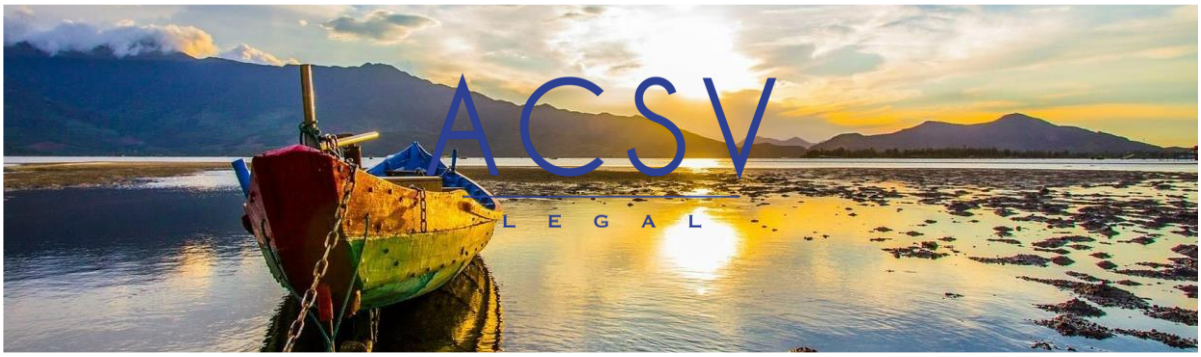


LEGAL UPDATE

2025 LAW ON CYBERSECURITY: UNIFIED STATE MANAGEMENT AND NEW COMPLIANCE OBLIGATIONS

1. Introduction

On 10 December 2025, the National Assembly officially passed the Law on Cybersecurity No. 116/2025/QH15 ("**2025 Law on Cybersecurity**"). This legislation represents a significant restructuring of Vietnam's cyber legal framework and is scheduled to take effect on 1 July 2026.[1]

Upon its entry into force, the 2025 Law on Cybersecurity will replace both the Law on Network Information Security No. 86/2015/QH13 ("**2015 Law on Network Information Security**") and the Law on Cybersecurity No. 24/2018/QH14 ("**2018 Law on Cybersecurity"**), consolidating Vietnam's cybersecurity framework into a single statute. This reform shifts the regulatory approach from a dual technical-security model to a unified, security-centric regime under centralised government management.

This legal update highlights the key changes introduced by the 2025 Law on Cybersecurity, with particular focus on enhanced operational obligations for service providers, strengthened data localisation requirements, and a streamlined licensing framework.

2. Timelines for Content Management and Information Provision

One of the notable changes introduced by the 2025 Law on Cybersecurity is the establishment of fixed statutory deadlines for information processing and content control. Under the 2018 Law on Cybersecurity and its guiding regulations, compliance obligations were largely expressed through qualitative standards such as "timely" or "immediate," allowing a degree of interpretative discretion. The 2025 Law on Cybersecurity removes this flexibility by embedding concrete time limits directly into the primary legislation.

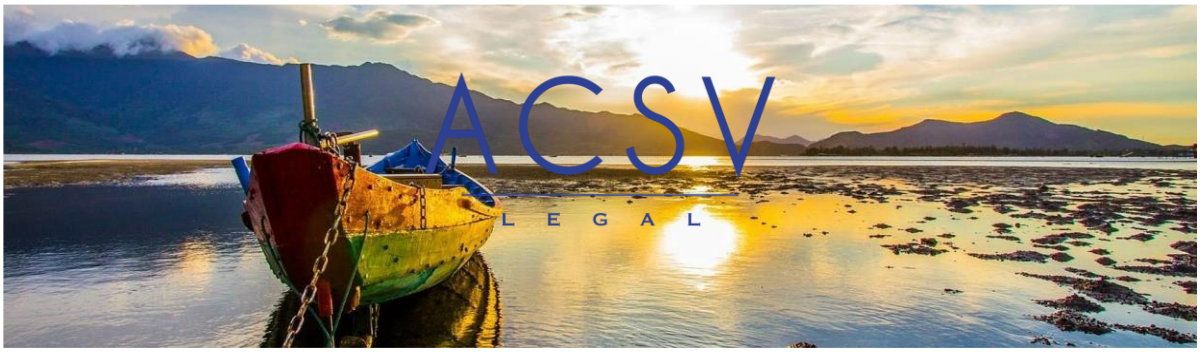
Enterprises providing services on telecommunications networks, the Internet, and in cyberspace are now subject to these deadlines. Upon receiving a request from the Ministry of Public Security ("**MPS**"), service providers are required to verify and provide user information within 24 hours in ordinary circumstances, or within three (3) hours in emergency cases involving national security or threats to human life.[2]

