NAVIGATING GDPR COMPLIANCE AND BANK DEBT COLLECTION IN VIETNAM: A SEMINAR WITH INSIGHTS FROM REAL CASE STUDY

28 FEB
2:00 PM
5:00 PM

VENUE: LNT & PARTNERS OFFICE

(Bài trình bày bản Tiếng Việt từ trang 53)

LNT & PARTNERS
INNOVATIVE LEGAL SOLUTIONS

COMPLIANCE WITH THE GENERAL DATA PROTECTION REGULATON (GDPR) OF THE EUROPEAN UNION IN VIETNAM

DR. Nguyen Van Tuan

Partner of LNT & Partners

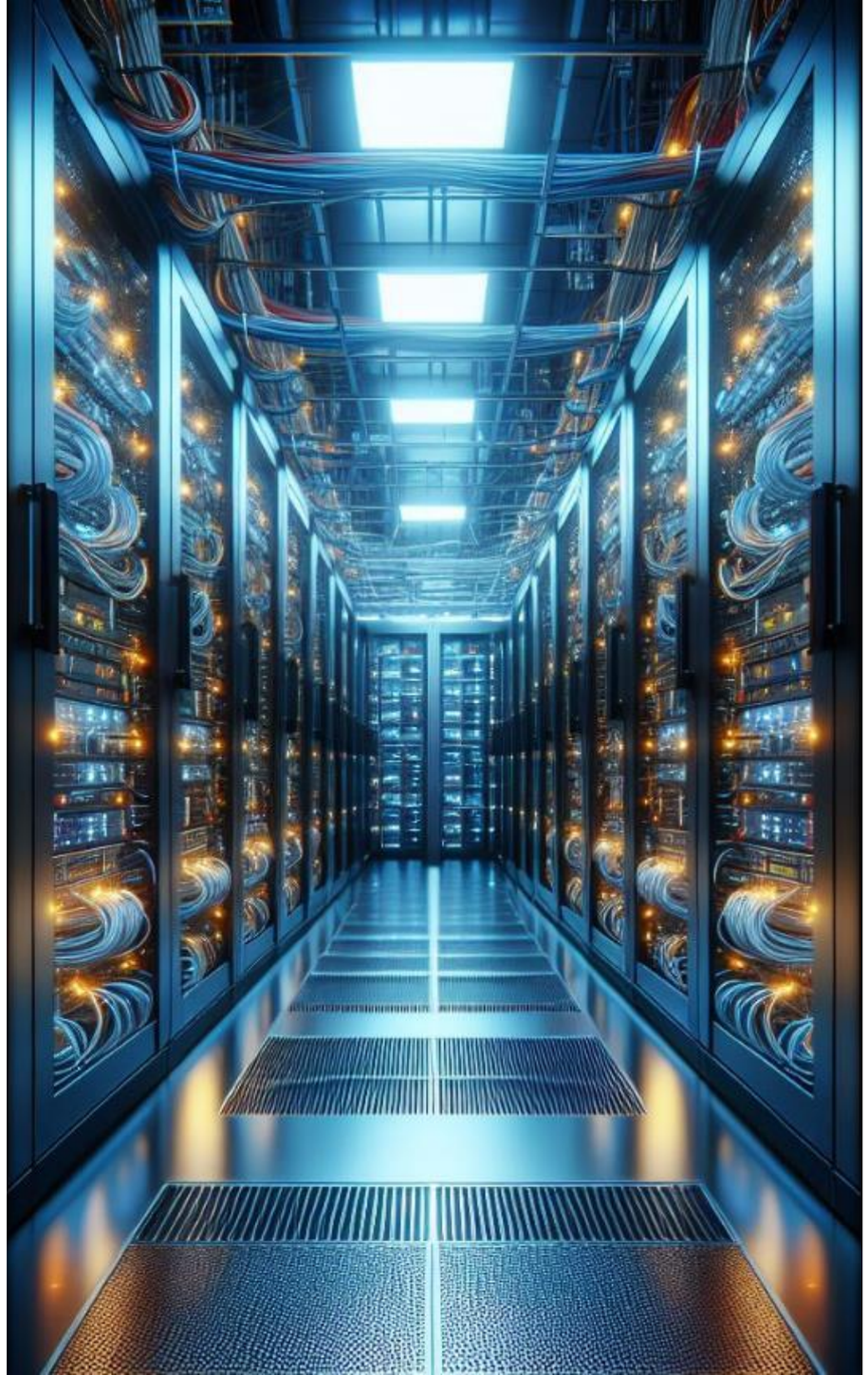
Ho Chi Minh City, 28 February 2024

MAIN CONTENT

1 | INTRODUCTION TO GDPR

2 | DECREE 13/2023/ND-CP ON PROTECTION OF PERSONAL DATA

3 | CURRENT STATUS OF PERSONAL DATA PROTECTION AT ENTERPRISE OPERATING IN THE AVIATION SECTOR (CASE STUDY)



1

INTRODUCTION TO GDPR

1 | INTRODUCTION TO GDPR

1.1. Geographical scope of the GDPR

Organizations/ Companies established in EU territory;

Organizations/ Companies not established in EU territory, where the processing activities are related to :

- The supply of goods or services to individuals taking place within the EU;
- The monitoring of individual behavior as far as individual behavior takes place within the EU.

1.2. The basic concepts

- **“Personal Data”** refers to specific individual information such as name, identification number, address, online information, or other special information related to the individual’s physical, physiological, genetic mental, economic, cultural, or social background.
- **“Data Processing”** refers to one or multiple activities that impact personal data, including collection, recording, analysis, confirmation, storage, rectification, disclosure, combination, access, traceability, retrieval, encryption, decryption, copying, sharing, transmission, provision, transfer, deletion, destruction or other relevant activities.
- **“Date Subject”** refers to an individual to whom the data relates.
- **“Consent”** means any specific, free, informed and unambiguous expression of the data subject’s wishes, whether by statement or by any clearly positive action that expresses the consent to the processing of personal data.
- **“Supervisory Authority”** is an independent public organization established by a Member state.

1.2. The basic concepts

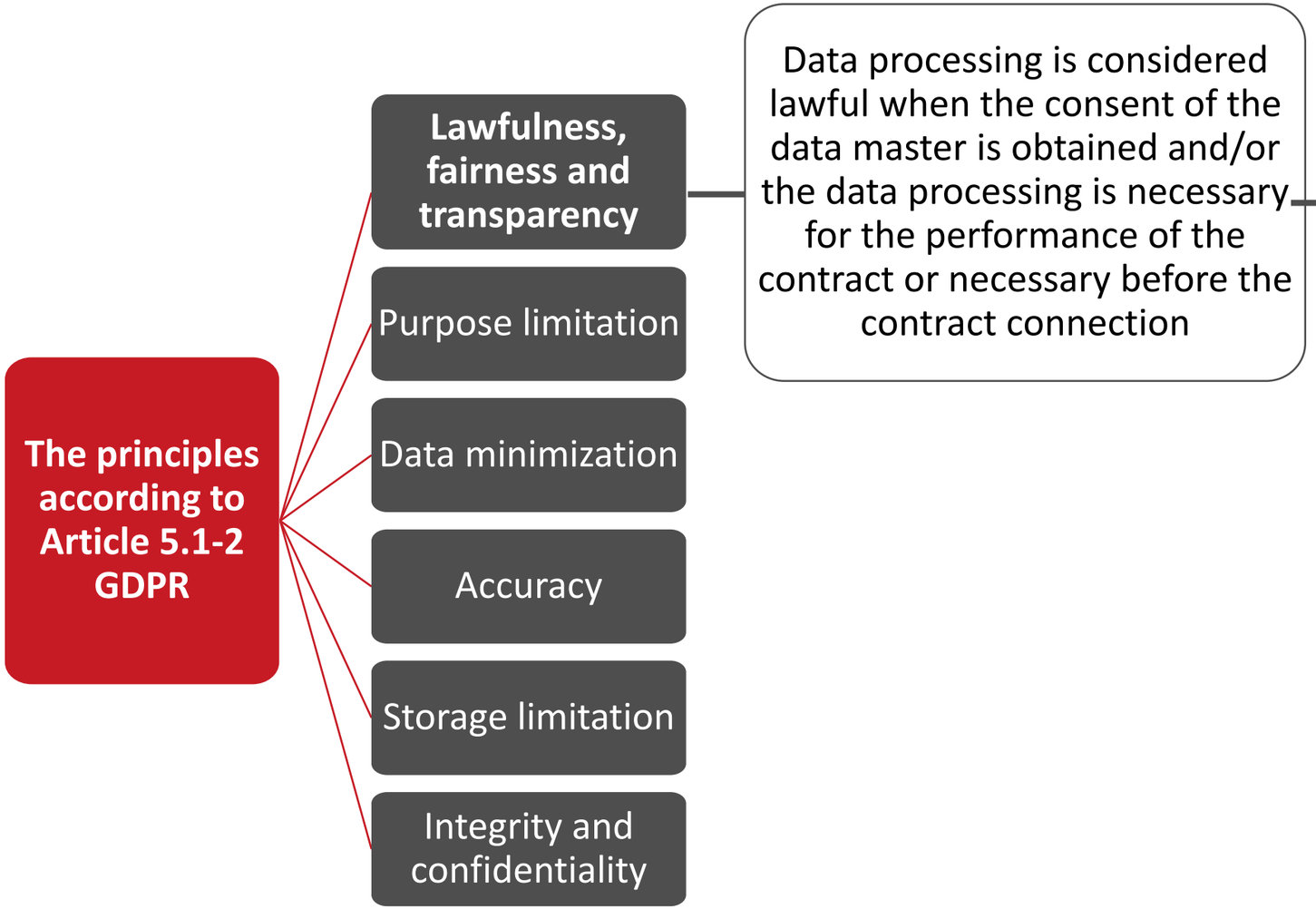
- **“Processor**” refers to an organization or individual that processes personal data on behalf of the Controller
- **“Controller”** refers to an organization or individual that is independent or accompanied by others to determine purposes and means of processing personal data; if the purposes and means of processing are determined by Union law or a Member State, the Controller or the specific criteria for an appointment can be provided by Union law or a Member State.
- **“Cross-border Processing”** is:
  - Processing of personal data takes place in the context of the activities of branches in more than one Member State of the Controller or Processor within the Union when the Controller or Processor is established in more than one Country member; or
  - Processing of personal data takes place in the context of the activities of only one branch of the Controller or Processor in the Union but affects or is likely to significantly affect data subjects in more than one Member State.

1.3. Classification of personal data

General personal data
• Name • Photo • Phone number • Bank account • Email • Digital account information • Certificate • Gender

Sensitive personal data
• Health record • Biometric or biology data • Judicial record • Racial and ethnic origin • Sexual orientation • Political opinions • Religious beliefs • Association membership • Data on crimes and criminal activities

1.4. Data protection principles



Conditions for consent (Article 7 GDPR):

1. When processing is based on consent, the controller shall be able to demonstrate clearly that the data subject has consented.
2. The consent is expressed easily and clearly.
3. The data subject shall have the right to withdraw his or her consent at any time.
4. Considering whether the consent was given freely, exceeding contractual obligations or not

** Where the children is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child.*

1.5. Right of access by data subject

1.5. Restrictions (Article 23 GDPR)

➢ *Some rights related to personal data may be limited in the following cases:*

- ❖ National security; defence; public security;
- ❖ The prevention, investigation, detection or prosecution of criminal offences;
- ❖ Other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State;
- ❖ The protection of judicial independence and judicial proceedings;
- ❖ The prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
- ❖ A monitoring, inspection or regulatory function connected;
- ❖ The protection of the data subject or the rights and freedoms of others;
- ❖ The enforcement of civil law claims.

