BL&S

BURKE LAW & STRATEGY

CLIENT ALERT · JUNE 2026

APAC Regulatory Developments: A Mid-2026 Briefing

Regulation has increasingly become an instrument of statecraft across Asia-Pacific. National security, industrial policy, data sovereignty, and financial-market integrity are being pursued through legislation and enforcement, not just diplomacy and policy. For a multinational, that shift changes the nature of the risk. A prevailing issue has become whether complying with one government's law places a company in breach of another's, and who inside the company decides what to do when it does. When geopolitical tensions rise, multinationals can find themselves entangled in an international quarrel that they neither started nor can end.

Three developments define the landscape at mid-2026:

China has continued to build out a defensive legal toolkit that can penalize a company for complying with U.S. or EU sanctions, export controls, or forced-labor rules. Data, cybersecurity, and artificial-intelligence regulation have moved from policy to enforceable obligations, with India, Korea, Vietnam, and China all crossing that threshold within roughly a year. And financial-services regulators in Hong Kong, Singapore, and Australia are setting a template that increasingly applies across the region: regulators now expect demonstrable governance and documented accountability, not written policies alone.

China

China remains the most consequential regulatory environment in the region, and in 2026 it refined a key instrument. In late March and early April, the State Council issued two decrees pushing back against what China views as hostile foreign measures. Decree No. 834, on industrial and supply-chain security, authorizes investigations and countermeasures where foreign conduct is viewed as threatening Chinese supply chains. Decree No. 835, on countering "improper" extraterritorial jurisdiction, builds on the Anti-Foreign Sanctions Law and gives the Ministry of Justice a lead role in declaring foreign measures improper, issuing prohibition orders, and adding offenders to a new "Malicious Entities List." It also allows Chinese companies to sue in Chinese courts persons and entities that implement the offending foreign measure.

The framework is already being applied. In May 2026, the Ministry of Justice ruled that the European Commission's foreign-subsidies investigation into Nuctech, a Chinese maker of airport scanners, was an improper exercise of extraterritorial jurisdiction. Much of the relevant terminology remains undefined, including "improper," "appropriate connection," and "discriminatory measures," preserving discretion for Chinese regulators.

China's expanding toolkit is largely reactive insofar as it responds to U.S. and European sanctions, export controls, forced-labor restrictions, and investment screening that Beijing regards as unjustified extraterritorial reach. The decrees are framed in those terms, and enforcement to date has been deliberate and geopolitically targeted, consistent with how the Anti-Foreign Sanctions Law and Unreliable Entity List have been applied since 2020.

For multinationals, the prospect of conflicting obligations is not a hypothetical one. A company may face U.S. export controls, an EU forced-labor diligence requirement, or a customer's demand to stop working with a sanctioned party on one side, and a Chinese anti-sanctions rule on the other. A good-faith decision by headquarters (e.g., halting a shipment, freezing a payment, dropping a counterparty) could be deemed by Chinese authorities to be unlawful implementation of a foreign discriminatory measure, with consequences that can extend to executives personally through exit bans and asset freezes.

A company with material China exposure is advised to develop a China-specific conflict-of-laws plan that names the senior person or people who own the decision when foreign-law compliance creates Chinese-law exposure, and sets out a written escalation path so that a frontline manager is never left to resolve a sovereign conflict under time pressure. It should pre-clear positions on the recurring flashpoints, such as how to handle offboarding a newly sanctioned counterparty, so that the analysis is complete before the need arises.

China's data regime adds a further layer of complexity. The certification route for outbound transfers of personal information took effect on January 1, 2026. Companies operating in China need to map their data flows, identify "important data" by sector, and account for provisions that bar producing China-based data to a foreign regulator without Chinese approval. The practical step is to know, in advance of any investigation or transaction, what data sits in China, what might be characterized as important data, which transfer mechanism applies to each category, and when and how to seek certification from the government.

India

India's Digital Personal Data Protection (DPDP) regime is gradually maturing. The government notified the DPDP Rules in November 2025 and is operationalizing the 2023 Act on a staggered timeline: the Data Protection Board was stood up first, consent-manager provisions follow roughly a year later, and the substantive compliance obligations take effect by mid-2027. Penalties run to ₹250 crore per contravention, and entities designated as Significant Data Fiduciaries are required to conduct annual data-protection impact assessments, independent audits, and algorithmic due diligence, and to appoint a designated officer. The framework is already shaping how deals are done, moving data governance from an afterthought to a key consideration in the Indian M&A context.

