Data Security & Cybercrime

Jurisdiction snapshot

Trends and climate

Would you consider your national data protection laws to be ahead or behind of the international curve?

Vietnam

Tilleke & Gibbins

Vietnam's data protection laws have gradually been developed to catch up with international standards, and are now consistent with the Organisation for Economic Cooperation and Development Privacy Principles. However, the enforcement of many of these data privacy rules can still be unpredictable.

Vietnam's existing data protection laws protect individuals – and organisations in certain circumstances – from having their personal information misused, especially for commercial purposes. The laws provide mechanisms to prevent, detect, stop and address spam, computer viruses and cyber attacks and protect information exchanged in cyberspace (ie, an environment where information is provided, transmitted, collected, processed, stored and exchanged over telecoms networks and computer networks).

Back to top

Are any changes to existing data protection legislation proposed or expected in the near future?

Vietnam

Tilleke & Gibbins

Vietnam recently adopted the Law on Cyber Information Security, effective as of July 1 2016. This is the first specific law issued in Vietnam on the security of 'cyber information', which has been defined as information exchanged in a telecoms or computer network environment. Key aspects of the new law include:

- assurances for the safety and security of cyber information;
- protection of personal information in the network environment;
- protection of information systems and infrastructure;
- production, trading and use of civil ciphers;
- standards and technical regulations on information security;
- provision of information security services;
- prevention of spam, computer viruses and harmful software; and
- emergency responses.

Corresponding to the enactment of the law, Vietnam's amended Penal Code specifically imposes criminal penalties for violations relating to cyber information and cybercrime. Previously, many such violations were not considered crimes unless they fit under more traditional crimes, such as theft or fraud. Like the new law, the new Penal Code was scheduled to come into force on July 1 2016. However, its implementation has been postponed indefinitely, following a vote by the National Assembly, due to the large number of errors discovered in the code.

Back to top

Legal framework

Legislation

What legislation governs the collection, storage and use of personal data?

Vietnam

Tilleke & Gibbins

No single comprehensive law governs the collection, storage and use of personal data in Vietnam. Vietnam's data protection

Contributors

Vietnam

Tu Ngoc Trinh
Tilleke & Gibbins

Legal updates

Vietnam

Waewpen Piemwichai
Tilleke & Gibbins

Legal updates

Vietnam

Jim Dao
Tilleke & Gibbins

Legal updates

Vietnam

Nu Thi To Nguyen
Tilleke & Gibbins

Legal updates

laws are scattered throughout different pieces of legislation. These include the Civil Code, the Penal Code, the Law on Cyber Information Security, the IT Law, the Law on Telecommunications, the Law on Consumer Protection, the Law on E-Transactions, Decree 52 on e-commerce, Decree 90 on anti-spam and Decree 72 on internet services and online information.

Back to top

Scope and jurisdiction

Who falls within the scope of the legislation?

Vietnam

Tilleke & Gibbins

The data protection laws mentioned above are broadly worded and there are few limitations to their application. In general, the laws apply to a large number of organisations and individuals. In other words, it is easy to find a jurisdictional hook – for example:

- the Law on Cyber Information Security applies to Vietnamese agencies, organisations and individuals and foreign organisations and individuals directly involved in or related to cybersecurity activities in Vietnam;
- the IT Law applies to Vietnamese and foreign organisations and individuals engaged in IT application and development activities in Vietnam;
- Decree 52 applies to traders, organisations and individuals engaged in e-commerce activities in Vietnam, including:
    - Vietnamese traders, organisations and individuals;
    - foreign individuals residing in Vietnam; and
    - foreign traders and organisations operating in Vietnam through investment operations, branches and representative offices or websites with Vietnamese domain names; and
- Decree 72 applies to Vietnamese and foreign organisations and individuals engaged in or related to the management, provision and use of internet services, online information, online games and assurance of information security. Notably, Decree 72 does not include the limiting language "in Vietnam" contained in the other laws.

Back to top

What kind of data falls within the scope of the legislation?

