



Shape the future
with confidence

Legal Alert

September 2026

Visit other Alerts [here](#).

Decree No. 333/2026/ND-CP providing detailed guidance on a number of articles of the Law on Cybersecurity

This Alert highlights key compliance requirements set forth in the Decree No. 333/2026/ND-CP dated 19 August 2026 provides detailed guidance on a number of articles of the Law on Cybersecurity (Decree 333).

Decree 333 retains a substantial part of the data-localization and cybersecurity-protection framework previously established under Decree No. 53/2022/ND-CP dated 15 August 2022 (Decree 53), while introducing several important refinements, including changes to the scope of regulated data, additional operational and compliance requirements, and greater clarity regarding the circumstances in which offshore enterprises may become subject to data localization and local commercial presence obligations.

Key highlights in Decree 333 include:

- Data subject to localization requirements
- Data localization and local commercial presence requirements
- Application of cybersecurity protection measures
- IP address identification and management
- Key changes from Decree 53 to Decree 333
- Business implications

1. Data subject to localization requirements

Types of data subject to localization (collectively, “regulated data”) includes:

- Personal information of service users in Vietnam
- Data generated by service users in Vietnam, including the account name used for the service, duration of service use, credit-card information, email address, IP addresses for the most recent login and logout, and the registered telephone number associated with the account or data¹

Unlike Decree 53, Decree 333 no longer lists “data on the relationships of service users in Vietnam” as a category of regulated data.²

2. Data localization and local commercial presence requirements

2.1. Companies subject to data localization and local commercial presence requirements

Under Article 25.3 of the 2025 Law on Cybersecurity, the data localization requirement may apply on an extra-territorial basis. Accordingly, not only onshore enterprises but also offshore enterprises (established or registered under foreign laws) providing services on telecommunications networks, the internet and value-added services in cyberspace in Vietnam that collect, exploit, analyze or process regulated data are required to store such data in Vietnam. Decree 333 continues to distinguish the obligations applicable to onshore and offshore enterprises and provides updated conditions for data localization and local commercial presence, as discussed in Sections 2.1.1 and 2.1.2 below.

2.1.2 Onshore enterprises

Decree 333 does not give more detailed guidance on the data localization requirements applicable to onshore enterprises as opposed to Article 25.3 of the 2025 Law on Cybersecurity. It just provides in general that onshore enterprises must store the regulated data in Vietnam.³ As such, Article 19.2 of Decree 333, when read in conjunction with Article 25.3 of the 2025 Law on Cybersecurity, may be interpreted as requiring any onshore enterprise meeting both conditions (a) and (b) below to comply with the data-localization requirement:

(a) Conducting one (1) of the following three (3) service groups in Vietnam:

- Services on telecommunications networks: telecommunications services and telecommunications application services
- Services on internet network: internet services and mobile telecommunications content information services
- Value-added services in cyberspace

(b) Having activities of collecting, analyzing, processing regulated data

2.1.3 Offshore enterprises

The data localization requirement applies more narrowly to offshore enterprises. In contrast to onshore enterprises, offshore enterprises are subject to the requirement only when a number of additional conditions are satisfied, including operating in a covered service sector, involvement

¹ Article 19.1.a-b of Decree 333.

² Article 3.11 and Article 25.1 of Decree 333.

³ Article 19.2 of Decree 333.

in a cybersecurity violation, receipt of three written requests from the competent authority within six months, and failure to take the required remedial measures.

In particular, an offshore enterprise is only required to store regulated data and to set up a representative office or a branch in Vietnam when **all of the following conditions** are met:⁴

