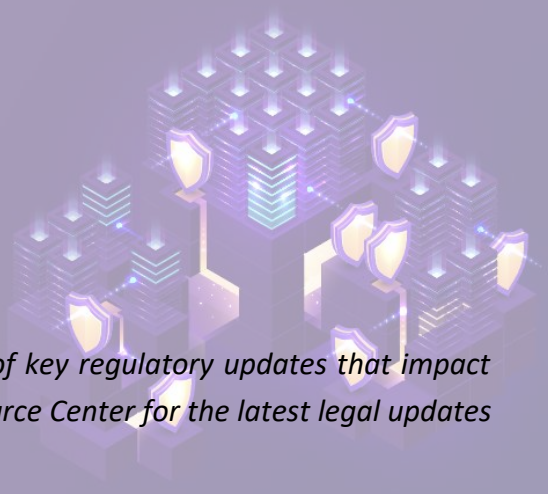
LNT & PARTNERS

LEGAL UPDATE



Our monthly publication is dedicated to provide a roundup of key regulatory updates that impact investment and business activities in Vietnam. Visit our Resource Center for the latest legal updates and firm news.

Vietnam Cybersecurity and Data Protection New Legal Framework – Key Considerations For Multinational Corporations

Nguyen Dieu Quynh – *Senior Associate*

Vo Kim Nguyen – *Trainee Associate*

1. Vietnam's Legal Framework for Cybersecurity and Data Protection

In 2025, Vietnam legislative system marks a significant step forward in strengthening its regulatory framework on cybersecurity and personal data protection. The adoption of Law on Data 2024, Law on Personal Data Protection 2025 ("**PDPL 2025**"), and Law on Cybersecurity 2025, alongside the continued developments of guiding legislations signal Vietnam's transition toward a more comprehensive and unified legal regime, reflecting a broader global trend toward tighter data governance.

In light of the forthcoming entry into force of the Law on Cybersecurity 2025 and its implementing decrees, a clear understanding of these regulatory developments will enable businesses to better navigate Vietnam's evolving legal landscape and mitigate potential legal and operational risks. In this context, entities are subject to a multi-layered compliance framework, requiring careful assessment of overlapping obligations and applicable regulatory thresholds.

2. Applicability and Regulatory Scope

Across Vietnam's data and cybersecurity legal framework, the scope of application is consistently defined in a broad and extraterritorial approach. These laws generally apply to (i) Vietnamese organizations and individuals; (ii) foreign organizations and individuals operating in Vietnam; and (iii) foreign entities that directly participate in or are involved in activities related to cybersecurity, personal data processing, or digital data in Vietnam.[1]

As a result, both domestic and foreign entities, including multinational corporations, may fall within the regulatory scope even in the absence of operating digital platforms or providing network services. This broad and unified approach underscores that regulatory exposure may arise not only from a local

[1] Article 1.2 Law on Cybersecurity 2025, Article 1.2 PDPL 2025, Article 2 Law on Data 2024.

presence in Vietnam, but also from cross-border operations, particularly where organizations process data or operate information systems involving Vietnamese users or data subjects.

3. Key Cybersecurity Compliance Obligations and Data Protection Compliance

Data Localization and Establishment of Local Presence in Vietnam

Data localization refers to the obligation of domestic enterprises and foreign enterprises providing services on telecommunications networks, the Internet, and value-added services in cyberspace in Vietnam that collect, utilize, analyze, and process personal data, data on relationships of service users, and data generated by service users in Vietnam to store such data in Vietnam.[2]

Specific data subject to storage locally in Vietnam is currently governed by Decree 53/2022/ND-CP, which shall be valid until 30 June 2026. The replacing Decree has not been officially issued yet, currently there is the Draft Decree elaborating the Law on Cybersecurity 2025, defining these types of data as follow:[3]

(i) Data on personal information of service users in Vietnam;

(ii) Data created by service users in Vietnam, including: service account names, service usage time, credit card information, email addresses, network (IP) addresses for most recent login and logout, registered phone numbers associated with accounts or data;

(iii) Data on relationships of service users in Vietnam, including friends and groups with which users connect or interact.

