THE CONSENT LEDGER · EDITION 2 · 4 NOVEMBER 2026

Six Asian countries brought in data laws before India. *Here's what happened next.*

Lessons for businesses, solution providers, legal teams and regulators, from Sri Lanka, Vietnam, Indonesia, Malaysia, Thailand and Singapore.

Not legal advice. consentree.in/research/asia-2026

In one page

Six Asian countries brought in data protection laws before India. Their regulators, businesses and advisers have already learned what works, what goes wrong, and what each side needs from the others. These are the eight lessons that stood out.

1. **"Give us a photocopy of your ID." Collecting too much was a top complaint.** In May 2026, Indonesia's population registry asked people to stop photocopying their national ID cards for routine paperwork, because copies were being misused for illegal online loans and fake bank accounts. In Thailand, collecting more than needed, or using data without a lawful basis, were among the most common of 2,672 complaints received by January 2026; one example was hospitals sending birthday cards from patient records.
2. **Front desks stopped keeping ID xeroxes.** Malaysia's code of practice gave retailers, travel agents and private schools ready-made forms to follow. Indonesia now points people to card readers and the digital ID on their phone instead of paper copies. Singapore gave businesses a year to stop taking full ID numbers at counters; cinemas, shops and building gates moved to phone numbers, booking references and partial IDs.
3. **Most leaks came from careless slips and insiders, not clever hackers.** In Vietnam, a 2023 Ministry of Public Security report said over two-thirds of the population had been affected by unlawful data collection and sale, and insiders, including a former police officer and a social insurance official, were prosecuted for selling data. Indonesia's national data centre was hit by ransomware in 2024 with only about 2% of its data backed up. In Singapore, 82% of 2023–24 cases involved weak security, such as an admin password that was the company's own name followed by "123".
4. **"Our vendor did it" was not accepted as an excuse.** In a 2021 survey of Vietnamese firms, 52% had no process for managing outside parties that receive personal data. Since April 2025, Malaysia's law binds service providers directly to keep data secure. In Singapore, a health-IT vendor was fined three times as much as its client; in Thailand, a booking-system vendor six times as much.
5. **People needed a simple checklist, not a legal opinion.** In August 2026, Sri Lanka's regulator gave its public sector six plain steps: make people aware, name an owner, list your data, find the gaps, write the few policies that matter, and train. In Indonesia, almost half of 135 digital businesses said in 2021 that they did not understand the rules. Malaysia lets one data protection officer serve several organisations, or be outsourced. In Singapore, about 60% of businesses wanted practical help with procedures, against about 40% wanting legal advice.

6. **Customers' trust, not fear of fines, kept businesses at it.** Between Deloitte's 2021 and 2024 surveys in Thailand, firms naming customer trust as a reason to comply rose from 59% to 75%, while those naming fines fell from 73% to 59%. Firms seeing significant benefits from compliance rose from 45% to 58%.
7. **Clear dates and simple guidance got businesses moving.** Sri Lanka withdrew its start date four days before it was due in 2025, then fixed 1 January 2027 for the first parts. Vietnam's first decree gave businesses about two months, and smaller firms struggled most. Where dates and guidance were clear, readiness rose quickly: Thai firms with a programme went from 30% to about 89%, and Singapore firms with adequate measures from about half to over 80% within a year.
8. **Regulators taught first and fined last.** Vietnam exempts household and micro businesses from appointing an officer, and gives small firms and startups five years. Malaysia wrote sector codes with worked examples for hospitals, finance, telecoms and others. Singapore's Do Not Call complaints halved in a year of outreach, and none of the 298 cases it investigated in 2024–25 needed a fine.

One line for each stakeholder

- **Businesses that hold data:** start with a list of what you hold and why, stop collecting what you don't need, name an owner, and fix the basics at the front desk and in IT.
- **Legal and advisory teams:** clients needed working processes, not just documents: notices, consent forms and vendor contracts that staff can actually follow.
- **Solution providers:** clients will ask for contracts, breach support and evidence; consent and request records built into the product are what they need most.
- **Regulators and policymakers:** templates, sector codes and clear dates moved compliance more than penalties did.

What regulators found going wrong

Across more than a decade of published decisions, the same nine kinds of failure come up again and again. Organisations are described here by type, as the regulators described them.