- (a) It provides one or more of the following services in Vietnam: (i) telecommunications services; (ii) data storage and sharing services in cyberspace; (iii) services for registration and maintenance of domain names for service users in Vietnam; (iv) e-commerce; (v) **online payment**;⁵ (vi) intermediary payment services; (vii) transport-connectivity services in cyberspace; (viii) social networks and social media; (ix) online electronic games; (x) online applications; or (xi) other services providing, managing or operating information in cyberspace in the form of messages, voice calls, video calls, email or online chat.
- (b) Its services have been used to commit a violation of Vietnamese cybersecurity laws; the specialized cybersecurity authority under the Ministry of Public Security has notified the enterprise and issued three written requests, within a period not exceeding six months, requiring it to coordinate in preventing, investigating and handling the violation **three times within six months**⁶; and the enterprise has failed to implement a remedial solution, has failed to comply or has incompletely complied with the requested scope or matters, or has prevented, obstructed, disabled or neutralized cybersecurity protection measures.
- (c) The Minister of Public Security has issued a written decision requiring the offshore enterprise to store the regulated data in Vietnam and establish a branch or representative office in Vietnam (the "Decision").

Compared with Decree 53, Decree 333 makes targeted refinements to the offshore-enterprise regime, most notably by adding online applications to the list of covered services and introducing a clearer "three written requests within six months" enforcement threshold before data localization and local presence requirements may be imposed.

Where, due to a force majeure event, a foreign enterprise is unable to comply with the requirements of Vietnamese cybersecurity laws, it must notify the specialised cybersecurity authority under the Ministry of Public Security within three working days so that the authority may verify the existence of the force majeure event. In such case, the enterprise shall have 25 working days to identify and implement a remedial solution, reduced from 30 working days under Decree 53.⁷

Of note, the offshore enterprises subject to data localization requirement, have 12 months as of the Decision's issuance date, to complete the storage of data and establishment of a representative office or a branch in Vietnam.⁸

2.2. Form and duration of data storage and local commercial presence in Vietnam

⁴ Article 19.3(a) and Article 19.6 of Decree 333.

⁵ While the list of covered services remains largely unchanged, Decree 333 expressly adds online applications as a separate category of service subject to the data localization and local commercial presence framework.

⁶ The "three times within six months" threshold under Decree 333 appears to have been introduced to provide greater clarity compared with the previous framework under Decree 53. In particular, Decree 333 clarifies that the threshold refers to three written requests issued by the specialised cybersecurity authority within a period not exceeding six months, requiring the offshore enterprise to coordinate in preventing, investigating and handling cybersecurity violations.

⁷ Article 19.3(a) of Decree 333.

⁸ Article 19.6(c) of Decree 333.

- **Form of data storage:**

Similar to Decree 53, Decree 333 allows enterprises to determine the form of data storage in Vietnam. However, Decree 333 introduces an additional requirement that the selected storage arrangement must ensure the prompt retrieval and provision of data upon request by a competent authority, as well as compliance with applicable national information security standards and technical regulations.⁹

- **Duration of data storage:**

The 24-month retention period should be understood as applying only to offshore enterprises upon receipt of the Decision.¹⁰ Notably, Decree 333 does not further clarify the scope or duration of the data localization obligation applicable to onshore enterprises. Accordingly, a number of practical implementation questions under the previous framework remain unresolved.

- **Duration for having a commercial presence in Vietnam:**

The period for maintaining a branch or representative office in Vietnam begins when the offshore enterprise receives the Decision and continues until it ceases operating in Vietnam or no longer provides the relevant regulated service in Vietnam.¹¹

- **System log:**

System logs to serve the investigation and handling of violations of the 2025 Law on Cybersecurity must be stored for at least 12 months.¹²

2.3. Other relevant data-localization obligations¹³

- **Cooperation with the specialized cybersecurity protection force under the Ministry of Public Security:**

Where an enterprise has not fully localized the regulated data that it collects, uses, analyses or processes, it must cooperate with the specialized cybersecurity protection force under the Ministry of Public Security to verify compliance and complete the localization of such data.¹⁴

- **Supplementing the data storage:**

If an enterprise subsequently collects, uses, analyses or processes additional categories of regulated data, it must coordinate with the specialized cybersecurity protection force under the Ministry of Public Security to update the list of data subject to localization in Vietnam. Notably, Decree 333 introduces a new transparency-related obligation requiring enterprises to publicly notify service users whenever additional categories of regulated data become subject to localization. This requirement was not expressly contemplated under Decree 53.¹⁵

3. Application of cybersecurity protection measures

3.1. Removal of unlawful information, false information and fake news in cyberspace

Decree 333 permits a competent cybersecurity authority to require an agency, organization or individual to remove unlawful information, false information or fake news in cyberspace where

⁹ Article 19.5 of Decree 333.