Vietnam

Tilleke & Gibbins

The definition of 'personal information' differs from one piece of legislation to another. In general, 'personal information' is defined as information associated with the identification of a specific person, including, among other things, name, date of birth, home address, phone number, medical information, ID card numbers, social insurance card numbers, credit or debit card numbers and information on personal payment transactions.

For e-commerce activities in particular, the definition of 'personal information' is broadened to include any information that an individual wishes to keep confidential, with the exception of work contact information and other information that he or she has published in the mass media. The subjective nature of this expanded definition is problematic in the sense that an individual is imbued with the ability to determine what is considered personal information.

Back to top

Are data owners required to register with the relevant authority before processing data?

Vietnam

Tilleke & Gibbins

No.

Back to top

Is information regarding registered data owners publicly available?

Vietnam

Tilleke & Gibbins

Not applicable.

Back to top

Is there a requirement to appoint a data protection officer?

Vietnam

Tilleke & Gibbins

No.

Back to top

Enforcement

Which body is responsible for enforcing data protection legislation and what are its powers?

Vietnam

Tilleke & Gibbins

The main body responsible for enforcing data protection legislation is the Ministry of Information and Communications. Its powers include conducting examinations and inspections, settling complaints and denunciations and handling data privacy violations.

Back to top

Collection and storage of data

Collection and management

In what circumstances can personal data be collected, stored and processed?

Vietnam

Tilleke & Gibbins

Personal data can be collected, stored and processed only after consent from the data owner is obtained. However, consent is not required where personal information is collected in order to:

- sign, modify or perform goods and services contracts;
- calculate prices or charges for the use of information, products and services online; and
- perform other obligations in accordance with the law.

Back to top

Are there any limitations or restrictions on the period for which an organisation may (or must) retain records?

Vietnam

Tilleke & Gibbins

No specific limitations or restrictions on the period are set out by law. However, the organisations and individuals collecting, processing and using personal information may retain this information only for a certain period, as agreed by the data owners.

Back to top

Do individuals have a right to access personal information about them that is held by an organisation?

Vietnam

Tilleke & Gibbins

Yes – if the personal information was collected, edited, used, stored, provided, shared or spread in cyberspace for commercial purposes. Data owners have the right to request the organisations or individuals collecting, processing and using their personal information to provide them access to their personal information.

In other cases, data owners have the right to request the organisations or individuals collecting, processing and using their personal information to check, correct or delete the information, but not to access it directly.

Back to top

Do individuals have a right to request deletion of their data?

Vietnam

Tilleke & Gibbins

Yes. Data owners also have the right to request the organisations or individuals collecting, processing and using their personal information to update or alter their information or have those organisations stop providing this information to third parties.

Depending on the requested action, the organisations or individuals collecting, processing and using the personal information must:

- comply with the request and notify the data owner or grant him or her the right to access the information in order to update, alter or delete it;
- take appropriate measures to protect personal information and notify the data owner if there is a failure to comply with the request due to technical reasons or otherwise;
- not supply or use relevant personal information until such information has been corrected; and
- delete stored personal information once the purpose for which it was collected is complete or the storage time has expired, and notify the same to the data owners.

Back to top

Consent obligations

Is consent required before processing personal data?

Vietnam

Tilleke & Gibbins

Yes – however, consent is not required when collecting personal information in order to:

- sign, modify or perform goods and services contracts;
- calculate prices or charges for the use of information, products and services online; or
- perform other obligations in accordance with the law.

The laws generally do not require a specific form in which consent must be given. However, the laws require express consent from data owners in relation to e-commerce and marketing activities. Consequently, it is unclear whether consent must be given affirmatively (ie, opt-in) or whether a notice and lack of objection suffices.

Back to top

If consent is not provided, are there other circumstances in which data processing is permitted?

Vietnam

Tilleke & Gibbins

See above.

Back to top

What information must be provided to individuals when personal data is collected?

Vietnam

Tilleke & Gibbins

If personal information is to be collected, used or processed in a network environment (eg, telecoms networks, the Internet and computer networks and databases), the form, scope, place and purpose therein must be notified to the data owners. In addition, both parties must agree on how long the organisation will store or process the information.

