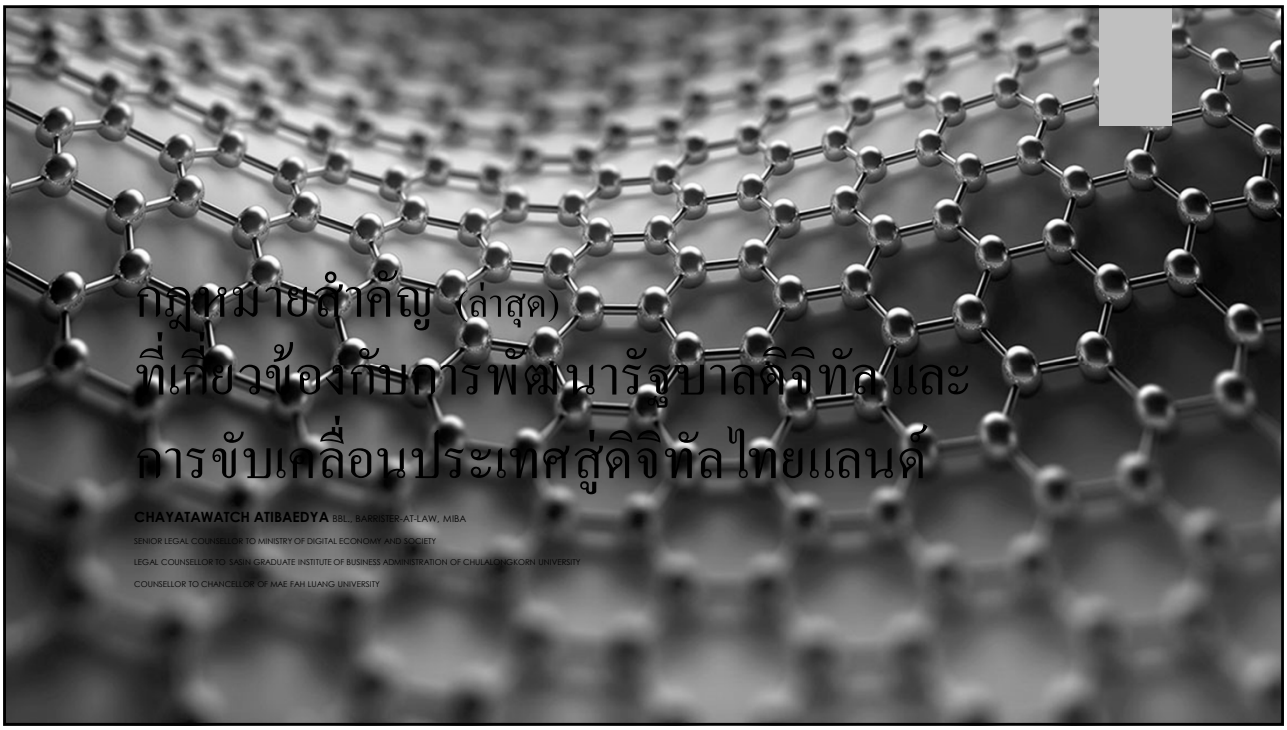
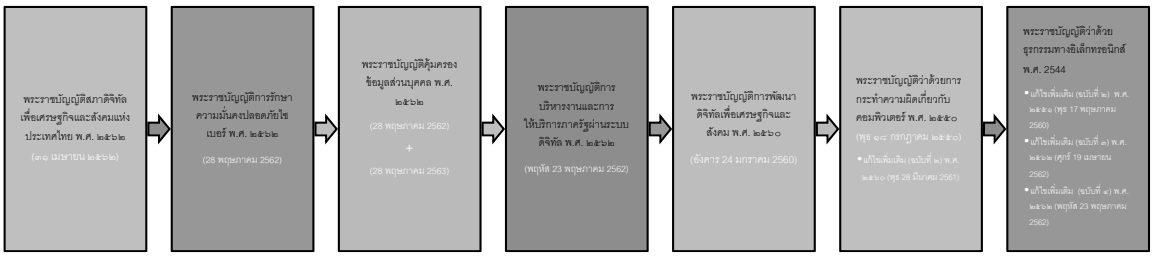


1

Thai Laws Governing National's Digital Movement



2

2. 1.76 billi… alone.

The year has barely s… …sting year as far as data leaks is concerned.

