Tilleke & Gibbins

Cambodia
Personal Data – Data Privacy

Jay Cohen, Partner

Sochanmalisphoung Vannavuth, Advisor

Tilleke & Gibbins (Cambodia) Ltd. | March 30, 2021

AGENDA

- Part 1 Legal and Regulatory Framework
- Part 2 Definition of Personal Data, and Stakeholders in Data Privacy
- Part 3 Collecting and Processing of Personal Data
- Part 4 Duties regarding the Processing of Personal Data
- Part 5 Sanctions

PART 1

Legal and Regulatory Framework

Regulatory Framework for Data Protection

- Cambodia has not yet enacted any comprehensive data protection legislation.
- E-Commerce Law contains provisions for the protection of consumer data that has been gathered over the course of electronic communication. The E-Commerce Law is thereby restricted in scope to virtual and/or digital data protection.
- Other matters pertaining to data protection typically fall under the Constitution of the Kingdom of Cambodia 2010 ('**the Constitution**'), the Civil Code of Cambodia 2007 ('**the Civil Code**'), and the Criminal Code of the Kingdom of Cambodia 2009 ('**the Penal Code**').

Laws That Implicate Data Privacy Matters

Laws	Rights
Constitution	All Cambodian citizens have the right to privacy of residence, and to the confidentiality of correspondences by mail, telegram, fax, telex, and telephone.
E-Commerce Law	Basic disclosure and data protection requirements for consumers engaged in transactions via electronic systems. Applies to all commercial and civil acts, documents, and transactions executed via an electronic system.
Civil Code	Provides broad personal rights, such as right to privacy, rights to life, personal safety, health, freedom, identity, and dignity. This legal provision may be interpreted as protecting individual personal data as part of the right to privacy.
Penal Code	Broadly prohibits (1) Recording private conversations and images, (2) Breaches of professional secrecy, (3) Secrecy of correspondences and telephone conversations, (4) IT crimes.

Sectoral Specific Regulations

- Financial Sector
- Health and Pharma Sector
- Telecommunication Sector

PART 2

Definition of Personal Data, and Stakeholders in Data Privacy

Definition of Personal Data

- Cambodian law fails to define the term "personal data".
- The E-commerce Law defines the term "data" as "a group of numbers, characters, symbols, messages, images, sounds, videos, information or electronic programs that are prepared in a form suitable for use in a database or an electronic system."
- Due to the absence of a definition of "personal data," it remains plausible that any data of a data subject may be viewed by the regulatory and enforcement authorities as personal data of that data subject.