1.6. Contractual relationships

In fact, between the subjects (Controller, Processor) the following contractual relationships can arise:

Relationship between Data Controller - Data Processor:	**Relationship between Joint Data Controllers:**	**Relationship between Data Controllers (not joint):**	**Complex relationship between Joint Data Controllers - Data Processor**	**Complex relationship between Data Controllers (not joint) - Data Processor**
Specified in Article 28 GDPR, which stipulates a number of specific provisions that need to be implemented in the contract	Specified in Article 26 GDPR, which includes instructions stipulating some of the content required in the contract	GDPR does not specifically stipulate, the contract also needs to have provisions stipulating the specific responsibilities of each party	GDPR does not specifically stipulate, the contract also needs to have provisions stipulating the specific responsibilities of each party	The content specified under Article 28 GDPR and provisions regulating the specific responsibilities of each Data Controllers (not joint) party need to be implemented in the contract

1.6. Transfer of personal data abroad

Transfer on the basis of an adequacy decision (Article 45): the Commission decide after assessing the adequacy of the level of protection of a third country

Transfer subject to appropriate safeguards (Article 46):

A determination of adequacy is not required, based on the safeguards provide by the Controller or Processor

Transfer or disclosure not authorized by Union law (Article 48)): Only recognized in any manner if based on an international agreement

Derogation for specific situations(Article 49): Specific conditions such as express consent or necessary for the performance of a contract without violating the rights of data subject

International cooperation for the protection of personal date (Article 50): Develop international cooperation mechanisms, provide international mutual assistance, engage relevant stakeholders and promote the exchange and documentation of personal data to enforce data protection law globally.

1.7. Notification of a personal data breach:

Notify to the supervisory authority

- In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it.
- Notify to the supervisory authority competent in accordance with Article 55 .
- *Where the notification to the supervisory authority is not made in 72 hours, it shall be accompanied by reasons for the delay.*

Communicate with the data subject

- When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.
- The communication shall describe in clear and plain language.
- The communication shall not be required if any of the following conditions are met:
  i) The controller has implemented protection measures that render the personal data unintelligible to any person (such as encryption);
  ii) The controller has taken subsequent measures which ensure the high risk to the rights and freedoms of data subjects;
  iii) The notification is ineffective

1.8. Form of handling violations

1. **Corrective measures , for example**:

- Require the organization to fully comply with individual rights under the GDPR
- Require direct contact with the individual when a breach of personal data occurs
- Apply temporary or permanent prohibition of processing personal data

2. **Fines:**

Fines may be imposed by the Authorities in addition to or in place of corrective measures, details:

20M€ or 4% of the firm's worldwide annual revenue	10M€ or2% of the firm's worldwide annual revenue
•The basic principles for processing; •The data subjects' rights; •The principles of information transfer; •Failure to comply with the Authority's decision to temporarily or permanently prohibit the processing of personal data	•Obligation to obtain consent when collecting information from children under 16 years old; •Obligation to appoint a DPO and Representative in the EU; •Obligation of the information processor; •Obligation to store information processing history; •Obligation to notify authorities and individuals when personal data is violated; •Obligation to assess impact on information security

1.9. Appoint data protection officer - DPO

The need to specify DPO

- The collecting and processing of personal data is carried out regularly and systematically
- The collecting and processing of personal data is carried out on a large scale

Tasks of DPO

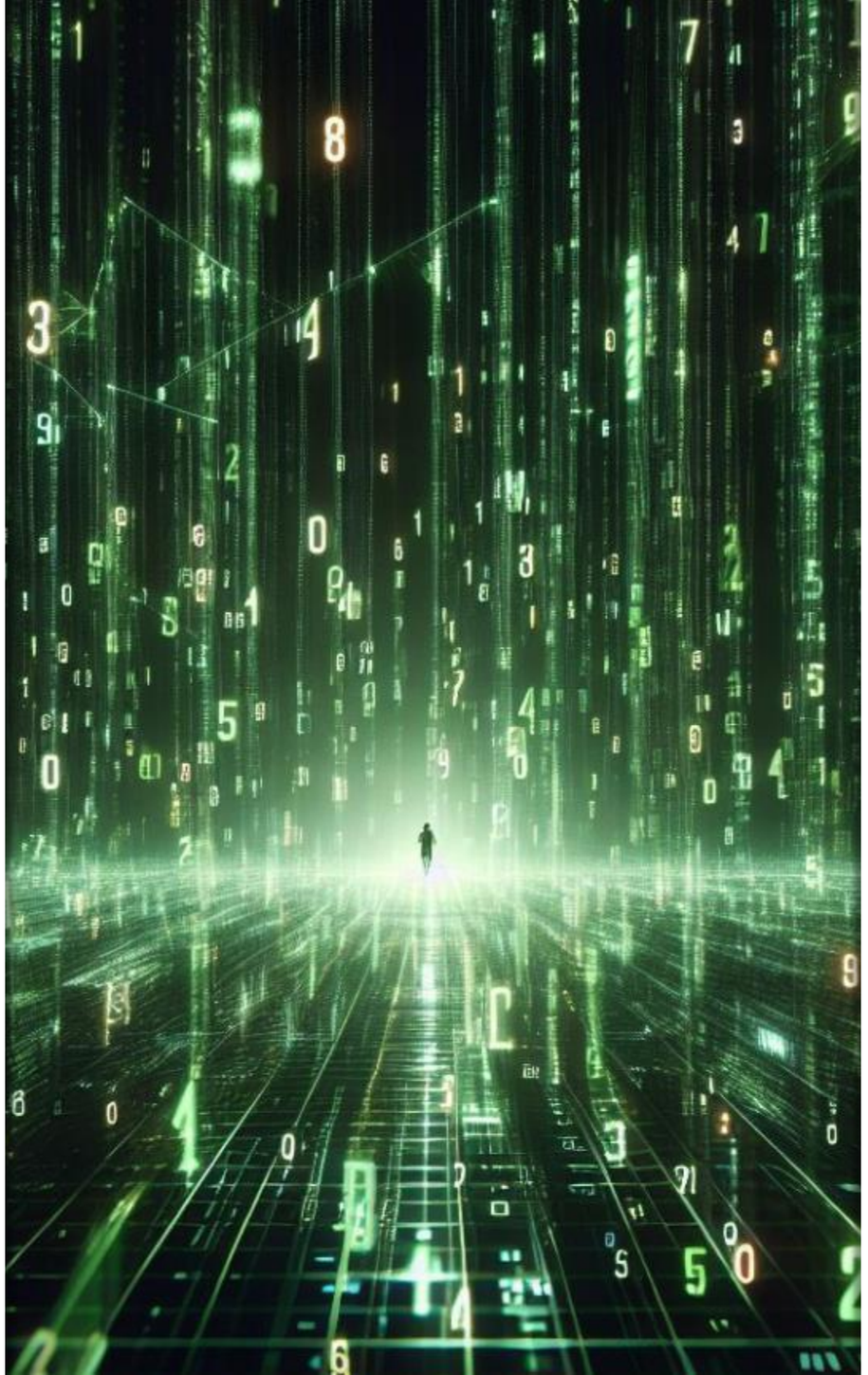
- Advise the enterprises, organizations, individuals who carry out processing of their obligations pursuant to regulations of GDPR ;
- Monitor GDPR compliance and implement of enterprise security regulations;
- Act as the contact point for the supervisory authority on issues relating to collecting and processing data

1.10. A data security supervisory authority

- A data security supervisory authority is established and operates in each EU Member State;
- When the processing of personal data is carried out in multiple EU Member States, a Lead Supervisory Authority on data security should be appointed to take the lead in receiving and handling complaints related to data processing.

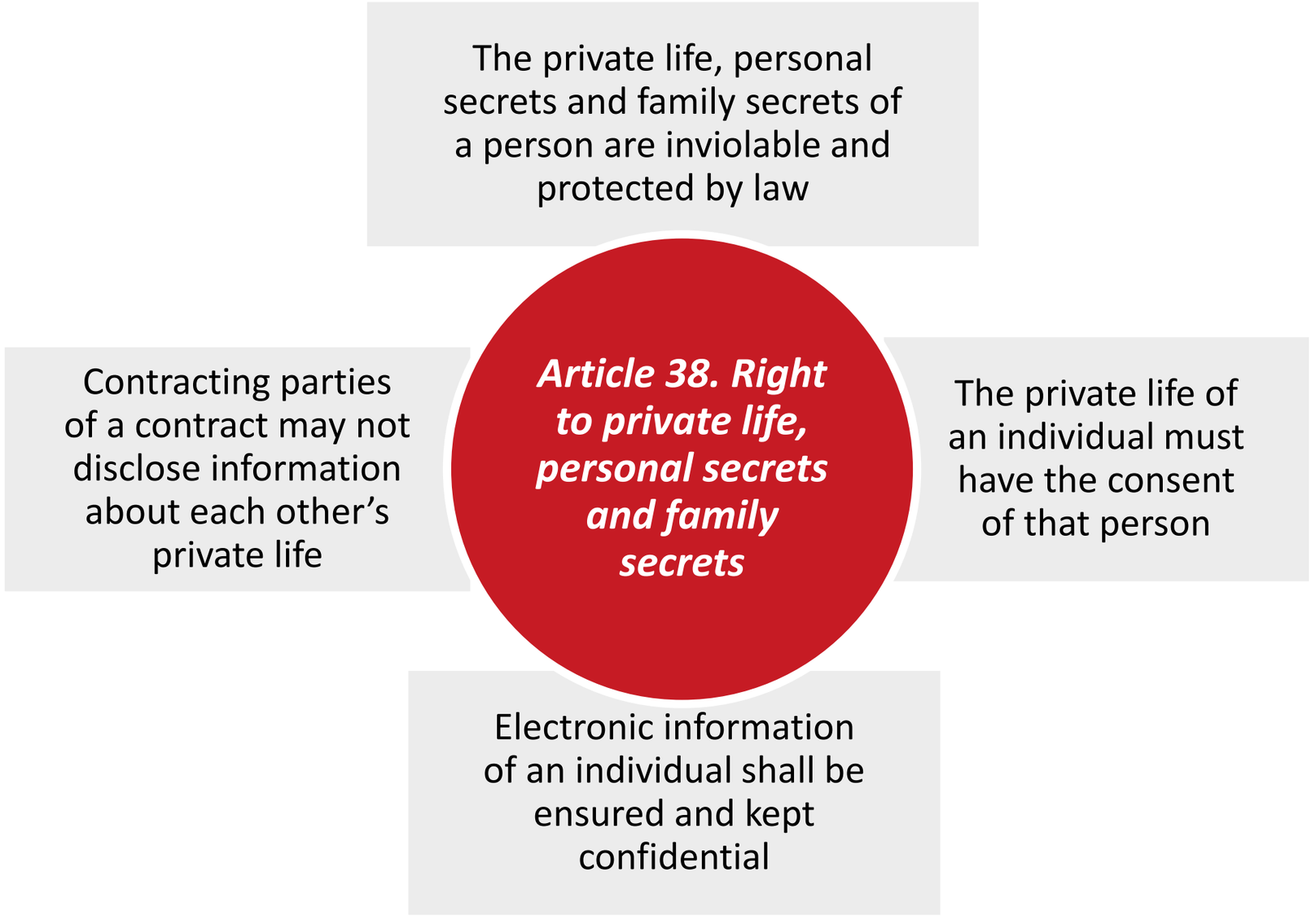
2

DECREE 13/2023/ND-CP ON PROTECTION OF PERSONAL DATA



2 | DECREE 13/2023/ND – CP ON PROTECTION OF PERSONAL DATA

2.1. Platform for developing regulations on personal data protection



2.2. The basic contents

Classification of personal data *Articles 2.3 and 2.4 Decree 13/2023/ND-CP*

- **General personal data**: Name; Gender; DOB; Nationality; Personal image; Phone number; ID card;….
- **Sensitive personal data**: Political and religious opinions; Genetic data; Data on crimes; Personal location identified;…

