VIETNAM

Data Protection Guide

January 2024

Indochine Counsel

Business Law Practitioners

Contents

Abbreviation

A05	Department of Cybersecurity and Hi-tech Crime Prevention
GDPR	General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC)
GOV	Government of Vietnam
MIC	Ministry of Information and Communications
MOIT	Ministry of Industry and Trade
MPS	Ministry of Public Security
NPBR	National Portal for Business Registration (https://dangkykinhdoanh.gov.vn/en/Pages/default.aspx)
NPDP	National Portal for Personal Data Protection (https://baovedlcn.gov.vn)
OPDTIA	Overseas Personal Data Transfer Impact Assessment
PDPIA	Personal Data Processing Impact Assessment
SBV	State Bank of Vietnam
VND	Vietnamese Dong

Overview

Information and data have become a precious “resource” in every aspect of contemporary life. Information exchange contributes to many aspects of the global economy, such as through business development, customer care, state management, etc. From business know-how and trade secrets to customer information and personal data, the possession of valuable information brings advantages to those who possess it. This has led to the massive, frequent and widespread dissemination of such information.

With the increase of the global cyber population, cyberspace is becoming a go-to environment for unauthorized personal information exchange or worse, cybercrime. Discerning this practice, regulators in Viet Nam have been putting non-stop effort into the formation of consolidated data protection legislation. While business know-hows and trade secrets are protected under the intellectual property (IP) regulations, the legal framework for managing and protecting the exchange of personal information is now ‘updated’ by the enactment of Decree No. 13/2023/ND-CP of the GOV, meeting the need to unify data protection regulations in Vietnam in order to catch up with the rapidly-changing data environment.

Data protection rules in Vietnam

Personal information / data

Entities involved in personal information / data protection

Back when the legal system in Vietnam had not had a consolidated legal document regarding data protection, definitions of entities involved in personal data protection and regulations applicable to these subjects were spread across different laws and regulations. However, with the promulgation of Decree No. 13/2023/ND-CP, entities participating in personal information / data protection can be identified as:

- ✓ Data Subject: means the individual being reflected by personal data;
- ✓ Personal Data Controller: means the entity (organization / individual) deciding the purpose for and the method of personal data processing;
- ✓ Personal Data Processor: means the entity (organization / individual) performing the personal data processing on behalf of the Personal Data Controller under a contract or agreement;
- ✓ Personal Data Controller and Processor: means the entity deciding the purpose for and the method of as well as directly performing the personal data processing; and
- ✓ Third Party: means the entity being allowed to process personal data other than the aforementioned subjects.

Consequently, entities involved in personal data protection can now have basis to primarily identify their role, be aware of their legitimate rights and obligations, as well as understand how to stay compliance.

Under Decree No. 13/2023/ND-CP, the regulators primarily in charge of data protection in Vietnam include the MIC and the MPS (or more particularly, the A05 under the MPS). While the MIC plays the role of a central policy-making and regulatory body in the fields of information technology, electronics, foreign information, domestic information, and national information and communication infrastructure, the MPS is primarily responsible for those cybersecurity issues related to national defense, national order and prevention of high-tech crimes, etc. In specialized sectors, data protection issues will be managed by specialized authorities (e.g., the MOIT for e-commerce sector, and the SBV for banking / financial sector).

Fundamental principles for personal information / data protection

One of the first types of data that has been protected under Vietnamese laws is an individual's image. The 1995 Civil Code clearly provided the moral right of each person in respect of his/her image and required other persons or entities not to use a person's image without his/her consent. These regulations remained in the 2005 Civil Code as well as the current 2015 Civil Code. Per the 2015 Civil Code, other information types attached to an individual were also protected, including information on private life, personal and family secrets. The various versions of the Civil Code have consistently placed the foundation for subsequent data protection regulations, forming one basic and prerequisite principle in respect of dealing with personal data, namely, to obtain the data subjects' consent. With the enforcement of Decree No. 13/2023/ND-CP, this principle is further detailed and supplemented, entitling data subject to specific rights in respect of their personal data, including inter alia, the right to know about, the right to access, delete and provide, the right to give and withdraw consent to, as well as the right to restrict and object the processing of their personal data.