WHAT WENT WRONG	EXAMPLES FROM THE REGULATORS' OWN DECISIONS
1. Consent and marketing: messages to people who had opted out, consent tied to a benefit, processing without consent	A hotel processing guests' data without consent (Malaysia, 2017) · An employer whose consent form was tied to a staff benefit (Thailand, 2023) · An insurer told to delete data used for sales calls without consent (Thailand, 2023) · A home-tuition agency messaging numbers on the Do Not Call registry (Singapore, 2014)
2. Collecting or using too much: more data than the purpose needs, or a new use nobody agreed to	ID card photocopies misused for illegal online loans and fake bank accounts, prompting the registry's advice to stop photocopying (Indonesia, 2026) · Hospitals using patient records to send birthday cards (Thailand) · Over-collection is among the most common of Thailand's 2,672 complaints (to January 2026)

WHAT WENT WRONG	EXAMPLES FROM THE REGULATORS' OWN DECISIONS
3. Sending data to the wrong people: letters, emails, attachments, group chats	Four customers' letters in one envelope, and policy letters printed two to a sheet (insurers, Singapore, 2018) · A preschool teacher posting a list with parents' ID numbers in a parents' WhatsApp group (Singapore, 2019) · A forwarded email carrying 214 registrants' details (professional society, Singapore, 2016) · Tutors' certificates indexed by search engines (tutoring website, Singapore, 2019)
4. No one in charge: no named officer, no written policy, no training	A computer retailer handling over 100,000 people's data with no officer (Thailand, 2024) · A sports federation running on an "unwritten" procedure when it exposed 782 students' ID numbers (Singapore, 2021) · A learning platform with no data protection officer until after its breach (Singapore, 2024)
5. Vendors left unmanaged: no contract, no checks, vendor not telling the client	A state agency with no data processing agreement with its software developer (Thailand, 2025) · A booking-system vendor that did not tell its client about a leak (Thailand, 2025) · A ferry operator with no vendor management (Singapore, 2024)
6. Disposal and retention: records not destroyed, data kept after it was needed	A private hospital whose records, sent for destruction, ended up wrapping snacks; the shredding contractor was penalised too (Thailand, 2025) · A recruiter who kept job applicants' ID scans after leaving his job and misused them (Singapore, 2021, criminal case)
7. Security basics: guessable passwords, no two-step sign-in, unpatched systems, files left open online	A government agency's web app that leaked 200,000 people's data (Thailand, 2025) · An online learning platform whose admin password was guessed (Singapore, 2024) · A cashback shopping site that accidentally published a cloud access key on a code-sharing site (Singapore, 2023) · A clinic group whose visitor health-declaration file was left reachable online because a default server setting was never changed (Singapore, 2022)
8. Breach handling: not reporting, reporting late, not telling the people affected	A computer retailer whose leaked customer data fed scam calls, with no report to the regulator (Thailand, 2024) · A cosmetics company whose data reached a scam call centre, again unreported (Thailand, 2025) · A shopping site that took 15 days to act after its key was exposed (Singapore, 2023)
9. Registration and records: not registering where the law requires it, no record of processing	A private college and an employment agency processing data without registering (Malaysia, 2017) · Gaps in records of processing flagged as common by Thailand's regulator (2026)

Two more patterns from the region

- **Data trading is treated as a crime, not a compliance gap.** Vietnam and Indonesia prosecuted people selling personal data, including insiders. Thailand found 139 incidents of officials selling citizens' data in a review of over 31,000 government units.
- **Government bodies are not exempt from mistakes.** Thailand's monitoring found 4,801 of 15,820 agencies' websites leaking data in seven weeks; Indonesia's national data centre was hit by ransomware in 2024 with only about 2% of its data backed up.

> **What this means:** almost every failure on this list is an ordinary operational gap that a front-desk procedure, an IT checklist or a vendor contract would have prevented. Very few turned on a fine legal point.

Lessons from implementation

What organisations found hardest

- **Fitting it into daily work, not understanding the law.** In Thailand's 2021 survey of 136 firms, the top challenges were building new processes into operations (75%), interpreting the law (68%) and staff knowledge (63%). After a year of the law in force, putting the right technology in place and finding skilled staff became the bigger hurdles.
- **Vendors and breach plans were the weakest links.** In a 2021 survey of Vietnamese firms, 52% had no process for managing third parties that receive personal data, 52% had no breach response procedure, and 66% had no compliance roadmap.
- **Smaller firms started late.** In the same Thai survey, 70% of firms with fewer than 50 staff had not started. Vietnamese smaller firms struggled most with the short window, and hotels and airlines with deletion requests.
- **Understanding was the first barrier in Indonesia,** where almost half of 135 digital businesses surveyed in 2021 said they did not understand the rules.