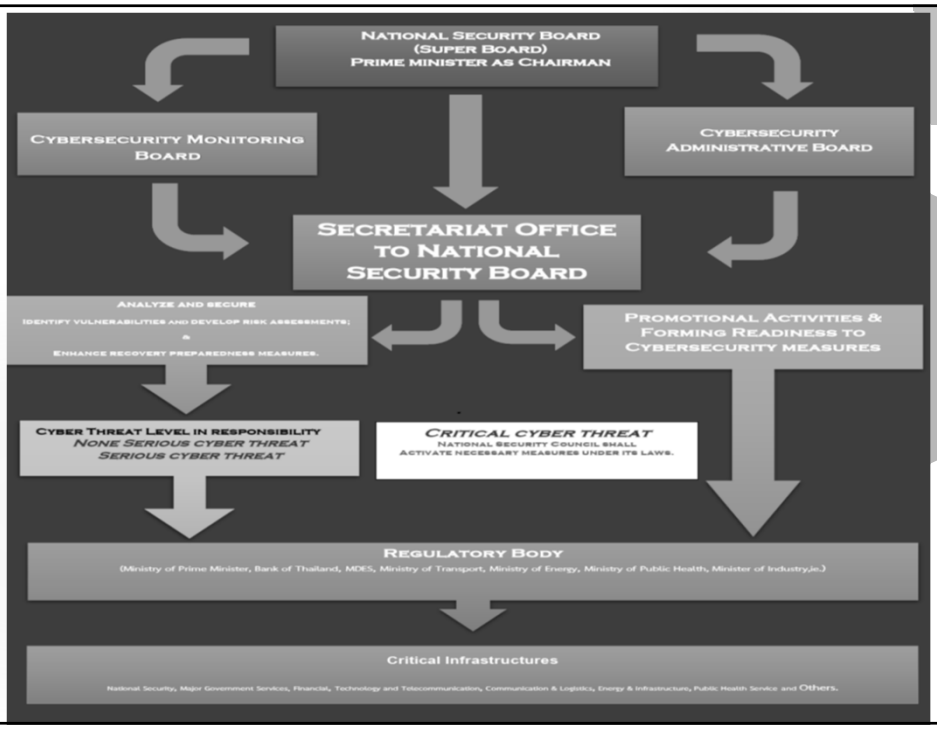
In January 2019 alon… …hese include records from the famous Coll… …asswords for about 772 million people compil… …ppened, a MongoDB instance containing 8… …nformation about 202 million Chinese users… …d 7 years of FBI investigations.

…urce: thebestvpn

3

Outline
Cyber Security & Personal Data Protection Law

4



5

Major Objectives of The Law

1. Establish standard and policy of Cybersecurity ➔ CI's **regulatory authority**
2. Monitoring cyber threat & develop risk management ➔ National Computer Emergency Response Team (CERT)
3. Forming coordination ➔ among CI when **RISKs** occurred.

Protect of Threat

⇩

Incident response

⇩

Minimize Risk

Bank of Thailand **(BoT)**

National Interbank Transection Management & Exchange **(NITMX)**

National Credit Bureau **(NCB)**

6

Law mainly regulates Critical Infrastructure bodies

Critical Infrastructure Bodies

1. National Security (Military, MDES)
2. Major Government Services (Administrative Office, Revenue, Police Department)
3. **Financial (Banking & Financial, SET, Insurance)**
4. Technology and Telecommunication (Mobile & Internet Service Provider)
5. Communication & Logistics (Harbor Authority, Aviation Service)
6. Energy & infrastructure
7. Health Service
8. To be announced by subordinate legislation.

Criminal

- To be investigated & enforce under

  Computer Crime Act B.E. 2550

Law might not define *Critical Services* for each sector; but their regulators will, such as: *Money Transfer, Cash withdrawal, e-Payment, Settlement etc.*

Normal People & Entrepreneurs

- Very less effects
- Grant minor coordination to Enforcing Authority under this law

7

Levels of Cybersecurity Threat

None Serious cyber threat

normal event when acceptable risk occurred and created none or minor damages to critical infrastructure's operation.

Serious cyber threat

the event whereas significant service of critical infrastructure unit is attacked, leading to initial system failure.

