APAC Data Residency

Researched by Hey Lefty

Automated research briefings on topics you choose — heylefty.com

TL;DR

The APAC data residency landscape is shifting toward a highly structured, zero-tolerance compliance environment where broad corporate exemptions are rapidly disappearing. While newly formalized certification frameworks and standardized filings offer predictable pathways for continuous data flows, regulators are backing these rules with strict volume-based thresholds and sudden, operational-stopping assessment triggers. At the same time, a sharp distinction between physical local access and remote digital access is emerging as a critical compliance boundary, forcing multinational companies to balance physical travel protocols against localized cloud hosting strategies.

The Narrowing of Compliance Exemptions and Strict Timelines

Compliance teams are facing a rapid contraction of standard data transfer loopholes as authorities enforce narrow exemptions and strict, non-negotiable assessment timelines.

> *"While the March 2024 Provisions on Promoting and Regulating Cross-Border Data Flows introduced helpful exemptions for contract performance and human resources management, the CAC's October 2025 FAQ warns that these exemptions must be narrowly construed."* — China PIPL Five Years On

> *"Once notified by relevant regulators (such as the National Medical Products Administration for life sciences) that they hold Important Data, processors must apply for a Security Assessment within two months."* — China PIPL Five Years On

This regulatory shift strips away the legal safety net of relying on broad, self-declared human resources or transactional exemptions to bypass regulatory filings. As detailed in an Arnold & Porter client advisory, companies must now verify that any exempted transfer is strictly necessary and minimizes employee impact, or face immediate compliance exposure. Furthermore, according to a China Briefing analysis, the lack of a grace period once a regulator flags "Important Data" means compliance teams must pre-emptively draft assessment materials to avoid an immediate operational freeze.

What to watch: Whether sector-specific regulators outside of the life sciences space begin actively issuing "Important Data" notifications to trigger the two-month compliance countdown.

Operationalizing Structured Pathways for Continuous Transfers

Standardized certification and consolidated Standard Contractual Clause (SCC) filings are transitioning from theoretical legal options to highly structured, repeatable compliance workflows.

> *"For continuous data transfers to the same recipient, processors can submit a single SCC filing based on a reasonable annual estimate, avoiding repetitive filings."* — China PIPL Five Years On

> *"The certification process involves technical verification, on-site review, and post-certification supervision by CAC-approved professional Certification Institutions."* — China PIPL Five Years On

These structured pathways provide multinational enterprises with a predictable, long-term blueprint for intra-group data flows, replacing fragmented, case-by-case filings with renewable certifications. However, as noted in recent Hunton Andrews Kurth regulatory guidance, this predictability is fragile; any substantial change in server locations, transfer purposes, or recipient identities completely invalidates the existing filing and forces a comprehensive re-submission.

What to watch: The rate at which multinational compliance teams adopt the newly active certification process over standard contractual clauses for complex, multi-entity corporate structures.

Physical Demarcation and the Redefinition of Local Access

The physical location of data access is emerging as a critical compliance boundary, offering operational relief for local travel while SaaS providers localize infrastructure.

> *"The FAQ clarifies that when overseas personnel travel to mainland China and access data locally without transferring the data abroad, such access is NOT deemed to be cross-border data transfer"* — China PIPL Five Years On

> *"Starting in May 2026, Notion is rolling out dedicated, localized data residency for Enterprise plan customers in Japan and South Korea."* — Multinational SaaS Adaptation

By clearly distinguishing between remote digital access and physical, on-the-ground access, regulators are providing a valuable operational carve-out for global audits and executive travel. At the same time, according to Notion's infrastructure rollout announcement and Loom's community updates, the parallel push by major software vendors to deploy local cloud nodes highlights that local storage remains the non-negotiable standard for day-to-day corporate data.

What to watch: Whether other APAC jurisdictions adopt similar physical-presence exemptions for traveling multinational staff to help ease the burden of cross-border compliance.

What surprised us

- **Physical presence completely bypasses the digital cross-border definition.** The Cyberspace Administration of China (CAC) clarified that when overseas personnel physically travel to mainland China and access data locally, it is *not* deemed a cross-border transfer China PIPL Five Years On. This provides an elegant, physical workaround for sensitive internal investigations or executive oversight that would otherwise trigger heavy regulatory assessments if conducted remotely.
- **The absolute stop-work order on "Important Data" transfers during assessments.** Once notified that they hold "Important Data," organizations must apply for a Security Assessment within two months, but crucially, *all transfers of that data must stop immediately* until the assessment is completed China PIPL Five Years On. This zero-grace-period freeze could paralyze active cross-border business operations.
- **Cumulative volume thresholds can silently invalidate active SCC agreements mid-year.** While a single Standard Contractual Clause (SCC) filing can cover continuous transfers based on annual estimates, crossing the cumulative threshold of 1 million individuals (or 10,000 for sensitive data) calculated from January 1 of that year instantly nullifies this coverage, requiring an immediate application for a full Security Assessment China PIPL Five Years On. This makes real-time volume tracking an absolute operational necessity.