Similar fixed timelines apply to content moderation obligations. Service providers must block access to or remove unlawful content within 24 hours of receiving a request, or within six (6) hours in emergency situations.[3]

The 2025 Law on Cybersecurity also introduces a more technically precise data retention requirement by expressly mandating the storage of users' IP addresses.[4] This represents a shift from the broader data retention obligations under the 2018 Law on Cybersecurity framework and provides clearer guidance on traceability and attribution standards.[5]

In practice, these obligations apply to a wide range of entities, including domestic and foreign cross-border platforms, social media and OTT service providers, Internet service providers, and data centre operators. Compliance with the shortened emergency response timelines may require enterprises to implement round-the-clock response mechanisms or automated processing systems, as

[1] Article 44.1 of the 2025 Law on Cybersecurity
[2] Article 25.2(a) of the 2025 Law on Cybersecurity
[3] Article 25.2(b) of the 2025 Law on Cybersecurity
[4] Article 25.2(d) of the 2025 Law on Cybersecurity
[5] Article 26.3 of the 2018 Law on Cybersecurity



reliance on standard business-hour operations is unlikely to be sufficient.

3. Data Localisation and Commercial Presence Requirements

The 2025 Law on Cybersecurity formally incorporates data localisation and local presence obligations into the statutory framework, rather than leaving them to subordinate regulations as under the previous regime. Under the new regulations, foreign enterprises providing telecommunications, Internet, or value-added services in Vietnam that engage in the collection, analysis, or processing of personal data or data relating to users' relationships are required to store such data within Vietnam. At the same time, these enterprises must establish a commercial presence in Vietnam through a branch or a representative office.[6]

In addition, the 2025 Law on Cybersecurity introduces a regulatory requirement governing cross-border data transfers. Specifically, cross-border transfers involving critical information systems related to national security, as well as data centres and databases[7], are subject to inspection and assessment by competent state authorities. This mechanism establishes a legal basis for state supervision of outbound data flows and operates separately from the data transfer impact assessments required under personal data protection regulations.

4. Consolidated Licensing Regime for Cybersecurity Products and Services

The 2025 Law on Cybersecurity restructures market entry conditions in the cybersecurity sector by consolidating the existing licensing framework.

Under the 2018 Law on Cybersecurity, licensing was divided between different authorities. Licences for network information security products and services were issued by the Ministry of Information and Communications[8], while licences for civil cryptography products and services were administered by the Government Cipher Committee. This dual-track system resulted in fragmented regulatory oversight.[9] The 2025 Law on Cybersecurity replaces this structure with a single licence for trading in cybersecurity products and services[10], administered under a unified regulatory framework. The consolidation is intended to enhance consistency and clarity in market access requirements.