About half of Vietnamese firms had no process for vendors or breaches

Survey of Vietnamese firms, 2021: share without each measure



PwC Vietnam personal data survey, 2021 (Appendix B)

What made it easier

- **Practical guidance and templates.** Singapore published 18 guides in its first year, including sector guides for telecoms, property, education, healthcare and social services, and worked through 65 trade associations to reach over 8,000 people.

- **A named owner and a readiness check.** In Thailand, firms with an in-house data protection officer rose from 56% to 72%, and firms that had done a readiness assessment from 45% to 80%.
- **Training as a budget line.** Thai firms naming training as a top budget area rose from 31% to 46% once the law was in force.
- **Self-assessment tools.** Thailand's regulator now offers a maturity model and a privacy index for organisations to check themselves.

Readiness jumped once dates and guidance were clear

Thailand: firms with PDPA processes, 2021 vs 2024 · Singapore: adequate measures, 2014 vs 2015



Deloitte Thailand surveys; PDPC Singapore industry readiness survey 2014 and annual report 2014/15 (Appendix B)

The order that worked

Across the guidance we reviewed, the same sequence recurs: make people aware, name an owner, list what data you hold and why, find the gaps, write the few policies that matter (requests, retention, notices, consent), then train. Sri Lanka's regulator set out exactly these six steps for its public sector in August 2026.

Lessons for businesses that hold data

Customers noticed, and used their new rights

- Over 792,000 phone numbers were added to Singapore's Do Not Call registry in its first year or so. By 2015, 9 in 10 people said they received fewer telemarketing messages.
- Thailand's complaints grew from 204 in one year to 616 the next, reaching 2,672 in total by January 2026. Breach reports roughly doubled over the same period.

In Thailand, customer trust overtook fines as the reason to comply

Share of firms naming each reason: 2021, before the law took effect, and 2024



Deloitte Thailand PDPA surveys (Appendix B)

The front desk changed

- When Singapore restricted the collection of national ID numbers in 2019, cinemas moved to booking references and SMS, shops asked for a phone number or email instead, and condominium gates switched to electronic visitor systems recording only a partial ID. The regulator gave a year's notice, template notices and a list of approved systems, and a government grant could cover up to 70% of new system costs.
- Regulators also corrected myths the other way. Two days after Thailand's law took effect, the government clarified that personal photos with people in the background, home CCTV and processing on legal grounds other than consent were all allowed.

It paid back

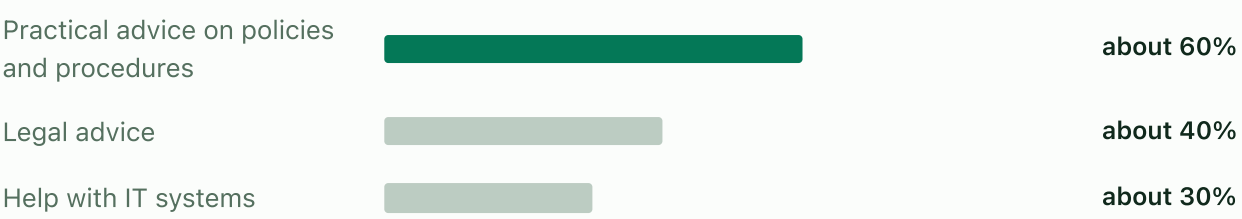
- In Thailand, firms expecting significant benefits from compliance rose from 45% to 58% once the law was in force.
- In Singapore in 2014, 70% of firms said compliance would build consumer confidence and 68% said it would make cross-border data transfers safer.
- In Cisco's 2022 survey of Asia-Pacific organisations, 91% said customers would not buy from a company that protects data poorly.

Help was available, especially for smaller firms

- Singapore's starter package for small firms covered policies, a data inventory, a breach plan, a named officer and training, from S$2,500, with a S$1,600 grant toward it.
- Malaysia's general code of practice includes ready-made consent templates for retailers, travel agents, private schools and others.
- Vietnam exempts household and micro businesses from impact assessments and from appointing an officer, and gives small firms and startups five years, unless they handle large volumes or sensitive data.

