GBA
German Business Association

MONTHLY BUSINESS MEETING

MONDAY, 3 JUNE 2024
5:30 PM - 9:30 PM
LE MÉRIDIEN SAIGON

DATA PRIVACY LAWS IN VIETNAM

THE BASICS & GUIDANCE FOR PRACTICAL HANDLING

DR. OLIVER MASSMANN
GBA Board Member
Director & Partner
DUANE MORRIS VIETNAM

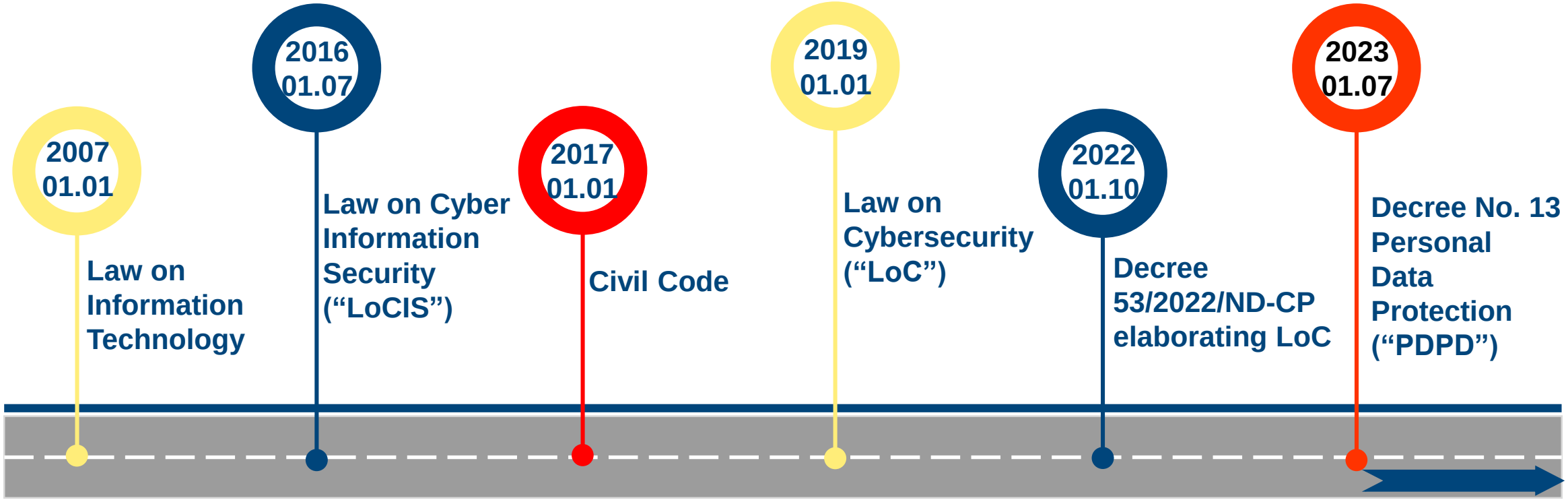
JOHANNES KLAUSCH
GBA Board Member
Lawyer & Partner
LUTHER LAW VIETNAM

Agenda

- Legal overview and Key Definitions
- Core principles of data protection
- Rights of data subjects
- Compliance challenges
- Data Protection Practices
- Outlook and Q&A