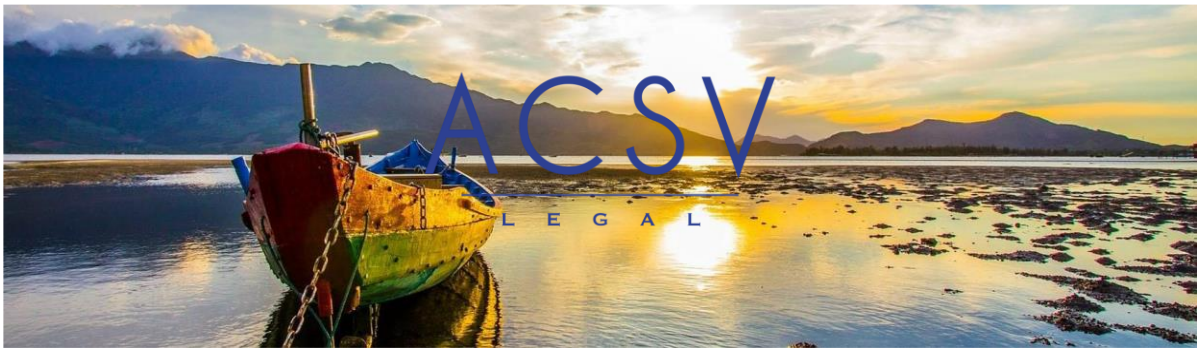
To preserve business continuity, the 2025 Law on Cybersecurity includes transitional provisions. Licences issued before 1 July 2026 for network information security products and services or civil cryptography products and services will remain valid until their stated expiry dates, and enterprises are not required to reapply upon the 2025 Law on Cybersecurity's effective date.[11]

From a transactional perspective, this transitional arrangement is particularly relevant for M&A activities involving technology companies. Investors should carefully assess the remaining validity of existing licences, as those expiring during the transition period may be subject to processing delays while the new licensing regime under the MPS is being implemented.

5. System Classification and Unified State Management

The 2025 Law on Cybersecurity retains the five-level classification framework for information systems based on their potential impact on national security, social order, and the lawful rights and interests of organisations and individuals[12]. This classification structure is carried forward from the 2015 Law on

[6] Article 25.3 of the 2025 Law on Cybersecurity
[7] Article 26.2(e) of the 2025 Law on Cybersecurity
[8] Articles 40 and 41 of the 2015 Law on Network Information Security
[9] Articles 31 and 32 of the 2015 Law on Network Information Security
[10] Article 29 of the 2025 Law on Cybersecurity
[11] Article 45.2 of the 2025 Law on Cybersecurity
[12] Article 8 of the 2025 Law on Cybersecurity



Network Information Security [13], but the governance model has been fundamentally restructured.

Under the new Law, cybersecurity is subject to unified state management by the Government, with the MPS designated as the central authority assisting in implementation.[14] This replaces the previous dual-management model, under which responsibilities were divided between the Ministry of Information and Communications for technical and civil matters and the MPS for security and content-related matters. As a result, future compliance obligations, including system classification, appraisal, and licensing, are expected to be applied through a more security-oriented regulatory lens.

For transitional purposes, information systems that have already been classified under the prior regulatory framework will retain their assigned classification levels. However, system owners are required to upgrade and supplement their technical and organisational protection measures to align with the standards introduced by the 2025 Law on Cybersecurity. A grace period of 12 months from the 2025 Law on Cybersecurity's effective date is provided for this purpose, ending on 1 July 2027.[15]

6. Conclusion

The 2025 Law on Cybersecurity marks a shift towards a unified governance framework for Vietnam's digital space. Through centralised state management under the MPS, together with the codification of fixed response timelines and data localisation requirements, the Law strengthens the State's capacity to prevent and respond to cyber risks.

For enterprises, particularly cross-border service providers and technology firms, the Law necessitates a review of compliance strategies. Actions should include assessing the readiness of 24/7 response protocols, preparing for mandatory local presence, and budgeting for system upgrades ahead of the July 2027 transitional deadline.

For more information, please contact our lawyers:

Nguyet Le / Special Counsel
nguyet.le@acsvlegal.com

Kim Nguyen / Associate
kim.nguyen@acsvlegal.com

[13] Article 21 of the 2015 Law on Network Information Security
[14] Article 39.2 of the 2025 Law on Cybersecurity
[15] Article 45.1 of the 2025 Law on Cybersecurity