In addition, foreign enterprises operating in specified sectors, such as telecommunications services, data storage and sharing on the internet, e-commerce, online video games, online applications, etc., may also be required to establish a branch or representative office in Vietnam. However, this requirement is not applied universally and is triggered only where the enterprise fails to comply with cybersecurity obligations after formal requests from competent authorities.[4] These requirements may have significant operational implications for multinational corporations, particularly where global data infrastructure relies on centralized storage or cloud-based systems located outside Vietnam.

Cross-border Data Transfer Compliance

Cross-border data transfer compliance obligations are regulated by both PDPL 2025 and Law on Data 2024. While PDPL governs personal data, Law on Data 2024 applies more broadly to all digital data, including public data, enterprise data, and notably, categories of “important” and “core” data.[5]

Under PDPL 2025, entities must prepare and submit a data transfer impact assessment dossier to the competent authority within 60 days from the date of the first transfer of personal data.[6] Notably, certain exemptions apply, including transfers of employee data stored on cloud systems and cases where data subjects independently transfer their own data abroad, for which no transfer impact

[2] Article 25.3 Law on Cybersecurity 2025
[3] Article 28.1 and 28.2 Draft of Decree Elaborating the Law on Cybersecurity 2025, Version 3
[4] Article 25.3 Law on Cybersecurity 2025, Article 28 Draft of Decree Elaborating the Law on Cybersecurity 2025, Version 3
[5] Article 1.1 PDPL 2025, Article 1, Article 3 Law on Data 2024
[6] Article 20.5 PDPL 2025

assessment is required.[7] The required dossiers, forms, and procedural steps for this process are set out in Decree 356/2025/ND-CP, together with its attached Appendices.

Meanwhile, data classified as important data or core data under Law on Data 2024 is subject to a separate regulatory regime. Entities must conduct a **data transfer impact assessment,** focusing on the legality of the transfer, potential risks (such as data leakage and national security concerns), and the obligations of the data recipient when conduct cross-border transfer of such data. The dossiers, templates, as well as the sequence and procedures for this process are prescribed in Decree 165/2025/ND-CP and its accompanying Appendices. Notably, where data qualifies as both personal data and core or important data, an impact assessment under the PDPL 2025 is not required.[8]

This dual-layer regime requires multinational corporations to reassess intra-group data flows and global governance structures, particularly where regional or global systems are designed without jurisdiction-specific segmentation.

4. Enforcement Mechanisms and Sanctions for Non-Compliance

Incident Reporting and Notification

When data breaches or cybersecurity incidents occur, enterprises are required to comply with reporting and notification obligations to competent authorities. Depending on the nature and severity of the event, different obligations are applied.

For instance, for personal data breaches, personal data processors are required to notify the data controller or controller-cum-processor upon detecting a personal data breach. Where a breach poses a risk of harm to national defense, national security, public order and safety, or the life, health, honor, dignity, or property of data subjects, party aware of such violation shall issue notices to the competent authority.[9] The Law on Cybersecurity 2025 also requires information system administrators to report incidents to competent authorities within specific timelines.[10]

Data Protection Officer Assignment

For personal data protection, organizations who are data controllers, processors are required to formally designate personnel/departments ("**DPO**"), who satisfy competency conditions, to take charge of personal data protection tasks, including but not limited to receiving and reporting violations of personal data protection, organizing the implementation of emergency response plans for personal data protection incidents.[11]

While the Law on Cybersecurity 2025 does not expressly require a designated function for cybersecurity incidents, draft implementing regulations indicate that entities, particularly those operating critical national information systems, should establish specialized cybersecurity units with appropriate expertise and independence.[12] Similarly, organizations handling core or important data must ensure the existence of dedicated functions for risk monitoring, assessment, training, and incident response.[13]

---

[7] Article 20.6 PDPL 2025
[8] Article 12 of Decree 165/2025/ND-CP
[9] Article 23 PDPL 2025
[10] Article 40 Law on Cybersecurity 2025
[11] Article 13.2 Decree 356/2025/ND-CP), Article 14.1.d,e Decree 356/2025/ND-CP
[12] Article 4.2 and 4.3 of the Draft Decree elaborating Law on Cybersecurity 2025
[13] Article 13 Decree 165/2025/ND-CP

Based on these requirements, businesses should carefully consider the assignment of qualified personnel or units responsible for data protection and cybersecurity to ensure effective compliance.