Legal overview and Key Definitions

Legal Overview



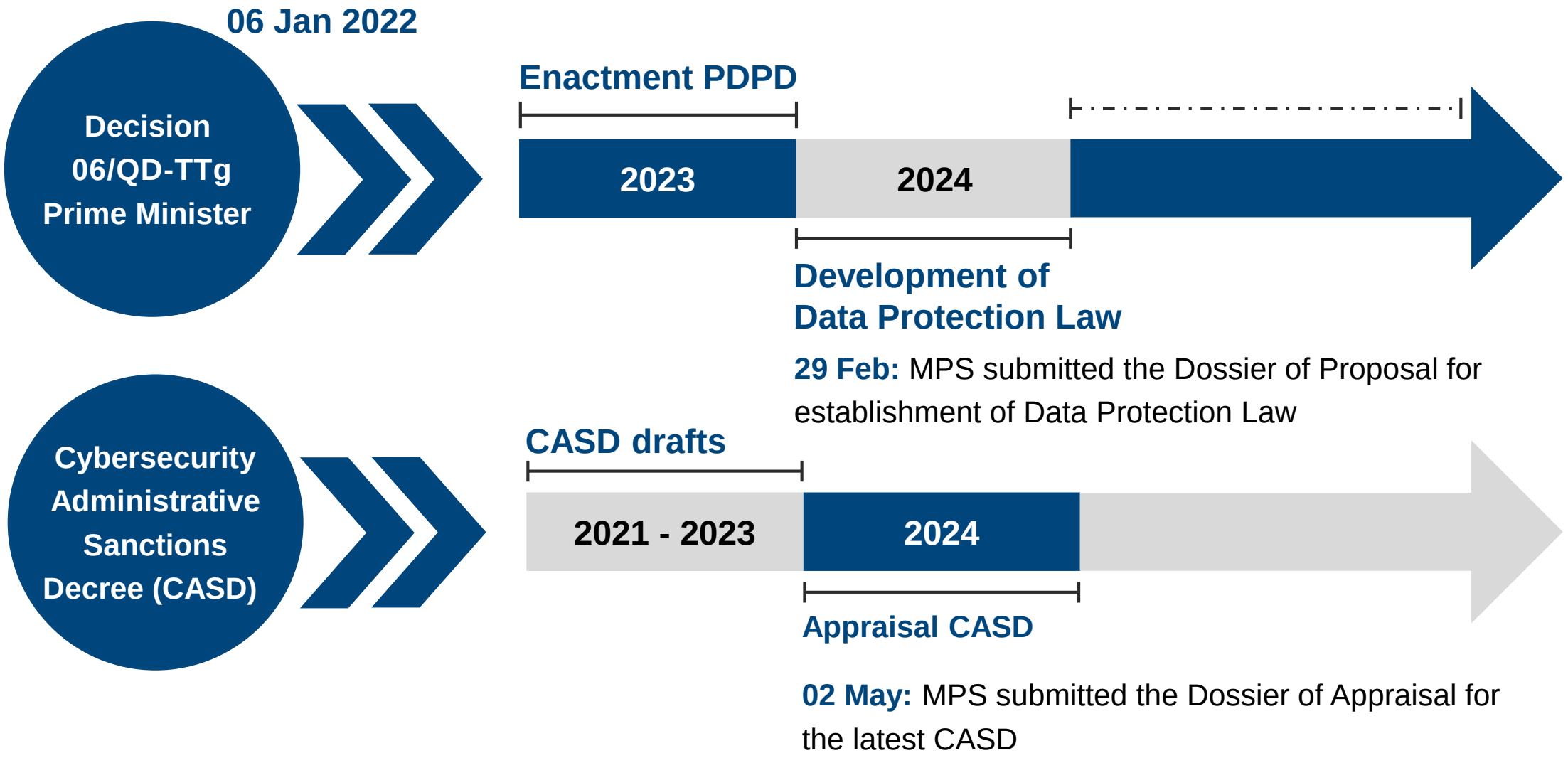
- Key regulations on personal data protection above are **not exhaustive.**
- For specific sectors (e.g., e-commerce, consumer protection, healthcare, telecommunications), rules on personal data protection are also governed in sectoral laws and its guiding decree(s) and circular(s).

The basics

- On 17 April 2023, Decree No. 13/2023/ND-CP on personal data protection (PDPD) was officially issued by the Vietnamese Government.

- The long-awaited and controversial decree is set to be the first ever legal document with comprehensive regulations on both personal data and its protection in Vietnam. With an exception being the grace period of 2 years from incorporation for SMEs with regards to the obligation to appoint a data protection officer (DPO) and data protection department.

Get Ready for the next level



Data Protection Authority

- The Ministry of Public Security (**MPS**) is the competent authority for data protection.
- The Department of Cybersecurity and Cybercrimes Prevention (**A05**) is the special force established by the MPS for the implementation of data protection regulations.

Data Protection Authority (cont.)

The MPS's and A05's authority includes:

- Assist the Government with the supervision of personal data protection;
- Provide guidance and implement personal data protection activities; protect the rights of data subjects against violations of regulations of personal data protection; propose the promulgation of personal data protection standards and recommendations;
- Operate the National Portal on Personal Data Protection;
- Evaluate the results of data protection activities of involved entities;
- Receive the submission of portfolios, forms, and information in relation to personal data protection in accordance with the PDPD;
- Conduct inspections, and handle complaints, denunciations, and violations against regulations on the protection of personal data.

