Data Protection in Vietnam: Overview

LE TON VIET, RUSSIN & VECCHI, WITH PRACTICAL LAW DATA PRIVACY ADVISOR

Search the Resource ID numbers in blue on Westlaw for more.

A Q&A guide to data protection in Vietnam.

This Q&A guide gives a high-level overview of data protection rules and principles, including obligations on the data controller and the consent of data subjects, rights to access personal data or object to its collection, and security requirements. It also covers cookies and spam, data processing by third parties, and the international transfer of data. This article also details the national regulator, its enforcement powers, and sanctions and remedies.

To compare answers across multiple jurisdictions, visit the Data Protection Country Q&A tool.

REGULATION

LEGISLATION

1. What national laws regulate the collection and use of personal data?

GENERAL LAWS

Vietnam provides a general framework for data protection in its Law on Network Information Security No. 86/2015/QH13 (Nov. 19, 2015).

Personal data protection is a constitutional right in Vietnam. The right is often reflected in other pieces of legislation as well. The rules for the collection, storage, processing, use, disclosure, and publication of personal data are also set out in Vietnam's Civil Code 2015 and in sectoral laws. These rules are drafted in broad language and are open to interpretation. That is, the application of these rules is not always clear. There is no repository for precedent.

SECTORAL LAWS

Data protection rules can also be found in the following sectoral laws, as amended:

- The Law on Electronic Transactions No. 51/2005/QH11 (Nov. 29, 2005). This law governs e-transactions by state agencies, and the civil, business, commercial, and other private sectors.
- The Law on Cinematographic No. 62/2006/QH11 (June 29, 2006). This law sets out rights and obligations for those involved in activities involving the film, cinematography, and television industry.
- The Law on Information Technology No. 67/2006/QH11 (June 29, 2006). This law governs information technology applications and development efforts, and sets out the rights and obligations of agencies, organisations, and individuals engaged in these activities.
- The Law on Telecommunications No. 41/2009/QH12 (Nov. 23, 2009). This law regulates telecommunications activities and the rights and obligations of those working in the telecommunication industry.
- The Law on Credit Institution No. 47/2010/QH12 (June 16, 2010). This law governs the establishment and operations of credit institutions in Vietnam.
- The Law on Postage No. 49/2010/QH12 (June 17, 2010). This law governs the administration of the postal service.
- The Law on Protection of Consumers' Rights No. 59/2010/QH12 (Nov. 17, 2010). This law sets out a variety of consumer rights, along with obligations for organisations and potential liability for violations of consumer rights.
- The Law on Publication No. 19/2012/QH13 (Nov. 20, 2012). This law sets out the rights and obligations of individuals and organisations in the publishing industry.
- The Press Law No. 103/2016/QH13 (Apr. 5, 2016). This law governs the press, including citizens' rights to freedom of press and freedom of speech in the press and the rights and obligations of agencies, organisations, and individuals involved in the media industry.

- The Law on Cybersecurity No. 24/2018/QH14 (June 12, 2018). This law regulates cyber activities that impact national security and social order and safety.
- The Ordinance on Protection of State Secrets No. 30/2000/PL-UBTVQH10 (December 28, 2000). This ordinance sets out the basics involving state secrets and specifies the different levels of State Secrets. This Ordinance will be replaced on July 1, 2020 by the Law on Protection of State Secrets No. 29/2018/QH14 (November 15, 2018)

SCOPE OF LEGISLATION

2. To whom do the laws apply?

Generally, the protections for personal data and privacy set forth in Vietnamese law apply to both:

- The personal data and privacy of all natural persons within Vietnam, regardless of nationality.
- Any personal data processed by a processor in Vietnam.

The Law on Network Information Security No. 86/2015/QH13 (Nov. 19, 2015) regulates the following subjects relating to personal data:

- Data subjects, who are identified or identifiable from personal data.
- Processors, who are individuals or entities that process personal data.

The concept of a data controller does not exist in Vietnam. Under Vietnamese law, both a data controller and a third-party processor are considered to be data processors.