Consent of a data subject *Articles 2.7 and 2.8 Decree 13/2023/ND-CP*

- The data subject permits the processing of his/her personal data in a clear, voluntary and affirmative manner

Third Party process personal data *Articles 2.12 Decree 13/2023/ND-CP*

- Organization or individual other than the data subject, Personal Data Controller, Personal Data Processor, and Personal Data Controller-cum-Processor that is permitted to process personal data

2 | DECREE 13/2023/ND – CP ON PROTECTION OF PERSONAL DATA

2.3 Personal Data Controller (Article 9)

- Right to be provided information
- Right to consent
- Right to access
- Right to withdraw consent
- Right to erasure
- Right to restriction of processing
- Right to refuse to provide data
- Right to object data processing
- Right to complain, denounce and sue
- Right to claim compensation for damages
- Right to self-defense

Note: The subject's silence is not considered consent

2.4. Prohibited acts of processing personal data (Article 8 Decree 13)

1. Process personal data in contravention of regulations of law

2. Provide information and data against regulations of the Socialist Republic of Vietnam

3. Provide information and data that affect national security, social order and safety

4. Obstruct protection of personal data by competent authorities

5. Take advantage of protection personal data to commit violations of law

2.5. Notification of violations against regulations on protection of personal data

The Processor detects a violation against on protection of personal data

The Personal Data Controller or the Personal Data Controller-cum-Processor detects detects a violation against on protection of personal data

No later than 72 hours after occurring a violation

Notify the Ministry of Public Security (the reason for the late notification shall be provided)

Note: If it is impossible to notify all the information specified, the notification may be given every time a piece of information is available

Notification contents: a)Description of the violation, b) Contact details, c) Description of consequences and damage, d) Description of measures for handling and minimizing the harm

Make a written confirmation of the violation and cooperate with the Ministry of Public Security

2.6. Outbound transfer of personal data (Article 25)

- Personal Data Controller
- Personal Data Controller-cum-Processor
- Personal Data Processor
- Third Party

Notify information about data transfer and contact details of the organization or individual in charge **in writing**

Prepare a dossier on assessment of impact of outbound transfer of personal data: information and contact details, description of objectives and data types, data protection measures, impact assessment, consensus intention of the data subject, biding document for the party receiving the data transfer

Send 01 original copy

Ministry of Public Security makes assessment and request to complete the dossier or stop transferring data

2 | DECREE 13/2023/ND – CP ON PROTECTION OF PERSONAL DATA

2.7. Handling violations against regulations on protection of personal data

"Agencies, organizations and individuals that commit violations against regulations on protection of personal data, depending on the severity violations, may be disciplined, or face administrative penalties or criminal prosecution according to regulations."" (Article 4 Decree 13/2023/ND-CP)

Administrative measures

- Fail to adopt measures to protect privacy or personal information of service users: A fine ranging from 30 – 50 million Dong (Article 65.1.c Decree 174/2013/ND-CP)
- Reveal illegally private information of users: A fine ranging from 50 – 70 million Dong (Article 66.4.a ND 174)
- Trade or exchange illegally private information of users of telecommunication services (Article 66.5.a ND 174)

Criminal measures

- Infringe upon secret information, mail, telephone, telegraph privacy or other means of private information exchange: up to 3 years' community sentence (Article 159 Criminal Code 2015)
- Provide or use illegally information on computer networks or telecommunications networks: maximum 7 years in prison (Article 288 Criminal Code 2015)
- Infiltrate illegally into the computer network, telecommunications network or electronic device of another person: maximum 5 years in prison, fine up to 300 million Dong (Article 289 Criminal Code 2015)

3

CURRENT STATUS OF PERSONAL DATA PROTECTION AT ENTERPRISE OPERATING IN THE AVIATION SECTOR (CASE STUDY)

3 CURRENT STATUS OF PERSONAL DATA PROTECTION AT ENTERPRISE OPERATING AN AVIATION SECTOR (CASE STUDY)

3.1. Apply GDPR to business

For branches established in EU territory:
Responsible for GDPR compliance

For headquarters in Hanoi: Responsible for GDPPR compliance when data collection and processing is related to one the following two factors:

- Service provision takes place within EU territory: can be implemented via (i) website (with language, website address, flag of EU country…) and/or (ii) agent or box office in the EU
- Regardless of where the service is provided, when the Enterprise's data processing activities related to the customer's behavior when the customer is present in the EU. This criterion is very broad because it does not depend on (i) the customer's nationality and (ii) where the ticket is booked (inside or outside the EU)

In conclusion

GDPR applies in the following cases:

1. **Customers book tickets through the website in the EU market;**
2. **Customers book tickets at agents or box offices in the EU;**
3. **Customers book tickets outside the EU and the Company collects and processes customer data when they are in the EU**

3 CURRENT STATUS OF PERSONAL DATA PROTECTION AT ENTERPRISE OPERATING AN AVIATION SECTOR (CASE STUDY)

3.2. Obligations when collecting information

Enterprises are obliged to obtain consent/ notify customers about the collection and processing of information

Obtain customers consent when:

- Collecting and processing sensitive personal data;
- Collecting and processing sensitive personal data for commercial marketing purposes (except for commercial marketing for the legitimate interests of the Enterprise). For the use of personal data under 16 years ole for marketing, Enterprises must obtain consent from the parents and guardians of that individual under 16 years old;
- Collecting and processing personal data to create customers' profiles that can affect customers' rights.

Notify customers when:

- In addition to the cases requiring approval, the remaining cases must be notified to the individual.
- Regarding the collection of personal data of customers to carry out passenger transportation contract, Enterprise are obliged to notify customers. This obligation has been fulfilled through notification emails to customers and the Privacy Policy content posted on the Enterprise's website.

3 | CURRENT STATUS OF PERSONAL DATA PROTECTION AT ENTERPRISE OPERATING AN AVIATION SECTOR (CASE STUDY)

3.3. Some specific contracts

- **Standard Ground Handling Agreement (SGHA)**

The relationship between the carrier and the ground handling service provider is the relationship between Data Controller – Data Processor, whereby the carrier will send passenger-related information to the ground handling service provider according to the specific regulations in the SGHA for the purpose of implementing the passenger transport contract.

- **Interline, Code-share and Joint Venture Contract**

The relationship between Enterprise and partners in these 3 types of contracts is all a relationship between Joint Data Controllers. Accordingly, both Enterprise and partners have the right to decide the purpose of processing passenger dât to fulfill passenger transportation contract (for Interline and Code-share contracts) or to create a basis General data for analysis, changing commercial policies or creating common customer files (for Joint Venture contract).

- **Wet lease contract**

The relationship between lessee and lessor is the relationship between Data Controller – Data Processor. Accordingly, the lessee will be required to notify the lessor of the passenger list so that the flight crew can obtain information for the purpose of implementing the passenger transportation contract between the lessee and the customer. Therefore, the lessee will hold the role of Data Controller and the lessor will hold the role of Data Processor.

- **Other contracts**

Determining the role of each party in the data processing (whether Data Controller, Data Processor or Joint Data Controllers) is the basis for determining the type of Contract relationship that will apply

3 CURRENT STATUS OF PERSONAL DATA PROTECTION AT ENTERPRISE OPERATING AN AVIATION SECTOR (CASE STUDY)

3.4. Obligation to receive and process requests from individuals regarding the exercise of data rights

- Enterprise are responsible for receiving and processing customer requests to exercise their rights within a period of 01 month from the date of receipt of the request.
- This period may be extended by up to 2 months considering the number and complexity of requests. In case of extension, the Enterprise is still responsible for notifying the customer within 01 month from the date of receiving the request about (i) the extension period, and (ii) the reason for the extension.
- In case the Enterprise does not accept to process the customer's request, the Enterprise must notify the customer within 01 month from the date of receiving the request about (i) the reason for not processing, and (ii) the ability of customers to submit complaints to a supervisory authority.

3 | CURRENT STATUS OF PERSONAL DATA PROTECTION AT ENTERPRISE OPERATING AN AVIATION SECTOR (CASE STUDY)

3.5. Data protection officer - DPO)

- 01 DPO in Hanoi has general responsibility
- 01 DPO in EU

3 CURRENT STATUS OF PERSONAL DATA PROTECTION AT ENTERPRISE OPERATING AN AVIATION SECTOR (CASE STUDY)

3.6. Data Privacy Supervisory authority

The business has appointed the Data Privacy Supervisory Authority in the EU as its Lead supervisory authority

For example: When a customer in Belgium sends a complaint against an Enterprise to the Belgian Supervision Agency, CNIL will be the agency to handle this complaint, based on coordination and collection of information from the Belgian Supervision Agency.

Conclusion

- **Issues that business need to notice to comply with GDPR:**

1. Personal information security policy ensures GDPR compliance
2. Develop and regulate personal data processing procedures
3. Regulate procedures related to processing data that is sensitive information
4. Regulations in case of a breach related to personal data
5. Appoint DPO and information collection channel when violations occur (contact address, DPO)
6. Build a channel that allows customers to refuse/approve the provision and processing of custormers' personal data
7. Contract samples
8. Assess the impact when building a system containing personal data
9. Develop regulatory processes to ensure information security

Thank you!

PRESENTED BY

Nguyen Van Tuan

Partner

Mobile: +84 942 545 568

Email: vantuan.nguyen@lntpartners.com

LNT & Partners

Website: www.LNTPartners.com

Blog: www.Vietnamlawinsight.com

Partners: Tran Thai Binh, Bui Ngoc Hong, Hoang Nguyen Ha Quyen, Le Net, Nguyen Anh Tuan, Nguyen Xuan Thuy, Vu Thanh Minh, Nguyen Cong Phu, Nguyen Van Tuan.

LNT & PARTNERS

Ho Chi Minh City Office
Level 21, Bitexco Financial Tower
No.02 Hai Trieu Street, District 1
Ho Chi Minh City, Vietnam
Tel: +84 28 3821 2357
Fax: +84 28 3910 3733

Hanoi Office
Level 12, Pacific Place Building
83B Ly Thuong Kiet Street, Hoan Kiem District
Hanoi, Vietnam
Tel: +84 24 3824 8522
Fax: +84 24 3824 8580

Singapore Office
Level 40, Ocean Financial Centre
10 Collyer Quay
Singapore 049315
Tel: +65 6808 6288

LNT & PARTNERS
INNOVATIVE LEGAL SOLUTIONS

ISSUES IN BANK DEBT COLLECTION PRACTICES

Nguyen Cong Phu
Partner, LNT & Partners
Arbitrator, VIAC

Ho Chi Minh City, 28 Febuary 2024

OUTLINE

1 | THIRD-PARTY GUARANTEE

2 | REFUNDING

3 | SUING FOR DEBT COLLECTION OR FOR COLLATERAL?