Businesses asked for help with procedures more than legal advice

Survey of 1,500 Singapore organisations, Jan–Feb 2015: share wanting each kind of help



PDPC Singapore industry survey, 2015 (Appendix B)

Lessons for solution providers

Software vendors, IT and managed-service firms, cloud and SaaS providers, implementers.

Regulators looked at what the vendor did, not only what the contract said

- **Singapore, 2016:** in the very first batch of decisions, a karaoke chain's IT vendor was penalised alongside its client, even though its contract never described it as handling personal data.
- **Singapore, 2019:** a public health group's IT agency was fined S$750,000, three times its client's S$250,000, for poorly managed servers, untested controls and known weaknesses left unfixed.
- **Singapore, 2023:** a healthcare provider's vendor was penalised for no periodic security reviews of an internet-facing drive; being a social enterprise was given no weight.
- **Thailand, 2025:** a toy company's booking-system vendor was fined THB 3 million, six times its client, for not containing the incident, not telling the client, and not helping the people affected. A state agency's software developer was penalised for building without access controls or risk assessments.
- **Malaysia, from April 2025:** processors are directly bound by the security duty, not only through their contracts.

What regulators expect from a vendor (Singapore's guide, echoed elsewhere)

1. A written contract that limits what the vendor may do with the data.
2. Reasonable security, such as encryption and access controls.
3. Telling the client about any incident without undue delay, and helping it respond.
4. No sub-contracting without the client's approval, with the same duties passed down.
5. Returning or deleting the data when the work ends.
6. Letting the client audit.

Where software helped most

- **Consent records** that show when, how and for what purpose consent was given. Vietnam now requires this proof and bans pre-ticked boxes; Malaysia's code requires consent and deletion records open to inspection.
- **Records of processing.** Indonesia's 2026 rules require a 13-item record; Thailand flags missing records as a common gap.
- **Request handling and breach logs,** so a client can show what it did and when.
- **Packaged offers for small firms.** Singapore channels small businesses to a short list of approved providers for a fixed-price starter package.

> **The opportunity:** in Singapore's 2015 survey, about 30% of firms wanted help with IT systems and about 60% with policies and procedures. Providers who combined the two, a working process plus the tool that records it, met the larger need.

Lessons for legal and advisory teams

Lawyers, chartered accountants, company secretaries, data protection officers.

Regulators moved away from consent-for-everything

- Singapore's 2020 amendments added deemed consent by notification, a legitimate-interests exception and a business-improvement exception, each requiring an assessment of the effect on people, and none available for marketing.
- Thailand's 2022 guidelines set out what valid consent and a clear notice look like: a clear positive act, given before or at collection; plain language; the legal basis stated; a prominent link to the full policy is acceptable.
- Indonesia's 2026 rules signal that consent buried in general terms and conditions may no longer count.

The data protection officer role settled into something practical

- Singapore published the first competency framework for the role in 2019, with three levels, and trained officers through partners including the accountants' institute.
- Malaysia (from June 2025) requires an officer above 20,000 people's data, or 10,000 for sensitive data; one person may serve several organisations, and the role can be outsourced.
- Vietnam sets qualifications for in-house and outsourced officers, and exempts the smallest businesses.
- **For CAs and CSs:** the outsourced and shared officer models in Malaysia and Vietnam are close to how many Indian firms already buy compliance support.

What regulators gave credit for

- Prompt notification, cooperation, quick fixes and admitting the problem.
- Singapore's expedited route closes a case in about five to six months, against up to eighteen for a full investigation, when liability is admitted up front.
- Voluntary undertakings, instead of a penalty decision, for organisations with good accountability practices such as a certified data protection programme.
- In Thailand, prompt help to the people affected was noted in a company's favour.

> **The lesson for advisers:** the documents mattered less than whether staff followed them. Several failures in the list above came where practice on the ground differed from the paper: a karaoke chain that did not enforce its own password policy, a sports federation working from an unwritten procedure.

Lessons for regulators and policymakers

Observations from the region, not recommendations to any government.