- For more on personal data, see Question 3. For more on processing personal data, see Question 4.

3. What data is regulated?

Personal data is defined as any information which relates to the identification of a data subject (Law on Network Information Security No. 86/2015/QH13 (Nov. 19, 2015), Article 3.16). This includes any information that relates to a data subject's:

- Personal life, such as name, date of birth, address, telephone number, identification number, or email address.
- Personal or family secrets.
- Personal communications, including written correspondence and the content of telephone calls.

(*Article 38, Civil Code 2015.*)

The Vietnamese government labels information as state secrets when:

- The information elates to a case, a circumstance, a document, an object, a location, a time, or a speech that contains important content in the fields of:
  - politics;
  - national defense;
  - national security;
  - foreign affairs;
  - economy;
  - science;
  - technology; or
  - other subjects designated by the government.
- The disclosure of the information may cause harm to the State of the Socialist Republic of Vietnam.

There are three levels of state secrets, each of which enjoys different levels of protection:

- Absolute secret.
- Top secret.
- Secret.

4. What acts are regulated?

Vietnamese law generally regulates the processing of personal data. The Law on Network Information Security No. 86/2015/QH13 (Nov. 19, 2015) (LNIS) defines processing personal data as engaging in one or more of the following activities with personal data:

- Collecting.
- Editing.
- Using.
- Storing.
- Providing to any third party.
- Transferring.
- Sharing.
- Publishing.

(*Article 3.17, LNIS*)

5. What is the jurisdictional scope of the rules?

The Law on Network Information Security No. 86/2015/QH13 (Nov. 19, 2015) and sectoral laws generally apply to the processing of personal data conducted by a processor located in both:

- Vietnam.
- Outside of Vietnam, if the processing relates to data subjects who are:
  - located in Vietnam; or
  - of Vietnamese nationality, meaning they hold a Vietnamese birth certificate, identification document, passport, or a decision of Vietnamese naturalization, of restoration of Vietnamese nationality, or of adoption of a Vietnamese child.

Processors located outside of Vietnam are not required to appoint a local representative for purposes of complying with Vietnamese law.

6. What are the main exemptions (if any)?

The Law on Network Information Security No. 86/2015/QH13 (Nov. 19, 2015) (LNIS) provides two primary exemptions from the data protection rules:

- The processing of personal data carried out by a competent authority or on the decision of a competent authority supported by law. The law does not define a competent authority in this context.
- The processing of personal data to:

- ensure national security;
- protect national defense;
- maintain public order; or
- meet non-commercial objectives in accordance with relevant laws.

(*Article 16.5 and 17.1(c), LNIS*)

NOTIFICATION

7. Is notification or registration required before processing data?

No.

MAIN DATA PROTECTION RULES AND PRINCIPLES

MAIN OBLIGATIONS AND PROCESSING REQUIREMENTS

8. What are the main obligations imposed on data controllers to ensure data is processed properly?

Before processing personal data of a data subject, the Law on Network Information Security No. 86/2015/QH13 (Nov. 19, 2015) (LNIS) requires the processor to:

- Obtain the consent of the data subject. For more on consent, see Question 9.
- Publish its policy regarding the processing and protection of personal data.
- Provide an adequate level of protection for the personal data, following the technical standards for protection of personal data.

LNIS requires all of these elements to be satisfied before processing the personal data.

Because LNIS does not define "an adequate level of protection" and "technical standards," data processors should implement an internationally recognized or higher standard to protect personal data, such as those set by the EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR).

For information on the GDPR standards for adequate protection and technical and organisational measures that data controllers and processors must meet, see Practice note: overview, Overview of EU General Data Protection Regulation: Obligations of controllers and processors (W-007-9580).

9. Is the consent of data subjects required before processing personal data?

While the Law on Network Information Security No. 86/2015/QH13 (Nov. 19, 2015) requires organisations to obtain a data subject's consent before processing that personal data, there is no specific requirement on the form or the content of consent. Because the nature and level of consent required is ambiguous, prudent organisations should record consent physically or electronically, and should not consider consent to be implied.