The official definition of "*personal information*" was provided in Decree No. 64/2007/ND-CP on applying information technology in activities of state management authorities. Accordingly, "*Personal information means information which is adequate to accurately identify the identity of an individual, covering at least one of the following information: full name, date of birth, profession, title, contact address, e-mail address, telephone number, ID number and passport number. Personal secrets include medical records, tax payment dossiers, social insurance card numbers, credit card numbers and other personal secrets*". Later on, the 2015 Cyberinformation Security Law also defined personal information as "*information attached to the identification of one person*". Most recently, a unified definition of personal data has been provided under Decree No. 13/2023/ND-CP in a more comprehensive way rather than enumerating method. In particular, "*personal data*" is defined as "*information in the form of symbol, letter, number, image, sound or the like in electronic environment which is attached to or helps to identify a specific person. Personal data includes basic personal data and sensitive personal data*", wherein, information which helps to identify a specific person is "*those generated from an individual's activities, which is capable of identifying a persona when being combined with other stored data, information*". As a result, lists of basic personal data as well as sensitive personal data are also regulated in Decree No. 13/2023/ND-CP, providing a clear basis for personal data classification.

Personal information / personal data is also mentioned in other specialized laws and under various forms for the purpose of professional management in a particular sector (e.g., information on health

status and private life in the 2009 Law on Medical Examination and Treatment; taxpayers' information in the 2006 Law on Tax Management; and consumers' information in the 2010 Law on Protection of Consumers' Rights which will be superseded by the 2023 Law on Protection of Consumers' Rights in mid-2024; etc.). In addition, specialized laws also provide specific principles to protect personal data in respective sectors (e.g., Decree No. 72/2013/ND-CP and Decree No. 52/2013/ND-CP which were subsequently promulgated, etc.).

In general, the most common principles for data protection include:

Principle 1: To obtain consent from the information / data subject

Prior to the promulgation of Decree No. 13/2023/ND-CP, this principle was stated in different pieces of legislation, including the 2015 Civil Code, Article 21 of the 2006 Information Technology Law, and Article 17.1(a) of the 2015 Cyberinformation Security Law. In general, these regulations require that before processing one's personal data the processor must first obtain the consent of that person, unless otherwise stated by the law. The definition of "*personal data processing*" is only provided under the 2015 Cyberinformation Security Law, being "*the implementation of one or some actions of collecting, editing, using, storing, providing, sharing and disseminating personal information online for commercial purposes*". A similar definition is not provided in the 2006 Information Technology Law.

Under Decree No. 13/2023/ND-CP, the requirement of obtaining Data Subject's consent comes with certain conditions for such a consent to be deemed valid. In particular, the validity of a Data Subject's consent depends on whether such data subject is voluntarily and clearly be aware of the type of and the purposes for which their personal data being processed, the entities allowed to conduct such processing, as well as the Data Subject's rights vested by the laws. Furthermore, such a consent must be stated in an explicit form (e.g., text, voice, clickwrap, etc.) which is printable and copiable (including electronic or verifiable forms). Consequently, a Data Subject's silence or no response shall not be deemed an acceptance. Notably, such a consent can be partial or conditional. A definition of "*personal data processing*" is also provided under Decree No. 13/2023/ND-CP, quoted as follows: "*personal data processing means one or some activities effecting personal data such as: collecting, recording, analyzing, confirming, storing, editing, publishing, combining, accessing, retrieving, recalling, encoding, decoding, copying, sharing, transmitting, providing, transferring, deleting, destroying personal data, or other related activities*".

Currently, under Decree No. 15/2020/ND-CP, collecting personal data without the prior consent of the data subject in terms of the scope and purposes for such collection is subject to a fine up to VND20 million (for organizations) or VND10 million (for individuals) as an administrative sanction. In the case of using a person's image in violation of this Principle 1, as per the 2015 Civil Code, the owner of such image is entitled to request for compensation by a court order, as well as other legally allowed remedial measures. Despite, the current legal system lacks specific legislation on sanctions in personal data protection.

