DATA PROTECTION LAWS OF THE WORLD

Vietnam

VIETNAM

Last modified 10 January 2022

LAW

There is not a single comprehensive data protection law in Vietnam. Instead, regulations on data protection and privacy can be found in various legal instruments. The right of privacy and right of reputation, dignity and honour and fundamental principles of such rights are currently provided for in Constitution 2013 ("**Constitution**") and Civil Code 2015 ("**Civil Code**") as inviolable and protected by law.

Regarding personal information, the key principles on collection, storage, use, process, disclosure or transfer of personal information are specified in the following main laws and guiding documents, among others:

- Criminal Code No. 100/2015/QH13, passed by the National Assembly on 27 November 2015; as amended from time to time ("**Criminal Code**");
- Law No. 24/2018/QH14 on Cybersecurity, passed by the National Assembly on 12 June 2018 ("**Cybersecurity Law**");
- Law No. 86/2015/QH13 on Network Information Security, passed by the National Assembly on 19 November 2015; as amended by Law No. 35/2018/QH14 dated 20 November 2018, on amendments to some articles concerning planning of 37 Laws ("**Network Information Security Law**");
- Law No. 59/2010/QH12 on Protection of Consumers' Rights, passed by the National Assembly on 17 November 2010; as amended by Law No.35/2018/QH14 dated 20 November 2018, on amendments to some articles concerning planning of 37 Laws ("**CRPL**");
- Law No. 67/2006/QH11 on Information Technology, passed by the National Assembly on 29 June 2006; as amended by Law No. 21/2017/QH14 dated 14 November 2017 on planning ("**IT Law**");
- Law No. 51/2005/QH11 on E-transactions, passed by the National Assembly on 29 November 2005 ("**E-transactions Law**");
- Decree No. 85/2016/ND-CP dated 1 July 2016, on the security of information systems by classification ("**Decree 85**");
- Decree No. 72/2013/ND-CP dated 15 July 2013 of the Government, on management, provision and use of Internet services and online information; as amended by Decree No. 27/2018/ND-CP dated 1 March 2018 and Decree No.150/2018/ND-CP dated 7 November 2018 ("**Decree 72**");
- Decree No. 52/2013/ND-CP dated 16 May 2013 of the Government; as amended by Decree No. 08/2018/ND-CP dated 15 January 2018, on amendments to certain Decrees related to business conditions under state management of the Ministry of Industry and Trade and Decree No. 85/2021/ND-CP dated 25 September 2021 ("**Decree 52**");
- Decree No. 15/2020/ND-CP of the Government dated 3 February 2020 on penalties for administrative violations against regulations on postal services, telecommunications, radio frequencies, information technology and electronic transactions ("**Decree 15**");
- Circular No. 03/2017/TT-BTTTT of the Ministry of Information and Communications dated 24 April 2017 on guidelines for Decree 85 ("**Circular 03**");
- Circular No. 20/2017/TT-BTTTT dated 12 September 2017 of the Ministry of Information and Communications, providing for Regulations on coordinating and responding to information security incidents nationwide ("**Circular 20**");
- Circular No. 38/2016/TT-BTTTT dated 26 December 2016 of the Ministry of Information and Communications, detailing

cross-border provision of public information ("**Circular 38**");

- Circular No. 24/2015/TT-BTTTT dated 18 August 2015 of the Ministry of Information and Communications, providing for the management and use of Internet resources, as amended by Circular No. 06/2019/TT-BTTTT dated 19 July 2019 ("**Circular 25**"); and
- Decision No. 05/2017/QD-TTg of the Prime Minister dated 16 March 2017 on emergency response plans to ensure national cyber-information security ("**Decision 05**").

Each aspect and each industry may have their respective regulating documents. In other words, applicability of legal documents will depend on the factual context of each case, e.g businesses in the banking and finance, education, healthcare sectors may be subject to specialized data protection regulations, not to mention to regulations on employees' personal information as provided in Labour Code 2019 ("**Labour Code**").

