

Special Alert

August 2022

www.indochinecounsel.com

Long-awaited Decree Implementing the Cybersecurity Law Finalized at Last

After waiting since the middle of 2018, the Government of Vietnam finally issued Decree No. 53/2022/ND-CP dated 15 August 2022 (“**Decree 53**”) detailing some articles of the Law on Cybersecurity No. 24/2018/QH14 (the “**Cybersecurity Law**”), following the last draft decree version released in August 2019 (the “**Last Draft Decree**”). Decree 53 will take effect from 1 October 2022.

Official “shape” of Decree 53

In general, Decree 53 uses the same governing scope and structure as the Last Draft Decree, comprising 6 chapters with 30 articles. A new schedule has been added, providing some templates to be used for the relevant procedures regulated in Decree 53.

In comparison with the Last Draft Decree, certain revisions have been made to some defined terms under Article 2, for example:

- “*service user*” covers both organizations and individuals, but is only limited to those participating in using services in cyberspace, instead of participating in activities in cyberspace in general;
- “*data generated by service user in Vietnam*” is limited to the prescribed data within the territory of the Socialist Republic of Vietnam;
- Department of Military Security Protection and the General Political Department are listed among the cybersecurity task forces (the “**CTF**”); and
- Definitions of “*domestic enterprise*” and “*foreign enterprise*” have been supplemented.

Major high-lights

Cybersecurity inspection obligation (Article 16, Decree 53)

Article 16.1 in the Last Draft Decree has been deleted, which stated that cybersecurity inspection is a technical method to be applied by administrators of information systems in their operation and use of such information systems. This, however, does not release the administrators of information systems from cybersecurity inspection obligations, since this obligation is still provided for under Article 17.2(a) of the Cybersecurity Law.

Requiring deletion of unlawful or false information in cyberspace which infringes national security, social order and safety, or lawful rights and interests of agencies, organizations and individuals (Article 19, Decree 53)

Heads of competent agencies attached to the Ministry of Information and Communications have been added as competent agencies to apply this cybersecurity protection method, in addition to the Director of the Department of Cybersecurity and Hi-tech Crime Prevention (the “DCHCP”) under the Ministry of Public Security (the “MPS”).

Moreover, such agencies are also entitled to actively exchange and share information in respect of the implementation of this cybersecurity protection method, save for information which falls within the scope of State secrets or professional requests of the MPS.

It is of note that the CTF under the Ministry of Defense has the power to determine the application of this cybersecurity protection method in respect of military information systems.

Collecting electronic data / e-data relevant to acts in cyberspace infringing national security, social order and safety, lawful rights and interests of agencies, organizations and individuals (Article 20, Decree 53)

“E-data” has been officially defined as “*information in the form of symbol, text, figure, image, sound or similar forms*”. This definition may yet yield confusion as it is the same as the definition of “*data*” in general provided under Article 4.20 of the Draft Amended Law on Electronic Transactions, which was released for public comments in May this year, if the Draft Amended Law is adopted as-is.

Requirements on data localization and branch/representative office establishment

Types of information to be stored

Information required to be stored in Vietnam also comprise three main types as previously provided in the Last Draft Decree, namely: (i) data on personal information of service users in Vietnam; (ii) data generated by service users in Vietnam; and (iii) data on the relationships of service users in Vietnam (the “**Prescribed Data**”). Wherein, the data generated by service users in Vietnam covers, among

others, registered phone numbers attached to accounts used for utilizing the service or attached to relevant data [in general]. In the Last Draft Decree, the relevant data was limited to only data about personal information.

Enterprises and services subject to the requirements

Similar to the Last Draft Decree, Decree 53 clearly requires that all domestic enterprises must store the Prescribed Data in Vietnam.

Foreign enterprises will be subject to the requirement on data localization and branch / representative office establishment (the “**Requirement**”) if the following conditions are all met:

- The foreign enterprise has business operations in Vietnam which fall in the sectors as prescribed under Article 26.3(a) of Decree 53, which include: (i) telecom services; (ii) services of data storage and sharing in cyberspace (cloud storage); (iii) supply of national or international domain names to service users in Vietnam; (iv) e-commerce; (v) online payment; (vi) intermediary payment; (vii) service of transport connection via cyberspace; (viii) social networking and social media; (ix) online electronic games; and (x) 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 foreign enterprise are used for committing a breach of the laws as to cybersecurity; and
- Such foreign enterprise has been notified and requested in writing by the DCHCP under the MPS for cooperation in handling / preventing such breach, but fails to comply, fails to fully comply, or otherwise challenges any cybersecurity protection method applied by the CTF.

Compared to the Last Draft Decree, the condition on “having activities of collecting, exploiting, analyzing and processing” the Prescribed Data is no longer mentioned. However, this inclusion may be deemed to remain as it has been stated as a prerequisite in Article 26.3 of the Cybersecurity Law.

