Baker McKenzie.

Client Alert

26 July 2021

Data localization requirements in Vietnam

In brief

In this age of technology, it is often said that the most valuable resource is no longer oil or gas but data. In recent years, the Vietnamese government has attempted to follow global best practices in regulating data. One critical aspect of these new legislative attempts has to do with Vietnam's data localization requirements. This article articulates the basic principles concerning these still-developing localization requirements.

Contents

In more detail

Definition and terms

The Law on Digital Transactions No. 51/2005/QH11 dated 29 November 2005, defines "data" (dữ liệu) as information in the form of symbol, script, number, image and sound or of other similar forms.

Data localization should be distinguished from the relatively similar but separate concept of data sovereignty. Data sovereignty refers to the idea that data are subject to the laws and governance of the jurisdiction in which they are collected. This is evident where national regulations state that they govern any personal data of the citizens of that country, regardless of where those data are stored. Indeed, each jurisdiction may have different rules relating to that same matter, and as such, each is said to claim "sovereignty" over such data. Data localization takes a step further by requiring that the initial collection, processing and storage of a citizen's data occur first within national boundaries.

Data localization in Vietnam

Data localization requirements in Vietnam are taking shape in three legislations. The first legislation is the Law on Cybersecurity 2018 ("Cybersecurity Law"). The relevant provision is as follows:

> Article 26. Ensure cyberspace security
>
> 3. Onshore and offshore enterprises providing services on telecommunication networks or the Internet, value-added services on the cyberspace in Vietnam and who collect, exploit, analyze, process data about personal information, data about the service users' relationships, data created by service users in Vietnam must store such data in Vietnam for a period specified by the Government.
>
> Foreign enterprises under the scope of this paragraph must establish a branch or a representative office in Vietnam.
>
> 4. The Government shall stipulate this paragraph in detail.

The scope of the above provision is broad and includes every enterprise that provides any service over cyberspace and that processes personal data (preemptive approach). Currently, there are no exceptions to this rule, and these service providers must store the customers'/users' personal data in Vietnam. Thus, for example, if a movie VOD service provider makes available their service on the internet, and users, to watch he movies, must create an account with their name, email or phone number, the VOD provider is required to physically store the data on such users within the Vietnamese border.

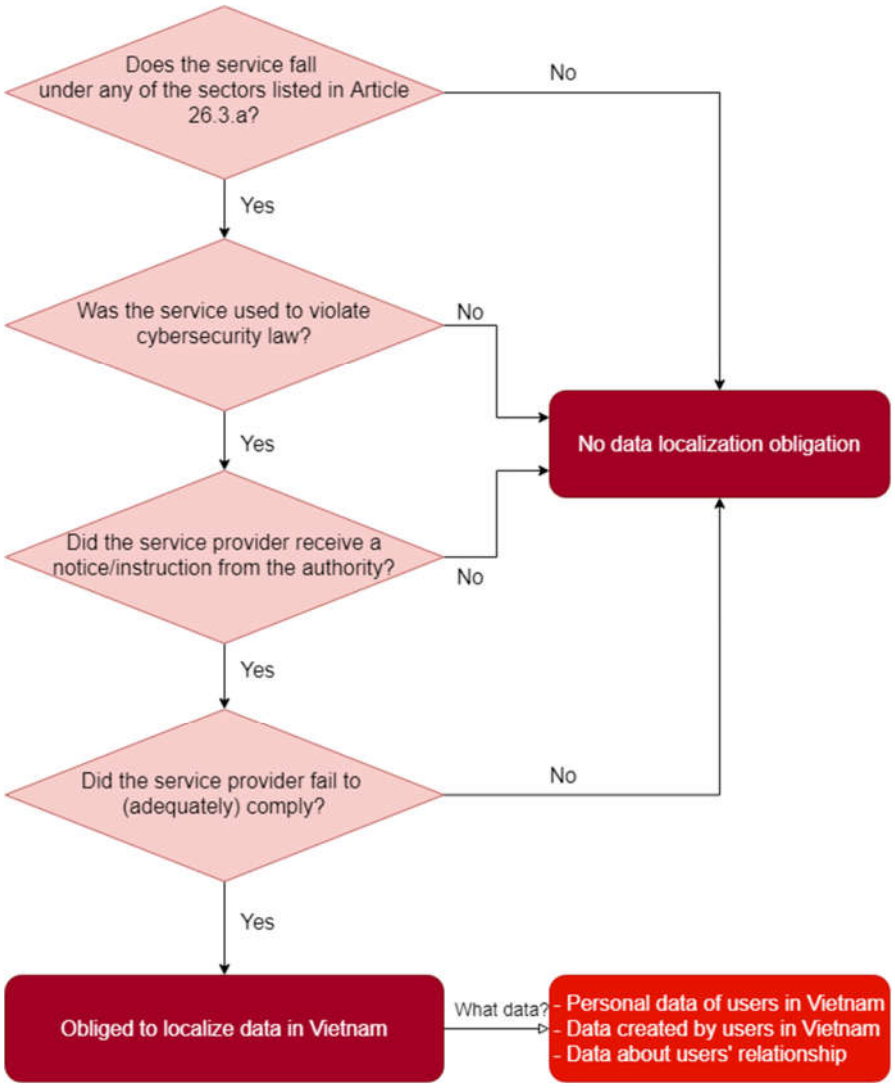
The government has drafted a decree clarifying several provisions of the Law on Cybersecurity ("Cybersecurity Decree"). Article 26 of the decree stipulates that only foreign providers of certain prescribed services (domain name service, e-commerce, online

