DATA PROTECTION LAWS OF THE WORLD

Vietnam

VIETNAM

Last modified 18 January 2024

LAW

In 2023, Vietnam passed its first comprehensive data protection law, namely Decree No. 13/2023/ND-CP of the Government dated 17 April 2023 on Personal Data Protection (“**PDPD**”). However, the PDPD does not supersede data protection rights and obligations set out under other legislations in Vietnam. In particular, the right of privacy and the right of reputation, dignity and honour, and the fundamental principles of such rights, are provided for in the 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. 19/2023/QH15 on Protection of Consumers' Rights, passed by the National Assembly on 20 June 2023 ("**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. 13/2023/ND-CP of the Government dated 17 April 2023 on Personal Data Protection (“**PDPD** ”);
- Decree No. 53/2022/ND-CP of the Government dated 15 August 2022 elaborating a number of articles of the Law on Cybersecurity of Vietnam ("**Decree 53**");
- 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. 91/2020/ND-CP of the Government dated 14 August 2020 on anti-spam messages, emails and calls ("**Decree 91**");

- 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**");
- Decree No. 98/2020/ND-CP of the Government dated 26 August 2020 prescribing penalties for administrative violations against regulations on commerce, production and trade in counterfeit and prohibited goods, and protection of consumer rights; as amended by Decree No. 17/2022/ND-CP of the Government dated 31 January 2022 ("**Decree 98**");
- Circular No. 12/2022/TT-BTTTT of the Ministry of Information and Communications dated 12 August 2022 on guidelines for Decree 85 ("**Circular 12**");
- 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 latest amended and supplemented by Circular No. 21/2021/TT-BTTTT dated 8 December 2021 ("**Circular 25**");
- 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**"); and
- Resolution No. 27/NQ-CP of the Government dated 7 March 2022 approving the Draft Personal Data Protection Decree ("**Resolution 27**").

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 PDPD, the Cybersecurity Law and the 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.

The PDPD took effect on 1 July 2023 without any transitional period (save in limited cases), and has affected all local and foreign enterprises which directly participate in or relate to personal data processing activities in Vietnam. The PDPD is the most comprehensive regulation governing the field of personal data protection. It sets out for the first time the key definitions of “personal data”, “sensitive personal data”, “data controller”, “data processor”, “personal data processing”, etc., which should be carefully examined in order to duly comply with the PDPD.

The PDPD is designed to have extraterritorial effect. The scope of the PDPD extends to foreign agencies, organizations and individuals directly involved in or related to the processing of personal data in Vietnam. Therefore, regardless of whether foreign entities have a local presence in Vietnam or not, to the extent that such entities are involved in the collection and processing of personal data of Vietnamese citizens, they are subject to the requirements of the PDPD.

Decree 53 took effect on 1 October 2022 and notably sets out the requirements relating to data localization and the establishment of branches / representative offices of foreign service providers, which will be discussed further below.

A Draft Decree on Sanctioning of Administrative Violations in the field of Cybersecurity ("**Draft Decree on Sanctioning**") was released by the Ministry of Public Security (“**MPS**”) for public consultation on 21 September 2021, notably including implementation guidelines for data localization requirements, together with a draft decree detailing the order of and procedures for the application of administrative sanctions against cybersecurity related violations and a draft decision of the Prime Minister promulgating a List of information systems important for national security, are being prepared by the MPS in coordination with other relevant ministries, ministerial-level agencies and bodies.

DEFINITIONS

Definition of personal data

Under the PDPD, personal data is defined as information on an electronic medium in the form of symbols, letters, numbers, photos, sounds, or the like that is associated with or helps to identify a specific individual. Information that helps to identify a specific individual is further clarified as information generated from an individual's activities that, when combined with other data and stored information, can identify a particular person.