Definition of Sensitive Data

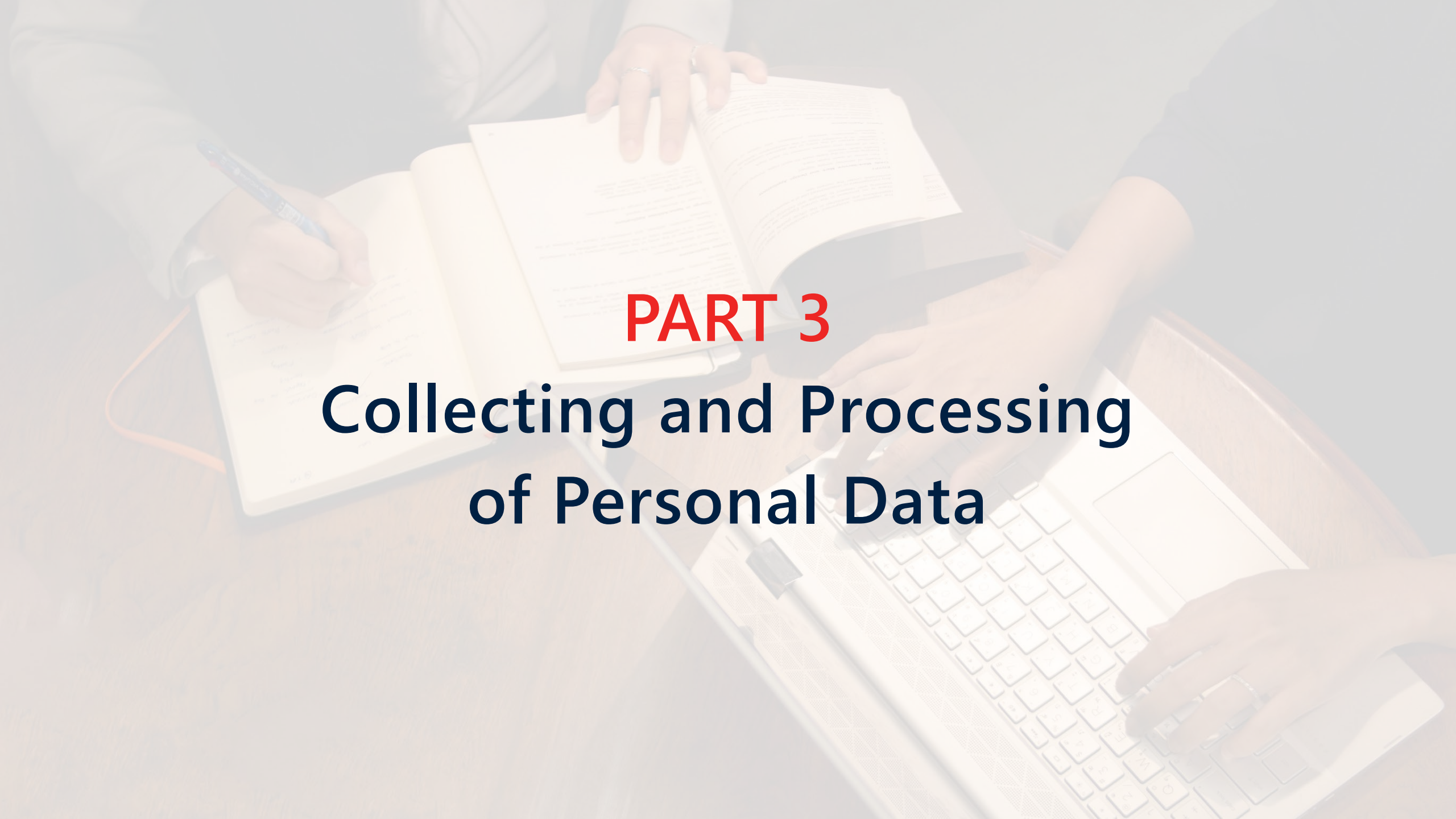
- There is no express definition of sensitive personal data.
- Based on laws applicable to persons and entities in other sectors (such as doctors and banks), the types of data below are generally considered to be of a more sensitive nature:
  - medical data;
  - financial data;
  - personal data of children; and
  - personal identifiers (e.g. national identification cards and passport details).
- It is highly recommended that each data of a data subject should be prudently treated as sensitive data to the greatest extent possible.

Stakeholders in Data

- As Cambodia does not have any comprehensive data protection laws, the concept of the stakeholders in data privacy has not been addressed; however, the following terms would be understood to have the following meanings:
  - Data Subject is an individual who is the subject of personal data.
  - Data Controller is a person that collects, uses, or discloses personal data.
  - Data Processor is an organization that processes personal data on behalf of another organization.

Competent Authorities

- There are no regulatory or enforcement authorities that are specifically tasked with handling, overseeing or implementing personal data protection matters in Cambodia.
- The governmental bodies below may have substantial powers over data protection matters:
  - Ministry of Commerce (the "MOC")
  - Ministry of Post and Telecommunications (the "MPTC"), and
  - Ministry of Interior (the "MOI").