4 | REGISTRATION OF SECURED TRANSACTIONS

1

THIRD-PARTY GUARANTEE

1 | THIRD-PARTY GUARANTEE

- Nature and name of the contract
- Validity and countervailing validity with third-party
- Guarantee by asset jointly owned by third party
- Relationship between mortgage and guarantee in the same contract
- Why not separate the guarantee and mortgage into two contracts?

1 | THIRD-PARTY GUARANTEE

Nature and name of the contract

- **Nature:** Guarantee and Collateral Agreement
- **Name:** Third party Mortgage Agreement

? **Does the asset secure the Borrower's obligation or the Guarantor's obligation?**

? **Is the validity of the contract affected by its name?**

1 | THIRD-PARTY GUARANTEE

Is the validity of the contract affected by its name?

- Relationship between validity and countervailing validity with third-party

? **How to apply third-party countervailing validity with third-party?**

1 | THIRD-PARTY GUARANTEE

Guarantee by asset jointly owned by third party

Summary of a case:

- The bank lends money to company A with collateral which is common property of husband and wife
- Only the husband signed into Mortgage Agreement (notarized); the wife **did not**
- First Trial Court: Invalidate a part of Mortgage Agreement (the wife's part)
- First Appellate Court: Invalidate entire Mortgage Agreement (due to inability to separate)
- Second Trial Court: Invalidate a part of Mortgage Agreement (like First Trial Court)
- Second Appellate Court: Invalidate entire Mortgage Agreement (like First Appellate Court)
- Cassation: Invalidate a part of Mortgage Agreement

? **Validity of Mortgage Agreement without signature of a co-owner?**

1 | THIRD-PARTY GUARANTEE

Relationship between mortgage and guarantee in the same contract

? **Invalid guarantee => Invalid mortgage?**

? **Invalid mortgage => Invalid guarantee?**

1 | THIRD-PARTY GUARANTEE

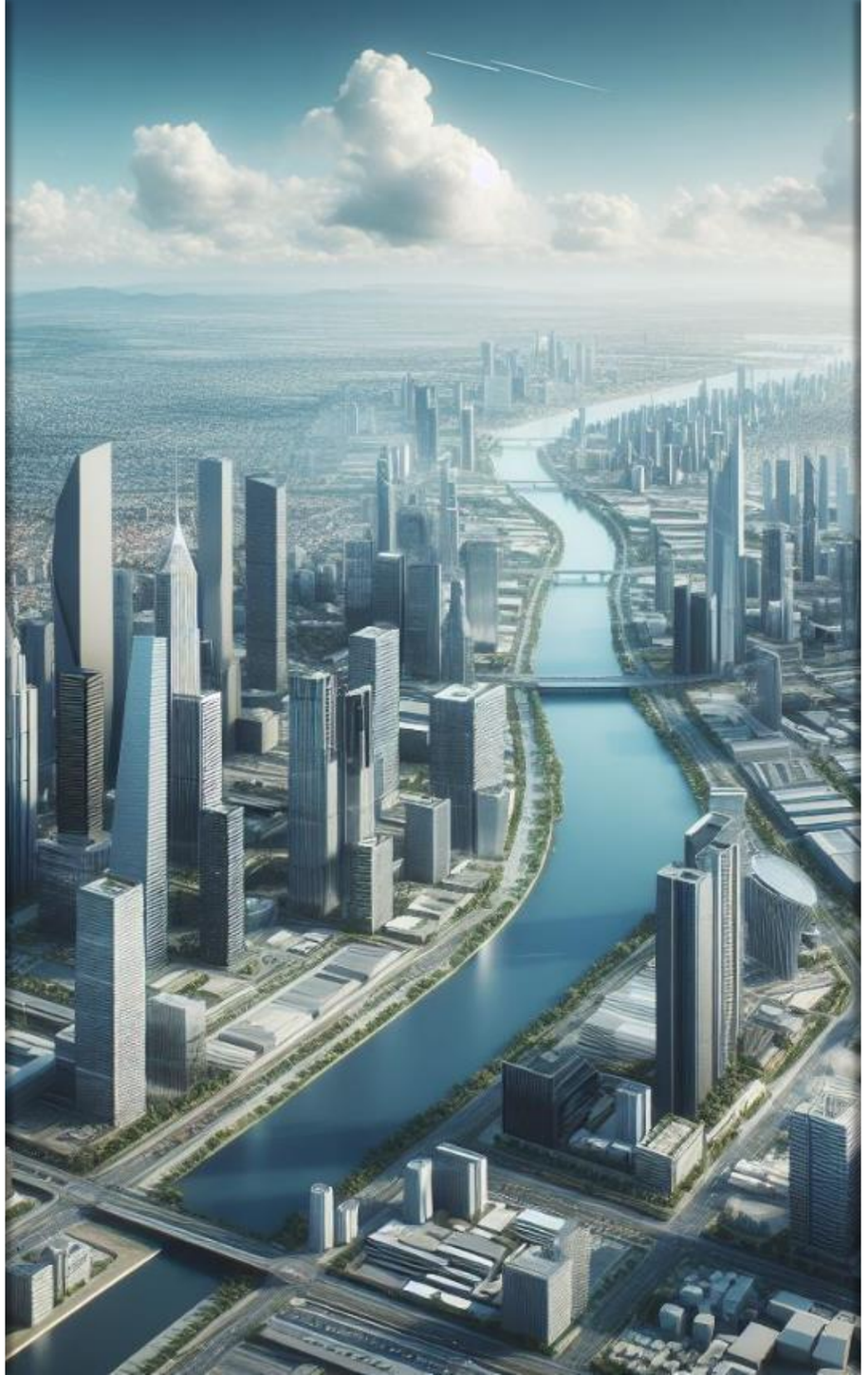
Why not separate the guarantee and mortgage into two contracts?

- The benefit of separating into two contracts

? Practice: Why can’t banks separate?

2

REFUNDING



2 | REFUNDING

- Legal and illegal refunding
- Burden of proving whether refunding is legal or illegal
- Guarantor’s obligation in case of illegal refunding

3

SUING FOR DEBT COLLECTION OR FOR COLLATERAL?

3 | SUING FOR DEBT COLLECTION OR FOR COLLATERAL?

- Right to sue and content of lawsuit’s request
- Distinguish between requests for transferring collateral and disposing of collateral
- When to sue for transferring collateral, when to sue for disposing of collateral?
- Is it possible to sue for debt collection without requesting for disposing of collateral?

4

REGISTRATION OF SECURED TRANSACTIONS

4 | REGISTRATION OF SECURED TRANSACTIONS

- Meaning of registration of secured transactions
- Particular case: Registration of Land Use Right Mortgage

THANK YOU!

PRESENTED BY

Nguyen Cong Phu

Partner

Mobile: +84 913 672 424

Email: phu.nguyen@lntpartners.com

LNT & Partners

Website: www.LNTPartners.com

Blog: www.Vietnamlawinsight.com

Partners: Tran Thai Binh, Bui Ngoc Hong, Hoang Nguyen Ha Quyen, Le Net, Nguyen Anh Tuan, Nguyen Xuan Thuy, Vu Thanh Minh, Nguyen Cong Phu, Nguyen Van Tuan.

LNT & PARTNERS

Ho Chi Minh City Office

Level 21, Bitexco Financial Tower
No.02 Hai Trieu Street, District 1
Ho Chi Minh City, Vietnam

Tel: +84 28 3821 2357
Fax: +84 28 3910 3733

Hanoi Office

Level 12, Pacific Place Building
83B Ly Thuong Kiet Street, Hoan Kiem District
Hanoi, Vietnam

Tel: +84 24 3824 8522
Fax: +84 24 3824 8580

Singapore Office

Level 40, Ocean Financial Centre
10 Collyer Quay
Singapore 049315

Tel: +65 6808 6288

BÀI TRÌNH BÀY BẢN TIẾNG VIỆT

LNT & PARTNERS
INNOVATIVE LEGAL SOLUTIONS

TUÂN THỦ CÁC QUY ĐỊNH CHUNG VỀ BẢO VỆ DỮ LIỆU (GDPR) CỦA LIÊN MINH CHÂU ÂU TẠI VIỆT NAM

TS. Nguyễn Văn Tuấn

Luật sư thành viên LNT & Partners

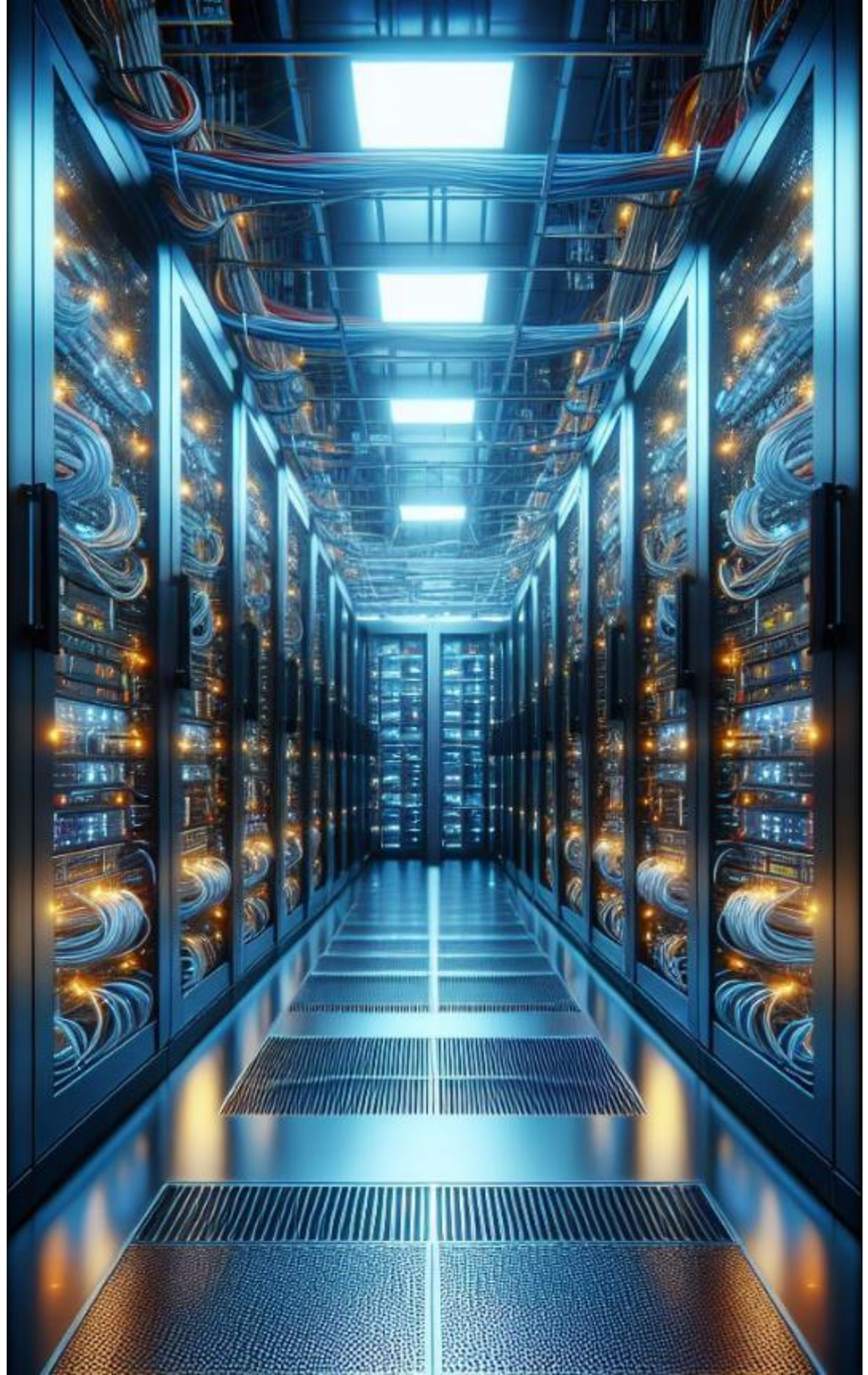
TP Hồ Chí Minh, ngày 28 tháng 02 năm 2024