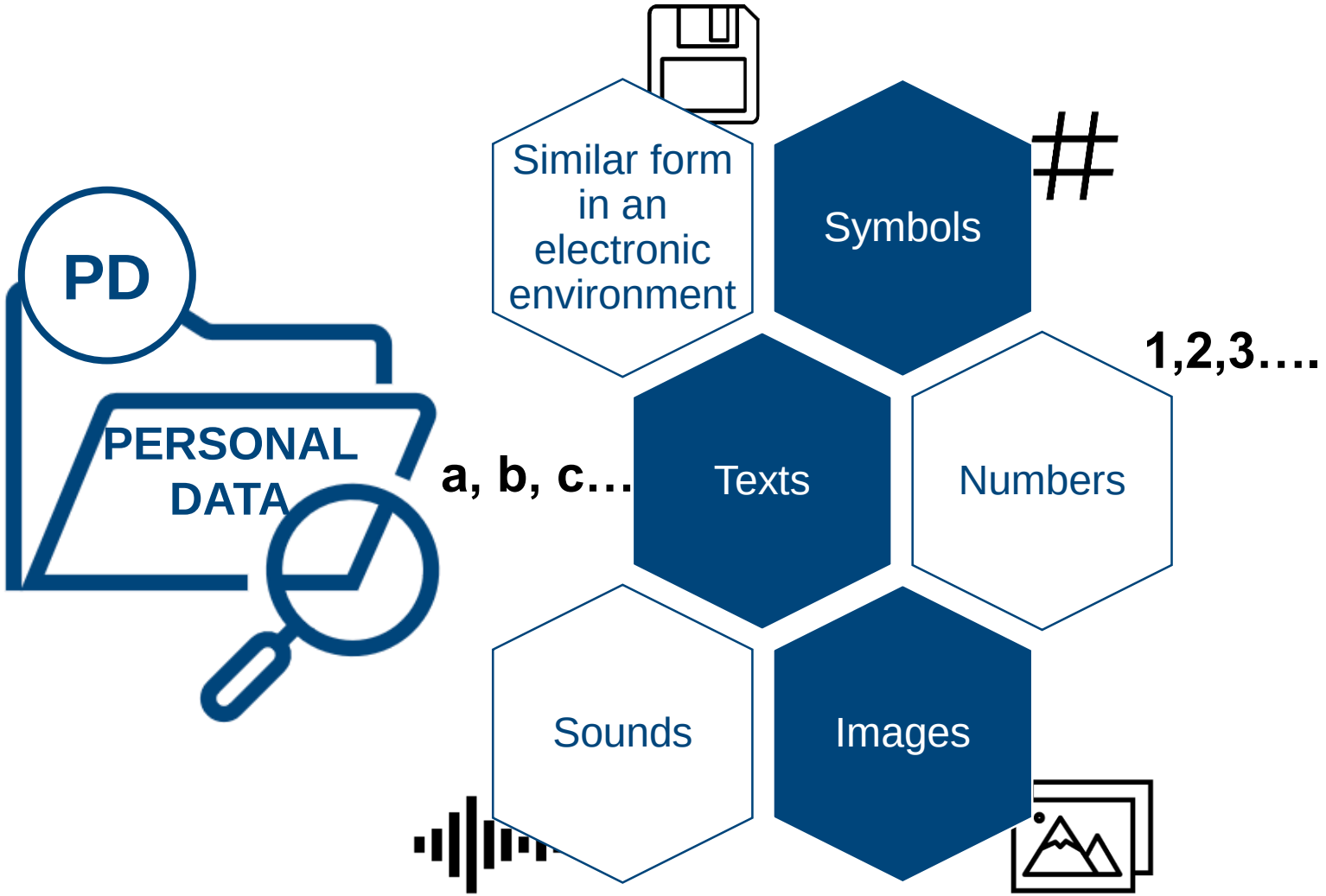
SCOPE OF APPLICATION

- The PDPD seeks to extend the reach of Vietnamese data protection regulation.
  - Vietnamese agencies, organizations, individuals, including those operating overseas
  - Foreign agencies, organizations, individuals in Vietnam, *or* directly participating in or involved in personal data processing activities in Vietnam

TO DO LIST FOR YOUR BUSINESSES

- Businesses (i) based in Vietnam or (ii) without a Vietnamese presence but process personal data of Vietnamese citizens should:
  - understand the impact of the PDPD to your businesses;
  - determine your obligations;
  - prepare documentation required;
  - determine an approach to compliance.