Critical cyber threat

the event whereas critical infrastructure is attacked, leading to wide-ranged service failure, affecting lives of several people and their security, and potentially causing vulnerabilities to other critical infrastructures

8

How the Law Works:

None Serious Cyber Threat

- Cyber Security Protection Readiness ➔ Issue National Security Policy & Plan as a Guideline.
- Forming National CERT to Assist CI's Regulators and/or Bodies (if needs).
- Monitor & Minor response.
- Information Sharing among CERTs.

Serious Cyber Threat

- Evaluate Risk
- Incidence Response
- Announcement & Information Sharing among CI.
- Seeking Coordination from existing CERTs for Protect/Minimize/Recovery/Cure

9

How the Law Works:

None Serious Cyber Threat

- Cyber Security Protection Readiness ➔ Issue **National Security Policy & Plan** as a Guideline.
- Forming National CERT to Assist CI's Regulators and/or Bodies (if needs).
- **Monitor & Minor response**.
- **Information Sharing** among CERTs.

Serious Cybe

- Evaluate Risk
- Incidence
- Anne
- Seeking Coordina
  CERTs for
  Protect/Mi

Verification & Evaluation Plan on Internal Cybersecurity Protection *(being audited annually.)*

Incidence Response Plan

Providing Contact List on Management& task force Team, Owners, Possessors & Service Providers of CI's Computer Systems ➔ its regulator(s) & *Cybersecurity Collaboration Centre.*

Forming internal Cybersecurity Drills & Tactics as well as those with other Cis and/or its regulators demanding by Law.

10

Critical cyber threat

Under avoidably urgency Competent officer could utilize necessary measure for prompt protection then immediately informs.

National Security Council

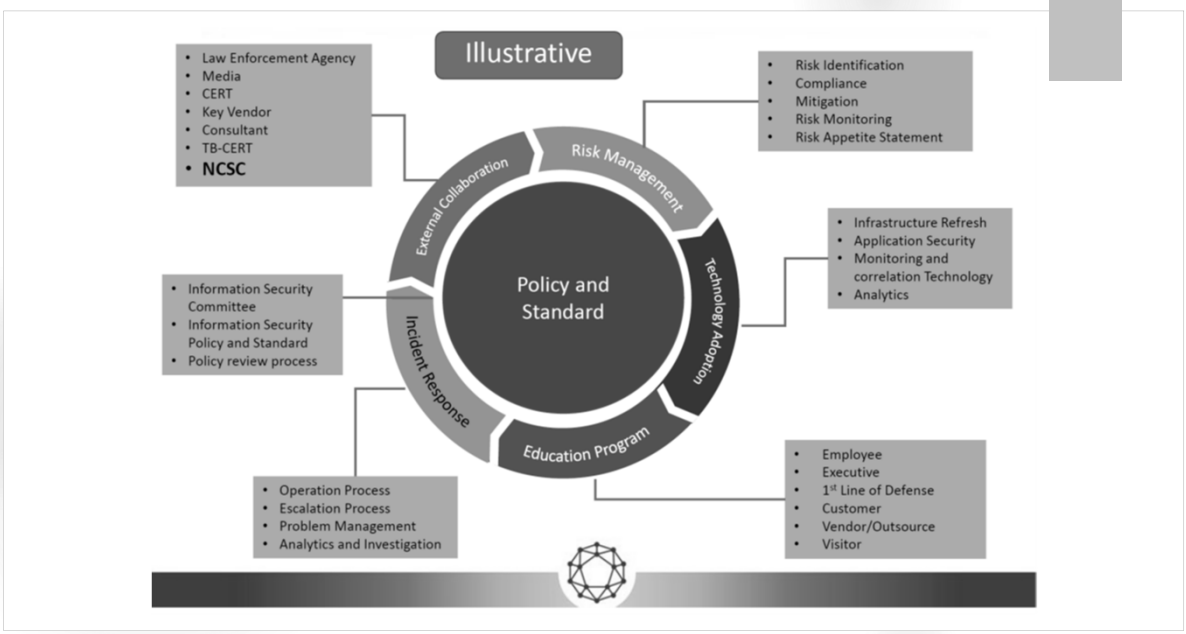
- **Utilize its own LAWS in consideration of National Security Threats.**

11

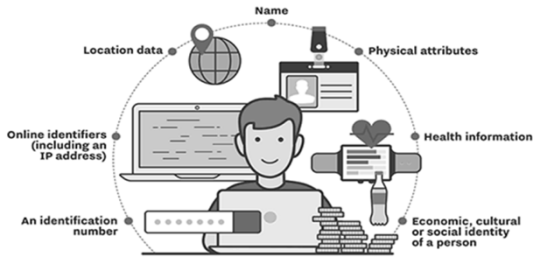
Proper Planning:

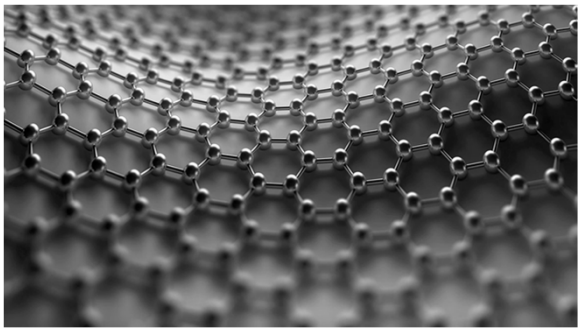
Cybersecurity Framework

12



13

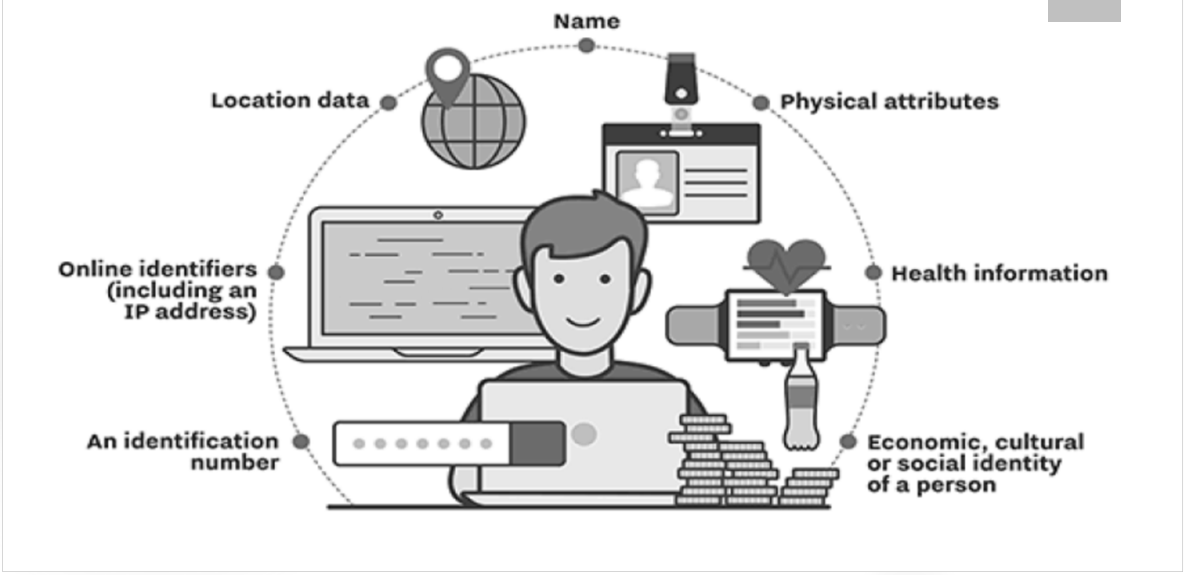




2019 Personal Data Protection Act in Thailand

CHAYATAWATCH ATIBAEDYA
BBL., BARRISTER-AT-LAW, MIBA
SENIOR LEGAL COUNSELLOR TO
MINISTRY OF DIGITAL ECONOMY AND SOCIETY

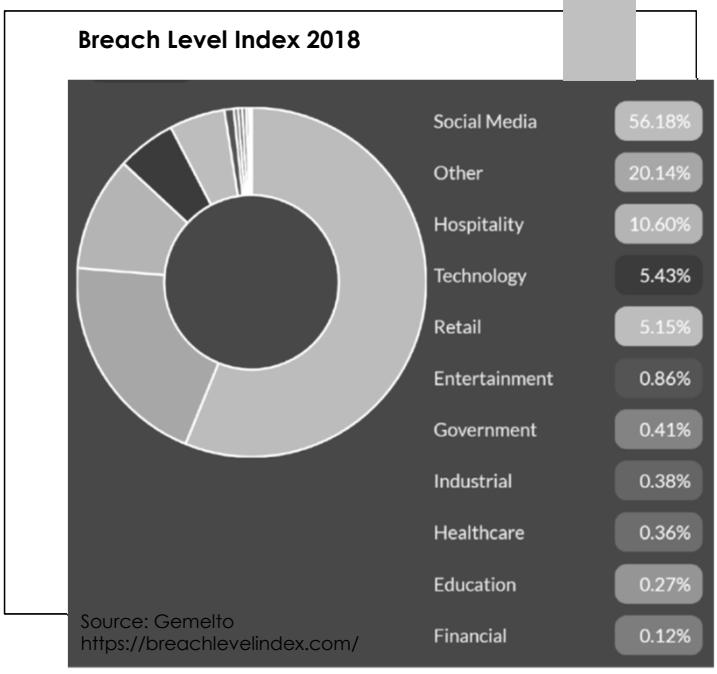
14



15

RISK of Personal Data

- ▶Identify theft
- ▶Profiling
- ▶Mis-using
- ▶Tracking Stalking



16

เหตุการณ์ละเมิดข้อมูลส่วนบุคคล

มิถุนายน 2560
ข้อมูลส่วนบุคคลของผู้มีสิทธิออกเสียงเลือกตั้งของสหรัฐฯ จำนวน **200 ล้านคน** ที่ **Deep Root Analytics** จัดเก็บ รั่วไหล เนื่องจากไม่มีการตั้งรหัสที่ดี

กรกฎาคม 2560
บริษัท **Equifax** **ข้อมูลส่วนบุคคล**ของผู้บริโภคชาวสหรัฐฯ **รั่วไหล 145 ล้านคน**

พฤศจิกายน 2560
บริษัท **Uber** **ข้อมูลส่วนบุคคล**ของคนขับรถและผู้ใช้บริการ **รั่วไหล 53 ล้านคน**

มกราคม 2561
ระบบฐานข้อมูลประชาชนของอินเดียตกเป็นข่าวว่ามีช่องโหว่ให้ผู้ไม่หวังดีเข้าถึงข้อมูลของประชาชน**กว่า 1,000 ล้านคน** ได้โดยไม่ได้รับอนุญาต

มีนาคม 2561
FACEBOOK ยอมรับว่าดูแลข้อมูลส่วนบุคคลของ User ไม่เพียงพอ ทำให้ Cambridge Analytica นำข้อมูล User กว่า 50 ล้านคน ไปวิจัยทำแคมแปญหาเสียงเลือกตั้ง

เมษายน 2561
มีรายงานว่า **ข้อมูลลูกค้า** **TrueMoveH** ที่จัดเก็บไว้บนระบบ Cloud Amazon S3 **รั่วไหล** โดยเข้าถึงข้อมูลได้ประมาณ **46,000 ไฟล์**

กรกฎาคม 2561

17

“sensitive data” <26>