¹⁰ Article 20.1 of Decree 333.

¹¹ Article 20.2 of Decree 333.

¹² Article 20.3 of Decree 333.

¹³ Article 19.4 of Decree 333.

¹⁴ Article 19.4(a) of Decree 333.

¹⁵ Article 19.4(b) of Decree 333.

such information infringes national security, social order and safety, or the lawful rights and interests of an agency, organization or individual, including information that:¹⁶

- Infringes national security, propagates against the State of the Socialist Republic of Vietnam, incites violence, disrupts security or causes public disorder
- Is humiliating or slanderous, infringes the economic-management order, or fabricates or distorts the truth and causes public confusion or serious damage to socio-economic activities
- Is otherwise expressly identified in the removal request as information falling within the prohibited acts in cyberspace

The competent cybersecurity authority may issue a written removal request to the relevant agency, organization, individual or enterprise providing services on telecommunications networks, the internet or value-added services in cyberspace. The recipient must remove the identified information within the period specified in the request and report the implementation result to the requesting authority.¹⁷

Decree 333 expressly expands the measure beyond unlawful or false information to include “fake news” and links the removal mechanism to infringements of the lawful rights and interests of agencies, organizations and individuals, in addition to national security and social order and safety.¹⁸

3.2. Collection of electronic data relating to unlawful activities in cyberspace

The collection of electronic data for the purpose of investigating and handling activities in cyberspace that infringe national security, social order and safety, or the lawful rights and interests of agencies, organizations and individuals must comply with the following principles and requirements:¹⁹

- Electronic data must not be interfered with or altered.
- The collection of electronic data must be approved by the competent authority and carried out in accordance with the prescribed procedures, using recognized and verifiable equipment and software that ensure the integrity of electronic data stored in electronic devices.
- The person collecting electronic data must possess appropriate professional competence and be assigned by the competent authority to perform the collection in accordance with law.
- The collection process must be documented in minutes and images and, where necessary, must be capable of being repeated to produce similar results. Where necessary, an independent third party may be invited to witness and confirm the collection process.

Decree 333 expressly requires approval by the competent authority, use of recognized and verifiable collection tools, assignment of personnel with appropriate professional competence, and documentation by minutes and images. It also expressly allows an independent third party to witness and confirm the collection process where necessary.²⁰

3.3. Suspension, temporary suspension or required cessation of an information system's operation, and revocation of a domain name

¹⁶ Article 11.1 of Decree 333.

¹⁷ Article 11.2 of Decree 333.

¹⁸ Article 11 of Decree 333.

¹⁹ Article 12 of Decree 333.

²⁰ Article 13 of Decree 333.

Upon a decision issued directly by the Minister of Public Security, an information system may be suspended or temporarily suspended or required to cease operation, and a domain name may be temporarily suspended or revoked, in either of the following circumstances:²¹

- There is evidence proving that the operation of the information system violates laws on national security or cybersecurity.

Or

- The information system is being used to infringe upon national security, social order or public safety.

The specialized cybersecurity force under the Ministry of Public Security implements the decision. In an urgent case requiring timely prevention of harm to national security or prevention of likely consequences, the Ministry of Public Security may communicate the request directly or by fax or email and must send the written request within 24 hours. If that written request is not sent within the prescribed period, the information system may resume operation.²²

Decree 333 expressly stipulates suspension, temporary suspension and required cessation of operation and expressly includes revocation of the internet domain name. It also formalizes the urgent procedure: an immediate request may be communicated directly or by fax or email, but a written decision must follow within 24 hours; otherwise, the information system may resume operation.²³

4. IP address identification and management

Decree 333 introduces specific obligations for telecommunications and internet service providers regarding the technical identification of IP addresses and the provision of IP-address identification information to the specialized cybersecurity force under the Ministry of Public Security. IP-address identification must ensure accuracy, integrity and unique traceability and must be maintained continuously throughout allocation, use and withdrawal.²⁴

