Amcham Webinar | May 4, 2023
Vietnam

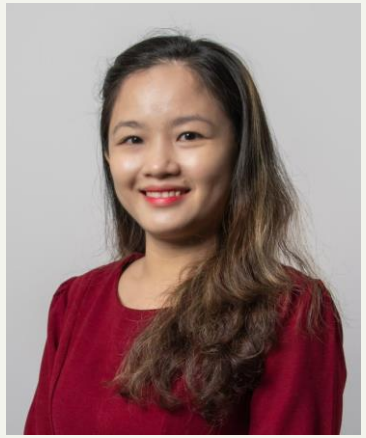
Decree 13/2023/ND-CP on Personal Data Protection

RUSSIN & VECCHI

Speakers

Nguyen Huu Minh Nhut
Partner
HCMC Office
Russin & Vecchi

NHMNhut@russinvecchi.com.vn



Tran Ngoc Han
Partner
HCMC Office
Russin & Vecchi

TNHan@russinvecchi.com.vn

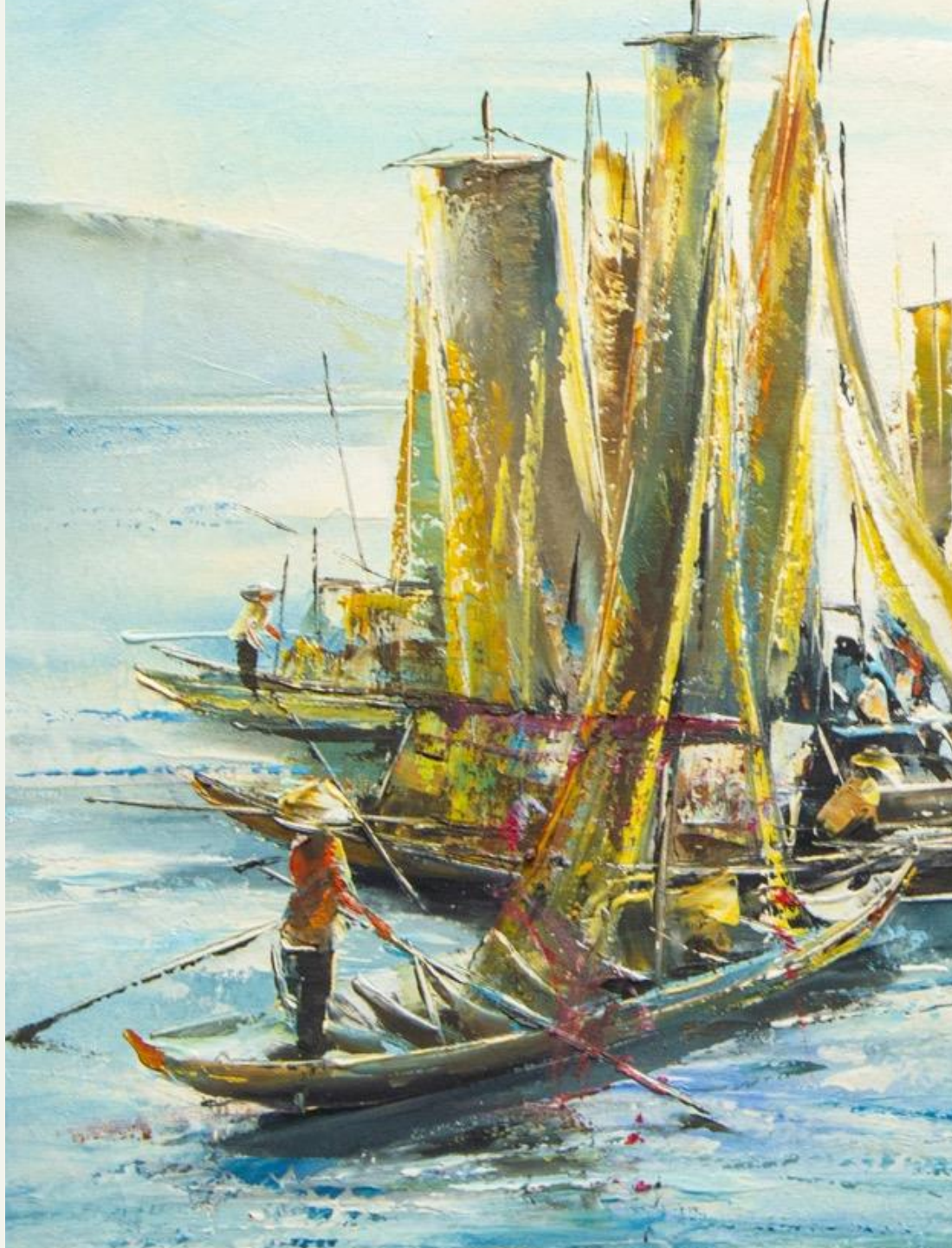
Philip Ziter
Senior Associate
HCMC Office
Russin & Vecchi