Companies are advised to complete a data-mapping exercise across Indian operations and vendors; assess whether the organization is likely to be designated a Significant Data Fiduciary and, if so, stand up the impact-assessment, audit, and algorithmic-review processes that the designation requires; appoint and properly resource a data-protection officer; rebuild consent notices and capture mechanisms to the standard set by the rules; refresh vendor and processor contracts to allocate DPDP obligations and breach responsibilities; and align the Indian program with the company's global privacy architecture. In transactions, DPDP due diligence, representations, and indemnities should now be a standard feature of any India-facing deal.

Japan

Japan continues its pivot toward an explicit economic-security model. A 2026 bill to amend the Economic Security Promotion Act, the first substantial amendment since the Act's 2022 enactment, passed the House of Representatives in May 2026 and is now before the upper house. It would add healthcare to the critical-infrastructure framework, bring "services essential to critical goods"

into scope, and support strategic overseas projects. Separately, Japan tightened inbound investment screening under the Foreign Exchange and Foreign Trade Act in 2025, removing certain pre-approval exemptions for higher-risk foreign investors. Japan does not appear to be building a U.S.-style CFIUS regime, and it remains broadly open to investment, but it is moving toward a more *selective* openness: a quick path for routine filings, a more demanding one where a transaction touches control, sensitive technology, defense-linked production, or critical infrastructure.

Companies in semiconductors, AI, healthcare, logistics, energy, cloud, and advanced manufacturing should screen Japan-facing transactions for Foreign Exchange and Foreign Trade Act exposure early, before terms are set; assess whether any Japanese entity in the structure is, or is likely to become, a designated core business or critical-infrastructure provider; prepare supply-chain, ownership, and technology-transfer information in the form regulators will request; and monitor the pending amendment, since the addition of healthcare and critical-goods services will add a new set of companies to the regime once it passes.

Hong Kong

Hong Kong has moved relatively quickly to build an institutional-grade digital-asset regime. The Stablecoins Ordinance took effect on August 1, 2025, making fiat-referenced stablecoin issuance a licensed activity, and in April 2026 the Hong Kong Monetary Authority granted the first two licenses to HSBC and a Standard Chartered-led group, after assessing 36 applications and signaling from the outset that the initial batch would be deliberately small. The message is that Hong Kong welcomes innovation on institutional terms. It creates an opportunity for serious participants, but the bar is high, with detailed and supervised requirements for licensing, full reserve backing, governance, anti-money-laundering and travel-rule compliance, custody, and disclosure.

Any firm contemplating Hong Kong digital-asset activity would do well to treat regulatory strategy as part of product design. That means bringing legal, compliance, treasury, technology, and risk together before the business model is fixed; building the reserve, custody, segregation, and redemption architecture to the published standards from the start; designing the anti-money-laundering, travel-rule, and wallet-verification controls into the product; and engaging the regulator early, given that it has been explicit about a measured, limited-batch approach to licensing.

Singapore and South Korea

Singapore and South Korea illustrate the two main paths Asian regulators are taking on AI, and the expectations under both have now become concrete.

Singapore continues to govern by framework and supervisory expectation rather than by a single statute. In March 2026, the Monetary Authority of Singapore released an AI Risk Management Toolkit for the financial sector, and the Association of Banks in Singapore followed with a handbook on generative-AI guardrails; these sit on top of proposed MAS guidelines, out for consultation since November 2025, that will carry a twelve-month transition once finalized. The expected substance, an AI inventory, materiality-based risk assessment, lifecycle controls, board-level accountability, and vendor governance, is fast becoming the standard a supervisor will look for.

South Korea took the statutory route. Its AI Basic Act took effect on January 22, 2026, making Korea the second major jurisdiction after the European Union with a comprehensive AI law. It requires advance notice of generative and high-impact AI, mandatory labeling of AI-generated

content, and stricter handling of deepfakes, with added obligations for high-impact systems in sensitive sectors such as healthcare, hiring, and biometrics. Notably, it applies extraterritorially, and foreign operators above certain thresholds must appoint a domestic representative. Fines are modest for now, and early enforcement is expected to emphasize guidance, but the compliance architecture is already required.