Open threads worth a vote

- South Korea PIPA Amendments Effective Date — South Korea's sweeping PIPA amendments, authorizing fines of up to 10% of total revenue for severe data breaches, expanding reporting obligations to forgery/alteration, and designating the business owner/representative as the 'ultimate responsible person', come into effect.

Appendix: Findings

China PIPL Five Years On: Cross-Border Transfer Pathways Mature, Certification Closes the Gap (2026)

China PIPL Five Years On: Cross-Border Transfer Pathways Mature, Certification Closes the Gap (2026)

The Cyberspace Administration of China (CAC) has significantly clarified and refined the practical compliance pathways for cross-border data transfers through its October 31, 2025 Q&A (FAQ) and the October 14, 2025 *Measures on Certification for Cross-Border Transfer of Personal Information* (effective January 1, 2026). These updates provide critical operational parameters for multinational compliance teams, establishing strict boundaries around exemptions, defining a hard two-month timeline for Important Data assessments, and formalizing the Personal Information Protection (PIP) Certification pathway.

1. Narrow Construction of Cross-Border Exemptions

While the March 2024 *Provisions on Promoting and Regulating Cross-Border Data Flows* introduced helpful exemptions for contract performance and human resources management, the CAC's October 2025 FAQ warns that these exemptions must be narrowly construed.

- **Contract Performance:** The examples listed in the 2024 Provisions (e.g., cross-border shopping, shipping, remittance, flight bookings) are illustrative and not exhaustive. To qualify, a transfer must meet two criteria: (1) it is for the conclusion or performance of a contract to which the individual is a party, and (2) it is strictly *necessary* to transfer the personal information abroad.
- **HR Management:** To qualify, the transfer must be strictly necessary for HR management, limited only to personal information directly relevant to HR, and executed in a way that minimizes the impact on employees. The CAC advises that companies should not transfer higher-risk data (such as national ID numbers, passports, or bank accounts) without first verifying that the transfer meets these criteria. Furthermore, basic obligations—such as individual notification, separate consent, and conducting a Personal Information Protection Impact Assessment (PIA)—remain mandatory even when an exemption applies.

2. Important Data and the Hard Two-Month Assessment Trigger

The processing of "Important Data" (data posing national security or public interest risks) remains heavily regulated. The CAC May 2025 and October 2025 FAQs clarify that while data processors do not need to self-diagnose "Important Data" in the absence of official notification or public announcement, they must act immediately upon receiving notification:

- Once notified by relevant regulators (such as the National Medical Products Administration for life sciences) that they hold Important Data, processors must apply for a Security Assessment within **two months**.
- Crucially, **all transfers of Important Data must stop** until the Security Assessment is completed. Because there is no grace period for this two-month deadline, compliance teams are advised to prepare draft assessment materials while the regulatory identification process is still ongoing.

3. Overseas Remote Access vs. Local Access

The *Guidelines for Data Export Security Assessment (Version 3)*, effective June 27, 2025, confirm that remote access to mainland China-stored data by overseas personnel constitutes a cross-border transfer. However, the October 2025 FAQ clarifies a vital distinction:

> "The FAQ clarifies that when overseas personnel travel to mainland China and access data locally without transferring the data abroad, such access is NOT deemed to be cross-border data transfer, and that whether a cross-border data transfer occurs depends on where the access takes place."

4. Standard Contractual Clauses (SCC) Filing for Continuous Transfers

For continuous data transfers to the same recipient, processors can submit a single SCC filing based on a reasonable annual estimate, avoiding repetitive filings. However:

- If cumulative transfer volumes exceed the Security Assessment thresholds (e.g., personal information of more than 1 million individuals or sensitive personal information of more than 10,000 individuals calculated from January 1 of that year), the processor must immediately apply for a Security Assessment.
- Any "substantial" changes (such as new recipients, new purposes, or server location changes) require a complete re-filing of the entire compliance package, as there is currently no simplified update process. Onward transfers by the overseas recipient to third parties must be explicitly disclosed in Appendix I of the SCC filing.

5. PIP Certification Pathway Formalized

The CAC's *Measures on Certification for Cross-Border Transfer of Personal Information* (issued October 14, 2025, effective January 1, 2026) and the national standard *GB/T 46068-2025 (Data Security Technology — Security Certification Requirements for Cross-Border Processing Activity of Personal Information)* establish PIP Certification as a highly practical compliance pathway, especially for intra-group transfers within multinational corporations.

