ANTARES

PDPA

THAILAND'S PERSONAL DATA PROTECTION ACT

LEGAL UPDATE & IMPLEMENTATION GUIDE THAILAND'S GLOWFISH THAILAND'S

MR. FLORIAN MAIER, LL.M.
MANAGING DIRECTOR, ANTARES ADVISORY LTD.

AUSTCHAM BREAKFAST BRIEFING
19 FEBRUARY 2020
GLOWFISH SATHORN THAILAND'S

PERSONAL DATA PROTECTION ACT?

- Personal Data Protection Act ("**PDPA**") B.E. 2562
- Published in the Government Gazette on 27 May 2019
- Grace period before penalties apply until 27 May 2020

- Same purpose and similar structure as EU's General Data Protection Regulation ("**GDPR**")

ANTARES

REACH

(EXAMPLE 1)?

Diving School in Cairns, Australia

- Customers are from all over the world, including individuals located in Thailand
- Bookings made via website or in person
- Company keeps customer database, incl. name, email, phone number, booked packages
- Promotional emails are sent to customers

Will the diving school be affected by PDPA?

WHO IS AFFECTED??

PDPA applies to any entity

- Offering goods or services to individuals located in Thailand
- Monitoring the behaviour of individuals located in Thailand
- Collecting, using, disclosing, or transferring Personal Data of individuals located in Thailand

(exceptions apply e.g. for private usage, certain government bodies, members of parliament, the media)

ANTARES

WAITING FOR COMMITTEE?

Awaiting establishment of Personal Data Protection Committee

- Tasked to set out subordinate law
- Tasked with protecting data owner's rights

So far, no Committee has been established, thus

- No subordinate laws
- No official guidelines or sample clauses
- No established interpretation of the law

In practice, a violation of the law will be enforceable only after the subordinate law has been passed by the Committee.

ANTARES

WHAT IS PERSONAL DATA?

- Any information which identifies an alive person, directly or indirectly

  Examples: name, address, email address, phone number, passport/ID card number

- Possibly: combination of internet device's technical data, e.g. IP address, MAC address, browser details, language and time zone settings, location data, cookie ID (depending on Committee's interpretation)

ANTARES

REACH

(EXAMPLE 2)?

International Fashion Label's Regional Office in Bangkok, Thailand

- Purpose: QC of suppliers in ASEAN
- No suppliers or QC activities in Thailand
- HR outsourced to Thai service provider

Will the regional office be affected by PDPA?

ANTARES

PERSONAL DATA?

Any Personal Data of individuals the company handles:

- Customers (incl. customer enquires or complaints)
- Employees
- Directors or shareholders
- Contractors/suppliers

ANTARES

BASIC PRINCIPLES?

- To collect, use, disclose or transfer Personal Data, a legal basis is needed (e.g. data owner consent or exemption under the law)
- Personal Data must be used only for its specific purpose

PDPD's principle of data economy vs. data approach of Sillicon Valley-style tech companies)

ANTARES

OLD DATA??

- Personal Data collected prior to PDPA, can be kept and used for the original purpose
- Data Controller must prepare and publicise a consent withdrawal method in order to facilitate the data owner to withdraw previous consent

ANTARES

DATA CONTROLLER

VS

DATA PROCESSOR?

Data Controller

- Person authorized to make decisions on the collection, use, and disclosure of Personal Data

Data Processor

- Person collecting, using, or disclosing Personal Data by order of or on behalf of the Data Controller

CONTROLLER VS PROCESSOR

(EXAMPLE 1)?

Outsourcing to Service Providers

Company A enters into contracts with Company M to carry out its mail marketing campaigns and with Company P to run its payroll.

- Company A gives clear instructions: e.g. what material to send out and to whom, and who to pay, what amounts, by what date
- Company M and P have some discretion: e.g. what software to use, advising on tax deductions, advising against sending mailings on Songkran

Are A, M and P Data Controllers or Processors?

Source: Article 29 Data Protection Working Party Opinion Paper

CONTROLLER VS PROCESSOR

(EXAMPLE 2)?

Recruitment Services

Company R assists Company E in recruiting new staff.

- Agreement states: "(1) *R shall act on behalf of E.*
  (2) R acts as data processor in processing personal data.
  (3) E is the sole data controller"
- R is paid only for employment contracts actually signed.
- To enhance chance for matching, R looks for suitable candidates both among the CVs received by E and in R's own extensive jobseeker database.

Are R and E Data Controllers or Processors?

Source: Article 29 Data Protection Working Party Opinion Paper

CONTROLLER VS PROCESSOR

(EXAMPLE 3)?

Travel Agency

A travel agency sends Personal Data of its customers to an airlines and a chain of hotels to make reservations for travel packages.

- Airline and hotels confirm the availability.
- Travel agency issues the travel documents/vouchers for customers.