Organisations and individuals that process personal information for commercial purposes must develop and publicise the means by which they process and protect the information.

Back to top

Data security and breach notification

Security obligations

Are there specific security obligations that must be complied with?

Vietnam

Tilleke & Gibbins

Yes. In general, organisations processing personal information must take appropriate management and technical measures to protect personal information that they have collected and stored and ensure that the personal information is not lost, stolen, disclosed, modified or destroyed without consent.

In addition, the new Law on Cyber Information Security introduces certain requirements to protect information and information systems (ie, a combination of hardware, software and databases for creating, transmitting and storing information in a network environment) as follows:

- When a cybersecurity incident occurs or may occur, those processing personal information must implement remedy and stoppage measures as soon as possible, and coordinate with competent state agencies and other organisations and individuals to ensure that the measures have been put in place.
- Organisations which own information must classify it based on various levels of secrecy in order to take appropriate protection measures. Further, they must formulate rules and procedures for processing information and recording authorised access to classified information.
- Those collecting information are subject to annual inspections and examination – or extraordinary inspections and examinations when deemed necessary – by the competent state management agency.
- Organisations that own information systems must classify their systems based on levels of security (Level 1 to 5, as set out under the Law on Cyber Information Security) in order to establish appropriate protection measures. They must also formulate policies and rules relating to cybersecurity in terms of designing, developing, managing, operating, using and updating or deactivating information systems.
- Organisations that own information systems are responsible for protecting their systems and must:
    - determine the security level of their information systems;
    - assess and manage security risks to their information systems;
    - supervise, monitor and check the protection of their information systems;
    - take measures to protect their information systems;
    - comply with the reporting regime; and
    - disseminate information and raise awareness about cybersecurity.
- Organisations and individuals that use civil cryptographic products provided by those other than enterprises licensed to trade in civil cryptographic products must declare such use to the Government Cipher Committee, with limited exceptions.

However, the Law on Cyber Information Security does not clearly define what suffices as compliance for many of the aspects set out above. Subordinate legislation under the Law on Cyber Information Security is expected to be issued in order to clarify and provide guidelines on the implementation of these requirements.

Back to top

Breach notification

Are data owners/processors required to notify individuals in the event of a breach?

Vietnam

Tilleke & Gibbins

No.

Back to top

Are data owners/processors required to notify the regulator in the event of a breach?

Vietnam

Tilleke & Gibbins

No.

Back to top

Electronic marketing and internet use

Electronic marketing

Are there rules specifically governing unsolicited electronic marketing (spam)?

Vietnam

Tilleke & Gibbins

Yes. Decree 90 on anti-spam sets out regulations regarding unsolicited messages sent by email and text message. In general, advertising emails and text messages can be sent only after obtaining clear prior consent from the intended recipients. Advertising emails and text messages can be sent only from email addresses and systems set out by the Ministry of Information and Communications. The details of each advertising email and text message must include opt-out information permitting recipients to decline receiving further ads. Senders must immediately cease sending ads once a recipient opts out.

Back to top

Cookies

Are there rules governing the use of cookies?

Vietnam

Tilleke & Gibbins

No specific regulation governs the use of cookies. However, if cookies are used to collect and process personal information, they must comply with the data privacy rules.

Back to top

Data transfer and third parties

Cross-border data transfer

What rules govern the transfer of data outside your jurisdiction?

Vietnam

Tilleke & Gibbins

Vietnamese law does not specifically distinguish between the transfer of data inside or outside Vietnam. As such, the rules for the transfer of personal information both inside and outside Vietnam are the same. According to the law, organisations and individuals (if they fall within the scope of applicable law) must refrain from providing or sharing with a third party personal information which they have collected, accessed or controlled, unless they obtain the data owner's consent or as required by the proper state agencies.

Back to top

Are there restrictions on the geographic transfer of data?

Vietnam

Tilleke & Gibbins

No, please see above.

Back to top

Third parties

Do any specific requirements apply to data owners where personal data is transferred to a third party for processing?

Vietnam

Tilleke & Gibbins

No specific requirement exists, but consent from the data owner is required.

