Official Draft Decree implementing the Law on Cybersecurity provides application scope and details on the data localization and local office requirements

The Ministry of Public Security (MPS) recently released the official draft decree ("Draft Decree") guiding the implementation of the Law on Cybersecurity ("LOCS"), which, among other things, defines entities subject to its requirements, and elaborates on the data localization and local office requirements. The Draft Decree, together with LOCS, will take effect on 01 January 2019. The Draft Decree is open for public comments until 31 December 2018.

Please see below for notable points of the Draft Decree.

1. Definition of Cyberspace Service Provider

Under Article 26.3 of the LOCS, local and foreign providers of services on telecommunication networks on the Internet and value-added services in cyberspace in Vietnam ("Cyberspace Service Providers") involved in the collection, exploitation, analysis, or processing of (i) data on personal information, (ii) data users' relationships, [and/or] (iii) data generated by service users in Vietnam are required to store such data in Vietnam.

The definition of Cyberspace Service Provider is provided in the Draft Decree. Under the Draft Decree, Cyberspace Service Providers are defined as local or foreign enterprises operating commercially in accordance with Vietnamese or international law, having operations in Vietnam, and providing the following services:

- Telecom services;
- Services for storing and sharing of data on cyberspace;
- Provide national or international domain names for service users in Vietnam;
- E-commerce;
- Online payment;
- Intermediary payment;
- Services of transportation connection via cyberspace;
- Social network and social media;
- Online games; and
- Email.
2. Data subject to localization and duration of data retention

Under the Draft Decree, the following data must be stored in Vietnam:

- Data on personal information of service users in Vietnam ("Personal Data") include name, date of birth, place of birth, nationality, occupation, title, place of residence, contact address, email address, telephone number, identity card number, personal identification number, citizen identification number, passport number, social security number, credit card number, medical records, and health status.

- Data generated by service users in Vietnam include information selected for upload, synchronised, or imported from devices.

- Data on personal relationships of service users in Vietnam include friends and groups that the users connect to or interact with.

The Draft Decree provides storage periods under Article 26, in particular:

- System logs under Article 26.2(b) of the LOCS must be stored for at least 12 months;

- Personal Data must be stored as long as the enterprise operates or up until the enterprises stops providing the service; and

- Data on relationships of service users and data generated by service users in Vietnam must be stored for at least 36 months.

It is unclear whether the data subject to these requirements must be stored exclusively in Vietnam, or whether the storage of a copy of such data in Vietnam will suffice.

3. Requirements on data localization and local branch/representative office establishment

In accordance with Article 25 of the Draft Decree, onshore and offshore entities having all of the following parameters must localize data, and establish a local branch or representative office in Vietnam:

(i) Being Cyberspace Service Providers;

(ii) Involved in the collection, exploitation, analysis, [and/or] processing of data required to be localized in Vietnam, as mentioned above;

(iii) Allowing service users to conduct prohibited activities listed out under Article 8.1 [and/or] 8.2 of the Cybersecurity Law; and

(iv) Violating Article 8.4, Article 26.2(a), or Article 26.2(b) of the Cybersecurity Law.

The Minister of Public Security will have the discretion to request specific enterprises meeting the conditions above to store data in Vietnam and set up a branch/representative office in Vietnam.
An enterprise requested by the Minister of Public Security to localize data and/or establish a local presence in Vietnam will have 12 months from the date of the request to comply with such requirements.

It is also generally provided under Article 25 that failure to comply will result in sanctions/punishment in accordance with the laws.

4. Identifying and establishing the List of Information Systems Critical to National Security

Article 3 of the Draft Decree provides that information systems critical to national security (“Critical Systems”) are information systems related to sectors identified under Article 10.2 of the LOCS, and which, upon being crashed, infiltrated, taken control of, falsified, interrupted, paralysed, attacked, sabotaged, will result in one of the following:

- Directly affecting the existence of the regime of the Socialist Republic of Vietnam;
- Seriously impairing the national defence, national security; weakening the capability of national defence and protection;
- Becoming a means of information, propaganda against the government, overthrowing the regime;
- Causing particularly serious consequences to the national economy;
- Causing disasters to human life, ecological environment;
- Seriously affecting the national cyberspace infrastructure;
- Seriously affecting the operation of level-I works and special-level works according to the classification of the laws on construction;
- Seriously affecting the research and development of policies, plans classified as State secrets; or
- Seriously affecting the direction, management of the Party and State agencies at the central level.

That said, a specific information system will only be considered a Critical System if it is listed under the List of Critical Systems.

For information systems under the management of ministries, ministry-level agencies, Government's bodies, provincial level authorities, and central political organizations, the head of each authority will be responsible for compiling a dossier proposing for their information system to be included into the List of Critical Systems. For other information systems and in case of necessity, the specialized cyber-security protection force will request the information systems’ owners to prepare the dossier for the inclusion of their information system into the List of Critical Systems.

Subsequently, owners of information systems listed under the List of Critical Systems issued by the MPS will have to oblige with technical and personnel requirements, as provided under the Draft Decree.
5. Process and procedures for unexpected cybersecurity audit

Under Article 24 of the LOCS, the specialized force in charge of cybersecurity protection under the MPS may carry out a cybersecurity audit in case there is an action violating the laws on cybersecurity, prejudicing national security, or causing serious harm to social order, safety. This can be considered a kind of unexpected cybersecurity audit, which is not initiated/requested by the information system owners.

Article 19.2 of the Draft Decree provides the process and procedures for unexpected cybersecurity audit as follows:

(i) Announce the plan of cybersecurity audit;

(ii) Establish the Audit Team as assigned;

(iii) Conduct the cybersecurity audit, coordinate with the information system owner during the audit;

(iv) Prepare minutes of the process and results of the cybersecurity audit and maintain them in accordance with the laws;

(v) Announce the cybersecurity audit results within 7 working days from the finished date of the audit.

6. CPTPP e-commerce chapter

On 12 November 2018, the Vietnam National Assembly official adopted the Comprehensive Agreement for Trans-Pacific Partnership ("CPTPP"). To-date, the agreement has already been ratified by Mexico, Japan, Singapore, New Zealand, Canada, and Australia, and will enter into force 30 December 2018 for those six countries. The CPTPP comes into effect for Vietnam 60 days after the date on which Vietnam has notified the Depositary (being New Zealand presently) in writing that it has completed its applicable legal procedures, which is likely to be in January 2019.

Under Articles 14.11 and 14.1 of the CPTPP e-commerce chapter, CPTPP members make commitments to:

- allow the cross-border transfer of information by electronic means; and
- not require data localization as a condition for conducting business.

We note, however, that there are several carve-outs:

- First, Vietnam may still adopt or maintain inconsistent measures for public policy objectives.
- Second, under Article 14.18 of the CPTPP e-commerce chapter, Vietnam makes an exception in which it will not be subject to the CPTPP dispute settlement mechanism for existing measures regarding its obligations under Articles 14.11 and 14.13 for a period of two years after the CPTPP enters into force.
Third, Vietnam's side letters with Canada, Japan and New Zealand commit the latter three countries to not seek recourse against Vietnam under the CPTPP's dispute settlement mechanism with respect to measures adopted or maintained based on Vietnam’s Cybersecurity Law or related legislations which may violate Vietnam’s CPTPP obligations under Articles 14.11 and 14.13 for a period of five years after the CPTPP comes into effect for Vietnam.