 5*(12), 6559–6565. https://doi.org/10.59141/jist.v5i12.1285

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *Official Journal of the European Union, L 119*, 1–88 (2016). https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng/

Simbolon, V. A., & Juwono, V. (2022). Comparative review of personal data protection policy in Indonesia and the European Union General Data Protection Regulation. *Publik (Jurnal Ilmu Administrasi), 11*(2), 178–190. https://doi.org/10.31314/pjia.11.2.178-190.2022

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi [Law of the Republic of Indonesia Number 27 of 2022 concerning Personal Data Protection], Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196 (2022). https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

Veale, M., Binns, R., & Ausloos, J. (2018). When data protection by design and data subject rights clash. *International Data Privacy Law, 8*(2), 105–123. https://doi.org/10.1093/idpl/ipy002

Widiatedja, I. G. N. P., & Mishra, N. (2023). Establishing an independent data protection authority in Indonesia: A future-forward perspective. *International Review of Law, Computers & Technology, 37*(3), 252–273. https://doi.org/10.1080/13600869.2022.2155793