What worked

- **Guidance before enforcement.** Singapore spent its 18-month run-in on workshops, sector guides and outreach through trade associations. Readiness rose from about half of firms to over 80% within a year of the start date.
- **Free, practical tools.** A data protection notice generator, templates, an assessment tool and a fixed-price starter package for small firms (Singapore); a maturity model and self-assessment index (Thailand).
- **Sector codes.** Malaysia's codes for hospitals, utilities, finance, telecoms, insurance and aviation, plus a general code covering eleven more types of business, gave each sector its own worked examples.
- **Lighter routes for those who own up.** Undertakings and expedited decisions in Singapore; corrective orders before fines in Thailand. Singapore accepted undertakings from small firms that had not known the rules, on condition they engaged outside help.
- **Published decisions as teaching material.** Singapore publishes its decisions in plain terms, with what went wrong and what should have been done, so other organisations can learn from them.
- **Clear notice for front-line changes.** Singapore's ID-number guidelines gave a year's notice, with templates and approved systems, before they applied.

What caused problems

- **A regulator not ready on the start date.** Thailand's committee was appointed months before its law took full effect; Sri Lanka withdrew its start date four days before it was due; Indonesia's law has been enforceable since 2024 without its agency.

- **Rules late or without consultation.** Indonesia's detailed rules arrived nearly two years after the law became enforceable, without a public draft. Businesses learned of them weeks after signing.
- **Unclear thresholds and formulas.** Commentators flagged Indonesia's fine method (up to 2% of revenue, no formula) and its breach-reporting clock as hard to plan around.
- **Very short windows.** Vietnam's first decree gave businesses about two months to comply.

What this means for India

Most DPDP duties apply from May 2027. The countries before India point to a short, practical list for each group.

Businesses that hold data

1. Name one person who owns data protection, even part-time.
2. List what personal data you hold, where it sits (including spreadsheets and messaging apps) and why you need it.
3. Fix the security basics: strong passwords, two-step sign-in, updates, nothing left open online.
4. Fix the front desk: collect only what the purpose needs, and record consent where you rely on it.
5. Write down how you would handle a breach and a customer request, and who does what.

Solution providers

1. Expect clients to ask for a processing contract, breach support and security evidence; have them ready.
2. Build consent records, request handling and breach logs into the product, not as add-ons.
3. Treat your own security as your client's compliance: in the region, vendors were penalised alongside clients.

Legal and advisory teams

1. Help clients turn notices and consent forms into front-desk and website steps staff will follow.
2. Review vendor contracts for the six points regulators expect.
3. Consider the shared or outsourced officer model for clients too small for a full-time role.

For the Data Protection Board and policymakers, the regional record suggests that templates, sector guidance, small-business toolkits, published decisions and clear dates did more for compliance than penalties alone.

Appendix A: Country profiles

COUNTRY	LAW	REGULATOR	KEY DATES	ENFORCEMENT SO FAR
Singapore	Personal Data Protection Act 2012	Personal Data Protection Commission (2013)	Main duties July 2014; breach reporting February 2021; higher maximum penalty October 2022	More than 180 published decisions by 2021; mostly security failures
Malaysia	Personal Data Protection Act 2010, amended 2024	Department of Personal Data Protection (2011)	In force November 2013; officer, breach reporting and portability from June 2025	Compounds and court cases since 2017; sector registration required
Thailand	Personal Data Protection Act 2019	Personal Data Protection Committee (2022)	Postponed twice; in force June 2022	Corrective orders from 2023; administrative fines from 2024
Sri Lanka	Personal Data Protection Act No. 9 of 2022, amended 2025	Data Protection Authority (2023)	Main duties from 1 January 2027; penalties and rights still to be dated	None yet
Indonesia	Personal Data Protection Law No. 27 of 2022	Agency not yet set up; ministry acts in the interim	Enforceable October 2024; detailed rules apply from January 2027	No administrative penalties yet; criminal cases on data trading
Vietnam	Decree 13 (2023); Personal Data Protection Law (2025)	Cybersecurity department, Ministry of Public Security	Decree July 2023; law January 2026; penalties decree August 2026	Criminal cases on data trading; administrative penalties now possible

Appendix B: Sources and method

Method. Desk research from public sources, 22 October 2026. Official gazettes and regulator releases first, then law-firm analysis and reputable press. Organisations are named only where the regulator named them. Rupee amounts use rounded October 2026 rates (₹65/SGD, ₹20/MYR, ₹2.8/THB, about 300 VND and 190 IDR per rupee, ₹0.29/LKR) and are approximate. Not legal advice.