4.1. Technical requirements for IP-address identification

When allocating an IP address to an organization or individual, apply technical measures to accurately identify the subscriber information associated with that IP address at the time of allocation.²⁵

Synchronize the logs of the IP-address allocation and management system with Vietnam's national time standard. At a minimum, the logs must contain the following information:²⁶

- Source IP address, source port, destination IP address, destination port and connection protocol
- Where network address translation is used, complete IP-address mapping information
- The start and end times of each connection session, synchronized with Vietnam's national time standard
- the identifier of the public IP-allocation gateway (gateway ID) and the connection-session identifier (session ID)

²¹ Article 13.1 and Article 13.2 of Decree 333.

²² Article 13.3 and Article 13.4 of Decree 333.

²³ Article 13 of Decree 333.

²⁴ Article 21 of Decree 333.

²⁵ Article 22.1 of Decree 333.

²⁶ Article 22.2 of Decree 333.

- The subscriber information and user-account information associated with the IP address at the relevant time

Retain the system-log data referred to above fully and continuously for at least 12 months.²⁷

Ensure that the log-storage system preserves the integrity, safety and confidentiality of the data; prevents unauthorized modification or deletion; and enables the real-time extraction and provision of the data to the specialized cybersecurity force for the implementation of cybersecurity protection measures.²⁸

4.2. Coordination with and provision of IP-address identification information to the specialized cybersecurity authority

Telecommunications and internet service providers must establish and maintain an appropriate technical mechanism capable of connecting with the technical system of the specialized cybersecurity force under the Ministry of Public Security and providing information necessary for IP-address identification in accordance with law.²⁹

A specific request for IP-address identification information must be based on a lawful written request or a valid electronic request issued by the specialized cybersecurity force for the purpose of implementing cybersecurity protection measures or preventing, detecting, investigating or handling a violation of cybersecurity laws.³⁰

Upon receiving such a request, the relevant telecommunications or internet service provider must provide complete and accurate IP-address identification information for the relevant time. The information must include, as applicable: the individual's full name; organizational information; personal identification number; subscriber name or subscriber code; the registered installation address of the internet connection for a fixed broadband network; and the registered telephone number for a mobile telecommunications network.³¹

The provider must supply the requested information no later than 24 hours after receipt of the request. In an urgent case relating to national security, prevention and combat of cyberterrorism, a cyberattack or an especially serious crime, the information must be provided within three hours.³²

IP-address identification information must not be used, disclosed or exploited for commercial purposes, unless otherwise provided by law.³³

5. Key changes from Decree 53 to Decree 333

Matter	Decree 53	Decree 333
Regulated data	Includes user relationship data	User relationship data removed

²⁷ Article 22.3 of Decree 333.

²⁸ Article 22.4 of Decree 333.

²⁹ Article 23.1 of Decree 333.

³⁰ Article 23.2(a) of Decree 333.

³¹ Article 23.2(b) of Decree 333.

³² Article 23.2(c) of Decree 333.

³³ Article 23.3 of Decree 333.

Covered services (onshore enterprises)	Refers to over-the-top content services on the internet , without further statutory definition or detailed guidance	Replaces the former concept with mobile telecommunications content information services , which is now specifically defined by reference to content services provided through mobile telecommunications networks
Covered services (offshore enterprises)	No specific reference to online applications	Online applications added
Enforcement trigger (offshore enterprises)	Written requests from cybersecurity authority	Three written requests within six months
Data retrieval requirement	Not expressly required	Prompt retrieval and provision to authorities
Public notification	No express obligation	Public notification to users required
Force majeure remedy period (offshore enterprises)	30 working days	25 working days

