THE CITY TOWER
Level 12, Unit 1-5
Jl. M.H. Thamrin No. 81, Menteng
Jakarta Pusat 10310
+62 858 6003 7557
info@drpattorneyatlaw.com

LEGAL BRIEF | PRIVACY AND TECHNOLOGY | 2 AUGUST 2026

Personal Data Processing: Lawful Basis, Governance, and Breach Readiness

Building accountable data practices under Indonesia's Personal Data Protection Law

EXECUTIVE SUMMARY

Personal-data compliance is an operating model, not only a privacy notice. Organisations need to know what data they hold, why it is processed, who receives it, how long it is retained, and how incidents and data-subject requests will be handled.

1. Background, Scope, and Strategic Significance

Legal analysis should begin with the governing instrument, the parties' authority, the relevant chronology, and the evidence that can support each proposition. The framework below is intended to help decision-makers identify issues requiring focused advice.

Personal Data Processing: Lawful Basis, Governance, and Breach Readiness should be approached as a connected legal, factual, and decision-making problem. In the privacy and technology context, the quality of the final position depends on whether the governing instruments, authority records, chronology, correspondence, operational facts, and available remedies are reviewed together. A conclusion reached from one document or one legal provision may overlook qualifications, implementing rules, later conduct, or evidence that changes the practical assessment.

This publication therefore focuses on the sequence of analysis rather than offering a universal answer. The first task is to define the relevant person, company, asset, permit, transaction, or government action. The second is to identify the legal source and the institution or contractual actor with authority. The third is to test the position against contemporaneous records and the procedure that governs any filing, objection, response, negotiation, investigation, or claim.

A legal brief is most useful when it distinguishes the rule from its application. Statutory text, contract wording, corporate instruments, court decisions, and administrative practice may point in the same direction, but they do not perform the same function. Decision-makers should also identify issues on which the law is unsettled, fact-dependent, or subject to transitional provisions. Where reasonable interpretations differ, the advice should state the assumptions and practical consequences of each interpretation.

The analysis is current as at 2 August 2026. The application of any law, regulation, court decision, administrative practice, or contractual provision depends on the specific facts and may change after publication.

2. Legal and Regulatory Framework

The principal authorities identified for this topic are listed below. They should be read together with any implementing measures, sector-specific instruments, later amendments, binding court decisions, official guidance, contractual provisions, corporate instruments, and transitional rules applicable to the matter. The legal hierarchy and the date on which an instrument became effective may be decisive.

- Law No. 27 of 2022 on Personal Data Protection

Before relying on an authority, confirm that it applies to the relevant person, entity, activity, asset, transaction, location, procedural stage, and period. Where an official system or institution maintains the operative record, the record should be verified rather than inferred from an earlier submission. The scope of any discretion, appeal, objection, cure, or review mechanism should also be mapped.

3. Detailed Analysis of the Core Issues

3.1 Each processing activity should have a defined purpose and an appropriate legal basis

This issue defines the legal scope of the assessment. Counsel should identify who holds the relevant right, duty, power, or exposure; the instrument from which it arises; and any limits on authority. The review should distinguish legal form from actual conduct and should record inconsistencies rather than silently choosing one version. Authority can depend on legislation, implementing rules, constitutional documents, delegations, contracts, licences, resolutions, or an institution's procedural mandate.

For Personal Data Processing: Lawful Basis, Governance, and Breach Readiness, the analysis should connect this point to the elements of the applicable legal rule, available interpretive material, and the relief or decision that may ultimately be required. The purpose is not merely to state a principle, but to show which facts could change its application and which documents are needed to support a reasoned legal position.

3.2 Controllers should apply transparency

The point must be tested against contemporaneous evidence. Useful material may include executed documents, official records, system data, correspondence, meeting minutes, reports, financial entries, technical records, witness knowledge, and proof of delivery or submission. The legal team should identify the source, custodian, date, completeness, and reliability of each record. Missing records and later-created summaries should be labelled so that decision-makers understand the evidentiary limits.

For Personal Data Processing: Lawful Basis, Governance, and Breach Readiness, the analysis should connect this point to the elements of the applicable legal rule, available interpretive material, and the relief or decision that may ultimately be required. The purpose is not merely to state a principle, but to show which facts could change its application and which documents are needed to support a reasoned legal position.

3.3 Vendor and cross-border arrangements require clear roles

Procedure and timing are central. The applicable framework may prescribe a form, authorised signatory, service method, supporting document, cure opportunity, objection route, hearing sequence, or deadline. A substantively reasonable position may still be weakened by using the wrong forum or failing to preserve a procedural step. A calendar should distinguish statutory deadlines, contractual deadlines, internal approval dates, and practical milestones for collecting evidence and preparing submissions.

For Personal Data Processing: Lawful Basis, Governance, and Breach Readiness, the analysis should connect this point to the elements of the applicable legal rule, available interpretive material, and the relief or decision that may ultimately be required. The purpose is not merely to state a principle, but to show which facts could change its application and which documents are needed to support a reasoned legal position.

3.4 Incident response should integrate legal

The operational consequences should be assessed before a position is implemented. Legal exposure can affect cash flow, licences, financing, contractual performance, insurance, governance, personnel, public statements, and relationships with authorities or counterparties. Scenario analysis should compare immediate action, conditional action, negotiated adjustment, and preservation of the status quo. Each scenario should state its assumptions, dependencies, reversible steps, and indicators that would require escalation.