Vietnamese law defines persons 16 years old or younger to be minors. To process the personal data of a minor, an organization must obtain the consent of the minor's parent or guardian.

10. If consent is not given, on what other grounds (if any) can processing be justified?

An individual or an entity may collect, use, and process the personal data of a data subject without consent if the processing is used to:

- Comply with obligations provided in the law.
- Execute, adjust, or perform contracts for the use of data, goods, or services over a network environment.
- Calculate premiums, fees for the use of data, goods, or services over a network environment.

(*Article 21.3, Law on Information Technology No. 67/2006/QH11 (June 29, 2006)*.)

The Law on Network Information Security No. 86/2015/QH13 (Nov. 19, 2015) does not list any exceptions to the consent requirement or any other legal bases justifying the processing of personal data.

SPECIAL RULES

11. Do special rules apply for certain types of personal data, such as sensitive data?

Certain types of personal data, such as bank account balances and medical records, are considered state secrets and enjoy additional protection. The rules for handling state secrets are provided in Decree 33/2002/ND-CP (March 28, 2002) as follows:

- Documents and objects containing state secrets must be:
  - stamped with Government-issued stamps for the which reflect the respective level of state secret (*see* Question 3);
  - stored in a secure container in a secure location;
  - removed from a secure location only with the approval of the authority managing the state secrets and if the removal is recorded;
  - disposed of in an irreversible manner and only with the approval of the authority managing the state secrets; and
  - encrypted, when the information is sent electronically.
- Reproduction, printing and scanning of the documents and objects containing state secrets must be done:
  - in a secure location;
  - with the approval of the authority managing the state secrets; and
  - offline.
- Additionally, any copies of this information must be protected in the same manner as the original.
- Publication and research on state secrets must be done:
  - within the approved scope of the publication and research;
  - in a secure location; and
  - with the approval of the authority managing such state secrets.

- Additionally, any records of the publication and research must be protected in the same manner as the original.
- Transportation and delivery of documents and objects containing state secrets must be done:
  - done by an authorized agency, including postal services;
  - done with the proper protection, in a sealed container;
  - recorded, tracked, and signed for; and
  - examined on delivery.

The Government determines and issues a list of information it deems to be state secrets in each sector.

There are no separate categories for sensitive data that does not constitute state secrets.

RIGHTS OF INDIVIDUALS

12. What information should be provided to data subjects at the point of collection of the personal data?

The data subject must be informed of the form, scope, place, and purpose for the collection, processing, and use of her personal data (*Article 21.1, Law on Information Technology; Article 17, Law on Network Information Security No. 86/2015/QH13 (Nov. 19, 2015)*). The notification can be in writing and in hard copy or electronic form, provided that the electronic form can be accessed and used as a reference when needed.

13. What other specific rights are granted to data subjects?

The Law on Network Information Security No. 86/2015/QH13 (Nov. 19, 2015) (LNIS) provides that data subjects have the right to request that the data processor:

- Provide the data subject's personal data that the data processor has collected or maintains, sometimes referred to as a right of access.
- Object to an organisation's processing of personal data.
- Update, amend, rectify, or delete the data subject's personal data that the data processor has collected or maintains.
- Stop providing the data subject's personal data to a third party.
- Notify the data subject of any third parties that the processor has disclosed the data subject's personal data (*see* Question 12).
- Indemnify the data subject for any damages caused by the data processor's violation of legal obligations when processing the data subject's personal data.

(*Article 17.3 and 18, LNIS*.) LNIS does not provide a right to transfer a copy of the personal data to another party, sometimes referred to as the right to data portability.

14. Do data subjects have a right to request the deletion of their data?

Yes. On receiving a request to delete a data subject's personal data, the data processor must either:

- Delete the data and inform the data subject.
- Provide the data subject with the access necessary to delete the data herself.
- Inform the data subject if deletion is not possible due to technical issues or other issues and apply appropriate measures to protect the data, though LNIS does not define the type of "appropriate measures" should be employed.