Definition of sensitive personal data

The PDPD classifies personal data into two categories of “basic personal data” and “sensitive personal data”. Accordingly, basic personal data includes:

- surname, middle name, and birth name, alias (if any);
- date of birth, date of death or date of going missing;
- gender;
- place of birth, place of birth registration, permanent residence, current residence, hometown, contact address;
- nationality;
- personal image;
- phone number, ID card number, personal identification number, passport number, driver's license number, plate number, personal tax identification number, social insurance number; health insurance card number;
- marital status;
- family relationship information (parents, children);
- digital account information, personal data that reflects activities and activity history in cyberspace; and
- information associated with an individual or used to identify an individual other than sensitive personal data.

On the other hand, sensitive personal data includes:

- political and religious views;
- health conditions and personal information stated in health record, excluding information on blood type;
- information about racial or ethnic origin;
- information about genetic data relating to inherited or acquired genetic characteristics of each individual;
- information about physical or biological characteristics of each individual;
- information about criminals and criminal acts collected and stored by law enforcement agencies;
- information about sex life and sexual orientation of each individual;
- information on customers of credit institutions, foreign bank branches, intermediary payment service providers and other licensed institutions, including: customer identification as prescribed by law, accounts, deposits, deposited assets, transactions, organizations and individuals that are guarantors at credit institutions, bank branches, and intermediary payment service providers;
- personal location data identified via location services; and
- other specific personal data as specified by law as special and subject to necessary confidentiality measures.

Definition of Data Controller, Data Processor, Data Controller-Processor and Third Party

The PDPD also provides the definitions and roles of different stakeholders involved in the collection and processing of personal data with their respective obligations, notably:

- Data controller

A data controller is an organization or individual that decides the purposes and means of processing personal data. The controller is responsible for serving privacy notices to and obtaining consent from the data subjects, preparing and filing to the authority a Data Processing Impact Assessment (“**DPIA**”) and Cross-border Transfer Impact Assessment (“**TIA**”), notifying the authority of violations of regulations on personal data protection, ensuring and honouring the data subjects’ rights, etc.

- Data processor

A data processor is an organization or individual that processes data on behalf of the controller via a contract or agreement with the controller. Accordingly, the processor must receive and process personal data strictly in compliance with the contract or agreement with the controller. In particular, after the completion of the data processing / agreed purposes, the law requires the processor to delete and return all personal data to the controller. The processor is responsible for preparing and filing to the authority a processor’s DPIA and a TIA, notifying the controller of violations of regulations on personal data protection, etc.

- Data controller-processor

A data controller-processor is an organization or individual that jointly decides the purposes and means, and directly processes personal data. Consequently, the controller-processor must fully comply with both the responsibilities of the controller and the processor.

- Third party

A third party is defined as “an organization or individual other than the data subject, data controller or the data processor that is permitted to process personal data”.

Definition of Personal Data Processing

Under the PDPD, “personal data processing”, or “processing” is rather broad. It refers to one or multiple activities that impact personal data, including collection, recording, analysis, confirmation, storage, rectification, disclosure, combination, access, tracing, retrieval, encryption, decryption, copying, sharing, transmission, provision, transfer, deletion, destruction or other relevant activities. With such wide and open-ended definition of personal data processing, it appears that all types of activities related to personal data could be considered processing personal data and subject to the requirements prescribed by the PDPD.

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 MPS, the Ministry of Information and Communications ("**MIC**") 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:

- The MPS, particularly the Department for Cybersecurity and High-tech Crime Prevention and Fighting ("A05"), is responsible for supervision of processing of personal data and national cybersecurity, e.g. to request cyberspace service providers to (i) store data and establish branches or representative offices in Vietnam (if applicable), (ii) provide users' information for serving investigation into cybersecurity crime. The MPS has established and is managing and operating the National Portal on personal data protection; and is tasked to assess the sufficiency of personal data protection by relevant agencies, organizations and individuals;
- The MIC, particularly the AIS, is responsible for management of the provision of cyberspace services (e.g. social networks, online gaming, e-commerce, etc.), such as requesting cyberspace service providers to delete illegal data uploaded on their system/network; and
- 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 current 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 in cases where:

- 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 Decree 53);
- 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 via post or email, informing the MIC of the following information:
    - 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.