PART 3

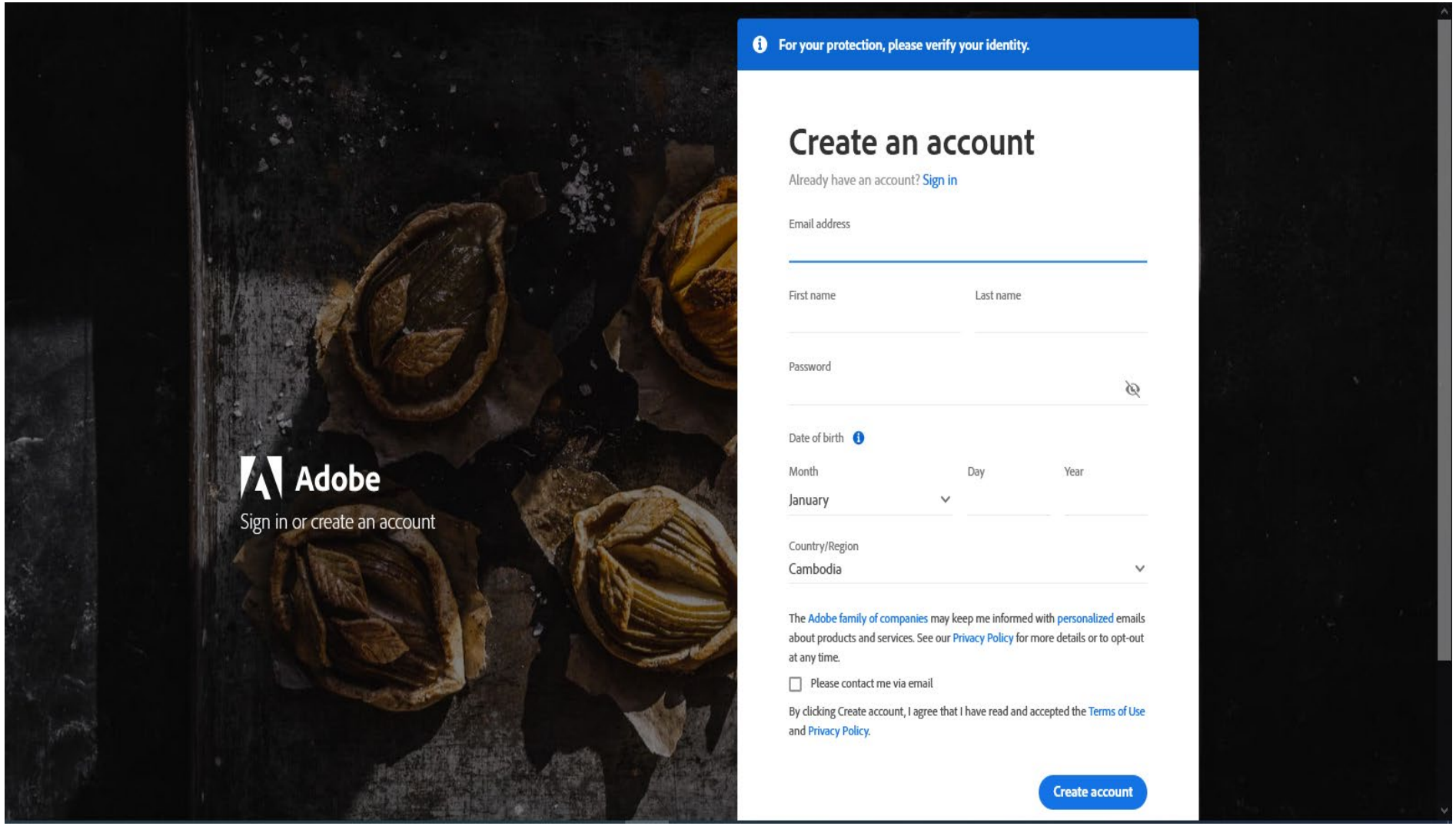
Collecting and Processing of Personal Data

Requirements to Collect and Process Data

Consent

- Organizations are required to obtain consent from data subjects before accessing, collecting, using, processing, or disclosing the personal data of data subjects.
- Consent must be freely given, specific, informed and unambiguous.