The most important Vietnamese legal documents regulating data protection are the Cybersecurity Law and Network Information Security Law. However, it is worth noting that, unlike cybersecurity laws in other jurisdictions that were inspired by the GDPR of the EU, the Cybersecurity Law of Vietnam shares similarities with China's Cybersecurity Law enacted in 2017. Such law focuses on providing the government with the ability to control the flow of information; meanwhile, the Network Information Security Law enforces data privacy rights for individual data subjects.

A draft Decree detailing a number of articles of the Cybersecurity Law ("**Draft Cybersecurity Decree**"), notably including implementation guidelines for data localization requirements, together with a draft Decree detailing the order of and procedures for application of a number of cybersecurity assurance measures and a draft Decision of the Prime Minister promulgating a List of information systems important for national security, are being prepared by the Ministry of Public Security ("**MPS**") in coordination with other relevant ministries, ministerial-level agencies and bodies.

MPS has drafted a Decree on personal data protection ("**Draft PDPD**"), which is contemplated to consolidate all data protection laws and regulations into one comprehensive data protection law as well as make significant additions and improvements to the existing regulations. The Draft PDPD was released for public comments in February 2021 and was originally scheduled to take effect by December 2021. However, due to the extreme sensitivity of the issues intended to be regulated by the Draft PDPD (including the data localization requirement and regulatory approval for sensitive data processing), the Draft PDPD received immense negative comments from the public and foreign governments. Thus, its finalization process has taken much longer than the MPS first anticipated. As of January 2022, the Draft PDPD still has not been finalized or submitted to the government and National Assembly for final approval. It is anticipated that the Draft PDPD might be finalized and take effect within 2022.

DEFINITIONS

Definition of personal data

There is no single, pervasive definition of personal data in Vietnam, but the concept of personal information, definition thereof and its variations can be found in the various laws, regulations and guidance that comprise the data protection framework in Vietnam. In summary, personal information is generally defined as information associated with the identification of a specific person, e.g. full names, date of birth, profession, title, contact addresses, email addresses, telephone numbers, ID numbers, passport numbers.

Definition of sensitive personal data

Currently, there is no particular definition of 'sensitive personal data' specified in the laws of Vietnam, except for highly controlled industries such as banking and finance.

However, under the Draft PDPD, 'personal data' is proposed to be defined as data about individuals or relating to the identification or ability to identify a particular individual. Personal data would be categorized into two groups: (a) basic personal data, and (b) sensitive personal data:

- *Basic personal data* is defined to include: (i) surname, middle name, birth name, alias (if any); (ii) date of birth; (iii) date of death or date of going missing; (iv) blood type and gender; (v) place of birth, place of birth registration, permanent residence, current residence, hometown, contact address, email address; (vi) education; (vii) ethnicity; (viii) nationality; (ix) phone number; (x) ID card number, passport number, citizen identification number, driver's license number, plate number,

personal tax identification number, social insurance number; (xi) marital status; and (xii) data reflecting online activities or activity history.

- *Sensitive personal data* is defined to include: (i) personal data on political and religious views; (ii) personal health data, i.e. information related to the physical or mental health status of the data subject collected and identified during the process of registration or provision of medical services; (iii) personal genetic data, i.e. information relating to inherited or acquired genetic characteristics of each individual; (iv) personal biometric data, i.e. information about physical and biological characteristics of each individual; (v) personal data on gender status, i.e. information about people identified as male, female, gender neutral, androgynous, or having both masculine and feminine characteristics or self-identifying a different gender from the gender identified at birth; (vi) personal data about life and sexual orientation; (vii) personal data about criminals and criminal acts collected and stored by law enforcement agencies; (viii) personal financial data, i.e. information used to identify an account, card or payment instrument provided by a financial institution to a data subject or information about the relationship between a financial institution, original financial data and data subjects, including records, financial status, credit history, and income level; (ix) personal location data, i.e. information about the individual's previous and current physical location; (x) personal data about social relationships; and (xi) other personal data as specified by law to be special and subject to confidentiality protection.