Checks completed, 27 October 2026

- **82% (Singapore):** confirmed. PDPC's report says 82% of its enforcement cases from January 2023 to December 2024 involved organisations that "failed to protect their data because of weak security measures".
- **Thailand's complaints:** 2,672 PDPA complaints recorded by January 2026. The regulator names collecting more than necessary, collecting without a lawful basis, and using or disclosing without a lawful basis as the highest-volume types, but does not rank them. The report's wording now says "among the most common".
- **Deloitte Thailand surveys:** the comparison is October 2021 (136 respondents, mostly firms with 500+ staff) against 2024 (sample size not published). Confirmed: customer trust 59% to 75%, fines 73% to 59%, reputation 66% to 81%, processes implemented 30% to 89%, significant benefits 45% to 58%. An earlier "no benefit 23% to 4%" figure could not be confirmed and has been removed from the report and the chart.
- **Singapore 2015 survey:** confirmed. 1,500 organisations, January to February 2015: about 60% wanted non-legal advice to develop policies and procedures, about 40% legal advice, about 30% help with IT and security systems.
- **Malaysia notice language:** confirmed. Section 7(3) of the PDPA 2010 requires notices in the national language and English. Malaysia's complaint categories are not used in the report.
- **Indonesia's agency:** still not established as of August 2026. A draft Presidential Regulation to create it is in progress; the Ministry of Communication and Digital Affairs enforces in the meantime.

Sources for these checks: PDPC breach landscape 2023–24 · Mondaq: Thailand Data Privacy Day 2026 · Bangkok Post: Deloitte 2021 · The Nation: Deloitte 2024 · PDPC industry survey 2015 · PDPA 2010 s.7(3) (iubenda summary) · HBT: Indonesia update, August 2026

Sources

Thailand: Hunton · DLA Piper · Tilleke: delay · Tilleke: first regulations · Rajah & Tann · DFDL: first fine · Tilleke: eight fines · Thai PBS World · OpenGov Asia · Legal 500: SME exemption · Deloitte survey

Indonesia: DFDL: GR 33/2026 · HLC · HBT · Adaptist · Antara · detik

Vietnam: FPF · Tilleke: PDP Law · Tilleke: Decree 356 · DFDL: Decree 330 · KPMG · VietnamNet survey · Do Not Call decree

Malaysia: Rajah & Tann: phased start · Legal 500: amendments · Chambers 2026 · Global Compliance News: first convictions · Conventus: first charge · Malay Mail: complaints · University of Hertfordshire study

Sri Lanka: PDP Act No. 9 of 2022 · Amendment Act No. 22 of 2025 · Gazette 2498/16 · DPA guidelines page · DPA Circular 01/2026 · Babl AI · Daily FT · Neelakandan

Singapore: PDPC 2013 release · PDPC first enforcement, 2016 · PDPC: SingHealth and IHiS · NUS TRAIL study · Allen & Gledhill · IMDA SME package · PDPC Do Not Call survey

Lessons, violations and surveys: PDPC: breach landscape 2023–24 · PDPC: industry readiness 2014 · PDPC: industry survey 2015 · PDPC annual report 2014/15 · PDPC: guide to managing data intermediaries · PDPC: NRIC guidelines · PDPC: DPO competency framework · MDDI: Do Not Call statistics · Clyde & Co 2024 · Clyde

& Co 2023 · Insurance Business: insurers fined · CNP Law: expedited decisions · Tilleke: Thailand Data Privacy Day 2026 · Tilleke: Thailand consent guidelines · Bangkok Post: Deloitte 2021 · Fulcrum: Thai government leaks · PwC Vietnam survey · ADB: Vietnam decree · Vietnam Briefing: Decree 356 · Katadata: Indonesia survey · CMS: Malaysia DPO guideline · Mondaq: Malaysia general code · Cisco APAC 2022 · Thai Post: myths corrected

Added 27 Oct: Indonesia: Dukcapil on e-KTP photocopies (RCTI+, May 2026) · Vietnam: illicit data trading (Tilleke, 2024) · Malaysia: amendments from June 2025 (ASEAN Briefing)