Example



Tilleke & Gibbins

Requirements to Collect and Process Data

Notification

- The organization must give prior notification to the data subjects of the purpose(s) for which it intends to collect, use or disclose the data subjects' personal data.
- The form of the notifications to obtain each data subject's consent should be as close to a formal contract as possible.
- The purpose of the collection, use, and disclosure of personal data must not be too vague or broad in scope; an appropriate level of specificity should be provided.

Requirements to Collect and Process Data

Requirement such as clicking on the consent button, typing a full legal name for the signature, and/or scrolling through all terms of the notification should be implemented.

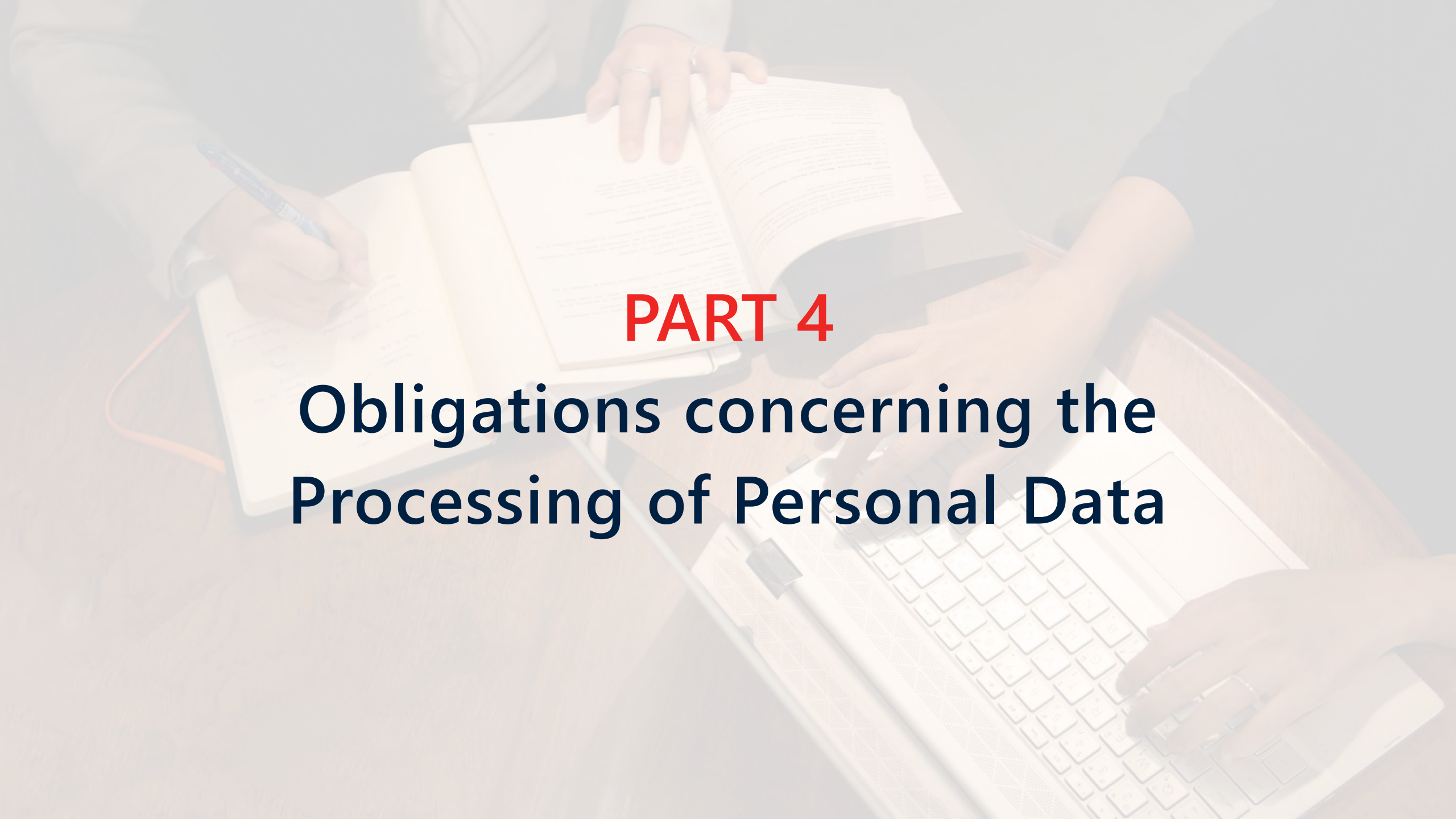
Example: https://www.dromansolutions.com/gdpr-data-collection-processing-notice