For most multinationals, the response is similar regardless of which model applies. Legal and compliance should actively participate in (if not own) AI governance. The practical steps are to maintain a current inventory of where AI is deployed across the region; to classify the higher-impact and generative uses against Korean, Singaporean, and sector-specific criteria; to put labeling and user-notice mechanisms in place where Korea requires them; to appoint a Korean domestic representative if the thresholds are met; and to write the acceptable-use policies, approval gates, documentation standards, vendor controls, and escalation triggers that a regulator could later inspect.

Southeast Asia

Across Southeast Asia, national data-protection regimes have begun to be enforced. Vietnam's Personal Data Protection Law took full effect on January 1, 2026, and it is among the strictest in the region, with no legitimate-interest basis, consent required for employee data, tight breach-notification timelines, and localization pressure that makes the country one of the more demanding compliance environments for any company with manufacturing, outsourcing, or workforce data in-country. Indonesia continues to operationalize its 2022 Personal Data Protection Law; Thailand's regulator has moved from rule-making to inspections and penalties; and Malaysia has paired amendments to its data-protection law with a new Data Sharing Act. Enforcement is broad, and not confined to data. Indonesian authorities arrested executives of a state-owned energy firm in a 2025 corruption sweep; the Philippines has been absorbed by an infrastructure corruption scandal reaching its most senior officials; and Malaysia continues to apply corporate criminal liability for the conduct of associated persons unless a company can show it had adequate procedures in place.

The overarching recommendation is to avoid treating the region as a single jurisdiction. A regional policy is a useful baseline, but it has to be localized country by country for breach-notification timelines, consent requirements, sensitive-data definitions, regulator-notification duties, and cross-border transfer mechanisms. For Vietnam in particular, a company should assess whether a local processing or storage arrangement is needed, and review whether its existing data flows can satisfy the transfer rules. On the anti-corruption side, the persistence of high-profile cases argues for a properly resourced compliance program and, given the Malaysian adequate-procedures defense, for contemporaneous documentation of third-party due diligence and the controls actually in place.

Australia

Australia tends to convert governance expectations into concrete operational requirements, and its anti-money-laundering reform is the clearest current example. The "Tranche 2" expansion extends AML obligations to lawyers, accountants, real-estate professionals, and dealers in high-value goods, on the order of tens of thousands of newly regulated businesses, phased in across 2026, while existing reporting entities face updated program expectations. This reaches well beyond the financial sector, and many of the newly covered businesses have never built a compliance function of this kind.

The work involves standing up customer due diligence and beneficial-ownership identification, transaction monitoring calibrated to the business's risk, suspicious-matter reporting, recordkeeping, and staff training, all supported by a written, board-approved AML program. The functional test a regulator will apply is whether the business can identify its customers, understand the risk each presents, monitor activity, and escalate suspicious matters through a process it can document and defend.

What it all means

Several recommendations follow from all of this.

1. Map potential conflicts of laws to identify where a U.S. or EU obligation, such as sanctions, export controls, or due diligence requirement, could place the company in breach of Chinese or other local law. For each one, name the senior decision-owner and the escalation path in advance so that a conflict between sovereigns is never resolved on the fly by someone without the authority to make the call.
2. Refresh data-transfer and localization assessments jurisdiction by jurisdiction. China, India, Vietnam, and Indonesia each warrant a current view of where data sits, who can reach it, how it may lawfully move, and which transfer mechanism applies to each category. The same map can be useful in an investigation, a transaction, and a regulatory inquiry.
3. Build and maintain an AI use register. Know where AI is being deployed across the region, including in HR, marketing, customer service, finance, and product; classify the higher-impact and generative uses against Korean, Singaporean, and sector rules; and put labeling, notice, and human-oversight controls in place where they are required.
4. Put Asia-Pacific regulatory risks on the board's agenda. These developments bear on market access, supply-chain continuity, data flows, product launches, and crisis exposure, all squarely within a board's purview.

The common thread is that regulatory activity across APAC increasingly reflects strategic and geopolitical calculation as much as legal doctrines. Companies that pair legal analysis with practical judgment will be better at anticipating and resolving problems.

This alert is provided for general informational purposes only and is not legal advice. Please contact Brian Burke (brian@burkelawstrategy.com) to discuss how these developments may apply to your situation.