- data that reveals:
  - Racial or ethnic origin
  - Political opinions
  - Religious or philosophical beliefs
  - Trade union membership
  - Genetic data
  - Biometric data for the purpose of uniquely identifying a natural person
  - Data concerning health or a natural person’s sex life and/or sexual orientation

18

General Data Protection Regulation (EU's **GDPR**)

Come into force since **25 May 2018**

19

The six legal bases:

- The **vital interest** of the individual
- The **public interest**
- **Contractual necessity**
- Compliance with **legal obligations**
- Valid **unambiguous consent** of the individual
- **Legitimate interest** of the data controller

20

GDPR's approaches

- lawfulness, fairness and transparency
  (อยู่ภายใต้กรอบของกฎหมาย, มีความเป็นธรรมและมีความโปร่งใส)
- purpose limitation (มีกรอบวัตถุประสงค์ที่จำกัด)
- data minimization (มีจำนวนข้อมูลที่น้อยที่สุด)
- Accuracy (มีความถูกต้อง)
- storage limitation (จัดเก็บเฉพาะเท่าที่จำเป็น)
- integrity and confidentiality (มีความสมบูรณ์และคงสภาพที่เป็นความลับอยู่ได้)
- accountability (ตรวจสอบได้)

21

lawfulness, fairness and transparency

- อยู่ภายใต้กรอบของกฎหมาย, มีความเป็นธรรมและมีความโปร่งใสในการปฏิบัติต่อเจ้าของข้อมูล

- processed lawfully, fairly and in a transparent manner in relation to the data subject.