- The certification process involves technical verification, on-site review, and post-certification supervision by CAC-approved professional Certification Institutions.
- GB/T 46068-2025 outlines specific requirements for data subject rights, notification, consent, and the retention of processing records, providing a standardized baseline for audit.

Sources

- China Issues Further Clarifications on Cross-Border Data Transfer Rules
- China's Cross-Border Data Transfer: Key Insights from Official Q&A (III)
- China CAC Issues Guidance on CBDT Security Management

Multinational SaaS Adaptation: Notion, Loom, and Jamf Expand Local Data Residency Across APAC (May 2026)

Multinational SaaS Adaptation: Notion, Loom, and Jamf Expand Local Data Residency Across APAC (May 2026)

As APAC jurisdictions implement stricter data localization, cross-border transfer restrictions, and operational risk standards, multinational enterprise software-as-a-service (SaaS) and technology vendors are rapidly adapting their infrastructure. Rather than relying on centralized global cloud environments, major providers are rolling out localized data residency options to help their enterprise clients comply with domestic regulations.

Several landmark data residency expansions in **May 2026** highlight this accelerating trend across Japan, South Korea, Australia, and India.

1. Notion Expands Local Data Residency to Japan and South Korea (May 2026)

In response to growing regulatory pressure and enterprise demand, collaborative workspace platform **Notion** announced a major expansion of its infrastructure in May 2026:

- **The Rollout:** Starting in **May 2026**, Notion is rolling out dedicated, localized data residency for Enterprise plan customers in **Japan** and **South Korea**.
- **Regulatory Drivers:** This expansion allows multinational and local enterprises to store their workspace data within physical servers located in Tokyo and Seoul. This directly aligns with Japan's upcoming APPI amendments (which tighten rules on third-party transfers and biometric/children's data) and South Korea's strict Personal Information Protection Act (PIPA) amendments (which impose heavy revenue-based fines for cross-border non-compliance starting in September 2026).

2. Loom (Atlassian) Launches Australian Data Residency (May 2026)

Atlassian-owned video messaging platform **Loom** has formalized localized hosting capabilities in Oceania:

- **The Rollout:** Starting in **May 2026**, Loom is officially launching localized data residency in **Australia**.
- **Regulatory Drivers:** Australia's regulatory landscape is undergoing significant tightening. Financial institutions and critical service providers are navigating the Australian Prudential Regulation Authority's (APRA) **CPS 230 Operational Risk Management** standard, which demands strict control over third-party data processing. Furthermore, Australia's ongoing **Privacy Act Reforms** are escalating penalties and establishing clearer expectations for domestic data handling. Localized residency allows Australian enterprise customers to keep video recordings, transcripts, and metadata onshore.

3. Jamf Deploys High-Compliance Cloud in India (2026–2027)

Apple device management and security vendor **Jamf** announced plans to deploy its first-ever dedicated high-compliance cloud environment in India, targeting full availability in **2027**:

- **The Rollout:** The deployment is designed to host Apple device management and security data locally within India.
- **Regulatory Drivers:** This localized cloud environment is a direct response to India's **Digital Personal Data Protection Act (DPDPA)** and the newly notified **DPDP Rules**, which establish strict consent and data-handling frameworks. By establishing an onshore cloud, Jamf enables Indian enterprises, public sector bodies, and highly regulated financial institutions to maintain strict compliance with the DPDPA's local storage and security mandates.

4. Compliance Takeaways for Multinational Operators

For compliance teams managing APAC operations, these developments signal a critical shift in SaaS vendor management:

1. **Incorporate Residency into Vendor Audits:** When procurement and IT teams onboard or renew enterprise software (such as Notion, Loom, or Jamf), compliance should mandate the activation of local data residency options (e.g., Tokyo, Seoul, Sydney, or Mumbai) to insulate the company from cross-border transfer liability.
2. **Review Enterprise Plan Tiers:** Many SaaS vendors restrict localized data residency to their highest-tier "Enterprise" plans. Compliance teams must budget for and coordinate these plan upgrades to meet their regulatory obligations under local laws like South Korea's PIPA or Australia's CPS 230.
3. **Update Data Mapping Registries:** Ensure that internal registries reflect the physical location of SaaS data hosting, particularly as vendors transition client databases from centralized US/EU cloud hubs to localized APAC instances.

Sources

- Notion is expanding data residency to Japan and South Korea
- Confirming data residency with my Loom data?
- Multinational Response: Jamf Launches India-Specific High-Compliance Cloud for DPDP Alignment (2026–2027)