Key Definitions



Data that is:

- ❑ Associated with a specific individual

or

- ❑ Enabling the identification of a specific individual

Classification

- ❑ **Basic personal data** (e.g., name, d.o.b, gender, images, etc.)
- ❑ **Sensitive personal data** (e.g., Political & religious opinion, certain clients' info of banks, criminal record, etc.)

Personal data under the prevailing regulations

Two types of personal data:

- **Basic data**: name, date of birth/death/going missing, gender, place of birth, permanent residence, temporary residence, hometown, current residence, contact address, nationality, personal image, phone number, ID/Passport number, marital status, etc.
- **Sensitive data**: political and religious opinions, health conditions, information on racial or ethnic origin, genetic data, biometric, sex life or sexual orientation, data on criminal activities, bank information, personal location identified via location services, etc.

Key Definitions

DATA SUBJECT

Natural person to who the PD relates

DATA CONTROLLER

Natural or legal person who determines the purposes and means of the processing of PD

DATA PROCESSOR

Natural or legal person who processes personal data on behalf of data controller

THIRD PARTY

Natural or legal person other than data subject, data controller, data processor, who is authorized to process PD

AUTHORITY

Department of Cybersecurity and High-tech Crime Prevention (**A05**) under the Ministry of Public Security (**MPS**)

Relevant parties in personal data protection

Data Subject: an individual to whom the personal data relates

Data Controller: an organization or individual that decides purposes and means of processing personal data

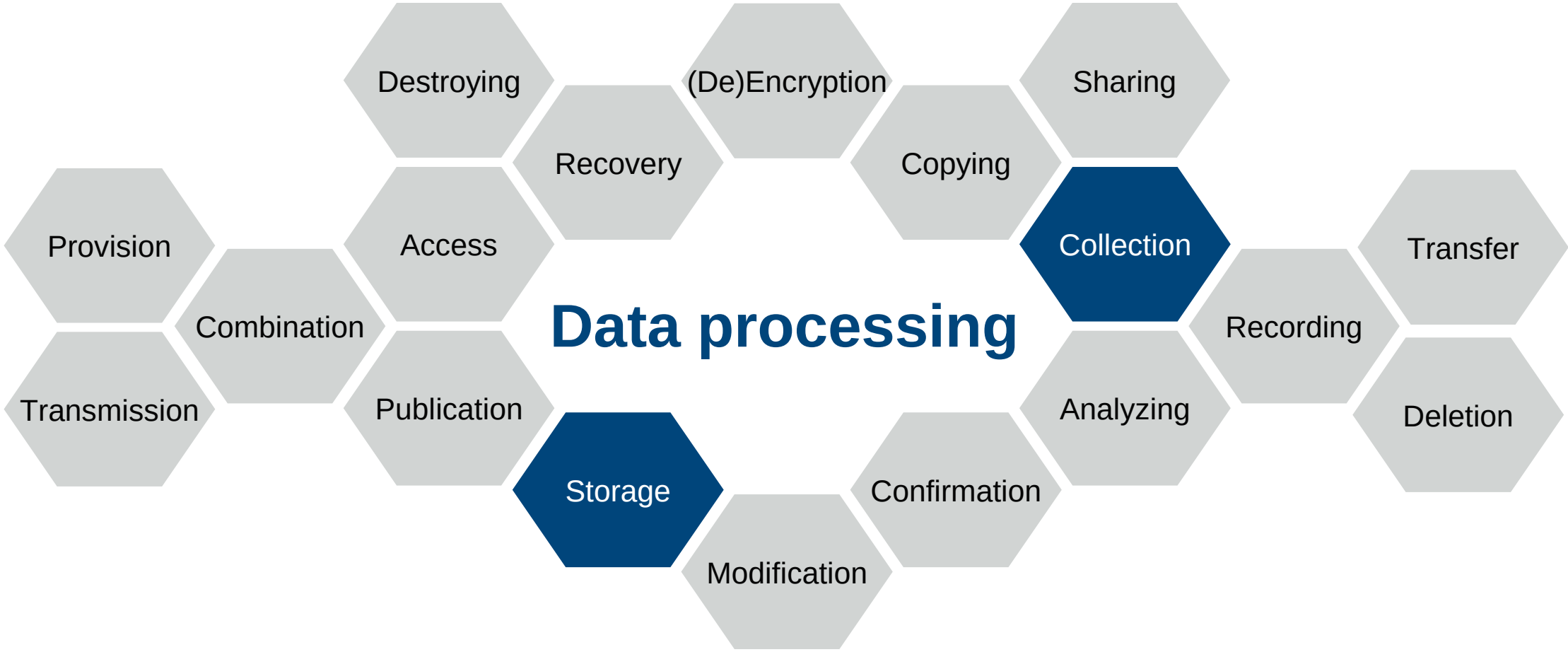
Data Processor: an organization or individual that processes data on behalf of the Data Controller via a contract or agreement with the Data Controller