PZiter@russinvecchi.com.vn

Le Ton Viet
Associate
Hanoi Office
Russin & Vecchi

LTViet@russinvecchi.com.vn

Table of contents

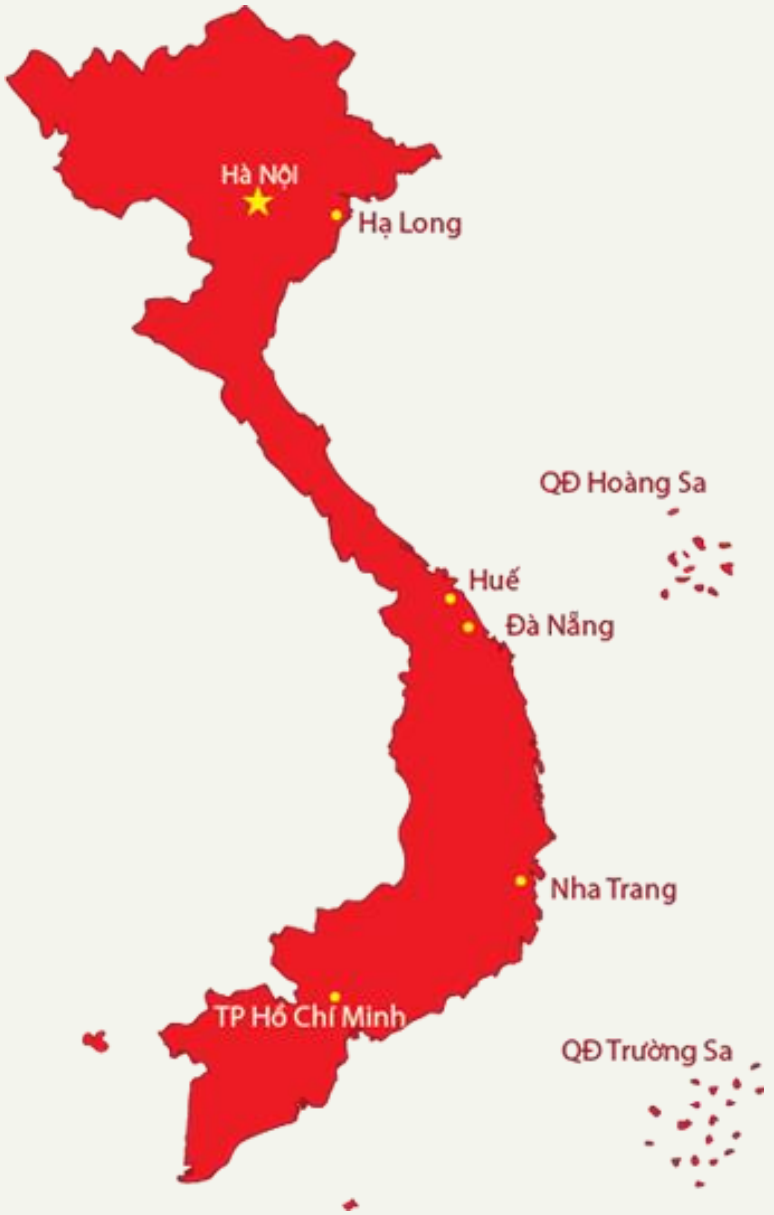


Scope of Decree 13

Decree 13 applies to:

- individuals, entities located in Vietnam, regardless of their nationality;
- Vietnamese individuals and entities located offshore; and
- Foreign individuals and entities involved in data processing activities in Vietnam.

“Personal data” is defined to be information in the form of signs, texts, numbers, pictures, sounds and similar forms which exist in a digital environment and which refer to a specific person or can identify a specific person when combined with other data and information.