As stated in Article 22.2 of the Information Technology Law, Article 17.1(c) of the 2015 Cyberinformation Security Law, and Article 6.2(dd) of the 2010 Law on Protection of Consumers' Rights (which will be superseded by the 2023 Law on Protection of Consumers' Rights in mid-2024),

once the consent to process a person's personal data is obtained, the entities in possession of such data are only allowed to transfer such personal data / information to third parties upon obtaining the data subject's consent. Violations of this requirement may lead to a fine up to VND30 million (for organizations) or VND15 million (for individuals) in addition to a remedial measure of destruction of the violating personal information.

Principle 2: To use the collected information / data within the scope and purposes of the consent

Personal data processors must notify data subjects in advance regarding to what extent and for what reason their personal information is to be handled. The obtained consent, therefore, is limited only in the scope and purposes as set forth in the notification from the data processors. This Principle 2 can be found in Article 17.1(a) of the 2015 Cyberinformation Security Law, Article 21.2(a) of the 2006 Information Technology Law, Articles 2.2(a) and 2.2(b) of the 2010 Law on Protection of Consumers' Rights, and Article 11.4 of Decree No. 13/2023/ND-CP.

Violations of this principle may lead to an administrative sanction of VND30 million (for organizations) or VND15 million (for individuals).

Principle 3: To ensure the information / data subjects' rights vested by law

On the basis of the right to have one's personal information protected, the laws provide specific rights to data subjects, which were previously scattered in different pieces of legislation (e.g., the right to access their personal data in possession of a processor (*Article 17.3, the 2015 Cyberinformation Security Law*), the right to request an update and/or rectification of inaccurate personal data (Article 18, the 2015 Cyberinformation Security Law)). As mentioned above, these rights have been gathered under Article 9 of Decree No. 13/2023/ND-CP.

Depending on its nature, a violation of this Principle 3 shall give rise to different rates of fines. For example, the act of continuing to provide personal data to third parties despite a cessation request from a data subject will face a fine of VND20 million (for organizations) or VND10 million (for individuals).

Principle 4: To prepare, submit and maintain the PDPIA and OPDTIA Dossiers

One remarkable point newly added in Decree No. 13/2023/ND-CP is the requirement on preparing, submitting and maintaining the PDPIA Dossier and OPDTIA Dossier. This requirement varies depending on relevant role of entities involved in personal data processing activities (as presented in the Section "*Entities involved in personal information / data protection*" below), in particular:

PDPIA Dossier: Personal Data Controller, Personal Data Controller and Processor shall prepare and maintain the PDPIA Dossier from the point starting processing personal data. Meanwhile, Personal Data Processor shall act the same in case concluding a contract with Personal Data Controller to process personal data thereunder. Depending on the role, the information to be declared in the PDPIA Dossier varies. In general, the content of the PDPIA to be conducted by Personal Data Processor is

somehow less complex than that of Personal Data Controller and Personal Data Controller and Processor. However, certain minimum contents must be included, such as information and contact details of the entities preparing the Dossier, types of personal data being processed, processing time, etc.

OPDTIA Dossier: This is one of the prerequisite conditions to legitimately transfer personal data of Vietnamese citizen offshore. According to Decree No. 13/2023/ND-CP, the entity conducting overseas personal data transfer include: Personal Data Controller, Personal Data Controller and Processor, Personal Data Processor, and Third Party, who is also the subject required to prepare, submit and maintain the OPDTIA Dossier. Contents of an OPDTIA Dossier are majorly similar to those of a PDPIA Dossier, further including specific information related to overseas personal data transferring activities such as: description and explanation of the purpose(s) of personal data processing activities after being transferred offshore; documents evidencing the commitment and obligations between the transferer and receiver of personal data in respect of personal data processing; etc.

Both of the PDPIA Dossier and OPDTIA Dossier must always be available to serve the inspection and assessment purposes of the competent agencies, shall be submitted to the A05 under the MPS and subsequently supplemented, amended in accordance with A05's instructions, if any. The submission of both Dossiers can be conducted directly to the A05, via postal service, or online through the NPDP, which also provides step-by-step instructions for dossiers filing as well as function for convenient management of successfully lodged Dossiers. Furthermore, via the NPDP, users can also access helpful information, including pivotal regulations related personal data protection. With a sleek and tidy design, the NPDP is accessible for most users. The operation is quite smooth and effortlessly navigating. Users can easily login using their identification accounts granted by the National Portal, by the MPS (via VNeID mobile application), or by the Vietnam Post.