NATIONAL DATA PROTECTION AUTHORITY

Vietnam does not have a single national data protection authority. Instead, the authority on State management of certain aspects of information and / or data protection has been given to a number of competent State authorities. To some extent, the key State competent authorities in charge of information and/or data protection would be the Ministry of Information and Communications ("**MIC**"), the MPS and the Vietnam Cybersecurity Emergency Response Teams / Coordination Center ("**VNCERT/CC**") directly managed by the Authority of Information Security ("**AIS**") under the MIC. Their key roles are particularly as follows:

- MIC, particularly the AIS shall be responsible for management of the provision of cyberspace services (e.g. social network, gaming online, e-commerce, etc.), such as requesting cyberspace service providers to delete illegal data uploaded on their system / network.
- MPS, particularly Department for Cybersecurity and High-tech Crime Prevention and Fighting, is responsible for supervision of national cybersecurity, e.g. to request cyberspace service providers to (i) store data in Vietnam and (ii) provide users' information for serving investigation into cybersecurity crime.
- VNCERT/CC acts as the National Coordination Center for response to cybersecurity incidents and information security testing.

In addition to the above, subject to each specific industry (e.g. banking and finance; education; healthcare; natural resources and environment; culture, sports and tourism; etc.), the State management authority in charge of such industry and its IT center shall be involved in relevant information system protection.

REGISTRATION

There is no requirement under Vietnamese laws whereby such data controller of private sector is required to have it or its activities registered with the local authorities (e.g. MPS, MIC or VNCERT/CC), except:

- Foreign enterprises which provide services on telecom networks and on the Internet and other value-added services in cyberspace in Vietnam **("cyberspace service providers")** may need to have branches or representative offices in Vietnam (subject to specific guidance of the Government under the Draft Cybersecurity Decree);
- Where organizations or individuals involved in cross-border public information provision activities rent digital information storage facilities within the territory of Vietnam so as to provide their services or are reported to provide public information to be used or accessed by at least 1 (one) million Internet users in Vietnam a month, they shall have the obligation to send a written notice to the MIC of their contact information, including:
    - In the case of an organization, registered name, transactional name, and name of the licensing country are required; in the case of an individual, name of such individual is required;
    - Main office address of an organization, permanent residence address and nationality of an individual owning an electronic information page and location of the main server system;

- Principal contact agent of an overseas organization or individual and principal contact agent operated within the territory of Vietnam, including the following information such as name of an organization, individual, contact email address and telephone number;
- in a direct manner, by post or to the email address report38@mic.gov.vn.

DATA PROTECTION OFFICERS

Under the laws of Vietnam there is no regulation mandating a typical company to appoint a "DPO". However, certain types of organizations (e.g. big information system owners and others such as telecoms enterprises, banks, State bodies, information system owners using State budgets, etc.) are required to appoint specialized information security focal points and contact persons to supervise and warn on cyber-information security, etc. These officers are expected to be in charge of incidents rather than data protection issues. Other strict requirements (under various legal documents) are also applicable to such kinds of organizations which do not cover "companies of the private sector".

COLLECTION & PROCESSING

According to Vietnamese laws, the solid legal basis for the processing of personal information (that means the performance of one or some acts of collecting, editing, utilizing, storing, providing, sharing or spreading personal information in cyberspace for commercial purpose) is a **prior explicit consent** given by the data subject. Specifically, it requires that organizations that process personal information shall collect personal information only **after** (i) having **notified** data subjects of the scope, purpose, storage period, form and location of collection, storage, processing, use, disclosure and transfer of such information (the relevant terminologies cover "collect, store, process, use, disclose and transfer" rather than just "collection and processing" of data); and (ii) **obtaining** their consents before. The traders or organizations collecting and using the consumers' personal information on E-commerce website must set up the mechanism for the consumers / subjects to clearly express their consent through online functions on the website, e-mail, messages or other methods as agreed by the two parties.