payment, social network and social communication, etc.) may be required to store data and set up a branch/representative office in Vietnam. Moreover, such an obligation only arises under the following circumstances:

1. The service has been used to violate cybersecurity laws.
2. Such a violation has been notified by the authority to the service provider.
3. The service provider has not complied (adequately) with the authority's instructions.

In the absence of one of the above elements, the foreign service provider is not required to store data in Vietnam. This is illustrated by the graph below:

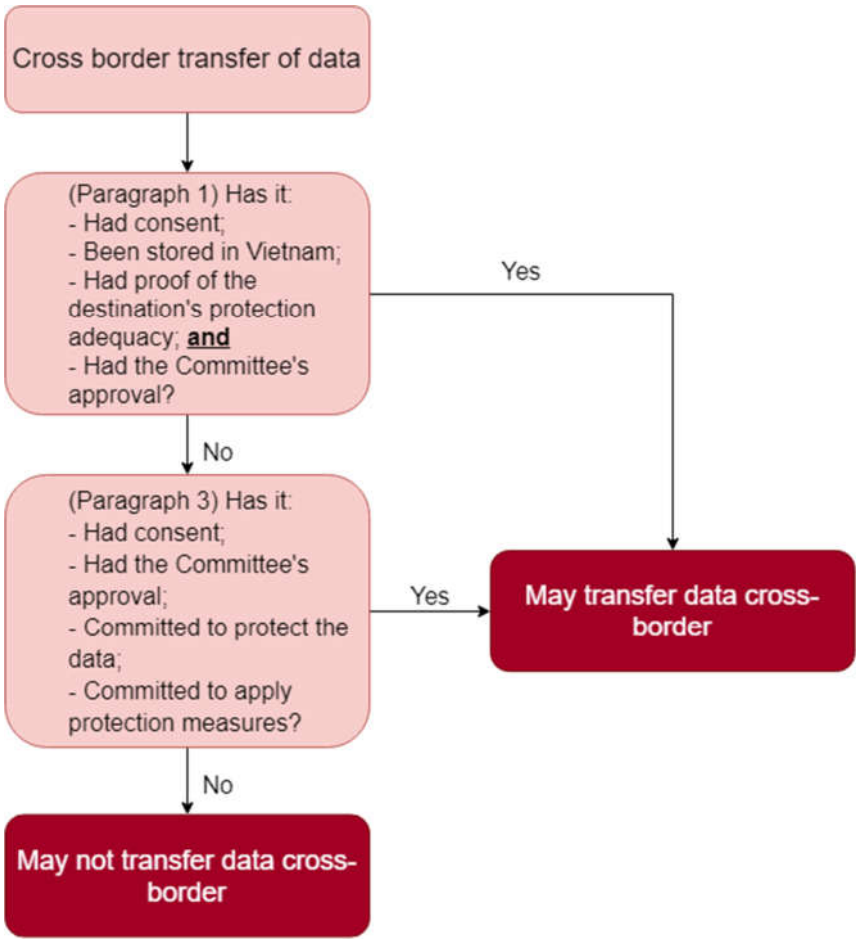
Figure 1. Is the foreign service provider required to store data and set up a branch/representative office in Vietnam?