NỘI DUNG CHÍNH

1 | GIỚI THIỆU VỀ GDPR

2 | QUY ĐỊNH VỀ BẢO VỆ DỮ LIỆU CÁ NHÂN THEO NGHỊ ĐỊNH 13/2023/NĐ-CP

3 | THỰC TRẠNG BẢO VỆ DỮ LIỆU CÁ NHÂN TẠI DOANH NGHIỆP HOẠT ĐỘNG TRONG LĨNH VỰC HÀNG KHÔNG (CASE STUDY)



1

GIỚI THIỆU VỀ GDPR

1 | GIỚI THIỆU VỀ GDPR

1.1. Phạm vi áp dụng

Các tổ chức/công ty được thành lập trên lãnh thổ EU;

Các tổ chức/công ty không được thành lập trên lãnh thổ EU, việc xử lý thông tin phải tuân thủ GDPR khi:

- Việc cung cấp dịch vụ cho cá nhân thực hiện trong EU; hoặc
- Việc giám sát hành vi của cá nhân và hành vi của cá nhân diễn ra trong EU.

1.2. Các khái niệm cơ bản

- "**Dữ liệu cá nhân"** (Personal Data) là thông tin liên quan đến một cá nhân cụ thể, như tên, số định danh, địa chỉ, thông tin trực tuyến hoặc các thông tin đặc biệt khác liên quan đến các khía cạnh về vật lý, sinh lý, di truyền, tâm thần, kinh tế, văn hóa hoặc xã hội của cá nhân đó.
- **"Xử lý dữ liệu"** (Processing) có nghĩa là bất kỳ thao tác hoặc tập hợp các thao tác nào được thực hiện trên dữ liệu cá nhân hoặc các tập dữ liệu cá nhân, có hoặc không thông qua các phương tiện tự động, như thu thập, ghi lại, tổ chức, cấu trúc hóa, lưu trữ, điều chỉnh hoặc thay đổi, truy xuất, tra cứu, sử dụng, tiết lộ qua truyền tải, phổ biến hoặc cung cấp thông tin, sắp xếp hoặc kết hợp, hạn chế, xóa hoặc hủy.
- **"Chủ thể dữ liệu"** (Data subject) là chủ thể mà dữ liệu cá nhân có liên quan tới.
- **"Sự đồng ý'** (Consent) của chủ thể dữ liệu có nghĩa là bất kỳ biểu hiện ý muốn cụ thể, tự do, được thông tin và không mơ hồ của chủ thể dữ liệu, bằng cách tuyên bố hoặc thông qua hành động tích cực rõ ràng, biểu thị sự đồng ý với việc xử lý dữ liệu cá nhân liên quan đến mình.
- **"Cơ quan giám sát"** (Supervisory Authority) là một cơ quan công cộng độc lập được thành lập bởi một Quốc gia thành viên

1.2. Các khái niệm cơ bản

- **“Bên xử lý”** (Processor) là một người tự nhiên hoặc pháp nhân, cơ quan công cộng, cơ quan hoặc tổ chức khác, thực hiện việc xử lý dữ liệu cá nhân thay mặt cho bên kiểm soát."
- **“Bên kiểm soát”** (Controller) là người tự nhiên hoặc pháp nhân, cơ quan công cộng, cơ quan hoặc tổ chức khác, độc lập hoặc cùng với người khác, xác định mục đích và phương tiện của việc xử lý dữ liệu cá nhân; nếu mục đích và phương tiện của việc xử lý được xác định bởi luật Liên minh hoặc của một Quốc gia thành viên, thì bên kiểm soát hoặc các tiêu chí cụ thể cho việc bổ nhiệm có thể được quy định bởi luật Liên minh hoặc của một Quốc gia thành viên."
- **“Xử lý dữ liệu xuyên biên giới”** (Cross-border Processing) là:
  - Xử lý dữ liệu cá nhân diễn ra trong ngữ cảnh các hoạt động của các cơ sở ở nhiều Quốc gia thành viên của Bên kiểm soát hoặc Bên xử lý trong Liên minh khi Bên kiểm soát hoặc Bên xử lý được thành lập ở nhiều Quốc gia thành viên; hoặc
  - Xử lý dữ liệu cá nhân diễn ra trong ngữ cảnh các hoạt động của một cơ sở duy nhất của Bên kiểm soát hoặc Bên xử lý trong Liên minh nhưng ảnh hưởng đến hoặc có khả năng ảnh hưởng đáng kể đến chủ thể dữ liệu ở nhiều Quốc gia thành viên.

1.3. Phân loại dữ liệu cá nhân

Dữ liệu thông thường	**Dữ liệu nhạy cảm**
• Tên • Ảnh • Số điện thoại • Tài khoản ngân hàng • Email • IT (địa chỉ IPv4, địa chỉ MAC, ...) • Chứng chỉ • Giới tính	• Hồ sơ y tế • Vân tay (dữ liệu sinh trắc học) • Hồ sơ tư pháp • Nguồn gốc sắc tộc • Xu hướng tình dục (hành vi/ sở thích) • Quan điểm chính trị • Niềm tin tôn giáo • Thành viên Hiệp hội • Hồ sơ hình sự hoặc hành vi phạm tội

1.4. Nguyên tắc xử lý dữ liệu cá nhân

Xử lý dữ liệu được coi **là hợp pháp** khi đạt được **sự đồng ý** của chủ thể dữ liệu và/hoặc việc xử lý dữ liệu là cần thiết để thực hiện hợp đồng hoặc cần thiết trước khi giao kết hợp đồng

Các điều kiện của sự đồng ý ***(Điều 7 GDPR)***:

1. Việc đã đạt được sự đồng ý phải được Bên kiểm soát thể hiện rõ
2. Sự đồng ý được thể hiện đơn giản, rõ ràng
3. Chủ thể dữ liệu có quyền rút lại sự đồng ý bất cứ lúc nào
4. Xem xét liệu sự đồng ý có được đưa ra một cách tự do hay không, có vượt quá nghĩa vụ hợp đồng không

** Đối với việc sử dụng dữ liệu cá nhân dưới 16 tuổi phải xin sự đồng ý của cha mẹ, người giám hộ của cá nhân dưới 16 tuổi đó.*

1.5. Quyền của chủ thể dữ liệu

1.5. Các trường hợp ngoại lệ (Điều 23)

➢ *Một số quyền liên quan đến dữ liệu cá nhân có thể bị hạn chế trong các trường hợp:*

- ❖ Quốc phòng; an ninh quốc gia, an ninh công cộng;
- ❖ Ngăn chặn, điều tra, phát hiện hoặc truy tố tội phạm;
- ❖ Mục tiêu quan trọng khác của lợi ích công cộng tổng quát của EU hoặc của một tiểu bang, bao gồm các vấn đề tiền tệ, ngân sách và thuế, y tế công cộng và an sinh xã hội
- ❖ Bảo vệ độc lập tư pháp và các thủ tục tư pháp;
- ❖ Ngăn chặn, điều tra, phát hiện và truy tố vi phạm đạo đức đối với các nghề nghiệp được quy định
- ❖ Thực hiện chức năng giám sát, kiểm tra hoặc thực thi quyền lực công
- ❖ Bảo vệ chủ thể dữ liệu hoặc các quyền và tự do của người khác;
- ❖ Thực thi các yêu cầu pháp luật dân sự.

1.6. Các mối quan hệ hợp đồng có thể phát sinh

Trên thực tế, giữa các chủ thể (Controller, Processor) có thể phát sinh những mối quan hệ Hợp đồng sau:

Quan hệ giữa Data Controller - Data Processor:	Quan hệ giữa các Joint Data Controllers:	Quan hệ giữa các Data Controllers (not joint):	Quan hệ phức hợp giữa Joint Data Controllers - Data Processor	Quan hệ phức hợp giữa Data Controllers (not joint) - Data Processor
Được quy định tại Điều 28 GDPR, trong đó có quy định một số điều khoản cụ thể cần triển khai trong Hợp đồng.	Được quy định tại Điều 26 GDPR, trong đó có hướng dẫn quy định một số nội dung cần có trong Hợp đồng.	GDPR không quy định cụ thể, trong Hợp đồng cũng cần có điều khoản quy định về trách nhiệm cụ thể của mỗi bên.	GDPR không quy định cụ thể, trong Hợp đồng cần có điều khoản quy định về trách nhiệm cụ thể của mỗi bên.	Các nội dung quy định theo Điều 28 GDPR và điều khoản quy định về trách nhiệm cụ thể của mỗi bên Data Controllers (not joint) cần được triển khai trong Hợp đồng.

1.6. Chuyển dữ liệu cá nhân ra nước ngoài

Chuyển Giao Dựa trên Quyết Định Về Sự Phù Hợp (Điều 45): do Ủy banq quyết định sau khi xem xét mức độ bảo vệ dữ liệu của QGT3

Chuyển Giao Dưới Sự Bảo Vệ Phù Hợp (Điều 46): Không cần một quyết định về sự phù hợp, dựa trên các biện pháp bảo vệ do Bên kiểm soát hoặc Bên xử lý cung cấp

Chuyển Giao Không Được Ủy quyền Bởi Luật Liên minh (Điều 48): Chỉ được công nhận nếu dựa trên các thỏa thuận quốc tế

Miễn Trừ cho Tình Huống Cụ Thể (Điều 49): theo các điều kiện cụ thể như sự đồng ý rõ ràng hoặc cần thiết để thực hiện hợp đồng, không vi phạm quyền của chủ thể dữ liệu.

Hợp Tác Quốc Tế cho Bảo Vệ Dữ Liệu Cá Nhân (Điều 50): Phát triển các cơ chế hợp tác, cung cấp trợ giúp tương hỗ quốc tế, tham gia các bên liên quan và thúc đẩy trao đổi thông tin để thúc đẩy việc thực thi pháp luật bảo vệ dữ liệu trên toàn cầu.