However, based on the **specific purpose** for processing of personal information, the laws provide an alternative legal basis besides consent. Particularly, organizations may collect, process, use, store, disclose and transfer personal information of other people without the consent when that information is used for the following purposes:

- Signing, modifying or performing contracts on the use of information, products or services *in the network environment* (generally defined as "the environment in which information is provided, transmitted, collected, processed and exchanged via information infrastructure");
- Calculating charges for use of information, products or services *in the network environment*; and
- Performing other obligations provided for by law (e.g. at request of competent authority as prescribed in the law of Vietnam).

In addition, the traders and organizations collecting and using consumers' personal information on E-commerce websites shall not need the consumers / subjects' prior consent in the following cases:

- Collecting personal information that has been publicized on E-commerce websites;
- Collecting personal information to sign or perform contract of sale and purchase of goods and services;
- Collecting personal information to calculate the price and charge of use of information, products and services on the network environment;
- Collection of personal information for performing other obligations in accordance with the law.

Especially, the data controller is required to:

- Provide the data subject with their personal information collected and stored by the data controller upon receipt of a request from the data subject;

- Immediately comply with the request and notify such data subject or grant him / her the right to access information or to do so upon receipt of a request from the data subject for re-examination, update, correction, modification or cancellation, or for the stoppage of the provision of personal information to a third party, and not supply or use relevant personal information until such information is corrected;

- Take necessary measures to protect personal information, and notify the data subject if the data controller fails to comply with its / his / her request for technical or other reasons; and

- Delete the stored personal information when they have accomplished their use purposes or the storage time has expired and notify the data subject thereof, unless otherwise prescribed by law.

TRANSFER

In general, if a data controller wishes to share, disclose or otherwise transfer an individual's personal information to a third party (including group companies), the data controller they must inform the data subjects and obtain prior explicit consent from such data subjects. In particular, the traders or organizations collecting and using the consumer's personal information on an E-commerce website must have specific mechanisms for the information subjects may choose the permission or refusal of using their personal information in the cases of using personal information to send advertisements and introduce products and other commercial information.

In cases of cross-border transfers, the data exporter / importer does not need to obtain authorization from or make a filing with the Vietnamese regulators, or notify the supervisory authority before carrying out any automatic processing operation or set of such operations, including a transfer of personal information from Vietnam to a foreign country or an international organization. There are exceptions for the transfer of information that is classified as being a State secret.

In addition to the above requirements, it is worth noting that data localization is an increasing trend in Vietnam, which is provided in certain legal documents, e.g.:

- According to Circular 24, electronic general information pages and social networks as entities licensed in Vietnam must use at least one domain name ".vn" and store information in servers identified by IP addresses in Vietnam.

- The Cybersecurity Law requires that domestic or foreign cyberspace service providers carrying out activities of collecting, exploiting / using, analysing and processing data being personal information, data about service users' relationships and data generated by service users in Vietnam must store such data in Vietnam for a specified period to be stipulated by the Government. In particular, according to Article 26 of the Draft Cybersecurity Decree, domestic and foreign enterprises providing telecoms and online services to customers in Vietnam may be required to locally store certain customer-related data in Vietnam for a certain period prescribed by law if the authority alerts them that their services/online platforms have been used to commit violations of Vietnam's laws but such online service providers fail to remedy the situation upon the request of the authority. According to the latest version of the Draft Cybersecurity Decree, the organizations which could be subject to the foregoing data localization requirements only include those engaging in the following services: (i) telecommunications; (ii) data storage and sharing in cyberspace; (iii) supply of national or international domains to service users in Vietnam; (iv) E-commerce; (v) online payment; (vi) intermediary payment; (vii) transport connection via cyberspace; (viii) social networking and social media; (ix) online electronic games; and (x) providing, managing or operating other information in cyberspace in the form of messages, phone calls, video calls, email or online chats. As of January 2022, the Draft Cybersecurity Decree has not yet been finalized. It is anticipated that the Draft Cybersecurity Decree might be finalized and take effect within 2022, at the same time as the Draft PDPD.