In contrast to the Cybersecurity Law's preemptive approach, the Cybersecurity Decree takes a reactive one – not all offshore service providers have the localization obligation, only those who have been notified of a breach and fail to comply do. Furthermore, while the Cybersecurity Law imposes the data localization obligation on all providers of services in cyberspace, under the Cybersecurity Decree, only foreign providers of listed services may have such an obligation. Under Vietnamese law, should there be a conflict between a decree and a law, the law prevails, so it will be interesting to see how the final version of the Cybersecurity Decree resolves this matter.

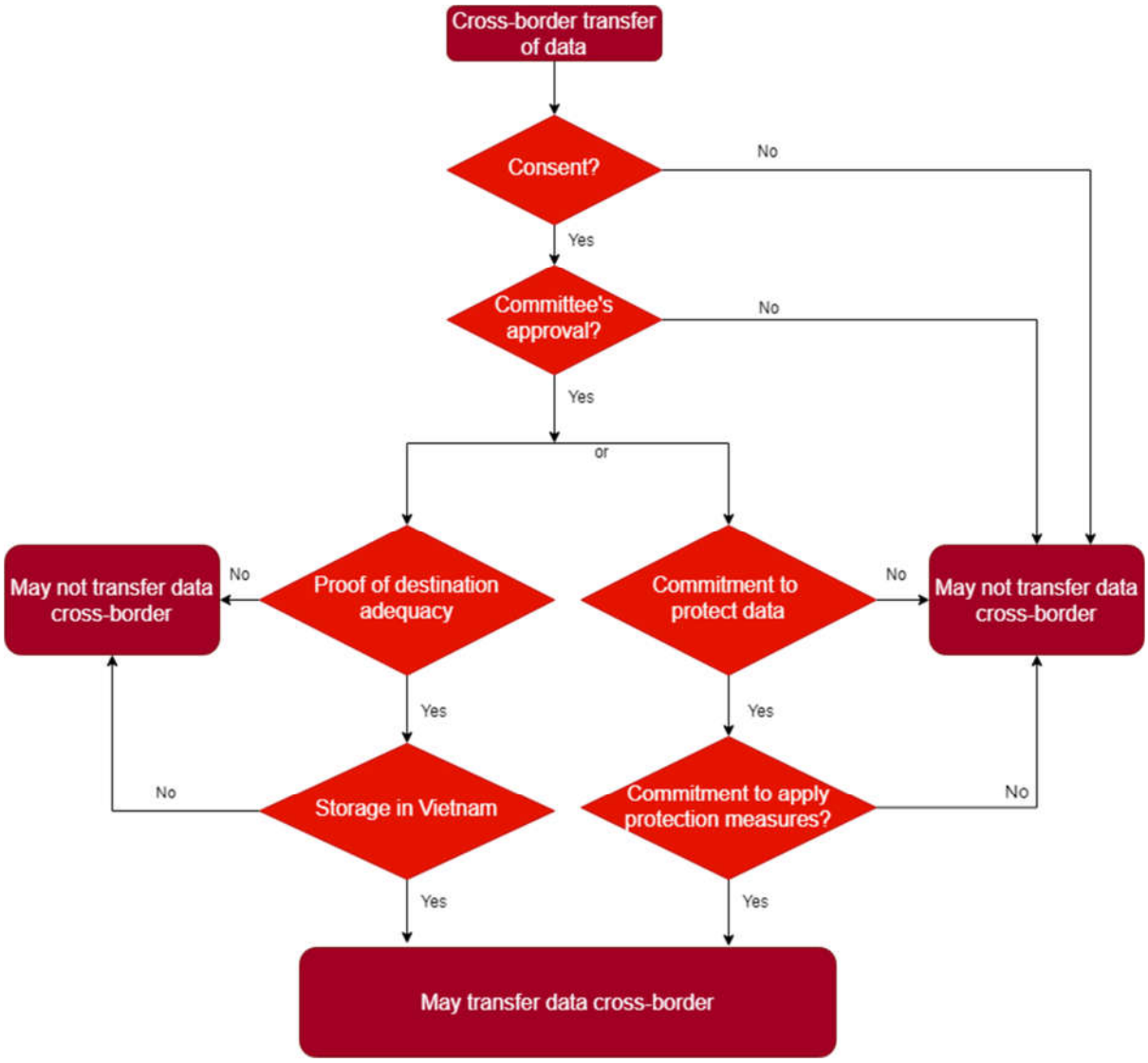
The last legislation relating to data localization is the Draft Personal Data Protection Decree (PDPD). Under Article 21.1, an enterprise may only transfer data abroad if it meets all four requirements, including storing the original data in Vietnam. However, should the exception(s) listed in paragraph 3 apply, the enterprise is exempted from such requirement(s).