Basic personal data

- Name, **nickname (if any)**
- 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 in relation to the family (parents, children);**
- **Information of a person's digital accounts** and data that reflects activity or history of activity of an individual on the internet;
- **Other data referring to a specific person or when combined with other data and information can identify a specific person, but is not sensitive personal data**

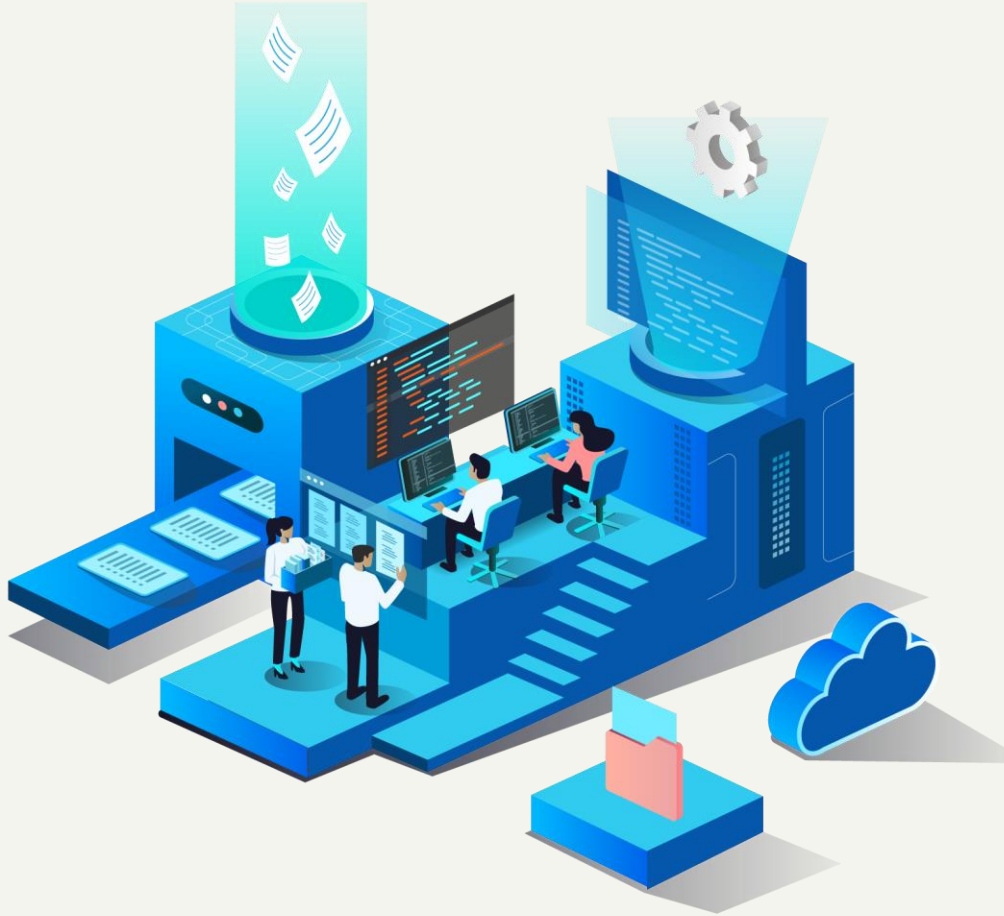
Sensitive personal data

- Political opinion, religious views;
- Medical status and private information in medical records, not including blood types;
- **Ethnicity information**;
- **Genetic information**;
- Biometrics and **physical information**,
- **Sexual orientation,**
- Criminal records collected and maintained by enforcement agencies;
- **Customers' information of financial institutions, intermediary payment service provider, including KYC information and account information, assets, transactions, guarantees/guarantors**;
- **Live location identified through location services**;
- **Other personal data that is determined by the law to be unique and needs to remain secure.**

Personal data processing

Any action(s) that affects personal data:

COLLECTION	RECORDING	ANALYSIS	STORAGE
ENCRYPTION	RECOVERY	RETRIEVAL	GRANTING OF ACCESS TO PERSONAL DATA
DECRYPTION	COPY	TRANSFER	DELETION, or DESTRUCTION of personal data or other relevant actions
ALTERATION	DISCLOSURE	**VERIFYING**	**COMBINING**



To whom does Decree 13 apply?

