Compliance Checklist – Vietnam's Law on Personal Data Protection

Le Ton Viet
RUSSIN & VECCHI

Tel: (84-24) 3825-1700
Email: LTViet@russinvecchi.com.vn
Web: www.russinvecchi.com.vn

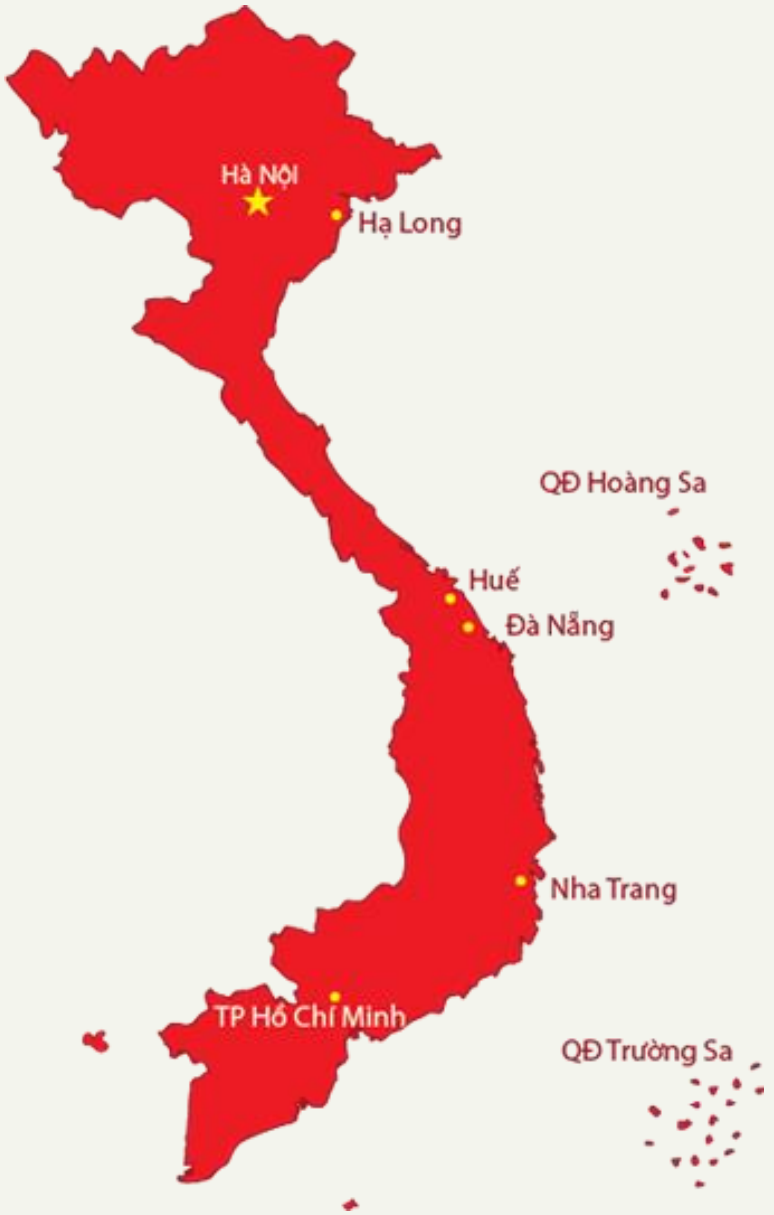
Applicability

- **Is the entity established and operating in Vietnam?**

If the answer is ‘yes’ and the entity processes personal data of any data subjects, then Vietnam’s personal data protection regulations will apply.

- **Does the entity processes data of Vietnamese citizens or persons of Vietnamese origin, who are residing in Vietnam?**