Concessions by the Government

The requirement for data localization and establishment of a local presence has caused a great deal of concern since it was first released with the promulgation of the Cybersecurity Law. Acknowledging this situation, the Government appears to be making some concessions in Decree 53 by providing some flexibility in compliance with these requirements. In particular:

- If unable to comply with the Requirement due to force majeure events, foreign enterprises are entitled to notify the DCHCP under the MPS in writing about the same within three (3) working days for inspection. In this case, the concerned foreign enterprise will be granted a period of thirty (30) working days to seek remedial measures;
- Enterprises are entitled to decide on the form of data storage within Vietnam; and

- Time for compliance with the Requirement by foreign enterprises has been extended to twelve (12) months (instead of six (6) months only) upon the date of a decision by the MPS Minister on data storage and/or branch/representative office establishment (the “**MPS Decision**”).

Non-compliance will be subject to sanctions. However, till date, no specific regulation on applicable sanctions has been provided.

Required period of storing data and maintaining a branch/representative office

For data storage, instead of regulating specific storage periods for each type of the Prescribed Data, Decree 53 generally sets out a storage period which commences when the enterprise receives the MPS Decision, and lasts until the request is terminated, with a minimum cap of twenty-four (24) months.

For branch/representative office establishment, the applicable period commences when the enterprise receives the MPS Decision, and lasts until the enterprise no longer operates in Vietnam or the prescribed service is no longer provided in Vietnam.

Potential Impacts

After a long wait, administrators of information systems, domestic and offshore enterprises can finally understand the compliance requirements with some certainty, which should ease the difficulty of adherence to the Cybersecurity Law.

Most importantly, the subjects for which data localization and branch/representative office establishment will be required has finally reached a relatively specific explanation. Accordingly, foreign enterprises with a high risk of being subject to this requirement can “have some peace of mind”, that, until an MPS Decision is submitted, there is no need to comply with the same requirements. On the contrary, domestic enterprises have been further burdened as they all have to ensure compliance, but Decree 53 neither provides a specific deadline nor offers a specific grace period for them to finalize their compliance efforts. It is highly recommended that foreign enterprises establish preliminary planning to respond appropriately should they receive a notice from the MPS, since the 12-month delay can be seen a short time period for behemoth entities operating globally.

The issuance of Decree 53 is an important piece to complete the puzzle in terms of data protection in Vietnam. Still, in the context where regulators are rushing to issue many legal documents, it still remains likely that some confusion or overlap may find its way into the relevant regulations for emerging technology issues.

About Indochine Counsel

Established in October 2006, Indochine Counsel is a leading commercial law firm in Vietnam. Our firm is ideally positioned to assist international investors and foreign firms to navigate the legal landscape in one of Asia's most dynamic and challenging countries. We also take pride in our services offered to domestic clients in searching for opportunities abroad. With over 45 lawyers many of whom have been trained abroad and staffs in two offices, Ho Chi Minh City and Hanoi, Indochine Counsel offers expertise in a dozen practice areas and provides assistance throughout the entire life cycle of your business.

Indochine Counsel represents and advises clients on all legal aspects in the following major areas of expertise:

- Anti-trust & Competition
- Banking & Finance
- Corporate & Commercial
- Energy, Natural Resources & Infrastructure
- Intellectual Property
- Inward Investment
- Labour & Employment
- Litigation & Dispute Resolution
- Mergers & Acquisitions
- Real Estate & Construction
- Securities & Capital Markets
- Technology, Media & Telecommunications

A full list of partners, associates and other professionals is available on our website. |

Contact Us

For further information or assistance, please contact the following Indochine professionals:



Dang The Duc

Managing Partner

E duc.dang@indochinecounsel.com



Thai Gia Han

Associate | Co-Head of IP & TMT
Practice Group

E han.thai@indochinecounsel.com

Ho Chi Minh City

Unit 305, 3rd Floor, Centec Tower
72-74 Nguyen Thi Minh Khai, District 3
Ho Chi Minh City, Vietnam

T +84 28 3823 9640

F +84 28 3823 9641

E info@indochinecounsel.com

Hanoi

Unit 705, 7th Floor, CMC Tower
Duy Tan Street, Cau Giay District
Hanoi, Vietnam

T +84 24 3795 5261

F +84 24 3795 5262

E hanoi@indochinecounsel.com

www.indochinecounsel.com

This Special Alert is designed to provide our clients and contacts with general information of the relevant topic for reference only, without the assumption of a duty of care by Indochine Counsel. The information provided is not intended to be nor should it be relied upon as a substitute for legal or other professional advice.

© 2022 Indochine Counsel | All Rights Reserved.