1.7. Thông báo Vi phạm Dữ liệu Cá nhân:

Thông báo cho Cơ quan có thẩm quyền

- Khi xảy ra vi phạm dữ liệu cá nhân, bên kiểm soát phải thông báo mà không chậm trễ và, nếu khả thi, <u>không muộn hơn 72 giờ</u> kể từ khi nhận thức được vấn đề.
- **Đối tượng thông báo:** Cơ quan giám sát có thẩm quyền (theo Điều 55)
- *Nếu không thực hiện thông báo cho cơ quan giám sát trong vòng 72 giờ, cần đi kèm với lý do cho việc trì hoãn.*

Trao đổi với Chủ thể dữ liệu

- Khi vi phạm có rủi ro xâm phạm quyền và sự tự do an toàn thông tin của chủ thể dữ liệu, Bên kiểm soát phải trao đổi về vi phạm <u>ngay lập tức</u> cho cá nhân đó
- Ngôn ngữ thông báo cần rõ ràng, đơn giản
- **Các trường hợp không cần trao đổi:**
  i) Bên kiểm soát đã có biện pháp khiến dữ liệu cá nhân không thể bị tiếp cận bởi hành vi vi phạm (VD: Mã hóa);
  ii) Bên kiểm soát đã thực hiện biện pháp tiếp theo để giải quyết rủi ro ảnh hưởng đến quyền lợi của chủ thể dữ liệu;
  iii) Việc thông báo không hiệu quả

1.8. Hình thức xử lý vi phạm

1. **Biện pháp khắc phục** (Corrective measures), **ví dụ**:
- Yêu cầu Tổ chức phải tuân thủ đầy đủ các quyền của cá nhân theo GDPR.
- Yêu cầu liên hệ trực tiếp với cá nhân khi xảy ra xâm phạm thông tin cá nhân
- Áp dụng hình thức cấm xử lý thông tin cá nhân tạm thời hoặc vĩnh viễn

2. **Phạt tiền:**

Hình phạt tiền có thể được Nhà chức trách áp dụng bổ sung hoặc thay thế các biện pháp khắc phục, chi tiết:

20M€ hoặc 4% doanh thu toàn cầu khi vi phạm:	**10M€ hoặc 2% doanh thu toàn cầu khi vi phạm:**
•Nguyên tắc cơ bản về thu thập thông tin; •Quyền của cá nhân; •Nguyên tắc chuyển giao thông tin; •Không tuân thủ quyết định của Nhà chức trách về việc cấm xử lý thông tin cá nhân tạm thời hoặc vĩnh viễn.	• Nghĩa vụ xin chấp thuận khi thu thập thông tin trẻ em dưới 16 tuổi; •Nghĩa vụ chỉ định DPO và Đại diện tại EU; •Nghĩa vụ của bên xử lý thông tin; •Nghĩa vụ về lưu trữ lịch sử hoạt động xử lý thông tin; •Nghĩa vụ thông báo cho nhà chức trách và cá nhân khi có xâm phạm thông tin cá nhân; •Nghĩa vụ đánh giá tác động về bảo mật thông tin.

1.9. Chỉ định cán bộ chuyên trách bảo mật dữ liệu (data protection officer - DPO)

Sự cần thiết chỉ định DPO

- Việc thu thập, xử lý dữ liệu cá nhân được thực hiện thường xuyên và có hệ thống
- Việc thu thập, xử lý dữ liệu cá nhân được thực hiện trên phạm vi rộng

Nhiệm vụ

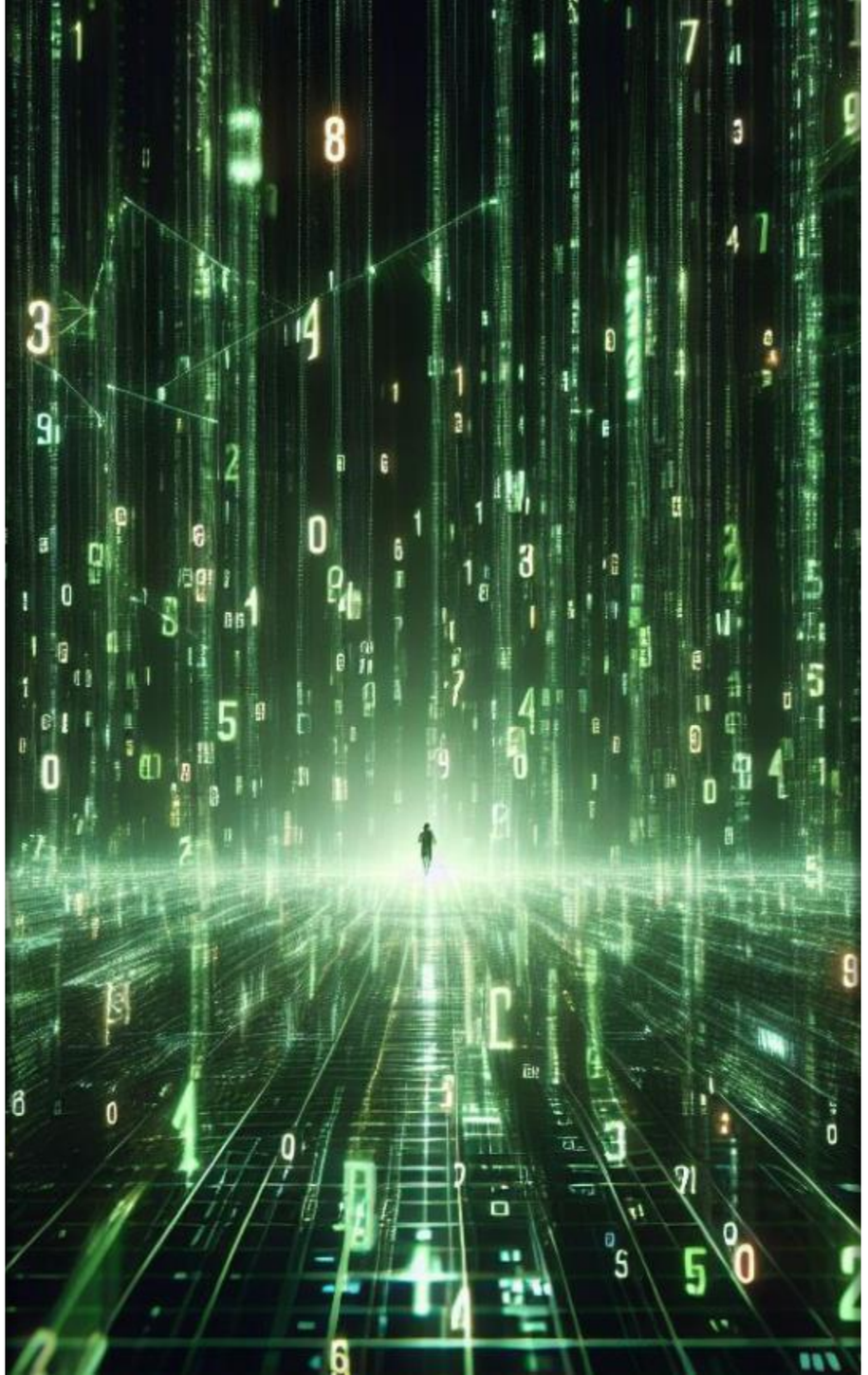
- Tư vấn cho Doanh nghiệp và các CQ, ĐV, cá nhân liên quan đến quá trình xử lý dữ liệu thực thi nghĩa vụ theo quy định tại GDPR
- Giám sát việc tuân thủ GDPR và việc thực hiện quy định về bảo mật của Doanh nghiệp;
- Là đầu mối liên hệ với Cơ quan giám sát tại các quốc gia thành viên về các vấn đề liên quan đến việc thu thập, xử lý dữ liệu.

1.10. Cơ quan giám sát về bảo mật dữ liệu (supervisory authority)

- Cơ quan giám sát về bảo mật dữ liệu được thành lập và hoạt động tại mỗi quốc gia thành viên EU;
- Khi việc xử lý dữ liệu cá nhân được thực hiện trên lãnh thổ nhiều quốc gia thành viên EU, Cơ quan giám sát chính (Lead Supervisory Authority) về bảo mật dữ liệu cần được chỉ định để chủ trì tiếp nhận, xử lý khiếu nại có liên quan đến việc xử lý dữ liệu.

2

QUY ĐỊNH VỀ BẢO VỆ DỮ LIỆU CÁ NHÂN THEO NGHỊ ĐỊNH 13/2023/NĐ-CP



2 | QUY ĐỊNH VỀ BẢO VỆ DỮ LIỆU CÁ NHÂN THEO NGHỊ ĐỊNH 13/2023/NĐ-CP

2.1. Nền tảng xây dựng quy định về bảo vệ dữ liệu cá nhân

2.2. Các nội dung cơ bản

Phân loại dữ liệu cá nhân

Điều 2.3 và 2.4 Nghị định 13/2023/NĐ-CP

- **Dữ liệu cơ bản**: Họ, tên đệm, tên; Ngày tháng năm sinh/chết/mất tích; Giới tính; Nơi sinh; Địa chỉ; Quốc tịch; Hình ảnh cá nhân...
- **Dữ liệu nhạy cảm**: Quan điểm chính trị, tôn giáo; Đặc điểm di truyền; Tội phạm; Thông tin định vị...

Sự đồng ý của chủ thể dữ liệu

Điều 2.7 và 2.8 Nghị định 13/2023/NĐ-CP

- Là việc thể hiện rõ ràng, tự nguyện, khẳng định việc cho phép xử lý dữ liệu cá nhân của Chủ thể dữ liệu.

Bên thứ ba xử lý DLCN

Điều 2.12 Nghị định 13/2023/NĐ-CP

- Tổ chức, cá nhân ngoài Chủ thể dữ liệu, Bên Kiểm soát dữ liệu cá nhân, Bên Xử lý dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân được phép xử lý dữ liệu cá nhân.

2 | QUY ĐỊNH VỀ BẢO VỆ DỮ LIỆU CÁ NHÂN THEO NGHỊ ĐỊNH 13/2023/NĐ-CP

2.3 Quyền của chủ thể dữ liệu (Điều 9)

- Quyền được biết
- Quyền đồng ý
- Quyền truy cập
- Quyền rút lại sự đồng ý
- Quyền xóa dữ liệu
- Quyền hạn chế xử lý dữ liệu
- Quyền từ chối cung cấp dữ liệu
- Quyền phản đối xử lý dữ liệu
- Quyền khiếu nại, tố cáo, khởi kiện
- Quyền yêu cầu bồi thường thiệt hại
- Quyền tự bảo vệ

Lưu ý: Sự im lặng của chủ thể không được coi là đồng ý

2.4. Hành vi bị nghiêm cấm trong xử lý dữ liệu cá nhân (Điều 8 Nghị định 13)

1. Xử lý trái quy định pháp luật

2. Tạo ra thông tin chống chính quyền

3. Tạo ra thông tin, dữ liệu gây ảnh hưởng tới an ninh quốc gia, trật tự an toàn xã hội

4. Cản trở hoạt động bảo vệ dữ liệu cá nhân

5. Lợi dụng hoạt động bảo vệ dữ liệu cá nhân để vi phạm pháp luật.

2.5. Trình tự thủ tục thông báo vi phạm quy định về bảo vệ dữ liệu cá nhân (Điều 23)

Bên Xử lý dữ liệu cá nhân phát hiện vi phạm

Bên Kiểm soát dữ liệu cá nhân và Bên Kiểm soát và xử lý dữ liệu cá nhân phát hiện vi phạm

Chậm nhất sau 72 giờ sau khi xảy ra vi phạm

Thông báo cho Bộ Công an (có lý do nếu thông báo chậm)
Lưu ý: Nếu không thể thông báo đầy đủ, có thể thực hiện theo từng giai đoạn.