So far, there is yet to be any guideline on detailed implementation of Decree No. 13/2023/ND-CP in general, and on the preparation of the PDPIA Dossier and OPDTIA Dossier in particular. Decree No. 13/2023/ND-CP is also silent on a grace period, which can be implied that any of its regulation shall be in force once it took effect on 1 July 2023. This fact brings certain burdens to entities subject to the government of Decree No. 13/2023/ND-CP, rushing them to comply despite the fact that no particular sanction has been provided for non-compliance.

Corporate information

For the purpose of transparency and protecting the party at a natural disadvantage in the relationship with enterprises, i.e., consumers, information attached to the identification of one enterprise / company is published on open sources of the State management agencies, as well as on websites of the enterprise / company in accordance with the laws of Vietnam (the "**Public Enterprise Information**"). In particular, enterprise registration information (e.g., company name, active status, legal representative, tax code, etc.) are all published on the NPBR. Some of the information is protected under the law, namely trademarks and enterprise names (see the 2005 Intellectual Property Law).

Besides the Public Enterprise Information, enterprises also have non-public information, typically such

as business secrets, trade secrets, know-how, etc. (the "**Non-Public Enterprise Information**"). According to the 2005 Intellectual Property Law (as revised in 2009 and 2019), "*trade secret means information obtained from activities of financial or intellectual investment, which has not yet been disclosed and which is able to be used in business*". Business / trade secrets are protected under the 2005 Intellectual Property Law if satisfying the following conditions:

- ✓ The relevant trade secret is neither common knowledge nor easily obtainable;
- ✓ When used in business activities, the trade secret will create for its holder advantages over those who do not hold or use it; and
- ✓ The owner of the trade secret maintains its secrecy by necessary means so that the secret will not be disclosed nor be easily accessible.

Secrets related to personal identification, state management, national defense and security, and other secrets not related to business are not qualified for protection under the 2005 Intellectual Property Law as trade secrets.

Stealing, disclosing, transferring or selling information in terms of trade secrets of an enterprise will result in a fine up to VND40 million (for individuals, twice as much for organizations) under Decree No. 98/2020/ND-CP. In case the party disclosing the trade secret has legal and appropriate access to an enterprise's trade secrets but fails or neglects to ensure the security of the same, a fine under Decree No. 98/2020/ND-CP of VND20 million (for individuals, twice as much for organizations) is applied.

Certain exceptions exist where the owner of trade secrets cannot prohibit others from using the same, including their disclosure of the concerned trade secret for community protection purposes or independently; using the concerned trade secret not for commercial purposes; etc.

Non-stop effort to meet the rising demand for data protection

With the rapid development and diversity of data and information, the demand for information protection has significantly increased, especially the protection of personal information in cyberspace. Given that, the GOV has been working non-stop to complete the legal system to cover this area.

In 2013, the Government promulgated Decree No. 72/2013/ND-CP regulating the management, provision and use of internet services and online information.

Also in 2013, the Government promulgated Decree No. 52/2013/ND-CP to govern the sector of e-commerce, supplemented by guiding Circular No. 59/2015/TT-BCT in 2015, and most lately amended by Decree No. 85/2021/ND-CP. Apart from those procedural and conditional regulations applicable to e-commerce operations, regulations in terms of data protection under this legislation are for the purpose of protecting consumers' rights. Decree No. 52/2013/ND-CP provides that if a consumer's personal information is collected via an e-commerce website, the collecting entity must publish an information protection policy (i.e., privacy policy) at an easy-to-see location on their website.

Furthermore, owners of e-commerce websites with an online ordering function must publish the privacy policy on protection of customers' payment information on their website.

The next remarkable steps taken by the state authorities in response to the rising demand for data protection was the promulgation of the Cybersecurity Law in 2018. The Cybersecurity Law's regulations aim at data protection for the purpose of ensuring national defense and security. Under the Cybersecurity Law, requirements on data protection, as well as the main principles mentioned in Section "*Founding regulations related to data protection*" above have been extended to reach an international scope. This is illustrated by the requirements on data localization and branch/representative office establishment in respect of foreign enterprises providing services on telecommunications networks, on the internet and providing value added services in Vietnam's cyberspace, and that handle (collect, exploit, analyze, process, etc.) personal information of users from Vietnam.