A data processor must also delete a data subject's personal data when either:

- The processor has completed using the personal data for the desired purpose.
- The time limit for storing the personal data, as set out in the relevant sectoral regulations, has expired.

Under these circumstances, the data processor must notify the data subject of the deletion, unless otherwise provided in the law. (*Article 18, Law on Network Information Security No. 86/2015/QH13 (Nov. 19, 2015)*.)

SECURITY REQUIREMENTS

15. What security requirements are imposed in relation to personal data?

The data processor must provide "an adequate level of protection" for personal data (*see* Question 8).

The Law on Network Information Security No. 86/2015/QH13 (Nov. 19, 2015) (LNIS) defines an information system as a system to establish, provide, transmit, collect, process, store, and transfer data, including personal data, online or over a network. With respect to an information system, a data processor must perform the following activities:

- Publish its security policy in terms of the design, construction, operation, management, use, upgrade, and deconstruction of the information system.
- Apply appropriate technical and management measures in accordance with the technical standards for information system security to:
  - minimize the risk of a security incident; and
  - repair the information system.
- Examine and supervise compliance with the security policy and evaluate the effectiveness of applied technical and management measures.
- Supervise the protection of the information system.

(*Article 23, LNIS*.) For information on securing state secrets, see Question 11.

16. Is there a requirement to notify personal data security breaches to data subjects or the national regulator?

There are no specific requirements to notify data subjects or a regulator of personal data security breaches. In case of a breach or a potential breach, a data processor is required only to apply remedies or preventive measures as soon as reasonably possible (*Article 19.2, Law on Network Information Security No. 86/2015/QH13 (Nov. 19, 2015)*).

PROCESSING BY THIRD PARTIES

17. What additional requirements (if any) apply where a third party processes the data on behalf of the data controller?

No additional requirements apply when a third party processes data on behalf of a data controller. Both the third-party processor and the data controller must comply with the obligations and requirements set out for the processor under the Law on Network Information Security No. 86/2015/QH13 (Nov. 19, 2015) (*see* Question 8, Question 9, and Question 10).

Under Vietnamese law, both the data controller and the third-party processor are considered data processors as defined in Question 4. Generally, each party is liable for its own violations. However, if the parties are subject to a data processing agreement, that agreement might provide for joint responsibility. Data processing agreements are generally not required. However, having a data processing agreement in place can limit the liability of each party to the extent of their action.

ELECTRONIC COMMUNICATIONS

18.Under what conditions can data controllers store cookies or equivalent devices on the data subject's terminal equipment?

Vietnamese law does not specify the conditions under which data controllers and processors can store cookies or equivalent devices on a data subject's terminal equipment.

Storing cookies or equivalent devices on the data subject's terminal equipment without consent, however, may be considered a violation of one key principle of the Law on Network Information Security No. 86/2015/QH13 (Nov. 19, 2015) (LNIS). The LNIS requires information and an individual's or entity's information system to be protected from unauthorized access, use, disclosure, interruption, modification, or destruction to ensure the completion, security and usability of the information. (*Article 4, LNIS.*)

Therefore, prudent organisations should obtain a data subject's consent before storing cookies or equivalent devices. For more on consent, see Question 9.

19. What requirements are imposed on the sending of unsolicited electronic commercial communications (spam)?

Government Decree No. 90/2008/ND-CP (Aug. 13, 2008) regulates unsolicited electronic commercial communications. Generally, the Decree prohibits sending unsolicited electronic commercial communications (spam).

An emails or messages is considered spam if it:

- Is intended to:
  - deceive;
  - harass; or
  - distribute viruses or malicious software.
- Is against the Socialist Republic of Vietnam or the unity of the people.
- Is contrary to the culture of the country or intended to:
  - encourage violence, war, or indifference between people; or
  - provoke sexuality, crimes, or superstition.
- Discloses national, military secrets and other secrets as indicated by law.
- Harms the reputation of an individual or an entity.
- Advertises goods and services that are prohibited.
- Violates the principles of sending advertisement emails and messages.