Figure 2. Statutory provision under the PDPD



It is unclear whether only one or all four requirements under paragraph 3 must be satisfied for the enterprise to be exempted from paragraph 1 obligations; and even so, whether the enterprise is relieved from all or just one of such obligations. Given that the list in paragraph 1 is to be taken as a whole, and the fact that half of the provisions in both paragraphs 1 and 3 overlap (both refer to the data subject's consent and the Committee's approval), it is logical to interpret them as complementary. Accordingly, cross-border transfer of data must satisfy all four requirements under paragraph 1. Nonetheless, if an enterprise meets all of the requirements under paragraph 3, it may be exempted from the obligations under paragraphs 1.b and 1.c. However, this view has not yet been endorsed or confirmed by any official authority.

Figure 3. Our suggested interpretation:



Remark

Four conclusions can be drawn from the above analysis of the legislations.

First, although both the draft Cybersecurity Decree and the PDPD are directed at "personal data," their approaches are significantly different. The Cybersecurity Law and the Cybersecurity Decree provide detail about data localization, according to which data must be stored in Vietnam and may not be transferred offshore. The PDPD, in contrast, requires mandatory storage of the original data in Vietnam (data mirroring, according to which only the original copy of the data must be stored in Vietnam; the transfer, copying, storing of other copies offshore are allowed). Thus, it can be said that there has been an inconsistency among the applicable regulations regarding the storing of data.

Second, the draft Cybersecurity Decree focuses only on regulating specific sectors; sectors that are not listed, such as manufacturing and F&B, are exempted. Even if a sector is covered, only enterprises satisfying specific requirements are obliged to store data and set up a branch/representative office in Vietnam.

Third, "storing of data" may be construed to include the storage in processing centers in Vietnam or the storage in systems of third-party storage service providers. Therefore, an enterprise does not necessarily have to set up a data storage center / server center in Vietnam.

Last but not least, in Vietnam, with respect to certain business activities and especially novel activities, the law may be interpreted to permit only acts that are “approved,” “explicitly permitted” or “licensed.” The fact that the law is silent does not

necessarily indicate that an enterprise may assume that it can carry out the activity. This means that as long as the current regulations on data localization requirement remain conflicting, there is no clear legal basis for businesses to ensure full compliance with the laws.

Contact Us

Manh Hung Tran
Partner
tmh@bmvn.com.vn