Data subject

Any identifiable natural person to whom the personal data relates

Data controller

An entity or individual who determines the purposes for which and the manner in which the 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 a data processor or the data subject

Rights of the data subject

01	Right to know about processing activities
02	Right to give consent
03	Right to withdraw consent
04	Right to delete or request to delete
05	Right to restrict processing activities
06	Right to access
07	Right to claim for damages
08	Right to data portability
09	Right to object to data processing activities
10	Right to make claim, to initiate legal action
11	Right to protect themself

Legal bases for personal data processing

- **Consent**
- In an emergency, which requires immediate processing of personal data to protect the lives, health of the data subject or of other individuals.
- Publishing personal data as required by law;
- Processing personal data in case of emergency or threat 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 riots, terrorists, criminals and threatened legal violations;
- To perform contractual obligations of the data subject vis-à-vis relevant entities or individuals;
- To support the activities of authorities as provided in any sectoral law..

Consent

1

Voluntary and informed

Consent must be voluntary and fully informed: **type of personal data to be processed**, **purpose of processing, who is permitted to process and the rights and obligations of the data subjects, 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 message, choosing technical option to agree or **other actions. Silence or non-action is not considered to be a 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 can be partial or conditional.

Validity

Consent is valid until the data subject decides otherwise or subject to the written request of a competent authority.

Prior Notifications

In case personal data is permitted to be processed without consent of the data subject, the data controller must send a notice to the data subject with the following information:

- Type of data being processed, the purposes and the manner of data processing;
- The parties involved in the processing activities;
- The unwanted consequences or damages that may occur;
- Time and duration of the processing activities.

Data Controller and Data Processor

Data controller

An entity or individual who determines the purposes for which and the manner in which the 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 a data processor or data subject

The Data Controller

- Implements **organizational and technical measures** and **appropriate safety and security measures** to protect the personal data and to prove that the personal data is being processed in accordance with the regulations
- Record and store **logs** of the processing of personal data.;
- **Notify the authority** in case of personal data breaches;
- **Only work with a Personal Data Processor that has implemented measures to protect personal data.**
- **Ensure the rights of data subjects;**
- Be **liable to the data subject for damages** caused by the processing of personal data.
- Cooperate with the Ministry of Public Security and other competent authorities to protect personal data

The Data Processor

- Only accept and process personal data if **an agreement with data controller** has been executed;
- Implement **appropriate safety and security measures** to protect personal data;
- Record and store **logs** that reflets the processing of personal data.;
- **Notify the data controller** in case of personal data breaches;
- Be **liable to the data subject for damages** caused by the processing of personal data;
- **Return and delete all personal data** to the data controllers after completion of the agreement;
- Cooperate with the Ministry of Public Security and competent authorities to protect personal data.

Measures to protect personal data

Measures to protect personal data:

- Management measures;
- Technical measures;
- Measures applied by competent authorities;
- Measures in relation to investigations or legal proceedings;
- Other measures provided by law.

To protect basic personal data:

- Develop and publish rules on protection of personal data;
- It is recommended that standards of protection of personal data be applied appropriately;
- Regularly perform examinations and tests of the systems and equipment used to process personal data.

To protect sensitive personal data:

- All of the above apply;
- A data protection department and personnel must be appointed;
- The data subject must be notified in case of a breach of such data.

The Impact Assessment

Personal data processing:

- Information of the Data Controller;
- Name and contact details of the data protection officer/department of the Personal Data Controller;
- Details of data processing (purposes, duration, parties, protection measures, etc.)
- Cases of offshore transfer of personal data;
- Assessment of impact of personal data processing; undesirable consequences and damage that may occur, measures to reduce or remove negative consequences and damage.

Offshore transfer of personal data of Vietnamese nationals:

- Information of the transferor and the receiver;
- Description of the data to be transferred;
- Description of the protective measures applied;
- Assessment of impact of personal data processing; undesirable consequences and damage that may occur, measures to reduce or remove such consequences and damage;
- Consent;
- Document to bind the transferor and the receiver.

Regulatory Body

The Department of Cybersecurity and prevention of cyber-crimes under the Ministry of Public Security

A National Portal on protection of personal data will be established

A Decree on sanctions for violations of personal data protection will be issued

Key Takeaways (1-8) and Recommendations (A and B)

01	Decree 13 will become effective on July 1, 2023
02	Different types of data will require that different protective measures be implemented.
03	There are very specific requirements on consent
04	There are circumstances where consent is not required
05	Data subjects have exercisable rights!
06	Impact assessments are required for processing and offshore data transfer, not required to be approved.
07	Data controller and Data processor have different obligations and responsibilities.
08	The regulatory body is the Ministry of Public Security
A	Companies should review their current data practices by performing a legal data audit.
B	Data transfer, including intragroup, should be performed under a data transfer agreement

Q&A

THANK YOU