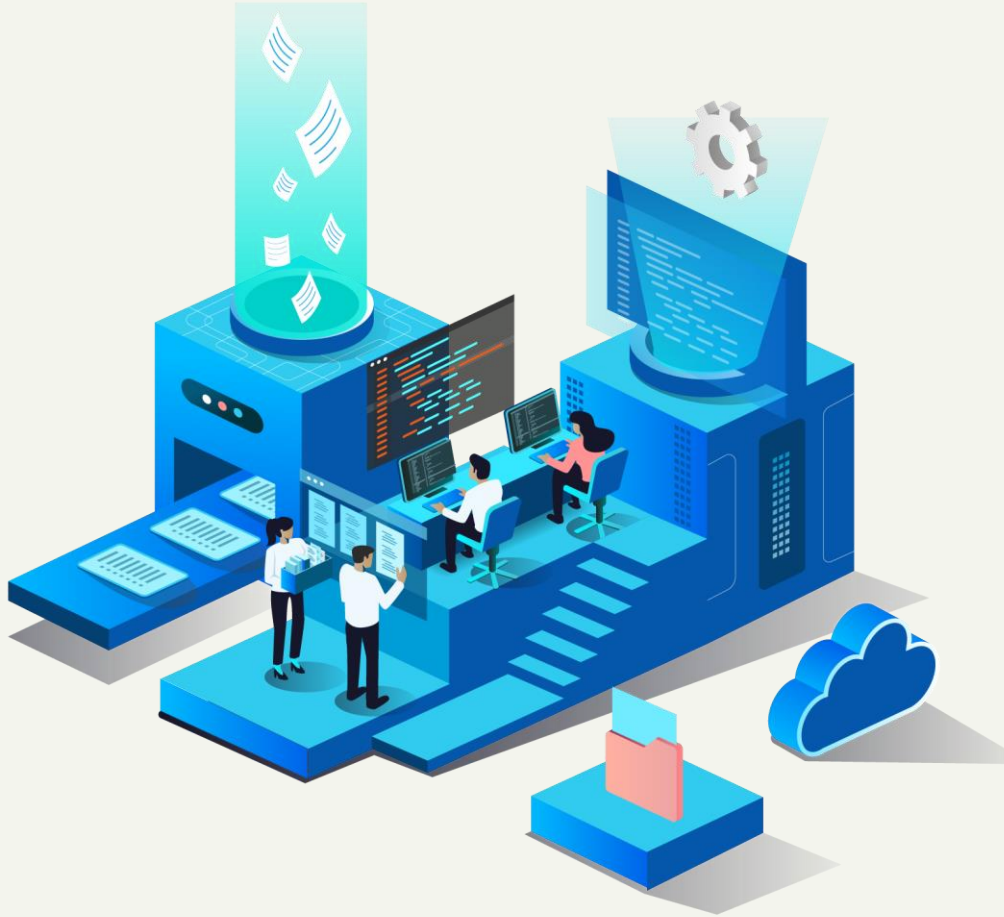
If the answer is ‘yes’, Vietnam’s personal data protection regulations will apply regardless of the location of the entity.



What are personal data processing activities?

Any action(s) that affects personal data:

COLLECTION	DISCLOSURE	ANALYSIS	DELETION
ENCRYPTION	TRANSFER	COMBINING	ALTERATION
DECRYPTION	DE-IDENTIFICATION	OTHER ACTIVITIES IN CONNECTION WITH PERSONAL DATA	



ROLE OF THE ENTITY

An entity can assume one or more of these roles depending on the type of transaction. For example, an entity can be both a data controller and a data processor in connection with personal data of an employee. An entity can also be a data processor for another entity.

It is essential that a Company understands its role in connection with each type of personal data involved and in each transaction.

Data controller

An entity or individual who determines the purposes for which, and the manner in which personal data is processed.

Data processor

Any entity or individual who processes personal data for and on behalf of the data controller in accordance with an agreement.

Third party

Any party engaging in some processing activities other than the data processors or data subjects.

Basic personal data

- Name, nickname;
- Date of birth, date of death or date missing;
- Gender;
- Location of birth, permanent address, temporary address, current address, contact address;
- Nationalities;
- Personal photos;
- Phone number, ID, passport, license plate, driver's license, tax, social security number, medical insurance number;
- Marriage status and information that relates to the family (parents, children);
- Information of digital accounts of a person; and
- Other data referring to a specific person or when combined with other data and information can identify a specific person, but is not itself sensitive personal data.

Sensitive personal data

- Political opinion, religious views;
- Medical status, ethnicity information;
- Biometrics and genetic information;
- Information in relation to sexual orientation;
- Criminal records collected and maintained by enforcement agencies;
- Login information of VNEID accounts, images of IDs,
- Names and passwords of banking accounts, bank card information, transaction history, financial and credit information, and information relating to customers' activities and transaction history in relation to securities, and insurance at authorized organizations;
- Live location identified through location services;
- Data that reflects activity or history of activity of an individual on the internet.