For Personal Data Processing: Lawful Basis, Governance, and Breach Readiness, the analysis should connect this point to the elements of the applicable legal rule, available interpretive material, and the relief or decision that may ultimately be required. The purpose is not merely to state a principle, but to show which facts could change its application and which documents are needed to support a reasoned legal position.

3.5 Sensitive or high-risk processing may require stronger controls and documented assessment

The position should anticipate how an authority, court, counterparty, shareholder, complainant, or other stakeholder may respond. That includes testing the strongest counterargument, not only confirming the preferred interpretation. Communications should be accurate, proportionate, and consistent across legal submissions, corporate records, regulatory filings, and operational instructions. Where uncertainty remains, the decision record should explain the chosen risk tolerance and the safeguards applied.

For Personal Data Processing: Lawful Basis, Governance, and Breach Readiness, the analysis should connect this point to the elements of the applicable legal rule, available interpretive material, and the relief or decision that may ultimately be required. The purpose is not merely to state a principle, but to show which facts could change its application and which documents are needed to support a reasoned legal position.

4. Risk and Evidence Matrix

The matrix is an initial organising tool. It should be replaced or supplemented by a matter-specific chronology, document index, authority map, issue list, and risk register once the relevant records have been reviewed.

ISSUE	KEY EVIDENCE	RISK IF UNMANAGED	IMMEDIATE CONTROL
Each processing activity should have a defined purpose and an appropriate legal basis	Primary instruments, authority records, and operative clauses	Applying the wrong rule or relying on an unauthorised act	Confirm scope, authority, and controlling instruments.
Controllers should apply transparency	Original documents, metadata, correspondence, and witness sources	An incomplete or unreliable factual foundation	Issue preservation instructions and build an evidence index.
Vendor and cross-border arrangements require clear roles	Service records, filing receipts, calendars, and procedural history	Loss of rights through forum, form, or timing errors	Create a procedural map with verified dates and owners.
Incident response should integrate legal	Financial, operational, contractual, and governance impact data	A legally sound position producing unmanaged business exposure	Quantify scenarios and assign continuity safeguards.
Sensitive or high-risk processing may require stronger controls and documented assessment	Counterarguments, comparable decisions, and implementation records	Inconsistent submissions or an untested interpretation	Test counterarguments and approve a communication protocol.

5. Recommended Action Plan

5.1 Create a data inventory and processing register.

Begin by defining ownership of the task, the decision required, and the documents that must be available. Record any assumptions and gaps so that later reviewers can distinguish confirmed facts from matters still under investigation. The output should be a controlled work product with a clear approval path, not an informal collection of opinions.

5.2 Review notices, consent language, contracts, retention, and access controls.

The work should reconcile legal requirements with the organisation's actual process and systems. Where records conflict, identify the source of truth, the person responsible for correction, and whether a notification, amendment, reservation of rights, or other protective step is required before the inconsistency becomes material.

5.3 Establish data-subject request and incident-response procedures.

Timing should be planned backwards from the external deadline or business decision. Allow time for authority checks, document collection, technical or financial input, internal review, translation where relevant, authorised signature, submission, and proof of delivery. Contingency time is important where portals or third parties are involved.

5.4 Assess processors, recipients, and international transfer arrangements.

Implementation should be proportionate to the assessed exposure. Immediate measures should prevent further harm and preserve options; longer-term measures should address root cause, ownership, training, monitoring, and recurrence. Remediation should be accurate and should not overwrite the historical record needed for advice or proceedings.

5.5 Train personnel and test breach-response roles periodically.

The final position should be communicated only through approved channels. Management should know which developments require board, insurer, lender, regulator, counterparty, employee, or public disclosure. After the decision, the team should monitor new evidence and legal developments and adjust the plan when its assumptions no longer hold.

6. Decision Framework

IMMEDIATE CONTROL	Preserve the relevant record, identify the decision-maker and authority, confirm procedural deadlines, and prevent avoidable escalation while the facts are verified.
LEGAL ASSESSMENT	Map the verified facts and documents against the applicable legal framework, contractual position, regulatory expectations, and realistic exposure scenarios.
STRATEGIC EXECUTION	Select a proportionate course of action, define approval and communication protocols, document implementation, and revisit the strategy as new evidence or legal developments emerge.

6.1 Questions for Decision-Makers

- What precise decision, right, obligation, or exposure is being assessed in relation to personal data processing: lawful basis, governance, and breach readiness?
- Which law, regulation, contract, licence, corporate instrument, or official decision controls the issue?
- Which facts are verified by contemporaneous evidence, and which remain assumptions or disputed allegations?
- What procedural step or deadline could determine whether a right, defence, approval, or remedy remains available?
- What operational, financial, governance, regulatory, and reputation consequences arise under each realistic scenario?
- Who is authorised to approve the strategy, communicate externally, implement controls, and monitor later developments?

7. DRP Perspective and Conclusion

Personal Data Processing: Lawful Basis, Governance, and Breach Readiness requires more than identifying an abstract legal rule. A reliable position connects legal authority to the actual documents, decision-makers, chronology, and remedy under consideration. The analysis should expressly state its assumptions, unresolved questions, procedural dependencies, and the evidence on which each conclusion rests.

A structured review allows clients to make informed decisions while preserving flexibility as facts or authorities develop. It also creates a record showing that material alternatives and risks were considered. Matter-specific advice remains necessary before a transaction, filing, termination, objection, disclosure, investigation response, or proceeding.

8. Key Authorities and Official Sources

- Law No. 27 of 2022 on Personal Data Protection: https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-