Data Controller-cum-Processor: an organization or individual that jointly decides purposes and means, and directly processes personal data.

Third party: an organization or individual other than the data subject, Data Controller, Data Processor, and Data Controller-cum-Processor that is permitted to process personal data.

*Similar to the famous EU's General Data Protection Regulation, the PDPD introduces the concept of "Personal data controller" and "Personal data processor" and a whole new concept of "Personal data controlling and processing entity" as mentioned.

Key Definitions




Core principles of data protection

Principles

PD shall be processed in accordance with the law

The controller has to demonstrate compliance with the law and these principles

The data subject to be informed about processing activity

PD stored only for period appropriate for the purposes of data processing

PD shall be processed in conformity with the registered and announced purposes

Adequate protection measures to be applied to PD in the course of data processing

Processing shall be limited to PD what is adequate and relevant for the purpose

PD shall be up to date and complete to ensure data-processing purposes.


Rights of Data Subjects

Rights of Data Subjects

- Right to be informed
- Right to access
- Right to rectification
- Right to erasure
- Right to object/opt-out
- Right to data portability

- Right not to be subject to automated decision-making
- Other rights: right to claim damages, initiate legal proceedings, and implement measures for self-protection.

Rights of Data Subjects

RIGHTS OF THE DATA SUBJECT

- Right to be informed
- Right to consent
- Right to access
- Right to withdraw the consent
- Right to delete PD
- Right to restrict data processing
- Right to data provision
- Right to object to data processing
- Right to complain, to denounce or to initiate lawsuit
- Right to claim damages
- Right to self-protect

OBLIGATIONS OF YOUR BUSINESS

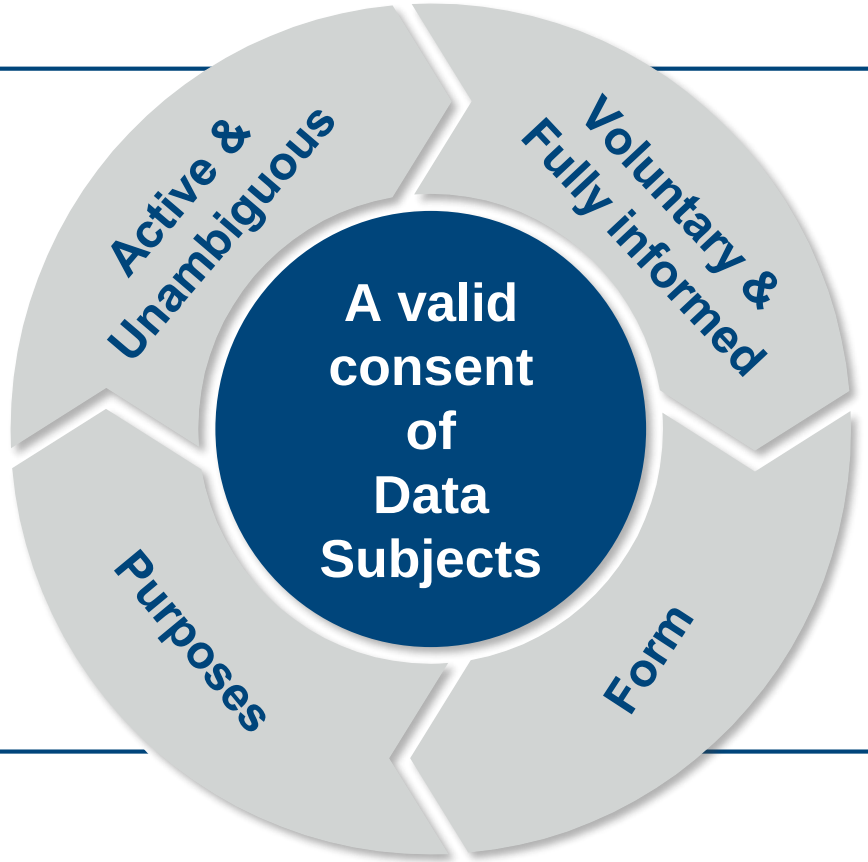
- Notification obligation
- Consent obligation
- Access and correction obligation
- Purpose limitation obligation
- Accuracy obligation
- Protection obligation
- Retention limitation obligation
- Data breach notification obligation
- Accountability obligation