Nội dung thông báo vi phạm: a) Mô tả vi phạm, b) Thông tin liên lạc, c) Hậu quả và thiệt hại, d) Biện pháp giảm thiểu tác hại

Lập biên bản xác nhận vi phạm và phối hợp với Bộ Công an xử lý

2.6. Quy định về việc chuyển dữ liệu cá nhân ra nước ngoài (Điều 25)

- Bên Kiểm soát dữ liệu cá nhân
- Bên Kiểm soát và xử lý dữ liệu cá nhân
- Bên Xử lý dữ liệu cá nhân
- Bên thứ ba

→ Thông báo thông tin về việc chuyển dữ liệu và chi tiết liên lạc của tổ chức, cá nhân phụ trách bằng **văn bản**

→ Lập Hồ sơ đánh giá tác động chuyển dữ liệu cá nhân ra nước ngoài (bao gồm: thông tin và chi tiết liên lạc, mô tả mục tiêu và loại dữ liệu, biện pháp bảo vệ dữ liệu, đánh giá tác động, sự đồng ý của chủ thể dữ liệu, văn bản rang buộc đối với bên nhận chuyển dữ liệu)

Nộp 01 bản chính

→ Bộ Công An đánh giá và đưa ra quyết định (hoàn thiện hồ sơ hoặc ngừng chuyển dữ liệu)

2 | QUY ĐỊNH VỀ BẢO VỆ DỮ LIỆU CÁ NHÂN THEO NGHỊ ĐỊNH 13/2023/NĐ-CP

2.7. Xử lý vi phạm quy định bảo vệ dữ liệu cá nhân

"Cơ quan, tổ chức, cá nhân vi phạm quy định bảo vệ dữ liệu cá nhân tùy theo mức độ có thể bị xử lý kỷ luật, xử phạt vi phạm hành chính, xử lý hình sự theo quy định." (Điều 4 Nghị định 13/2023/NĐ-CP)

Các biện pháp hành chính

- Hành vi không có biện pháp bảo vệ TTCN của người dùng: phạt tiền 30 – 50 triệu đồng (Điều 65.1.c Nghị định 174/2013/NĐ-CP)
- Hành vi tiết lộ trái phép TTCN của người dùng: phạt tiền từ 50 – 70 triệu đồng (Điều 66.4.a NĐ 174)
- Hành vi Mua bán/trao đổi trái phép TTCN người dùng dịch vụ viễn thông (Điều 66.5.a NĐ 174)

Các biện pháp hình sự

- Tội xâm phạm bí mật thông trao đổi cá nhân: đến 3 năm tù (Điều 159 BLHS 2015)
- Đưa/sử dụng thông tin trái phép TTCN trên mạng: cao nhất 7 năm tù (Điều 288 BLHS 2015)
- Lấy cắp, thay đổi, hủy hoại, làm giả dữ liệu cá nhân: cao nhất 5 năm tù, phạt tiền lên tới 300 triệu đồng (Điều 289 BLHS 2015)

3

THỰC TRẠNG TUÂN THỦ GDPR TẠI DOANH NGHIỆP HOẠT ĐỘNG TRONG LĨNH VỰC HÀNG KHÔNG (CASE STUDY)

3 | THỰC TRẠNG TẠI DOANH NGHIỆP HÀNG KHÔNG (CASE STUDY)

3.1. Áp dụng GDPR đối với doanh nghiệp

Đối với Chi nhánh thành lập trên lãnh thổ EU:
Có trách nhiệm tuân thủ GDPR

Đối với trụ sở tại Hà Nội: Có trách nhiệm tuân thủ GDPR khi việc thu thập, xử lý dữ liệu có liên quan đến 1 trong 2 yếu tố sau:

- ✓ Việc cung cấp dịch vụ diễn ra trong lãnh thổ EU: có thể được triển khai qua (i) website (với ngôn ngữ, địa chỉ website, quốc kỳ của quốc gia EU…) và/hoặc (ii) đại lý hoặc phòng vé tại EU.
- ✓ Bất kể dịch vụ được cung cấp tại đâu, khi hoạt động xử lý dữ liệu của Doanh nghiệp liên quan đến hành vi của khách hàng khi khách hiện diện tại EU. Tiêu chí này rất rộng bởi nó không phụ thuộc vào (i) quốc tịch của khách hàng và (ii) nơi vé được book (trong hoặc ngoài EU).

Như vậy,

GDPR được áp dụng trong các trường hợp:

1. KH book vé qua website tại thị trường EU;

2. KH book vé tại đại lý hoặc phòng vé tại EU;

3. KH book vé ngoài EU và Doanh nghiệp thu thập, xử lý dữ liệu của khách khi khách ở EU.

3.2. Nghĩa vụ khi thu thập thông tin

Doanh nghiệp có nghĩa vụ phải xin chấp thuận/thông báo tới khách hàng về việc thu thập, xử lý thông tin

Xin chấp thuận của khách hàng khi:

- Thu thập, xử lý dữ liệu cá nhân nhạy cảm (sensitive personal data);
- Thu thập, xử lý dữ liệu cá nhân phục vụ mục đích tiếp thị thương mại (marketing purposes) (trừ trường hợp tiếp thị thương mại vì lợi ích hợp pháp (legitimate interest) của Doanh nghiệp). Đối với việc sử dụng dữ liệu cá nhân dưới 16 tuổi phục vụ mục đích marketing, Doanh nghiệp phải xin chấp thuận của cha mẹ, người giám hộ của cá nhân dưới 16 tuổi đó;
- Thu thập, xử lý dữ liệu cá nhân để tạo hồ sơ cá nhân của khách hàng (profiling) mà có thể ảnh hưởng đến quyền lợi của khách hàng.

Thông báo cho khách hàng khi:

- Ngoài các trường hợp cần xin chấp thuận, các trường hợp còn lại phải thông báo cho cá nhân.
- Đối với việc thu thập các dữ liệu cá nhân của khách để thực hiện hợp đồng vận chuyển hành khách, Doanh nghiệp có nghĩa vụ thông báo cho khách hàng. Nghĩa vụ này **đã** được thực hiện qua các email thông báo tới khách và nội dung Chính sách bảo mật thông tin (Privacy Policy) đăng tải trên website của Doanh nghiệp.

3.3. Một số hợp đồng cụ thể

- **Hợp đồng dịch vụ phục vụ mặt đất (SGHA)**

Mối quan hệ giữa nhà vận chuyển và bên cung cấp dịch vụ PVMĐ là mối quan hệ giữa Data Controller - Data Processor, theo đó nhà vận chuyển sẽ gửi các thông tin liên quan đến hành khách cho bên cung cấp dịch vụ PVMĐ theo các quy định cụ thể trong HĐ SGHA nhằm mục đích thực hiện HĐ vận chuyển hành khách.

- **Hợp đồng Interline, Code-share và Joint Venture**

Mối quan hệ giữa Doanh nghiệp và đối tác trong 03 loại HĐ này đều là mối quan hệ giữa **Joint Data Controllers**. Theo đó, cả Doanh nghiệp và đối tác đều có quyền quyết định mục đích của việc xử lý dữ liệu của khách nhằm thực hiện hợp đồng vận chuyển hành khách (đối với HĐ Interline, HĐ Code-share) hoặc nhằm tạo một cơ sở dữ liệu chung để phân tích, thay đổi chính sách thương mại hoặc tạo tệp khách hàng chung (đối với HĐ Joint Venture).

- **Hợp đồng thuê ướt (wet lease)**

Mối quan hệ giữa bên thuê và bên cho thuê là mối quan hệ giữa Data Controller - Data Processor. Theo đó, bên thuê (lessee) sẽ được yêu cầu phải thông báo cho bên cho thuê (lessor) danh sách hành khách để tổ bay nắm thông tin nhằm mục đích thực hiện HĐ vận chuyển hành khách giữa bên thuê và khách hàng. Vì vậy, bên thuê sẽ giữ vai trò Data Controller và bên cho thuê giữ vai trò Data Processor.

- **Các Hợp đồng khác**

Việc xác định vai trò của mỗi bên trong quá trình xử lý dữ liệu (là Data Controller, Data Processor hoặc Joint Data Controllers) là cơ sở để xác định loại quan hệ Hợp đồng sẽ áp dụng.

3.4. Nghĩa vụ tiếp nhận, xử lý yêu cầu của cá nhân v/v thực hiện quyền đối với dữ liệu

- Doanh nghiệp có trách nhiệm tiếp nhận và xử lý yêu cầu của khách hàng về việc thực hiện các quyền của khách trong khoảng thời gian **01 tháng** kể từ ngày nhận được yêu cầu.
- Khoảng thời gian này có thể kéo dài thêm 02 tháng khi xét đến số lượng và sự phức tạp của các yêu cầu. Trong trường hợp gia hạn thời gian, Doanh nghiệp vẫn có trách nhiệm thông báo cho khách trong vòng 01 tháng kể từ ngày nhận được yêu cầu về (i) khoảng thời gian gia hạn đó, và (ii) lý do gia hạn.
- Trường hợp Doanh nghiệp không chấp nhận xử lý yêu cầu của khách hàng, Doanh nghiệp phải thông báo cho khách hàng trong vòng 01 tháng kể từ ngày nhận được yêu cầu về (i) lý do không xử lý, và (ii) việc khách hàng có thể đệ trình khiếu nại lên cơ quan giám sát.

3.5. Cán bộ chuyên trách về bảo mật dữ liệu (data protection officer - DPO)

- 01 DPO tại Hà Nội chịu trách nhiệm chung
- 01 DPO tại EU

3.6. Cơ quan giám sát về bảo mật dữ liệu (supervisory authority)

Doanh nghiệp đã chỉ định Cơ quan giám sát về bảo mật dữ liệu tại **EU** là cơ quan giám sát chính.

Ví dụ: Khi khách hàng tại Bỉ gửi khiếu nại đối với Doanh nghiệp tới Cơ quan giám sát của Bỉ thì CNIL sẽ là cơ quan xử lý khiếu nại này, trên cơ sở phối hợp, thu thập thông tin từ Cơ quan giám sát của Bỉ.

Kết luận

- **Các vấn đề Doanh nghiệp cần lưu ý để tuân thủ GDPR:**

1. Chính sách bảo mật thông tin cá nhân đảm bảo tuân thủ GDPR.
2. Xây dựng và quy định quy trình xử lý dữ liệu cá nhân.
3. Quy định quy trình liên quan đến xử lý dữ liệu là thông tin nhạy cảm.
4. Quy định trong trường hợp có vi phạm liên quan đến dữ liệu cá nhân.
5. Bổ nhiệm DPO và kênh thu thập thông tin khi xảy ra vi phạm (địa chỉ liên lạc, DPO)
6. Xây dựng kênh cho phép khách từ chối/chấp thuận việc cung cấp, xử lý dữ liệu cá nhân của khách hàng
7. Các mẫu hợp đồng.
8. Đánh giá tác động khi xây dựng hệ thống chứa dữ liệu cá nhân.
9. Xây dựng quy trình quy định đảm bảo an ninh thông tin

Trân trọng cảm ơn!