- The Draft PDPD also suggests imposing restrictions on cross-border data transfer (including registration of transferring personal data from Vietnam to foreign countries). However, details of most provisions under the Outline (including cross-border data registration) have not yet been fully developed. There have been no further developments on this version of the Outline and/or the Draft PDPD since December 2019. The MPS and the Government have not set out any specific timeline to promulgate the Draft PDPD.

- The Draft PDPD also suggests imposing restrictions on cross-border data transfer (including registration of transferring personal data from Vietnam to foreign countries). In particular, according to the Draft PDPD, subject to a specific exemption and prior approval from the Personal Data Protection Commission ("**PDPC**"), before transferring personal data of Vietnamese citizens out of Vietnam, the following four conditions must be fulfilled: (i) consent must be obtained from the data subjects; (ii) the original data must be stored in Vietnam; (iii) the data transferor must have proof that the

recipient country has personal data protection at a level equal to or higher than the level specified in the Draft PDPD; and (iv) a written approval for transfer must be obtained from the PDPC via registration procedures. Moreover, the Draft PDPD also requires a personal data controller/processor that transfers data abroad to build a system to store data transfer history for three years.

SECURITY

Organizations must take necessary managerial or technical measures to ensure that the personal information shall not be lost, stolen, disclosed, modified or destroyed. Remedial measures must be taken immediately if personal information is being or is likely to be disclosed or destroyed.

Indeed, generally, the data controller shall classify information based on its secrecy in order to take appropriate protection measures; and agencies and organizations that use classified and unclassified information in activities within their fields have to develop regulations and procedures for processing information, and determine contents and methods of recording authorized accesses to classified information.

In which:

- Personal information protection policies to be developed and published by traders and organizations collecting and using the consumers' personal information on E-commerce websites must provide the purpose of collection; scope of use; storage period; organizations and persons authorized to access to such personal information; address of data controller, including way of contact for the consumers to ask about the collection and processing information related to them; methods and tools for data subjects to access and modify their personal information on the E-commerce system of the data controller.
- The above contents must be clearly displayed for the consumers before or at the time of information collecting. The language is Vietnamese. The contents are clear and understandable. The font size of the text is at least 12. The paper background and ink colour used in the terms must contrast.
- If the information collection is done through E-commerce website of the data controller, the personal information protection policies must be made public in a conspicuous place on the website.
- The traders, organizations or individuals that own E-commerce websites with online payment functions must publish on their website policies on security of customer's payment information.

BREACH NOTIFICATION

The laws of Vietnam introduced a general requirement for the reporting and notification of actual or suspected personal information security incidents. A data breach reporting / notification requirement in Vietnam will be triggered if the data incident falls within any of the following criteria:

Criterion 1. The affected data system is located in Vietnam.

Criterion 2. The services provided to customers in Vietnam fall under the categories of Regulated Services, including (1) telecommunication services; (2) data storage and sharing in cyberspace; (3) services providing national or international domain names to service users in Vietnam; (4) e-commerce; (5) online payment; (6) payment intermediary; (7) connecting transportation in cyberspace; (8) social networks and social media; (9) online games; and (10) other services that provide, manage and operate information in cyberspace in the form of messages, voice calls, video calls, email, or online chatting.

Criterion 3. The incident causes "significant loss" to the legitimate rights and interests of the affected Vietnamese persons.

Where there is a data security incident, organizations must promptly take relevant measures to mitigate and notify relevant data subjects and / or relevant competent State authorities, as the case may be, in a timely manner, e.g. 5 days after detection of the security incident, and must provide an update on the incident status when it is completely resolved, Affected organizations and individuals must be notified of the data incident if the incidents fall under Criterion 2 or Criterion 3.

In the case of an incident under Criteria 1 that is beyond the control of the organization, the operator of the information system must immediately prepare an initial report on the incident to report such incident to the relevant agencies and a final report on

response to the incident within five days after finishing responding to the incident. Moreover, if the information system of a trader, organization or individual engaged in e-commerce is attacked causing risk of loss of consumer's information, the data controller must notify the authorities within 24 hours after the detection of incident.