Logging, Retention Requirements and Record-keeping

Certain domestic and foreign enterprises providing services on telecommunications networks, the Internet, and value-added services in cyberspace are required to retain system logs for the purpose of verification, investigation, and handling of cybersecurity violations.[14] Such logs should include key technical information (e.g. user account details, login/logout activities, IP addresses, and processing logs) and be retained for a defined period to ensure accessibility and compliance.[15]

For information systems critical to national security, additional requirements apply, including centralized logging, periodic backups, and the recording of system activities, errors, and security incidents.[16] Similarly, under Decree 165/2025/ND-CP, organizations managing core or important data must maintain logs throughout the data processing lifecycle and implement regular contingency planning and incident response drills.[17]

In addition to logging obligations, organizations are required to maintain key documentation to demonstrate compliance with data protection and cybersecurity regulations. These include impact assessment reports for personal data processing and cross-border transfers under Decree 356/2025/ND-CP[18], as well as risk assessment reports for core or important data under Decree 165/2025/ND-CP[19]. Supporting records such as core and important data processing logs, access logs of administrative personnel, incident response drill documentation, and backup and recovery logs should also be retained to facilitate inspections, audits, and investigations by competent authorities.[20]

Sanctions and Penalties for Violations

Recent enforcement practice indicates that violations are addressed in accordance with the prevailing legal framework. Administrative offences are primarily governed by Decree No. 15/2020/ND-CP, which continues to be actively enforced, while criminal conduct is subject to the Penal Code 2015. Under Decree 15/2020/ND-CP, the principal sanctions consist of warnings and fines.

The Draft Decree on administrative sanctions in the fields of cybersecurity and personal data protection based on PDPL 2025 and Law on Cybersecurity 2025 proposes a streamlined penalty framework, with fines as the primary sanction, reflecting a move toward a more stringent and deterrence-oriented enforcement regime. The Draft introduces specific penalties, including revenue-based fines of up to 5% of annual turnover for certain violations related to cross-border data transfers. Violations involving the buying or selling of personal data may be fined up to 10 times the illegal gains derived from such conduct.[21]

---

[14] Article 25.2.b Law on Cybersecurity 2025
[15] Article 25.6.b,c Draft Decree elaborating Law on Cybersecurity 2025
[16] Section 4.dd Annex 2, Article 33.2 Draft Decree elaborating Law on Cybersecurity 2025
[17] Article 19.8 Decree 165/2025/ND-CP
[18] Article 18, 19 Decree 365/2025/ND-CP
[19] Article 17 Decree 165/2025/ND-CP
[20] Article 17, 19 Decree 165/2025/ND-CP; Article 31, 33, Section 4.b and Section 4.dd Annex 2 Draft Decree elaborating Law on Cybersecurity 2025
[21] Article 6, Draft of Decree on administrative sanctions in the fields of cybersecurity and personal data protection based on PDPL 2025 and Law on Cybersecurity 2025

For multinational corporations, revenue-based penalties may significantly increase financial exposure, particularly in the context of large-scale cross-border data operations. Accordingly, close attention to compliance obligations is essential to mitigate potential legal and financial risks.

5. Key Takeaways for Multinational Corporations

To ensure compliance pending the issuance of implementing regulations, multinational corporations should prioritize controls that are clearly required under primary laws and unlikely to materially change, with a particular focus on cross-border data flows, intra-group data transfers, and the localization of global data governance frameworks, especially in areas of immediate legal exposure.

(i) **Data governance and classification**

Identify and classify data based on general criteria, including classification by data type (e.g., personal data, particularly sensitive personal data such as health data) and by regulatory significance (e.g., potential core and important data).

(ii) **Cross-border data transfer compliance**

- Prepare personal data transfer impact assessment dossiers.
- Identify whether any data could fall under core/important data regime (triggering stricter requirements).
- Align intra-group agreements with Vietnam law requirements.

(iii) **Legal basis and consent framework**

- Ensure valid consent mechanisms, especially for sensitive personal data (health, pharmacovigilance).
- Review and update privacy notices and internal policies.

(iv) **Incident detection and reporting readiness:** Establish internal procedures, define escalation thresholds and decision-making authority.

(v) **Logging, monitoring, and evidence retention:** Implement logging systems capable of tracking user access and system activity, retaining logs, ensure audit trails are inspection-ready.

