3 September 2021

THAILAND Newsletter

Key Contacts


Wongsakrit Khajangson
+66-2-009-5162
wongsakrit.k@mhm-global.com


Panupan Udomsuvannakul
+66-2-009-5159
panupan.u@mhm-global.com


Suphakorn Chueabunchai
+66-2-009-5168
suphakorn.c@mhm-global.com


Thanachart Osathanondh
+66-2-009-5151
thanachart.o@mhm-global.com

New Regulations on Categorization and Obligations of Service Providers Under the Computer Crimes Act

Introduction

On 13 August 2021, the Notification of the Ministry of Digital Economy and Society re: Rules Related to Storage of Computer Traffic Data by Service Providers, B.E. 2564 (2021) (the "**Notification**") was published in the Royal Thai Government Gazette to replace the former notification issued in 2007.

New Category of Service Providers

While some provisions under the Notification remain the same or similar with the former notification, the Notification mainly expands on the categorization of service providers which must store computer traffic data pursuant to the Computer Related Crime Act, B.E. 2550 (2007). The new categorizations are as follows:

1. internet access or communication service provider for the general public via a computer system, which includes services provided directly or by proxy, as follows:
    - telecommunications and broadcast carrier;
    - access service provider;
    - host service provider;
    - internal café service provider;
    - online application store service provider; and
    - social media service provider, whether there is a member system or not.
2. data storage service provider as follows:
    - content and application service provider;
    - cloud computing service provider to end user; and
    - digital service provider

Annex A of the Notification further provides examples for each type of service provider while Annex B dictates the content and type of computer traffic data which each category of service provider is required to store under the law.

Obligation of Service Providers

The Notification also sets 2 new security measures for all service providers, i.e., digital identification process and access control system.

Digital identification process and access control system

The service providers must arrange for a digital identification process for all of their users pursuant to the standard prescribed under the Electronic Transactions Act, B.E. 2544 (2001) and stipulates that the identification system must include an administrative safeguard policy, technical safeguard policy, and physical safeguard policy for an access control system, which must at least consist of the following:

1. control of access to data and storage devices;
2. specify the approval or privilege in accessing data from the identification system;
3. user access management system;
4. prescribe user responsibilities in accessing data from the identification system; and
5. provide means to check log ins which access, change, delete, or transfer data from identification system.

The aim of the above access control system is to protect the reliability of data and personal data of users. Note that this required access control system is mostly the same as with the security measures under the Notification of the Ministry of Digital Economy and Society re: Security Measures of Personal Data, B.E. 2563 (2020) which currently regulates all data controllers during the transitional period pending enforcement of Personal Data Protection Act, B.E. 2562 (2019).

Storage of computer traffic

Other than the above security measures, the security measures for collecting computer traffic data under the Notification remain the same as the former notification, which include:

1. store data in a form of media or device which can protect the integrity of the data and identify the person who can access the data;
2. have clearance levels for accessing the data to protect the integrity of the data and prevent administration from revising the stored data;
3. appoint personnel to coordinate with the authority under the Computer Crime Act; and
4. the computer traffic storage system must be able to identify and authenticate the user.

Furthermore, this Notification explicitly prescribes that even if the service provider enters into an agreement with a third party in regards to the storage of computer traffic data, the service provider is still required by law to store the data and submit such data to the relevant authority immediately upon request.

The service provider must store the computer traffic data for at least 90 days, and if there is a request from the relevant authority, the storage period can be extended for 6 months on each occasion, but the total period must not exceed 2 years.

Effectiveness

The Notification became effective on 14 August 2021. There is an exception for internet café service providers and digital service providers which must start storing computer traffic data within 1 year and 180 days from the effective date, respectively.

If you would like to discuss any of the legal implication of the matters discussed above, please contact the authors listed in left-hand column.

Contact Us
Chandler MHM Limited
17th and 36th Floors
Sathorn Square Office Tower
98 North Sathorn Road
Silom, Bangrak, Bangkok 10500 Thailand
www.chandlermhm.com