PRESENTED BY

Nguyen Van Tuan

Partner

Mobile: +84 942 545 568

Email: vantuan.nguyen@lntpartners.com

LNT & Partners

Website: www.LNTPartners.com

Blog: www.Vietnamlawinsight.com

Partners: Tran Thai Binh, Bui Ngoc Hong, Hoang Nguyen Ha Quyen, Le Net, Nguyen Anh Tuan, Nguyen Xuan Thuy, Vu Thanh Minh, Nguyen Cong Phu, Nguyen Van Tuan.

LNT & PARTNERS

Ho Chi Minh City Office

Level 21, Bitexco Financial Tower
No.02 Hai Trieu Street, District 1
Ho Chi Minh City, Vietnam

Tel: +84 28 3821 2357
Fax: +84 28 3910 3733

Hanoi Office

Level 12, Pacific Place Building
83B Ly Thuong Kiet Street, Hoan Kiem District
Hanoi, Vietnam

Tel: +84 24 3824 8522
Fax: +84 24 3824 8580

Singapore Office

Level 40, Ocean Financial Centre
10 Collyer Quay
Singapore 049315

Tel: +65 6808 6288

LNT & PARTNERS
INNOVATIVE LEGAL SOLUTIONS

NHỮNG VẤN ĐỀ PHÁT SINH TRONG THỰC TIỄN HOẠT ĐỘNG THU HỒI NỢ CỦA NGÂN HÀNG

Nguyễn Công Phú

Luật sư thành viên LNT & Partners

Trọng tài viên VIAC

TP Hồ Chí Minh, ngày 28 tháng 02 năm 2024

NỘI DUNG CHÍNH

1 | BẢO LÃNH BẰNG TÀI SẢN CỦA BÊN THỨ BA

2 | TÁI CẤP VỐN

3 | KIỆN ĐÒI NỢ HAY KIỆN ĐÒI GIAO TÀI SẢN BẢO ĐẢM?

4 | ĐĂNG KÝ GIAO DỊCH BẢO ĐẢM

1

BẢO LÃNH BẰNG TÀI SẢN CỦA BÊN THỨ BA

- Bản chất và tên gọi của hợp đồng
- Hiệu lực và hiệu lực đối kháng với người thứ ba
- Bảo lãnh bằng tài sản thuộc sở hữu chung của bên thứ ba
- Quan hệ giữa thế chấp và bảo lãnh trong cùng một hợp đồng
- Vì sao không tách riêng bảo lãnh và thế chấp thành hai hợp đồng?

Bản chất và tên gọi của hợp đồng

- **Bản chất:** Hợp đồng bảo lãnh có thế chấp tài sản
- **Tên gọi:** Hợp đồng thế chấp tài sản của bên thứ ba

? **Tài sản bảo đảm cho nghĩa vụ của bên vay hay của bên bảo lãnh?**

? **Hiệu lực của hợp đồng có bị ảnh hưởng bởi tên gọi?**

Hiệu lực của hợp đồng có bị ảnh hưởng bởi tên gọi?

- Quan hệ giữa hiệu lực và hiệu lực đối kháng với người thứ ba

? **Hiệu lực đối kháng với người thứ ba áp dụng với người thứ ba thế nào?**

Bảo lãnh bằng tài sản thuộc sở hữu chung của bên thứ ba

Tóm tắt một vụ án trong thực tiễn:

- NH cho Cty A vay tiền có tài sản thế chấp thuộc sở hữu chung vợ chồng
- Chỉ có chồng ký, vợ không ký hợp đồng thế chấp (có công chứng)
- Sơ thẩm lần 1: Vô hiệu một phần hợp đồng thế chấp (phần người vợ)
- Phúc thẩm lần 1: Vô hiệu toàn bộ HĐ thế chấp (do không thể phân chia)
- Sơ thẩm lần 2: Vô hiệu một phần hợp đồng thế chấp (giống ST lần 1)
- Phúc thẩm lần 2: Vô hiệu toàn bộ HĐ thế chấp (giống PT lần 1)
- Giám đốc thẩm: Vô hiệu một phần hợp đồng thế chấp

? **Hiệu lực của hợp đồng thế chấp mà có chủ sở hữu chung không ký?**

Quan hệ giữa thế chấp và bảo lãnh trong cùng một hợp đồng

? **Bảo lãnh vô hiệu => Thế chấp vô hiệu?**

? **Thế chấp vô hiệu => Bảo lãnh vô hiệu?**

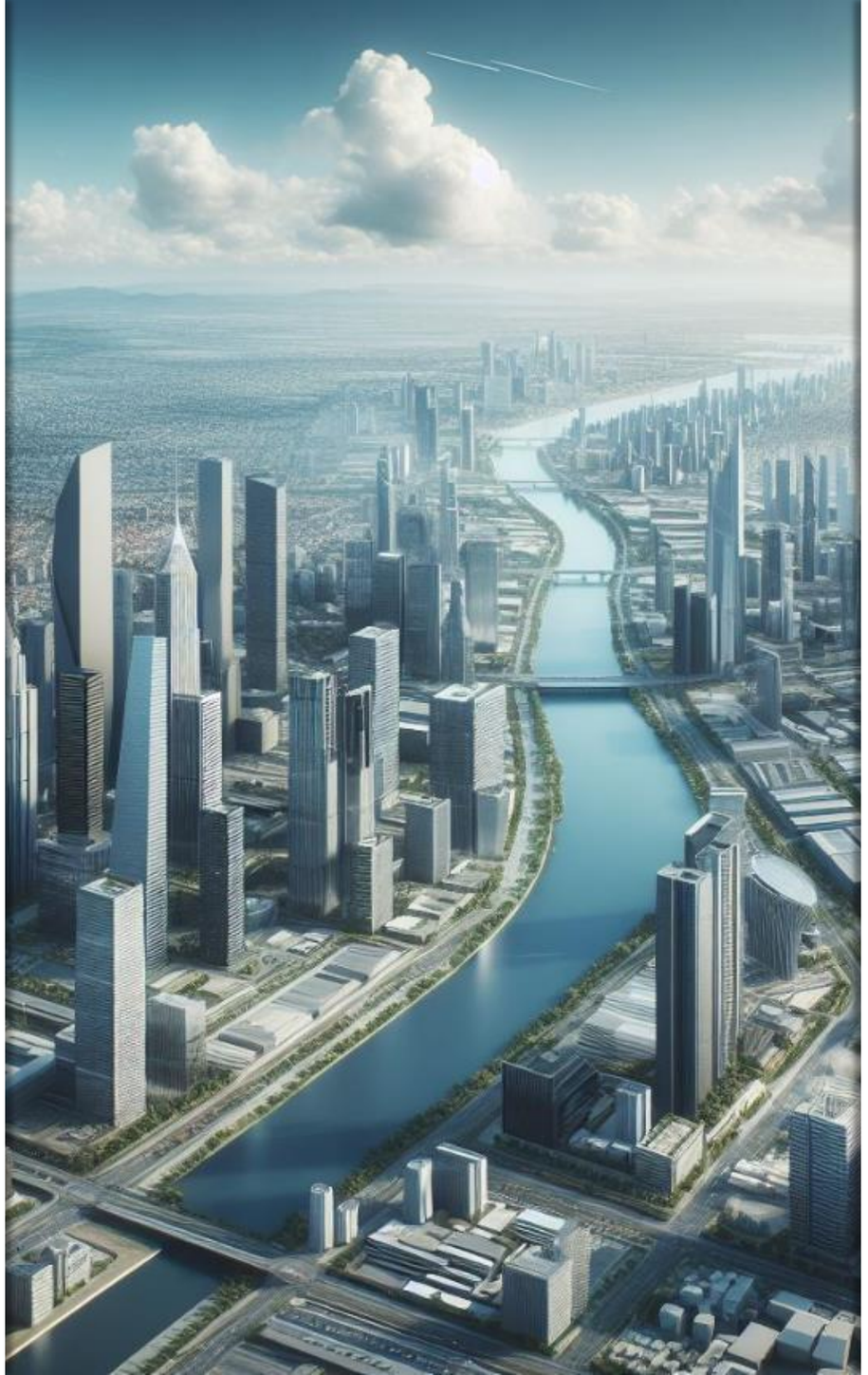
Vì sao không tách riêng bảo lãnh và thế chấp thành hai hợp đồng?

- Lợi ích của việc tách riêng thành 2 hợp đồng

? **Thực tiễn: Vì sao các ngân hàng không thực hiện được?**

2

TÁI CẤP VỐN



2 | QUY ĐỊNH VỀ BẢO VỆ DỮ LIỆU CÁ NHÂN THEO NGHỊ ĐỊNH 13/2023/NĐ-CP

- Tái cấp vốn hợp pháp và không hợp pháp
- Nghĩa vụ chứng minh tái cấp vốn hợp pháp hoặc không hợp pháp
- Nghĩa vụ của người bảo lãnh khi tái cấp vốn không hợp pháp

3

KIỆN ĐÒI NỢ HAY KIỆN ĐÒI GIAO TÀI SẢN BẢO ĐẢM?

3 | THỰC TRẠNG BẢO VỆ DỮ LIỆU CÁ NHÂN TẠI DOANH NGHIỆP HOẠT ĐỘNG TRONG LĨNH VỰC HÀNG KHÔNG (CASE STUDY)

- Quyền khởi kiện và nội dung yêu cầu khởi kiện
- Phân biệt yêu cầu giao tài sản bảo đảm và xử lý tài sản bảo đảm
- Khi nào khởi kiện đòi giao, khi nào khởi kiện đòi xử lý TSBĐ?
- Có thể khởi kiện đòi nợ mà không yêu cầu xử lý TSBĐ?

4

ĐĂNG KÝ GIAO DỊCH BẢO ĐẢM

4 | ĐĂNG KÝ GIAO DỊCH BẢO ĐẢM

- Ý nghĩa của đăng ký giao dịch bảo đảm
- Trường hợp đặc biệt: Đăng ký thế chấp quyền sử dụng đất

Trân trọng cảm ơn!

PRESENTED BY

Nguyen Cong Phu

Partner

Mobile: +84 913 672 424

Email: phu.nguyen@lntpartners.com

LNT & Partners

Website: www.LNTPartners.com

Blog: www.Vietnamlawinsight.com

Partners: Tran Thai Binh, Bui Ngoc Hong, Hoang Nguyen Ha Quyen, Le Net, Nguyen Anh Tuan, Nguyen Xuan Thuy, Vu Thanh Minh, Nguyen Cong Phu, Nguyen Van Tuan.

LNT & PARTNERS

Ho Chi Minh City Office

Level 21, Bitexco Financial Tower
No.02 Hai Trieu Street, District 1
Ho Chi Minh City, Vietnam

Tel: +84 28 3821 2357
Fax: +84 28 3910 3733

Hanoi Office

Level 12, Pacific Place Building
83B Ly Thuong Kiet Street, Hoan Kiem District
Hanoi, Vietnam

Tel: +84 24 3824 8522
Fax: +84 24 3824 8580

Singapore Office

Level 40, Ocean Financial Centre
10 Collyer Quay
Singapore 049315

Tel: +65 6808 6288