However, data controllers and data processors who collect / process personal data of Vietnamese citizens and / or collect / process personal data in Vietnam are required to submit a DPIA and / or a TIA to the authority (i.e. the A05), as the case may be.

The DPIA must be prepared in a written form and be made available at all time for the inspection and evaluation by the A05. In addition, the controller / processor / controller-processor must send an original copy of the DPIA to the A05 according to a standard form (included in the PDPD) within 60 days from the date of the personal data processing. The A05 will then appraise the DPIA and request revision if it finds that the DPIA is incomplete. Any change to the DPIA’s contents must be submitted to the A05.

Please refer to the section of “Transfer” for details relating to the requirement on preparation and submission of the TIA.

DATA PROTECTION OFFICERS

When sensitive personal data is collected and processed, information on the Data Protection Department (“**DPD** ”) and Data Protection Officer (“**DPO**”) must be notified to the authority. In practice, the notification will be made by providing the information in the DPIA and the TIA dossiers submitted to the authority.

The PDPD does not set out any specific qualifications of the person eligible to be appointed as a DPO. In practice, the DPO should be an employee of the company, rather than an external counsel. However, if the company does not have any person suitable for taking the DPO position, the company may appoint an employee of its parent company and / or affiliated company within the same organization to take the DPO position for the company, if needed.

In addition, the appointment of a DPD / DPO must be made in the form of a written decision made by the company (i.e. a board resolution or a letter of appointment signed by the company's legal representative and affixed with the stamp of the company) and a copy of this written decision is required to be submitted alongside the DPIA / TIA dossiers.

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. Consent requirements are among the most important regulations under the PDPD, and also among the most remarkable / novel changes brought about by the PDPD compared to the existing legal regime on data privacy.

Under the PDPD, the consent obtained from the data subjects must be clear, affirmative and in strict compliance with the consent form under the PDPD.

The PDPD sets out that consent must be voluntarily made based on the data subject's full understanding of (i) the purpose of the personal data processing; (ii) the type of personal data to be processed; (iii) the entities authorized to process personal data; (iv) the data subject's rights and obligations; and (v) the data to be processed that is sensitive personal data, if any. In addition, consent must be expressed clearly and specifically in writing, by voice, by ticking a consent box, by text message, by selecting consent technical settings, or via other actions which demonstrates the same. Moreover, consent must be expressed in a format that can be printed out or reproduced in writing, including in electronic or verifiable formats.

Importantly, the PDPD also explicitly points out that silence or non-response by the data subject is not construed as consent. Furthermore, consent must be made for a single purpose. That is to say, multiple purposes need to be demonstrated in a way that data subjects can give consent to one or more of them. Additionally, the data subjects may also opt to provide a partial or conditional consent.

However, the PDPD stpiulates that the processing of personal data could be carried out without consent in the following circumstances:

- In urgent cases where it is necessary to immediately process relevant personal data to protect the life or health of the data subject or others. The controller, processor, controller-processor and third party are responsible for proving such situation;
- Where the public disclosure of personal data is in accordance with the law;
- When the processing of data is performed by competent state agencies in the event of a state of emergency related to national defense, national security, social order and safety, major disaster, or dangerous epidemic; when there is a threat to security and national defense but not to the extent that a state of emergency must be declared; or when the processing is to prevent and combat riots and terrorism, crimes, and violations of the law;
- When the processing is to fulfill the contractual obligations of the data subject with relevant agencies, organizations, and individuals as prescribed by law; or
- When the processing is to serve the activities of state agencies prescribed by sector-specific laws.

In addition, the PDPD allows data subjects to withdraw their consent given. However, such consent withdrawal shall not affect the lawfulness of the processing to which consent was given before it was withdrawn. The withdrawal of consent shall be expressed in a format that can be printed and reproduced in writing, including in electronic or verifiable format.