Normally, the data controller would be required to give relevant notifications to the following State authorities:

- Local police agency (i.e. Police Department of Cybersecurity and High-Tech Crime Prevention and Fighting under the MPS with regard to offshore service providers, provincial police department where the head office of data controller is located); and
- VNCERT/CC directly managed by the AIS under the MIC.

ENFORCEMENT

Subject to specific data protection laws and the regulations breached, the sanctions in relation to data protection breaches are scattered across various different laws and regulations. In general, amongst others, the major type of sanction would be administrative penalty. For example, failure to obtain prior consent of the data subjects on collection, processing and use of their information shall be subject to a monetary fine varying from VND 10 million to VND 20 million. In serious cases, according to the Criminal Code, any person who commits illegal use of information on the computer or telecommunications network may be liable to a monetary fine varying from VND 30 million to VND 1 billion or face a penalty of up to 3 years' community sentence or 6 months –- 7 years' imprisonment; and the offender might also be liable to a monetary fine varying from VND 20 million to VND 200 million or prohibited from holding certain positions or doing certain jobs for 1 - 5 years.

Although, in practice, the Ministries have not been actively enforcing laws and regulations on data protection, individuals are increasingly aware of their data protection rights. It is foreseen that the enforcement environment will be evolving rapidly.

ELECTRONIC MARKETING

According to Vietnam's new anti-spam regulation (i.e. Decree No. 91/2020/ND-CP on anti-spam text messages, emails and calls), advertisements by text message, email and call may only be sent or made in compliance with specific requirements, notably including:

- it is prohibited to send advertising messages or make advertising calls to phone numbers on the Do-Not-Call Register;
- for phone numbers not included in the Do-Not-Call Register, only one initial advertising registration message (i.e. a message inquiring whether the user would like to receive advertising communications from the advertiser) is allowed;
- if the user refuses to receive advertising messages after receiving the initial advertising registration message, no further advertising message is allowed;
- immediately after receiving a refusal request from a user, the advertiser must terminate providing advertising messages, email or calls to such user;
- no more than three advertising messages/three advertising emails/one advertising call per day may be sent or made to the same user;
- advertising messages are only allowed from 7 a.m. to 10 p.m.; advertising calls are only allowed from 8 a.m. to 5 p.m.; and
- advertising contents must comply with advertising laws.

Once again, the traders or organizations collecting and using the consumers' personal information on E-commerce websites must have a specific mechanism for the information subjects to choose the permission or refusal of using their personal information in the cases of using personal information to send advertisements and introduce products and other commercial information.

Additionally, the organization shall not be allowed to hide their names or use unlawfully the name of others when sending advertisements via e-mail or text message. Specific information must be stated in each electronic message: for example, information about the advertiser and the advertising service provider, opt-out function (refusing acceptance of advertisements), and a label identifying "QC" or "ADV" [QC means Adv. in Vietnamese].

With regard to the method of advertising into Vietnam (i.e. to target Vietnam-based recipients), foreign organizations which do not operate in Vietnam (i.e. do not have commercial presence in Vietnam) but wish to advertise their products, goods, services

and operation in Vietnam, are required to hire a Vietnam-based advertising service provider (a company with business lines of provision of advertisement) to conduct relevant advertising activities.

ONLINE PRIVACY

To some extent, by assisting in tracking the information on a specific person, the cookies and location data could be deemed as tools preinstalled on the users' computers for collecting, storing and using their personal information, which may disclose his / her private life, e.g. hobbies, favourite websites and locations usually visited by him / her.

As such, it is currently understood that all rules on data protection are applicable to cookies as well as location data. For example, cyberspace service provider must seek for users' prior acceptance before some certain technologies (e.g. cookies, positioning service) are activated.

KEY CONTACTS

Tilleke & Gibbins
www.tilleke.com/

Waewpen Piemwichai
Senior Associate
Tilleke & Gibbins
T +84 24 3772 6688
waewpen.p@tilleke.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.