An organization that sends electronic commercial communications must comply with the following rules:

- Individuals and entities can send electronic commercial communications only after obtaining the recipient's consent.
- Individuals and entities must implement an opt-out mechanism for the electronic commercial communications and stop sending electronic commercial communications after the recipient has opted out.
- Electronic commercial communications must:
  - be labelled correctly as an advertisement or a commercial communication; and
  - identify the advertiser or advertisement service provider.
- Not more than one commercial email or message can be sent to one email address or one phone number within 24 hours (commercial messages can only be sent between 7:00 am and 22:00 pm).

INTERNATIONAL TRANSFER OF DATA

TRANSFER OF DATA OUTSIDE THE JURISDICTION

20. What rules regulate the transfer of data outside your jurisdiction?

There are no restrictions on transferring personal data outside of Vietnam. However, with respect to personal data of Vietnamese data subjects, the data processor and any secondary processors outside of Vietnam must meet requirements for data processors (*see* Question 8, Question 9, and Question 10).

There are no conditions under which a company may transfer personal data to another company within in their corporate group that is situated outside of Vietnam. However, as a general rule, transferring personal data to another company will often make such party a data processor under Vietnamese laws. As a result, that new party assumes the legal rights and obligations of a data processor, including the requirement to inform the data subject of the transfer.

21. Is there a requirement to store any type of personal data inside the jurisdiction?

The Law on Cybersecurity requires domestic and foreign enterprises to store personal data (as described below) in Vietnam where the organisations both:

- Provide:
  - services over a telecommunications network or the internet; or
  - value-added services on the internet in Vietnam.
- Collect, exploit, analyse, and process:
  - personal data;
  - data regarding the user's relationship; or
  - other data created by users located within Vietnam.

Foreign enterprises subject to this requirement must establish their presence in Vietnam through a branch or a representative office.

This law came into effect on January 1, 2019. The government has not yet issued official guidance on how this requirement will be enforced.

DATA TRANSFER AGREEMENTS

22. Are data transfer agreements contemplated or in use? Have any standard forms or precedents been approved by national authorities?

Data transfer agreements can be used in Vietnam but are not required. The government has not published any regulated forms or model precedents for data transfer agreements. A data transfer agreement does not negate the consent requirement. However, consents are often drafted to permit a data processor to transfer data to a third party.

23. Is a data transfer agreement sufficient to legitimise transfer, or must additional requirements (such as the need to obtain consent) be satisfied?

Under the Law on Network Information Security No. 86/2015/QH13 (Nov. 19, 2015), the transfer of a data subject's personal data constitutes the processing of personal data and requires the data subject's consent, whether or not:

- There is an applicable data transfer agreement.
- The transfer is domestic or cross-border.

For more on processing personal data, see Question 4. For more on consent, see Question 9.

24. Does the relevant national regulator need to approve the data transfer agreement?

No.

ENFORCEMENT AND SANCTIONS

25. What are the enforcement powers of the national regulator?

The Ministry of Information and Communications (MIC) is the national regulator for information security. Among its enforcement powers and responsibilities are its ability to:

- Examine, investigate, and handle claims or reports about, or violations of, information security regulations and laws. For more on these laws and regulations, see Question 1. MIC's enforcement authority extends data protection violations under any of the sectoral laws, in addition to Law on Network Information Security No. 86/2015/QH13 (Nov. 19, 2015) (LNIS).
- Coordinate with other authorities and enterprises to protect information security.
- Supervise compliance with information security regulations.

(*Article 52, LNIS.*)

The MIC works with both the Ministry of Public Security and the Ministry of National Defense to handle criminal breaches of information security regulations and threats to national security.

26. What are the sanctions and remedies for non-compliance with data protection laws?

Non-compliance with the data protection laws can be subject to both administrative penalties and criminal penalties. An administrative penalty may be imposed as follows:

- Between VND 2 million and VND 5 million for storing a data subject's personal data for longer than legally required or agreed by the parties.
- Between VND 5 million and VND 10 million for failing to check, adjust, or delete a data subject's personal data after receiving a request from the data subject.
- Between VND 10 million and VND 20 million for:
  - failing to provide a data subject's personal data as it relates to terrorism or criminal activities if the data is requested by a competent authority;
  - disclosing a data subject's personal data without consent; or
  - failing to maintain the necessary management and technical measures to protect a data subject's personal data.