In addition, the traders and organizations collecting and using consumers' personal information on E- commerce websites shall not require 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; or
- Collection of personal information for performing other obligations in accordance with the 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 PDPD defines cross-border personal data transfer as any activity involving the use of cyberspace, electronic equipment, electronic means or other forms to transfer personal data of Vietnamese citizens to a location outside Vietnam. The use of a location outside Vietnam to process Vietnamese citizens’ personal data is also considered cross-border transfer of personal data, including:

i. Organizations, enterprises or individuals transferring personal data of Vietnamese citizens to organizations, enterprises or management bodies located overseas for processing in accordance with the purposes consented by the data subjects;
ii. Processing of personal data of Vietnamese citizens by use of automated systems located outside of Vietnam by the controller, controller-processor or processor in accordance with the purposes consented by the data subjects.

Given the foregoing, the transfer of personal data to other companies which are located overseas or processing of personal data of Vietnamese citizens merely by servers located overseas, without any local presence in Vietnam, are both considered cross-border transfer of personal data and subject to relevant requirements of the PDPD, notably the preparation and submission of the TIA to the authority.

The TIA shall be made available at all times for the inspection and evaluation by the A05/the MPS. In addition, the transferor shall send one original copy of the TIA to the A05 according to a standard form issued under the PDPD within 60 days from the date of the personal data processing. The A05 will then appraise the TIA and request the transferor to revise the dossier in case it finds that the TIA is incomplete. Moreover, any change to the TIA’s contents must be submitted to the A05 within 10 days from the date of request.

In addition to the above requirements, it is worth noting that data localization could also be imposed on certain businesses providing services in Vietnam. The data localization requirements are 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 Decree 53, 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 Decree 53, while all domestic organizations providing telecoms services and online services to customers in Vietnam would be required to store their customer data in Vietnam, the foreign organizations which could be subject to the foregoing data localization requirements only include those engaging in the following 10 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. Pursuant to Decree 53, only the following types of data is required to be stored in Vietnam:
    - Data on personal information of service users: i.e. data on information in the form of symbols, letters, numbers, images, sounds, or equivalent to identify an individual (“**Personal Data**”);
    - Data created by service users in Vietnam: i.e. data on information in the form of symbols, letters, numbers, images, sounds, or equivalent reflecting the process of participating, operating, and using cyberspace of service users and information on devices and network services used for connection with cyberspace in the territory of the Socialist Republic of Vietnam. It should be noted that the information under this category of data which is required to be stored in Vietnam only includes information on service account name, service usage time, credit card information, email address, IP addresses for the latest login and logout, registered phone number associated with account or data (“**Account Data**”); and
    - Data on the relationships of service users: i.e., data on information in the form of symbols, letters, numbers, images, sounds, or equivalences reflecting and identifying relationships of service users with other people in

cyberspace. Decree 53 further specifies that the information under this category of data which is required to be stored in Vietnam only includes information on friends and groups with which the service user connects or interacts in cyberspace (“**Relationship Data**”).

Moreover, foreign enterprises engaging in the abovementioned services are also required to establish branches or representative offices in Vietnam in case the authority alerts them that their services / online platforms have been used to commit violations of Vietnam’s laws but failed to remedy upon the request of the authority. The time for such establishment shall commence when the enterprises receive the request to do so until such enterprises terminate their operation in Vietnam or the prescribed services are no longer available in Vietnam.

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; and
- 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.

Under the PDPD, the data controller and processor shall implement the following personal data protection measures:

a. General personal data protection measures, including:
    i. Management measures adopted by an organization or individual related to processing of personal data;
    ii. Technical measures adopted by an organization or individual related to processing of personal data;
    iii. Measures adopted by a competent authority according to regulations in the PDPD and relevant law;
    iv. Investigation and procedure measures adopted by a competent authority;
    v. Other measures as prescribed by law.
b. Data protection measures applicable to the processing of basic personal data, including:
    i. Formulation and promulgation of regulations on personal data protection, which specify tasks to be performed in accordance with the PDPD;
    ii. Encouragement of application of standards of personal data protection in conformity with fields, industries and activities related to the processing of personal data;
    iii. Cybersecurity inspection for systems, means and equipment for processing of personal data before processing, permanent deletion or destruction of devices containing personal data.