Requirements for Consent

- Consent for processing of personal data must be made based on the Data Subject's full understanding of the following factors:
  - the purpose of the personal data processing;
  - the type of personal data to be processed;
  - entities authorized to process personal data;
  - Relevant rights of Data Subjects.
- For one to legally obtain the consent of Data Subjects, consent must be expressed clearly in a format that can be printed out or reproduced in writing, including in electronic or verifiable formats.
- The PDPD also explicitly points out that silence by the Data Subjects means a "no".
- With regard to sensitive personal data, the data owner must be fully informed of the nature of the data to be processed. In case of dispute, the burden of proof lies on the Data Processor.

Consent - A legal basis for data processing

- Affirmative action
- May not rely on silence, inactitvity or pre-ticked boxes
- Explicit, specific, clear, consise statement of consent



- Freely given
- Can be withdrawn
- At least the following information is required: (i) type of PD; (ii) purpose of processing; (iii) the data controller‘s identity; (iv) rights & obligations of data subjects

- Consent for the relevant purpose
- Several purposes require separate consent each

- Recorded in a format that can be printed, copied in writing, including electronic formats and other verifiable formats

Other legal basis for PD processing

To protect the life and health of people in emergencies

To disclose PD as required by laws

By State agencies in states of emergencies, threats to national security and defense; fighting riots, terrorism, criminals and legal violations

Performing contractual obligations of the data subject to relevant entities

To serve State agencies' activities as required by specialized laws

Recordings in public locations by competent State agencies

NOTES FOR YOUR BUSINESS

- ❑ Other alternative lawful bases for PD processing (e.g., contract, vital interests, legal obligation, public interests)
- ❑ Even if an exception applies, your business is required to comply with its other legal obligations
- ❑ Assess and document your decision to rely on the legal basis


Compliance challenges
under the PDPD

DPIA

- The Data Controller and the Data Processor are required to prepare, maintain, and submit to A05 a Data Protection Impact Assessment (DPIA).

  The form of DPIA is provided in Decision No. 4660/QD-BCA-A05, separated from the PDPD.

- The DPIA must be submitted to the Cybersecurity Department within 60 days after the personal data processing activities are started.

DPIA Dossier for your business

Timeline to conduct & Parties related to the DPIA

- 60 days after the date of data processing, any change to the content of DPIA Dossier must be updated to the MPS
- Data controller, data processors, third parties, developer (platform, automated means integrated, if any)

Description of the PD processing & impact assessment

- Types of PD, purpose, scope, volume, time of the PD processing
- Consent of data subject, method of obtaining consent
- Period for processing, retention
- Time & method of deletion of PD
- Cross-border transfer of PD, if any
- Data protection measures
- Outcome of consultation process
- Assessment of impact on rights & interests of data subjects, eco - social aspects, administrative procedures, legal compliance, etc.

Supporting documents

- Notification on submission
- ERC/ Certificate of Incorporation of the applicant
- Written documents about the designation of data protection department
- Agreement/ written documents on PD processing between involved parties (DPA)
- Annexes (e.g., the calculation of costs & benefits of data protection measure, if any, etc.)

Cross-border Transfer of Personal Data

- To transfer personal data of Vietnamese citizens abroad, the transferor of personal data must first create a dossier of Transfer Impact Assessment ("**TIA**") for the Cross-Border Transfer of Personal Data before transferring personal data out of Vietnam.
- The dossier must be made available at all times for the inspection and evaluation by the authority. In addition, the transferor must submit one original copy of the dossier to A05 within 60 days from the date of the personal data processing.
- Other conditions on cross-border transfer of personal data of Vietnamese citizens: (i) The data owner consented the transfer; (ii) Original data is stored in Vietnam.

