

LEGAL FORUM



THE SOVEREIGN DATA WALL: HOW VIETNAM'S NEW DATA REGIME REWRITES THE CROSS-BORDER INVESTMENT PLAYBOOK

1. Introduction: The New Cost of Doing Business in Vietnam

Vietnam remains an elite global destination for Foreign Direct Investment (FDI), driven by supply chain diversification, a highly skilled digital workforce, and a pro-growth economic agenda. However, the regulatory price of entry for cross-border capital has fundamentally shifted.

With the full implementation of the statutory Personal Data Protection Law (PDPL) and its guiding framework, Decree 356, Vietnam has moved resolutely from a light-touch administrative environment to an active, sovereign, state-supervised enforcement era. The ultimate indicator of this shift lies in its teeth. Serious compliance failures now carry a serious statutory penalty of up to 5% of a company's preceding-year fiscal revenue in the Vietnamese market. Data privacy is no longer an administrative exercise. It now has immediate financial repercussions.

2. Beyond GDPR: State-Supervised Transfer Model

A mistake made by multinational general counsels when evaluating the Vietnamese market is assuming that their pre-existing European General Data Protection Regulation (GDPR) or regional APEC Cross-Border Privacy Rules (CBPR) frameworks are sufficient. Western regimes rely primarily on independent, passive privacy commissioners who investigate after a breach occurs. In contrast, Vietnam operates a strict, state-supervised data flow model administered directly by the Ministry of Public Security (MPS) through its specialized cybersecurity divisions.



Under the PDPL, data sovereignty is aggressively enforced through pre-transfer compliance barriers. Before any personal data belonging to a Vietnamese resident can cross the state border, international enterprises must compile and formally submit a comprehensive Transfer Impact Assessment (TIA) dossier directly to the MPS. The state actively reviews these dossiers to evaluate local security measures, storage destinations, and third-party downstream liability. Furthermore, the law has extraterritorial reach. Any foreign entity processing data tied to a Vietnamese citizen falls squarely within the MPS's long-arm jurisdiction. This is regardless of whether they possess a physical corporate entity within Vietnam's borders.

Investors frequently misunderstand what constitutes a 'transfer.' Under Decree 356, a cross-border transfer is not limited to the physical migration of a database file to an overseas server. Simply granting remote read-only viewing access to an internal network hosted in Ho Chi Minh City to an analyst sitting at a corporate headquarters in Singapore for example, triggers the statutory definition of an outbound data transfer, invoking immediate filing obligations.

3. The Cross-Border M&A and Due Diligence

In current cross-border M&A transactions, proprietary user networks, customer databases, and integrated digital platforms represent a massive chunk of enterprise valuation.

Yet, target assets within Vietnam are frequently severely misaligned with the new statutory regime. For inbound private equity and corporate acquirers, failing to expose these liabilities during pre-deal due diligence can result in inheriting immediate exposure on day one.



To successfully evaluate a target asset under the PDPL framework, cross-border deal teams must review their diligence checklists, to look out for the following issues:

- **The Consent Audit:** The era of implied, passive, or blanket consent in Vietnam is over. Decree 356 explicitly prohibits pre-checked terms-of-service boxes, opt-out mechanisms, or multi-bundled data use clauses. Acquirers must verify that the target firm's database was built on clear, active, and fully auditable affirmative consent. If a target company cannot provide verifiable user opt-ins for every specific processing purpose, that entire database is subject to sanctions.
- **The Vendor Certification Trap:** Multinationals heavily rely on local third-party ecosystems for payroll processing, IT hosting, marketing execution, and logistics management. Under the current law, any local vendor handling employee or customer data must hold formal processing certificates issued by the MPS. Investors who acquire companies without auditing their vendor networks implicitly inherit the liability of uncertified, non-compliant third parties, opening the door to the 5% revenue penalty.
- **The 72-Hour Breach Clock:** The PDPL demands that any corporate entity detecting a security incident or data breach must report the full details to the MPS within a strict 72-hour window. Deal teams must thoroughly test whether a target company possesses the localized technical architecture and incident-response procedures required to execute this mandate. A lack of internal logging tools represents a regulatory failure.

4. HR Exemptions



While the structural demands of the PDPL are intensely rigid, Decree 356 provides a strategic operational carve-out explicitly designed to ensure corporate continuity for multinational enterprises. This carve-out addresses the constant cross-border flow of internal business operational data.

Specifically, outbound data transfers executed exclusively for the purpose of cross-border transfers of personal data for cross-border human resources management are exempt from the burdensome pre-transfer compliance submissions. This operational relief allows global parents to seamlessly sync employee profiles, performance reviews, and compensation metrics to central global servers without waiting for formal MPS approval. However, this exception is narrow and heavily conditioned.

To safely claim this exemption, the cross-border data transfer must align with valid, localized internal labour regulations, formal corporate handbooks, and registered collective labour agreements that have been legally vetted within Vietnam. If a multinational firm accidentally aggregates internal employee files for secondary commercial analytics or discloses internal directory details to an external third-party marketing vendor without separate, explicit user consent, the personnel exemption will no longer apply. The company is then automatically exposed to the full weight of the cross-border transfer violation framework.



5. Priorities for the Boardroom



To insulate cross-border operations and secure long-term valuations against Vietnam's sovereign data wall, global executive teams must transition from defensive legal posture to proactive operational due diligence. Boardrooms must immediately execute a concrete risk-mitigation strategy built on four clear pillars:

1. Appoint a Localized Data Protection Officer (DPO): Foreign firms can no longer manage compliance remotely from regional hubs. Enterprises must formally appoint an on-the-ground, localized DPO or retain licensed local legal counsel to act as the permanent, accessible interface with the MPS cybersecurity divisions.

2. Isolate and Segment Data Infrastructure: Review regional cloud systems to enforce data localization by default. Keeping core Vietnamese citizen databases physically or logically isolated within domestic borders drastically minimizes the volume of data that triggers complex, external TIA review cycles

3. Review Internal Labour Frameworks: Immediately audit and update all localized employment agreements, internal labour rules, and corporate handbooks. Formally securing the narrow personnel management exception under Decree 356 must be a priority for corporate legal teams.

4. Review Data Processing Contracts: Review all commercial joint venture, vendor, and distribution agreements to explicitly outline strict data deletion timelines, clear audit rights, and indemnity clauses if a third-party vendor triggers an official MPS investigation.



For foreign investors, data privacy in Vietnam has transcended the realm of technical IT management. It is a critical layer of regulatory risk. Those who adapt early will protect their market share or risk severe financial repercussions.

by Benjamin Yap
Senior Partner

Vietnam operates a strict, state-supervised data flow model administered directly by the MPS. ”



DATA PRIVACY IS NO LONGER AN ADMINISTRATIVE EXERCISE. IT NOW HAS IMMEDIATE FINANCIAL REPERCUSSIONS.



ANY FOREIGN ENTITY PROCESSING DATA TIED TO A VIETNAMESE CITIZEN FALLS SQUARELY WITHIN THE MPS'S LONG-ARM JURISDICTION