c. Data protection measures applicable to the processing of sensitive personal data, including: appointment of a department with the function of protecting personal data (i.e. DPD) and personnel in charge of protection of personal data (i.e. head of the DPD (i.e. DPO)), and notification about the establishment of the DPD and the appointment of the DPO to the A05;
d. Notification to the data subject about the sensitive nature of the personal data to be processed; and the processing of such sensitive person.

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.

Criterion 4: The PDPD sets out a new reporting requirement that upon detection of any violation against regulations on personal data protection (which can be interpreted to include data breach incidents), the controller / controller-processor shall notify the A05 within 72 hours of the occurrence of such violation. The reason for late notification, if any, must be provided.

The information to be notified will include:

i. Description of the nature of the violation, including: time, place, violation, organization, individual, types of personal data and the amount of relevant data;

ii. Contact details of the employee(s) assigned to protect the data or organizations or individuals that are responsible for protecting personal data;
iii. Description of consequences and damage that may occur;
iv. Description of measures for handling and minimizing the harm caused by the violation.

If the abovementioned contents cannot be fully notified, the notification may be made in multiple stages. Thereafter, the controller / controller-processor shall prepare written minutes confirming the occurrence of the violation of the regulations on personal data protection, and coordinate with the A05 to handle the violation. In practice, as the 72-hour timeframe is very tight, more often than not, data controllers find it very challenging to comply with this timeframe. To the best of our knowledge, the regulator has not yet penalized any data controllers that file the report, but failed to meet the deadline.

In addition to the four criteria mentioned above, there are also data breach notification requirements imposed by sector-specific laws / regulation, such as laws / regulations governing financial services, e-commerce services, etc.

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.

As of early 2024, the MPS is preparing to promulgate the Draft Decree on Sanctioning. Once this decree takes effect, the MPS will have a basis to start imposing sanctions on non-compliance with the requirements under the PDPD.

This Draft Decree on Sanctioning was first released for public comments in September 2021, and its updated version was released to the public for the second round of consultation on 31 May 2023. The official Decree on Sanctioning is expected to be adopted by the middle of 2024.

Violators of the PDPD’s regulations, depending on the severity of their violations, may be warned, disciplined, or face administrative penalties or criminal prosecution. Generally, for PDPD-associated violations, the Draft Decree on Sanctioning has proposed a monetary fine of up to VND 1 billion (approx. USD 42,500). Additional penalties, applicable to certain violations, include: (i) deprivation of the right to use licenses for business lines requiring personal data collection; (ii) confiscation of exhibits and means of administrative violations. Remedial measures include: (i) 1-3 months of forcible suspension of processing personal data; (ii) forcible destruction or unrecoverable deletion of personal data; (iii) forcible return of illegal profits obtained from the violations; (iv) public apology; (v) forcible implementation of personal data processing notification measures; (vi) forcible personal data provision; (vii) forcible request to allow personal data correction; (viii) forcible implementation of personal data protection measures.

Notably, under the Draft Decree on Sanctioning, a penalty of up to 5% of the violating enterprise’s turnover of the immediately preceding fiscal year in the Vietnamese market applies to:

a. disclosing and misplacing the personal data or cross-border transfer of 5 million data subjects who are Vietnamese citizens; and
b. a second violation of the regulations on:
    - personal data protection in marketing and advertising activities; and
    - illegal collection, transfer, purchase and selling of personal data.

In addition, the MPS has set up a National Portal of Personal Data Protection to receive reports on violation of the PDPD. Once this portal is fully operational, companies are expected to be more vulnerable to inspection actions in this area, as the portal would enable data subjects like employees or clients to easily report on companies’ acts of non-compliance with the PDPD and breach of their personal data.

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
Counsel
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.