Condition and Requirements to Collect and Process Data

- For cross-border data transfer , the organization has a disclosure / notification obligation, implied under Cambodia's existing legal framework applicable to data protection.
- Personal data can only be collected, used, or disclosed for purposes that the individual understands and has given consent to at the time of giving initial consent or a new consent.
- Such purposes must be disclosed or notified to data subjects in a reasonable manner based on the circumstances.

Rights of Data Subjects

Right to Access	Data subjects have the right to access their information to the extent necessary for the data subjects to exercise their rights to correct or delete incorrect or inaccurate personal data.
Right to Correct	Data subjects have the rights to correct or delete incorrect or inaccurate personal data.



PART 4

Obligations concerning the Processing of Personal Data

Obligations Concerning Processing of Personal Data

1	Consent Obligation	Obtain consent from the individual before collecting, using, or disclosing his or her personal data for a purpose. Organizations should allow an individual who previously gave consent to withdraw his or her consent.
2	Purpose Limitation Obligation	Collect, use, or disclose personal data about an individual only for purposes that are reasonable and that have been notified to the individual concerned.
3	Notification Obligation	Notify the individual of the purpose(s) for which the organization intends to collect, use or disclose the individual's personal data on or before such collection use or disclosure of the personal data. The purposes notified must be reasonable.

Obligations Concerning Processing of Personal Data

4	Correction Obligation	Correct any incorrect or inaccurate personal data of a data subject that is in the possession or under the control of the organization upon request of the data subject.
5	Access Obligation	Allow data subjects to access their personal data in the possession or under the control of an organization for correcting the information under the Correction Obligation.
6	Protection Obligation	Protect personal data in its possession or under its control by taking necessary measures to prevent loss, unauthorized access, use, alterations, leaks, disclosures, or otherwise.
7	Retention Obligation	Retain all personal data that is in its system, and that may give rise to civil and criminal liability.

PART 5

Sanctions

Part V – Sanctions

Violating data protection under the Criminal Code will result in the following penalties:

Violation	Penalty
Recording private conversations and images	Imprisonment of between one month and one year and a fine of KHR 100,000 (approx USD25) to KHR 2 million (approx USD500).
Breaches of professional secrecy	
Violation of Secrecy of correspondences and telephone conversations	
IT crimes	Imprisonment of between one month and two years and a fine of KHR 100,000 (approx USD25) to KHR 4million (approx.USD1,000).

Tilleke & Gibbins

Part V – Sanctions

Violating data protection under the E-commerce Law will result in the following penalties:

Violation	Penalty
Failure to provide clear and straightforward opt-out instructions for unsolicited marketing communications	(1) a written warning; (2) suspension or revocation of business licenses and permits, and/or (3) disabling the means of marketing and communication to individuals
Failure to comply with the Consent, Purpose Limitation, Disclosure / Notification, and Protection Obligations	Imprisonment from 1 to 2 years and a fine amounting to KHR 2 million to KHR 4 million (approx. USD 500 to USD 1,000)
Failure to comply with the Retention Obligation	Imprisonment from 1 month to 1 year and a fine amounting to KHR 100,000 to KHR 2 million (approx. USD 25 to USD 500)
Failure to comply with the Correction and Access Obligations	No specific penalties apply

www.tilleke.com

Jay Cohen
jay.c@tilleke.com

Sochanmalisphoung Vannavuth
sochanmalisphuong.v@tilleke.com

Tilleke & Gibbins

CAMBODIA • INDONESIA • LAOS • MYANMAR • THAILAND • VIETNAM