Who is a Data Controller or Processor?

Source: Article 29 Data Protection Working Party Opinion Paper

DATA PROTECTION OFFICER?

Some Data Controllers and Date Processors must appoint a Data Protection Officer, e.g.

- Public authorities
- Companies whose core activity is the use of sensitive Personal Data
- Companies holding "large numbers" of Personal Data (to be described by the Committee).

DATA OWNER'S RIGHTS?

Data Processors must guarantee data owner's

- Right to access/request a copy
- Right to be informed
- Right to be forgotten
- Right to withdraw consent
- Right to object/restrict of processing
- Right to data portability

ANTARES

BASIC RULES:

INFORMATION & CONSENT?

1. Request consent
   - Prior to or at the time of data collection
   - In writing or via electronic means
   - In simple and straightforward language
2. Explain what the data will be used for
3. Explain how long it will be retained
4. Explain how their rights can be exercised, incl. company (contact) details

(Consent form samples to be prepared by the Committee)

ANTARES

EXCEPTIONS FROM CONSENT?

Personal Data can be collected/used without consent

- To comply with applicable laws and regulations
- To perform a contract to which the individual is a party
- To prevent/suppress danger to a person's life, body or health
- To prepare historical documents/archives, research or for statistical purposes
- For public interest or upon assignment of official authority
- If legitimate interest of data processor/others necessitates, but not if overridden by an individual's fundamental rights

OTHER OBLIGATIONS?

If Personal Data is shared with 3rd parties:

- Ensure that 3rd party (e.g. Data Processors) uses data legally (no unauthorized disclosure, no breach, no usage for unauthorized purposes)

If Personal Data is transfer overseas:

- By default, foreign country must meet Thai Personal Data protection standards
  (exceptions apply, e.g. consent of data owner)

IT SAFEGUARDING MEASURES?

- Data economy: Delete Personal Data if
  (1) Requested to do so by Data Owner
  (2) Retention period has lapsed
  (3) Data is no longer required
- Implement security measures against unauthorized access, loss or disclosure of Personal Data
- Keep records of all processing activities
- In case of any breach or violation of PDPA, notify the Office of Personal Data Protection Commission within 72 hours

CRIMINAL PENALTIES &

ADMINISTRATIVE FINES?

For failures to comply with or violations of PDPA:

- Penalty fines from THB 500,000 - THB 1 million, imprisonment from 6 months to 1 year
- Administrative fines THB 500,000 - THB 5 million, based on severity of offence.

Example: Data Controller discloses (or uses) personal information without consent of the data owner.

ANTARES

DAMAGES (CIVIL LAW)

In case of a Data Controller/Processor's violation of or failure to comply with PDPA:

- Compensation of actual damages caused (whether intentionally or negligently)

  Exempted if Data Controller/Processor can prove that:

  - Damages were causes by action/omission of data owner or force majeure
  - Damages are the result of complying with lawful order of government body

- Punitive damages (up to 2 times actual damages) based on a court order (incl. class action lawsuits if requirements met)

ANTARES

HOW TO BECOME COMPLIANT?

Phase 1: Analysis

- Data Mapping: Which kind of Personal Data is collected? How is it collected? How is it used? How has access?
- Legal Basis: What is the legal basis? Which obligations come with it?

Phase 2: Execution

- Draft/update legal documents (e.g. Consent Forms, Privacy Policies, Data Processing Agreements)
- Conduct employee training

Phase 3: Maintenance

- Regular, ongoing training/legal updates/procedure reviews

ANTARES

CONTACT USTHAILAND'S

Antares Advisory Ltd.

571 RSU Tower, 10th Floor, Sukhumvit 31 Road,
Klongtoeynuer, Wattana, Bangkok 10110 Thailand
Tel: +66 2 026 3277 Fax: +66 2 662 3416
www.antaresgroup.com

Mr. Florian Maier, Managing Director
florian@antaresgroup.com

PDPA

Florian is a German Attorney-at-Law and also holds a LL.M. degree from Auckland University, New Zealand. He joined Antares in 2014. Prior to that, Florian has been working for a German-owned law firm in Bangkok and, subsequently, for 5 years for a law firm in Stuttgart, Germany, advising mid-sized German companies with respect to international contract law.

He speaks German, English and French and he has an extensive experience in all legal matters, including tax law.

Mr. Phi Ploenbannakit, Director
phi@antaresgroup.com

Phi holds a LL.B. and subsequently a LL.M. in Business Laws, program held in English, from Thammasat University. He is a member of the Lawyers Council of Thailand and the Thai Bar Association. Phi is a Thai licensed lawyer and Notarial Services Attorney.

His area of practice covers corporate & commercial law, M&A, legal due diligence, labor law, property law, family law, litigation and arbitration.