BritCham VIETNAM

ACSV LEGAL

SEPTEMBER 2022

LEGAL UPDATE

DECREE 53: IMPLEMENTING THE LAW ON CYBERSECURITY

The Law on Cybersecurity (**LOC**) was adopted and came into force on 1 January 2019, but some provisions of the implementation were not yet clear. After more than three years, the Government issued Decree No. 53/2022/ND-CP; providing detailed guidance for certain articles of the LOC (**Decree 53**). Decree 53 will come into effect on 1 October 2022.

In this update, we summarise some of the main points.

1. Definition of Localised Data

Prior to Decree 53, the LOC required domestic and overseas entities to store certain data in Vietnam if it was related to telecommunication networks, internet and value-added services in Vietnam's cyberspace. It would apply if entities collect, exploit, analyse or process:

a. data on personal information;
b. data generated by service users; and
c. data on the relationships of service users in Vietnam, (collectively, **Localised Data**).

However, definitions of each type of Localised Data had not been set out in the LOC. This has now been done in Decree 53. Localised Data can be in the form of symbols, writing, numbers, images, sounds, or similar forms.

Data on Personal Information

This is any data that is or can be used to identify an individual.

Data Created by Service Users in Vietnam

This is data that reflects how service users use and operate on Vietnam's internet and telecommunication networks. It also covers information about the equipment and services used to connect with these networks in Vietnam. This would for example be account names, duration of use, credit and debit card information, email addresses, IP addresses for the most recent login and logout, and registered phone number associated with the account or data.

Data on the Relationships of Service Users in Vietnam

This is data that illustrates the relationship interactions between a service user and other people in cyberspace such as friends communicating with each other.

2. Definition of Domestic and Overseas Entity

Decree 53 also clarifies how to identify a domestic or overseas entity. A domestic entity is defined as an entity established under the laws of Vietnam and having its head office based in Vietnam, whereas a foreign entity is defined as an entity established under a foreign jurisdiction. Under these definitions, domestic entities also include foreign-invested enterprises.

3. Data Storage for Overseas Entity in Vietnam

Under Decree 53, an overseas entity is not required to store the data locally, or open a branch or a representative office in Vietnam unless both of the following conditions below apply:

- The entity does business in Vietnam involving or related to
  a. telecommunication services;
  b. data storage and sharing in cyberspace;
  c. supply of national or international domain names to service users in Vietnam;
  d. e-commerce;
  e. online payment services;
  f. intermediary payment services;
  g. service of transport connection via cyberspace;
  h. social networking and social media;
  i. online gaming; or
  j. services of providing, managing, or operating other information in cyberspace in the form of messages, phone calls, video calls, email, or online chat.
- The services provided by the overseas entity have been used by service users to commit acts that violate the LOC, and the Department for Cybersecurity and Prevention of High-Tech Crime under the Ministry of Public Security has sent

a written notice requesting the coordination, prevention, investigation and handling of such acts, but the entity fails to (inadequately) comply, resists, obstructs or disables cybersecurity measures applied by a specialised task force for cybersecurity protection.

An overseas entity has 12 months from the date of receiving such a request by the Public Security Minister to store the data locally and to establish a branch or representative office in Vietnam. The period for establishing and maintaining a branch or representative office in Vietnam will commence from the date the entity receives a request to set up a branch or representative office and continues until the entity is no longer operating in Vietnam or no longer provides any regulated services in Vietnam.

4. Form and Duration of Data Storage in Vietnam

The form of data storage in Vietnam is to be decided by the enterprises. The duration of data storage in Vietnam starts on the date that the entity receives the request to store the data in Vietnam and lasts until the request is lifted, with a minimum of 24 months.

5. Measures for Cybersecurity Protection

Decree 53 contains several provisions and detailed procedures aimed at cybersecurity. These provisions include the evaluation of cybersecurity, assessments of cybersecurity conditions, inspections of cybersecurity, examinations of cybersecurity, responses to and remedying any cybersecurity incidents, using cryptography to protect network information, requiring the deletion of unlawful or false information in cyberspace, collection of infringing e-data relevant to acts in cyberspace, suspending or permanently shutting down the operation of information systems or withdrawing domain names.

6. Deletion of Unlawful or False Information

For this update, we will focus on the measure of requiring the deletion of unlawful or false information in cyberspace, which infringes upon national security, social order and safety, or the lawful rights and interests of individuals, organisations and agencies. It is expected that the competent authority in charge of checking information published on social networks will apply this measure frequently. *Unlawful or false* information includes information which:

- is published in cyberspace that is determined by the competent authority to infringe upon national security, propagandise against the State, incite violence, disrupt security or public order;
- based on legal grounds, is humiliating or slanderous, infringes economic management order, fabricates and falsifies leading to confusion among people, and causes severe damage to social economic activities; and
- violates the LOC, for example, offensive language against any religion, gender or race, or incites crime or violence.

The competent authorities are the Head of the Department for Cybersecurity and Prevention of High-Tech Crime, the Heads of the competent authority of the Ministry of Information and Communications or the specialised force for cybersecurity under the Ministry of National Defense. Depending on each specific matter, these authorities will issue a decision on applying the measure of requiring the deletion of unlawful or false information and then send a written request to the service provider of telecommunication networks, internet and value-added services, the owner of the information system to delete the relevant information.

7. Responsibilities in Implementing Measures for Cybersecurity Protection

Organisations and individuals shall promptly coordinate with and assist the specialised cybersecurity force in implementing the necessary and requested measures to protect cybersecurity. When the competent authorities announce that cross-border service providers are in violation of Vietnamese law, Vietnamese organisations and enterprises will, within their scope of power and responsibilities, need to coordinate with the competent authorities in preventing and handling these violations.

8. Conclusion

If an entity fails to comply with the LOC and Decree 53 such as failure to store data locally, open a branch or a representative office in Vietnam upon request, the authorities shall deal with the violation based on the nature and level of the violation and in accordance with the regulations and laws. Any activity of taking advantage of cybersecurity measures to violate the law might even result in the obligation to compensate if the violation has infringed the lawful rights and interests of others.

For more information, please contact:

Phuong Huynh / Senior Associate
phuong.huynh@acsvlegal.com

Phuong Nguyen / Associate
phuong.nguyen@acsvlegal.com