Back to top

Penalties and compensation

Penalties

What are the potential penalties for non-compliance with data protection provisions?

Vietnam

Tilleke & Gibbins

Depending on the nature and severity of the violation, infringements of the data protection provisions may lead to disciplinary actions or administrative or criminal penalties.

For administrative penalties, a fine between D10 million and D70 million (approximately $450 and $3,150) may be imposed. For certain violations, the administrative fines for organisations (rather than individuals) may be twice the aforementioned amount. In addition to administrative fines, other remedial measures may also be imposed (eg, suspension of activities and seizure of gains from the activities).

Back to top

Compensation

Are individuals entitled to compensation for loss suffered as a result of a data breach or non-compliance with data protection provisions by the data owner?

Vietnam

Tilleke & Gibbins

Yes – in general, compensation for any resulting damages must be provided by anyone that intentionally or unintentionally:

- harms the life, health, honour, dignity, reputation, property or other legal rights or interests of an individual; or
- harms the honour, reputation or property of a legal entity or other subject.

In relation to data privacy, individuals can claim compensation for loss caused by a breach during the transfer of personal information.

Back to top

Cybersecurity

Cybersecurity legislation, regulation and enforcement

Has legislation been introduced in your jurisdiction that specifically covers cybercrime and/or cybersecurity?

Vietnam

Tilleke & Gibbins

Yes, the Law on Cyber Information Security governs cybercrime and cybersecurity in Vietnam. According to the law, the following acts are considered violations therein:

- blocking the transmission of information in cyberspace or improperly intervening, accessing, harming, deleting, altering, copying or falsifying information in cyberspace;
- improperly affecting or obstructing the normal operation of information systems or users' access to information systems;
- improperly attacking or nullifying electronic information security protection measures within information systems;
- attacking, seizing control of or sabotaging information systems;
- spreading spam or malware or establishing fake and deceitful information systems;
- improperly collecting, using, spreading or trading personal information;
- abusing the weaknesses of information systems to collect or exploit personal information;
- hacking cryptographic secrets and lawfully enciphered information from agencies, organisations or individuals;
- disclosing information on civil cryptographic products or information on clients that lawfully use civil cryptographic products; and
- using or trading in civil cryptographic products of unknown origins.

Agencies, organisations and individuals engaged in cybersecurity activities must coordinate with the proper state agencies and other organisations and individuals to ensure that electronic information is properly secure and provide appropriate notice where information has been breached.

Back to top

What are the other significant regulatory considerations regarding cybersecurity in your jurisdiction (including any international standards that have been adopted)?

Vietnam

Tilleke & Gibbins

Vietnam has cooperated with a number of cybersecurity bodies, including those from the United States, the United Kingdom and China, in order to exchange intelligence and information and jointly investigate cases relating to cybercrime. Vietnam has also cooperated with its international counterparts in training and sending its officers to meetings, conferences and training courses.

Back to top

Which cyber activities are criminalised in your jurisdiction?

Vietnam

Tilleke & Gibbins

According to the new Penal Code (the implementation of which has been postponed indefinitely), the following activities are criminalised:

- manufacturing, dealing in, exchanging or giving out instruments, equipment or software meant to attack a computer network, telecoms network or electronic device;
- spreading software programs that harm computer networks, telecoms networks or electronic devices;
- deleting, damaging or changing a software program or electronic data;
- illegally obstructing the transmission of data from a computer network, telecoms network or electronic device, or otherwise obstructing or disturbing a computer network, telecoms network or electronic device;
- illegally providing or using information on computer networks or telecoms networks, including:
    - illegally uploading information onto a computer or telecoms network;
    - trading, exchanging, giving, changing or publishing lawfully private information of an organisation or individual on a computer or telecoms network without consent; and
    - other acts that involve the illegal use of information on a computer or telecoms network;
- illegally infiltrating a computer network, telecoms network or electronic device, including by deliberately bypassing the warning, password or firewall or using the administrative rights of another person to infiltrate a computer network, telecoms network or electronic device in order to:
    - take control of or interfere with the operation of the electronic device;
    - steal, change, destroy or fabricate data; or
    - illegally use services;
- appropriating property by using a computer network, telecoms network or electronic device, including:
    - using an organisation's information or individual's bank account or card in order to appropriate the property of the account holder or cardholder or make illegal purchases;
    - making, storing, trading or using fake bank cards in order to steal money from cardholders or make illegal purchases;
    - illegally accessing the account of an organisation or individual in order to appropriate its property;
    - committing fraud in electronic commerce, electronic payment, online currency trading, online capital raising, online multi-level marketing or online securities trading in order to appropriate property; and
    - illegally establishing or providing telecoms or internet services for the purpose of appropriating property;
- illegally collecting, storing, exchanging, trading or publishing information about bank accounts; and
- illegally providing services on computer networks or telecoms networks, including:
    - trading gold on accounts;
    - electronic commerce exchange;
    - multi-level marketing;
    - payment services;
    - online video games; and
    - other services on computer networks or telecoms networks as set out by law.

Back to top

Which authorities are responsible for enforcing cybersecurity rules?

Vietnam

Tilleke & Gibbins

There are three ministries responsible for enforcing cybersecurity rules:

- The Ministry of Information and Communications assumes the primary responsibility for, and coordinates with the other two ministries in, preventing, detecting, stopping and handling cybersecurity violations;
- The Ministry of National Defence has jurisdiction over cybersecurity violations against national sovereignty and territorial integrity; and
- the Ministry of Public Security has jurisdiction over cybercrime issues and may cooperate with Interpol to investigate cybercrime cases.

The Vietnam Computer Emergency Response Team, a government body under the Ministry of Information and Communications, is tasked with responding to incidents relating to preventing, handling and remedying Internet incidents in Vietnam. It also acts as a hub for exchanging information in cases where Vietnam is cooperating with international computer emergency response teams.

Back to top

Cybersecurity best practice and reporting

Can companies obtain insurance for cybersecurity breaches and is it common to do so?

Vietnam

Tilleke & Gibbins

Yes, several insurers in Vietnam provide cybersecurity breach coverage. While there are studies showing that a high number of Vietnamese companies do not see privacy as a top priority, certain companies are aware of cybersecurity and thus obtain insurance.

Back to top

Are companies required to keep records of cybercrime threats, attacks and breaches?

Vietnam

Tilleke & Gibbins

No.

Back to top

Are companies required to report cybercrime threats, attacks and breaches to the relevant authorities?

Vietnam

Tilleke & Gibbins

Yes. Agencies, organisations and individuals must issue certain notices immediately in the event of a breach involving their electronic information security activities.

For the e-commerce sector in particular, if an information system is hacked or may lose consumer information, those storing the information must notify a functional agency within 24 hours of detection.

Back to top

Are companies required to report cybercrime threats, attacks and breaches publicly?

Vietnam

Tilleke & Gibbins

No.

Back to top

Criminal sanctions and penalties

What are the potential criminal sanctions for cybercrime?

Vietnam

Tilleke & Gibbins

Potential criminal sanctions range from a fine to non-custodial reform or imprisonment. The offender may also be prohibited from holding certain positions or doing certain jobs for an established period or have part or all of its property confiscated.

Back to top

What penalties may be imposed for failure to comply with cybersecurity regulations?

Vietnam

Tilleke & Gibbins

The penalties vary depending on the type of violation. Fines range between D20 million and D500 million (approximately $900 and $22,500). Violators may also face a penalty of up to three years' community service or three to 60 months' imprisonment.

The penalties may be higher if, among other things, the violations:

- are committed by an organisation;
- are committed more than once;
- are committed in a professional capacity;
- meet certain profit thresholds (ie, above D50 million (approximately $2,500));
- result in property damage of D100 million (approximately $4,500) or more; or
- are considered likely to be repeated – defined under the law as "dangerous" recidivism.

Back to top

Law stated date

Correct as of

Please state the date of which the law stated here is accurate.

Vietnam

Tilleke & Gibbins

July 1 2016.

Back to top