6. Business implications

- **Potential optimization of storage infrastructure and compliance costs:** The removal of user relationship data from the definition of regulated data may allow some businesses to simplify their localization architecture and reduce storage, maintenance and compliance costs.
- **Need to reassess service classification:** Businesses should revisit how their services are categorized under the revised framework, particularly in relation to mobile telecommunications content information services (for onshore enterprises) and online applications (for offshore enterprises).
- **Higher operational readiness requirements:** Although enterprises remain free to determine the form of data storage in Vietnam, they must now ensure that localized data can be promptly retrieved and provided to competent authorities upon request and that storage arrangements comply with applicable information security standards and technical regulations.
- **Additional compliance and governance obligations:** Enterprises should establish processes to monitor newly collected categories of regulated data and comply with the new requirement to publicly notify service users whenever additional categories of data become subject to localization requirements.
- **Greater certainty for offshore enterprises:** The introduction of the "three written requests within six months" threshold provides a clearer enforcement trigger for the imposition of

data localization and local commercial presence requirements, reducing uncertainty under the previous framework.

- **Heightened enforcement risks for non-compliance under Decree No. 330/2026/ND-CP dated 19 August 2026:** Enterprises failing to comply with the data localization and local commercial presence requirements may be subject to administrative fines ranging from VND60 million to VND100 million. In addition, the competent authorities may require non-compliant enterprises to store regulated data in Vietnam and establish a branch or representative office in Vietnam in accordance with the cybersecurity regulations. More significantly, for serious violations, authorities may order telecommunications and internet service providers to suspend the provision of telecommunications or internet services, or disconnect telecommunications and internet connectivity in Vietnam, effectively preventing the enterprise from continuing to provide services to users in the Vietnamese market. These enforcement measures highlight the importance of reassessing compliance frameworks and addressing any gaps in data storage and local presence arrangements at an early stage.

Please note that the application of the data localization framework to specific business models remains fact-dependent and should be assessed on a case-by-case basis, particularly for digital services that may fall within the evolving definitions under the cybersecurity and telecommunications regulations.



Shape the future
with confidence

Contacts

Ho Chi Minh City Office



Robert King | EY Vietnam, Laos, Cambodia Tax Leader
EY Consulting Vietnam Joint Stock Company
robert.m.king@vn.ey.com



Hieu Duy Nguyen | Managing Director
EY Law Vietnam Limited Liability Company
hieu.d.nguyen@vn.ey.com



Robert Tran | Partner
EY Digital & Cyber Company Limited
robert.tran@vn.ey.com



Thach Thi Cam Tran | Director
EY Law Vietnam Limited Liability Company
thach.cam.tran@vn.ey.com

Hanoi Office



Anh Thuy Pham | Associate Partner
EY Law Vietnam Limited Liability Company
anh.thuy.pham1@vn.ey.com



Linh Hoang Anh Nguyen | Director
EY Law Vietnam Limited Liability Company
linh.hoang.anh.nguyen@vn.ey.com

Japanese Business Services (JBS)



Takahisa Onose | EY Vietnam, Laos, Cambodia JBS Leader
Ernst & Young Vietnam Limited
takahisa.onose@vn.ey.com



Takaaki Nishikawa | Associate Partner
Ernst & Young Vietnam Limited
takaaki.nishikawa@parthenon.ey.com



Yuka Otomi | Associate Director
Ernst & Young Vietnam Limited
yuka.otomi@vn.ey.com

Korean Business Services (KBS)



Binh Thanh Phan | EY Vietnam, Laos, Cambodia KBS Leader
EY Consulting Vietnam Joint Stock Company
binh.thanh.phan@parthenonvnpnparthenon.ey.com



Kyung Hoon Han | Associate Partner
Ernst & Young Vietnam Limited
kyung.hoon.han@vn.ey.com

Chinese Business Services (CBS)



Truong Duc Le | EY Vietnam, Laos, Cambodia CBS Leader
Ernst & Young Vietnam Limited
truong.duc.le@vn.ey.com



Owen Tsao | Director
Ernst & Young Vietnam Limited
owen.tsao@vn.ey.com



Trinh Kiet Luong | Assistant Director
Ernst & Young Vietnam Limited
trinh.kiet.luong@vn.ey.com

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

©2026 EY Law Vietnam Limited Liability Company. All Rights Reserved.

APAC No. 16160901

ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com/en_vn