Criminal penalties may be imposed for violations of rules governing confidentiality and safety concerning an individual's email, mail, telephone, and other forms of communications. The criminal sanction imposed depends on the severity of the crime and may include:

- A warning.
- A fine between VND 5 million and VND 50 million.
- Non-custodial reform, similar to probation or supervised release in other jurisdictions, of up to three years.
- A prison sentence of between one and three years.

Additionally, any person who suffers damages caused by an infringement of the data protection laws is entitled to compensation from the infringing party. To obtain compensation, the claimant must prosecute a a legal action and meet the burden of proof for actual damages.

Many sectoral laws provide additional administrative penalties for non-compliance with data protection obligations.

Government Decree No. 185/2013/ND-CP (Nov. 15, 2013) on administrative penalties concerning commercial production activities and consumer protections provides the following administrative penalties:

- **Violations of consumers' rights.** An administrative penalty of between VND 10 million and VND 20 million may be imposed for:
  - failing to inform data subjects of the purpose of the collection and processing personal data;
  - using personal data for purposes other than those communicated to the data subject;
  - failing to protect and maintain a complete and accurate version of personal data when collecting, using, or transferring the data;
  - failing to revise or update, or allow the data subject to revise or update, inaccurate personal data; or
  - transferring a data subject's personal data to a third party without consent.
- **Improper e-commerce activities.** An administrative penalty of between VND 5 million to VND 30 million may be imposed for:
  - collecting personal data without the data subject's consent;
  - using personal data for purposes other than those communicated to the data subject;
  - setting up a mechanism that compels consent for the collection, disclosure, or use of personal data for advertisement purposes or for other commercial purposes; or
  - failing to have a privacy policy or disclose the privacy policy to consumers as legally required.
- Additionally, repeat and multiple violations of e-commerce business requirements may cause the business to be suspended for up to 12 months.

Although the law provides for many administrative penalties for non-compliance with data protection regulations, in practice, the regulations are not effectively enforced. Statistics on the number of enforcement actions are not made public.

REGULATOR DETAILS

THE AUTHORITY OF INFORMATION SECURITY OF THE MINISTRY OF INFORMATION AND COMMUNICATIONS (*CỤC AN TOÀN THÔNG TIN THUỘC BỘ THÔNG TIN VÀ TRUYỀN THÔNG*)

W https://ais.gov.vn/

Main areas of responsibility. The authority's main areas of responsibility are to:

- Supervise compliance with information security regulations, as directed by the Ministry of Information and Communications (MIC).
- Research, collect, and analyse information to publish reports on the status of information security in Vietnam.
- Receive complaints concerning breaches of information security regulations.
- Other responsibilities as instructed by the MIC.

ONLINE RESOURCES

W http://vbpl.vn/pages/portal.aspx

Description. National, up-to-date, database of Vietnamese legislation. All Vietnamese legislation in Vietnamese. All legislation referred to in this survey is also available in English on this site, but the English translation should be used for reference purposes only.

W http://mic.gov.vn/Pages/VanBan/VanBanQuyPhamPhapLuat.aspx

Description. Official website of the Ministry of Information and Communications. The site contains all official, up-to-date, guidance of the MIC on information security. The website is up-to-date.

CONTRIBUTOR PROFILE

LE TON VIET, LL.M., ASSOCIATE
RUSSIN & VECCHI

T +84 24 3825 1700

F +84 24 3825 1742

E ltviet@russinvecchi.com.vn

W http://www.russinvecchi.com.vn

Areas of practice. Privacy and data protection; insurance law; franchise law; hotel management

Non-professional qualifications. BA in International Commercial Law and BA in Business English, Foreign Trade University, Vietnam, 2014; LLM in International Commercial Law, private international law, University of Aberdeen, 2016.

Languages. Vietnamese, English.

04-19