(vi) **Internal governance and roles:** Appoint data protection personnel (DPO or equivalent) and define clear responsibilities between IT, Legal, and Compliance.

At the same time, businesses should take into account key regulatory developments, particularly the expansion of prohibited acts in cyberspace to address emerging technological risks. Notably, the explicit prohibition on the use of artificial intelligence to fabricate or impersonate individuals. The framework also strengthens safeguards against online harm, including enhanced protections for children, and broadens the scope of prohibited content to encompass misinformation and false representations. Against this backdrop, businesses should anticipate increased regulatory scrutiny in the near term.

As Vietnam's regulatory framework continues to mature, proactive and well-structured compliance will become a key differentiator for businesses operating in the market. In practice, multinational corporations should consider whether their global data governance models require adjustments to align with Vietnam's evolving regulatory expectations. Such engagement not only helps enterprises stay informed of regulatory trends but also provides opportunities to contribute to policy discussions and ensure that practical business perspectives are considered in the development of new legal instruments.

***Disclaimer**: This Legal Update is intended to provide updates on the Laws for information purposes only, and should not be used or interpreted as our advice for business purposes. LNT & Partners shall not be liable for any use or application of the information for any business purpose. For further clarification or advice from the Legal Update, please consult our lawyer: **Ms. Nguyen Dieu Quynh** at dieuquynh.nguyen@LNTpartners.com.*

CONTACT US

For more information about any of these legal briefs, please contact our Partners:

Mr. Hong Bui

Corporate/M&A, Foreign Investment, Compliance & ABAC, Employment, Litigation & ADR

Hong.Bui@LNTpartners.com

Mr. Binh Tran

Corporate Governance, Employment, Foreign Investment, Litigation & ADR, Real Estate, Corporate/M&A, Tax

Binh.Tran@LNTpartners.com

Ms. Quyen Hoang

Corporate/M&A, Compliance & ABAC, Employment, Insolvency & Restructuring

Quyen.Hoang@LNTpartners.com

Dr. Net Le

Banking & Finance, Real Estate, Litigation & ADR, Corporate/M&A, Tax

Net.Le@LNTpartners.com

Dr. Tuan Nguyen

Antitrust/Competition, Corporate/M&A, Employment, Compliance & ABAC, Foreign Investment

Tuan.Nguyen@LNTpartners.com

Mr. Thuy Nguyen

Corporate/M&A, Foreign Investment, Employment, Tax

Thuy.Nguyen@LNTpartners.com

Ms. Minh Vu

Tax, Foreign Investment, Banking & Finance, Corporate Governance, Corporate/M&A, Projects

Minh.Vu@LNTpartners.com

Mr. Phu Nguyen

Litigation & ADR

Phu.Nguyen@LNTpartners.com

Ms. Nhi Luong

Litigation & ADR, Employment

VanNhi.Luong@LNTpartners.com

Ms. Diep Nguyen

Litigation & ADR, Banking & Finance, Employment, Tax, Intellectual Property, Compliance & ABAC

Diep.Nguyen@LNTpartners.com

Mr. Hai Ngo

Banking & Finance, Corporate Governance, Litigation & ADR, Real Estate

Hai.Ngo@LNTpartners.com

Ms. Thinh Vu

Foreign Investment, M&A, Compliance & ABAC, Litigation & ADR, Infrastructure, Energy & Natural Resources

ThiThinh.Vu@LNTpartners.com

For further information, please contact us:

Ho Chi Minh City (HQ)

Level 12A, Saigon Marina IFC, No.2 Ton Duc Thang St., Saigon Ward

+84 28 3821 2357

Hanoi

Level 12, Pacific Place Building
83B Ly Thuong Kiet St., Cua Nam Ward

+84 24 3824 8522

About us

LNT & PARTNERS ("LNT") is a full-service independent Vietnam law firm, which focuses on advisory and transactional work in the areas of corporate and M&A, competition, pharmaceutical, real estate, infrastructure and finance as well as complex and high-profile litigation and arbitration matters. The firm is among Vietnam's most prominent, representing a wide range of multinational and domestic clients, including Fortune Global 500 companies as well as well-known Vietnamese listed companies.

For more information about any of these legal briefs, please contact the individual authors or your usual LNT contact.