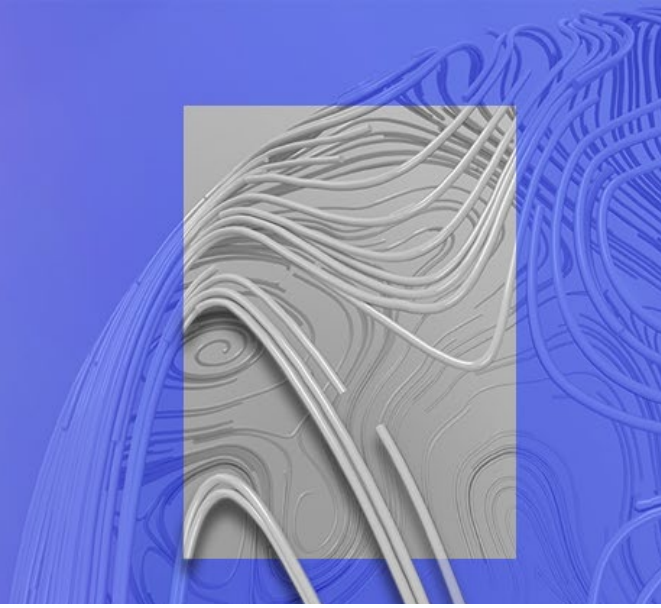
KPMG

Legal Alert

September 2022



Decree No. 53/2022/ND-CP guiding the Law on Cybersecurity 2018

On 15 August 2022, the Government of Vietnam issued Decree No. 53/2022/ND-CP guiding the Law on Cybersecurity 2018 ("**Decree 53**"), which will take effect **from 01 October 2022**. Decree 53 has a wide governing scope which impacts **both local and foreign entities**, especially it devotes a chapter providing guidelines on the data localization requirements as stipulated by Article 26 of the Law on Cybersecurity 2018.

Below are the key highlights of Decree 53:

1. Type of data which must be stored in Vietnam ("Compulsory Stored Data"):

The type of data subject to local storage include:

(i) **personal data of service users in Vietnam** (i.e., organizations and individuals using services in cyberspace in the territory of Vietnam);

(ii) **data generated by service users in Vietnam** (i.e., account name, service using time, credit card information, email address, IP address used for logging in and logging out, phone number registered with the account or data); and

(iii) **data on the relationship of service users in Vietnam** (i.e., friends, groups with which the user connects or interacts with).

The method of storing Compulsory Stored Data and format thereof is to be decided by the concerned entities.

2. Data storage requirement for entities incorporated in Vietnam:

The storage requirement of Compulsory Stored Data applies to all Vietnamese entities which are established under Vietnamese laws, including foreign-invested enterprises, and providing (i) services on telecommunication networks (including telecommunication services and telecommunication-based application services), (ii) service on the internet (including internet services and content distribution services on the internet) and (iii) value-added services in Vietnam's cyberspace that collect, exploit, analyze or process personal data or data about relationships of their service users or data created by their service users in Vietnam. The above categories of services are quite broad, and it remains to be seen how State management authorities will define their scope in practice.

3. Data storage and local office requirements for foreign entities:

Foreign entities having business activities in Vietnam and being involved in:

(i) telecommunication, storing and sharing data in cyberspace,

(ii) providing national or international domain names to service users in Vietnam,

(iii) e-commerce, online payment, payment intermediary, transport connection services through cyberspace, social networks and social media, online video games;

(iv) providing, managing or operating information in cyberspace in the form of messages, voice calls, video calls, e-mails, online chats.

(collectively "**Online Services**") are required to store Compulsory Stored Data in Vietnam and to establish a local office (i.e. a branch or representative office) in Vietnam if:

(i) their services have been misused [by service users] for committing violations of Vietnam's cybersecurity regulations; **and**

(ii) they are notified and requested by the Department of Cybersecurity and High-Tech Crime Prevention and Control (under the Ministry of Public Security) for coordination in investigation and prevention of the violations, **but**

(iii) they fail to comply with such request **or** they prevent/obstruct/disable the network security protection measures implemented by the cybersecurity protection taskforce.

In such instance, the foreign entity must complete the data storage exercise and set up the local office in Vietnam within **12 months** from the receipt of an order from the Minister of Public Security.

In such instance, the data must be stored locally for at least **2 years** from the date of receipt of the order mentioned in above. Meanwhile, the local office will only need to be maintained until the affected foreign entity no longer conducts business in Vietnam or no longer provides the Online Services in Vietnam.

4. Enforcement of cybersecurity regulations

Critically, a main feature of Decree 53 is the use of an administrative enforcement system to prevent cybersecurity violations. Decree 53 provides the State management authorities with several legal bases to initiate takedown actions, request disclosure of information for investigative purposes and to require the shutdown of apps, websites and information systems that are used for illegal purposes.

The Department of Cybersecurity and High Tech Crime Prevention and Control (under the Ministry of Public Security); and the Department of Military Security Protection (under the Ministry of National Defense), the General Department of Politics and the Cyber Command (under the Ministry of National Defense) will have the power to take enforcement actions (such as issuing takedown or removal notices, requesting information system shutdown or suspension of withdrawal of domain names, disclosure of information and inspection) if the relevant competent authorities determine one of the following violations has occurred:

(i) content that infringes national security, propagandizes against the State; incites violence; disrupts security or public order;

(ii) content that is humiliating or slanderous; infringes upon economic management order; or fabricates or distorts the truth, causing confusion among the people or causing serious damage to socio-economic activities; and

(iii) other illegal contents such as: distortion of history, denial of revolutionary achievements, undermining national solidarity, blasphemy, discrimination by gender or race; prostitution, vice, human trafficking; posting pornographic or criminal information; damaging Vietnam's good traditions, social ethics or public health; enticing, persuading or tempting others to commits crime.

The procedures do not require the relevant competent authorities to hold prior consultation with the concerned entities prior to making their decisions. Further, no appeal process is made available under Decree 53. We envisage that a more detailed guidance of Decree 53 will be soon released by the Ministry of Public Security, as well as the issuance of the Decree on handling administrative sanctions in this area of cybersecurity.

Remarks:

Vietnamese companies should review their existing practices to check if the Compulsory Stored Data is already stored in Vietnam.

Generally, entities handling Compulsory Stored Data should be aware of the powers granted to the relevant competent authorities relating to illegal activities and, where required by the relevant competent authorities, must act expeditiously to remove or disable access to information to avoid any sanctions.

For foreign companies, although the data storage and local office requirements will not be applied immediately to foreign entities, they should be aware of the regulations and the triggering events for such requirements. On the other hand, foreign entities should ensure that they have the resources and process in place to respond to the requests from the Vietnamese cybersecurity authorities to avoid being required to comply with the data storage and local office requirements. We also expect that the Vietnamese cybersecurity authorities will be more active in the protection of the cyberspace to enhance the level of compliance.

Contact us

Hanoi

46th Floor, Keangnam Landmark 72,
E6 Pham Hung, Me Tri, Nam Tu Liem

T: +84 (24) 3946 1600

Ho Chi Minh City

10th Floor, Sun Wah Tower,
115 Nguyen Hue, Ben Nghe, District 1

T: +84 (28) 3821 9266

Da Nang

D3, 5th Floor, Indochina Riverside Towers,
74 Bach Dang, Hai Chau I, Hai Chau

T: +84 (236) 351 9051

Scan to visit our website: kpmg.com.vn

Email: kpmghcmc@kpmg.com.vn