TIA Dossier for your business
(PD of Vietnamese citizens)

Timeline to conduct & Parties related to the DPIA

- 60 days after the date of data processing, any change to the content of TIA Dossier must be updated to the MPS
- Data transferor, data receiver, third parties

Description of the PD transfer & impact assessment

- Types of PD
- Purpose, scope, volume, time of the PD processing
- Consent of data subject, method of obtaining consent
- Period for processing & retention
- Time & method of deletion of PD
- Data protection measures
- Outcome of consultation process
- Assessment of impact on rights & interests of data subjects, eco - social aspects, administrative procedures, legal compliance, public security of Vietnam, etc.

Supporting documents

- Notification of submission
- ERC/ Certificate of Incorporation of the applicant
- Written documents about the designation of data protection department
- Agreement/ written documents on PD processing between involved parties
- Annexes (e.g., the calculation of costs & benefits of data protection measure, if any, etc.)

Penalties - today

- **Administrative penalty:** From VND 2 million to VND 70 million

  The administrative penalty is expected to increase significantly after the new Cybersecurity Administrative Penalty Decree ("**CASD**") is officially issued.

- **Criminal penalties:** Criminal sanction imposed depends on the severity of the crime, include:
  - A warning;
  - A fine between VND 5 million (approx. $210) and VND 50 million (approx. $2,140)
  - Non-custodial reform (similar to probation or supervised release in other jurisdictions) of up to three years
  - Prison sentence of between one and three years.

- **Additional penalties:** Suspend the processing of personal data up to 3 months, deprive the right to use written consent issued by the Personal Data Protection Committee to process sensitive personal data and cross-border transfer of data, forcible payment of money gained from committing acts of violation.

Cybersecurity Administrative Sanctions Decree (CASD)

Personal data protection principles		Rights of data subjects
Data subject consent		Withdrawal of consent
Personal data processing notices		Providing personal data
Editing personal data	**VIOLATION**	Illegal collection, transfer, buying and selling of personal data
Storing, deleting and destroying personal data		Notification of violations of regulations on personal data protection of data controller, data controller and processor, data processor
Processing personal data obtained from audio and video recording activities in public places		Personal data protection in the business of marketing services & introducing advertising products
DPIA & TIA		Personal data protection measures

Administrative sanction regime

STATUTE OF LIMITATION

- **01 year** from the date of terminating the violation;
- Where CASD does not stipulate legal liability or stipulates less legal liability for acts occurred before the effective date of CASD, the CASD shall apply to handle.

FORMS OF SANCTIONS

❖ **Main sanctions:**
- Warning; Monetary fine

❖ Additional sanctions:
- Temporary suspension of business license;
- Confiscate evidence & means of administrative violations; or
- (Temporarily) suspend personal data processing

❖ Remedial measures:
- Destruction or deletion of personal data;
- Return of illegal profits;
- Publicly apologize to data subjects

AUTHORITY

UNCENTRALIZED national authority for handling

- Head of Department of Cybersecurity and High-tech Crime Prevention (A05)
- Chairperson of District/ Provincial People Committee
- District/ Provincial Public Security Depart.


Data Protection Practices
Your way to compliance

Internal Labor Rules and Labor Contracts

- Employer should adapt all relevant obligations in relation to personal data over its employees, staff, directors, etc. as well as those in relation to the employer's customers, members and their staff into the employer's internal labor rules/ codes and collective labor agreement (if any).
- The labor contracts should clearly indicate that they must comply with requirements on personal data protection promulgated by the employer and the applicable law.
- It is advisable to negotiate and agree with the employees in the relevant labor contracts about the possible data processing made by the Employer again such employees' personal data for the purpose of employment such as tax information, CVs, health information, etc.

☑	TO DO LIST
☐	Conduct and submit DPIA Dossier & TIA Dossier
☐	Technical and Organizational Measures (TOMs)
☐	Establish Data Protection Policy, Data Retention Procedures
☐	Establish Privacy Notice
☐	Review/Create Consent Form, templates and reports
☐	Review/Create Data Processing Agreement
☐	Appointment of Data Protection Officer
☐	Routine audit and training of employees on data protection issues


THANK YOU!

Q&A