In the same year, the State Secrets Protection Law was ratified, under which, "*state secrets mean information with important contents as identified by heads of competent agencies and/or organizations in accordance with the State Secrets Protection Law, which are not published, and are potentially harmful to the country and nation's interests if disclosed and/or lost*". Under the State Secrets Protection Law, any illegal collection, exchange, provision and transfer of state secrets, as well as any other actions which potentially cause harm, leakage and disclosure to state secrets is prohibited. The act of willingly leaking state secrets; appropriating, trading or destroying state secrets items and/or documents may constitute criminal offences under the Criminal Code.

Most recently, the formation and application of Decree No. 13/2023/ND-CP provides the very first ever legal framework for the protection of personal data. In a general view, Decree No. 13/2023/ND-CP adheres to the key rules of the GDPR with characterized adoption to make it suitable for and enforceable in Viet Nam. Notwithstanding, Decree No. 13/2023/ND-CP is set to be more of a framework with general regulations rather than digging into detailed instructions.

Consumers' data protection

Data subjects often have their data collected in the position as consumers when entering into transactions with goods sellers and/or services providers. As such, regulations in the sector of consumers' rights protection also govern this issue, particularly the 2010 Law on Protection of Consumers' Rights (which will be superseded by the 2023 Law on Protection of Consumers' Rights in mid-2024) and its guiding regulations. Here, too, the core of the main principles mentioned in Section "*Fundamental principles for personal information / data protection*" is inherited (except for Principle 4 which has just been updated with the promulgation of Decree No. 13/2023/ND-CP). However, as the regulators opine that consumers are disadvantaged in their relationship with goods sellers / services providers, sanctions applicable to sellers / service providers for violations are stricter, including those in terms of data protection. For instance:

- ✓ With regards to violations of Principle 2 as mentioned above, if the information / data subjects are consumers, purchasing goods and/or using services provided by the violating entities, the fine will be VND40 million (for organizations) or VND20 million (for individuals) under Decree

No. 98/2020/ND-CP, and will be doubled if the information involved in the violation is a personal secret;

- ✓ For violations of transferring personal data to third parties without consent of the information / data subjects, if the information / data subject is a consumer, the fine will be up to VND40 million (for organizations) or VND20 million (for individuals), and doubled if the information involved in the violation is a personal secret; and

- ✓ In addition, the act of stealing, disclosing, transferring or selling personal information of consumers in the e-commerce sector will result in a fine up to VND40 million (for individuals, twice as much for organizations) under Decree No. 98/2020/ND-CP.

Under the 2023 Law on Protection of Consumers' Rights, regulations on protection of consumers' information have been specified to achieve a more comprehensive and effective protection, as well as to conform with Decree No. 13/2023/ND-CP, on the basis of keeping the core principles as previously explained. Accordingly, the 2023 Law on Protection of Consumers' Rights identifies the entities being allowed to process consumers' information with respective applicable obligations and requirements.

Conclusion

Decree No. 13/2023/ND-CP coming to force marks a significant milestone in the development of Vietnam legal system, claiming itself as the very first official consolidated legislation for personal data protection, conforming with the worldwide legislative trends. Despite the fact that more guidelines are required for a straightforward and stable implementation Decree No. 13/2023/ND-CP, its impact toward the personal data protection practices in the country is undeniable. All transformations lead to the race for adoption. With the enactment of Decree No. 13/2023/ND-CP, more legislative amendments can be expected to take place, putting both competent agencies and enterprises in standby mode to react to any possible compliance requirement.

Contact Us

For more information or assistance, please contact us:

Nguyen Thi Hong Anh
Partner, Head of IP&T Practice Group
anh.nguyen@indochinecounsel.com

Dang The Duc
Managing Partner
duc.dang@indochinecounsel.com

Thai Gia Han
Associate
han.thai@indochinecounsel.com

Tran Tu Xuan
Legal Assistant
xuan.tran@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