Data subject's Rights

01	Right to know about processing activities
02	Right to give or withdraw consent
03	Right to view and adjust or to request
04	Right to request a copy, delete or restrict data processing
05	Right to request authority or relevant parties to implement legal measures in relation to personal data

Data subject's Obligations

01	protect her own personal data
02	Respect and protect personal data of others
03	Provide complete and accurate personal data
04	Comply with personal data regulations

Legal bases for personal data processing

- **Consent**
- To protect the lives, health, reputation, dignity, legal rights and benefits of data subjects or other persons in an emergency; to protect the legitimate rights and benefits of an individual or benefits of the government or of an organization against violations;
- Processing of personal data in case of emergency to national defense, national security, social safety and order, natural disaster, diseases; or potential risks to national security but not required to declare an emergency state; or to fight against riot, terrorists, criminals, etc;
- To perform contractual obligations of the data subject vis-a-vis relevant entities or individuals in accordance with law;
- To serve the activities of the authorities as provided in any sectoral law

Consent - Checklist

1

Voluntary and informed

Consent must be voluntary and fully informed and must contain the type of personal data to be processed, purpose of processing, who is permitted to process and the rights and obligations of the data subjects, and whether the data is sensitive personal data**.**

2

Expressed and specific

Consent must be expressed and specific in writings, voice recordings, tick to agree, text messages, choosing technical option to agree or other actions. Silence or non-action will not be considered valid consent.

3

Verifiable

Consent must be in a format that can be printed, copied in writing, including electronic formats and other verifiable formats.

4

Additional requirements

Consent could be partial or conditional.

Does the entity provide any of the following services to a third party?

If yes, the entity must comply with the next slide.

- Provide and operate systems and automated software to act on behalf of the data controller or the data processor in carrying out personal data processing activities.
- Assessment, ranking, and scoring the creditworthiness or trust level of data subjects.
- Collecting and processing personal data from (i) websites, applications, software, and social networks, (ii) healthcare websites, applications, software, health-monitoring tools, and medical services and (iii)) educational applications and software involving monitoring elements such as attendance tracking, video recording, behavioral scoring, and emotion recognition.
- Analyzing and exploiting personal data; Encrypting personal data during transmission and storage.
- Automated personal data processing based on big data technologies, artificial intelligence, blockchain, and virtual environments (metaverse). Application platform services that provide personal location data.

Data processing services

Entity providing data processing services:

- Duly established and operating in Vietnam;
- Head of department in charge of processing data must be Vietnamese and must reside in Vietnam;
- At least 3 qualified persons;
- Has the appropriate infrastructure, equipment and facilities;
- The data processing impact assessments and data transfer impact assessments of the entity are **deemed 'satisfactory'.**

Qualified Personnel:

- Has a college degree;
- At least 2 years of experience in one of the following fields: legal, IT, cybersecurity, data security, risk management, compliance, HR;
- Has been trained in legal knowledge and professional skills in relation to data protection.

Licensing procedure:

- Under the authority of the Ministry of Public Security;
- Documentation includes a detailed plan for the implementation of services;
- Statutory timeline for this procedure may be 40 days.

Impact Assessments--check list

- **Does the entity transfer data to a location outside of Vietnam? (this includes using a cloud service)**

If the answer is yes, a Data Transfer Impact Assessment is required.

- **Has the entity submitted impact assessments in accordance with Decree 13/2023/ND-CP?**

If the answer is yes, a new submission is not required, but the entity will have to update the impact assessments in accordance with current regulations.

- **Has the authority responded to the submitted impact assessments?**

If the answer is no, please follow up with the authority;

- **How long has it been since the impact assessments were submitted to the authority?**

Impact assessments are required to be updated every six months or immediately under certain circumstances.

Data protection personnel or DPO

Data protection personnel:

- Can be employed or outsourced;
- Can be exempted from liability by agreement in certain circumstances.

Supporting documents checklist:

- Appointment decision;
- Copy of relevant degrees and qualifications;
- Contact information.

Qualified Personnel:

- Has a college degree;
- At least 2 years (3 years if outsourced) of experience in one of the following fields: legal, IT, cybersecurity, data security, risk management, compliance, HR;
- Has been trained on legal knowledge and professional skills in relation to data protection.

Entity providing data protection services:

- Must have the appropriate business lines (IT, legal or consulting);
- Must have at least 3 qualified personnel;
- Must have a portfolio showing its capabilities.

Further Considerations

Does the entity operate in any of the following businesses: AI, blockchain, metaverse, cloud computing, advertisement, finance, insurance. If yes, there are additional requirements.

Does the entity organize training for its employees on protection of personal data? The answer must be yes. Training should be documented.

Does the entity have a breach response plan, Privacy Policy, Information Security Policy, Data Classification, Training Plan? The answer must be yes.

Main Compliance Checklist

01	Consent from data subjects has been obtained properly
02	Submitted impact assessments will be carried forward. Impact assessments will be reviewed by the authority and be deemed ‘satisfactory’ or ‘unsatisfactory’.
03	There are new requirements in relation to data protection personnel.
04	There are new requirements in relation to data processing services.
05	Entity must have the appropriate measures to protect personal data. Such measures should be documented and disseminated to the entity’s employees.

RUSSIN & VECCHI
LTVIET@russinvecchi.com.vn