[GDPR Article 5 (1) (a)]

22

purpose limitation

- ได้รับการจัดเก็บเพื่อวัตถุประสงค์ที่มีความเฉพาะเจาะจง, แจ้งชัด, และมีผลบังคับตามกฎหมายและไม่ดำเนินการไปในทางที่ไม่สอดคล้องต่อวัตถุประสงค์ดังกล่าว
- วัตถุประสงค์เกี่ยวกับการจัดทำจดหมายเหตุเพื่อประโยชน์แห่งสาธารณะ เพื่องานวิจัยหรือเพื่อการจัดเก็บสถิติด้านวิทยาศาสตร์ หรือประวัติศาสตร์

- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes.

[GDPR Article 5 (1) (b)]

23

data minimization

- พอสมควร มีความเกี่ยวข้อง และจำกัดข้อมูลที่มีความจำเป็นต่อการนำข้อมูลเหล่านั้นไปใช้ตามวัตถุประสงค์

- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

[GDPR Article 5 (1) (c)]

24

accuracy

- มีความเที่ยงตรง และหากจำเป็นให้มีการทำให้ทันสมัยอยู่เสมอ และมีการดำเนินการทุกขั้นตอนเพื่อที่จะมั่นใจได้ว่าข้อมูลส่วนบุคคลซึ่งไม่มีความเที่ยงตรงได้ถูกกำจัดหรือได้รับการแก้ไขอย่างไม่ชักช้า

- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

[GDPR Article 5 (1) (d)]

25

storage limitation

- ได้ถูกจัดเก็บในรูปแบบที่สามารถระบุตัวต้นของเจ้าของข้อมูลได้ โดยไม่เกินกว่าเวลาที่จำเป็นสำหรับวัตถุประสงค์ในการนำข้อมูลส่วนบุคคลนั้นไปใช้ ข้อมูลส่วนบุคคลอาจถูกจัดเก็บไว้นานกว่านั้นหากเป็นไปเพื่อวัตถุประสงค์ในการการจัดทำจดหมายเหตุเพื่อประโยชน์แห่งสาธารณะ เพื่องานวิจัยหรือเพื่อการจัดเก็บสถิติด้านวิทยาศาสตร์ หรือประวัติศาสตร์

- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject.

[GDPR Article 5 (1) (e)]

26

integrity and confidentiality

- ข้อมูลส่วนบุคคลจะถูกนำไปใช้ในลักษณะที่มีมาตรการการรักษาความปลอดภัยที่ รวมถึงการป้องกันการเข้าถึงหรือการดำเนินการอันไม่ชอบด้วยกฎหมาย การสูญหายโดยอุบัติเหตุ การถูกทำลายหรือถูกทำให้เสียหาย ทั้งนี้ด้วยการใช้เทคนิคหรือการจัดการองค์กรที่เหมาะสม
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

[GDPR Article 5 (1) (f)]

27

accountability

- ผู้ควบคุมข้อมูลมีหน้าที่ที่จะต้อง และสามารถแสดงว่าตนสามารถปฏิบัติภายใต้มาตรการข้างต้นได้ทั้งหมด
- The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1.

[GDPR Article 5(2)]

28

Personal Data Protection Act B.E. 2562 (TH's PDPA)

29

Published on Government Gazette 27th May 2019

Coming into Force:

- **Phrase A. → 28 May 2019 :**
  - **Chapter I. (PDPA Board Committee) &**
  - **Chapter IV. (Office of PDPA Board Committee)**
- **Phrase B. → 27 May 2020:**
  - **Chapter II. (Protection of Personal Data)**
  - **Chapter III. (Use or Disclosure of Personal Data)**
  - **Chapter V. (Complaint-Dispute Resolutions)**
  - **Chapter VI (Civil Responsibility)**
  - **Chapter VII (Penalty)**
  - **Section 94 – Initial Operations for Office of PDPA Board Committee**
  - **Section 96 – Supervision on Issuance of Subordinate Laws and Regulations by Gov.**

30

Ministry of Digital Economy & Society as the Interim Office to PDPA Board

- **Phrase A: ➔ Issuance 12 Subordinate Laws or Regulations for Formulation of PDPA Board & Office of PDPA Board by 180 days after promulgation of PDPA.**
- **Phrase B: ➔ Issuance 29 Subordinate Laws or Regulations for Technical Features related to Operation of Law by 1 year after promulgation of PDPA (to be monitored by Government Committee)**

31

Legal Aspect of PDPA

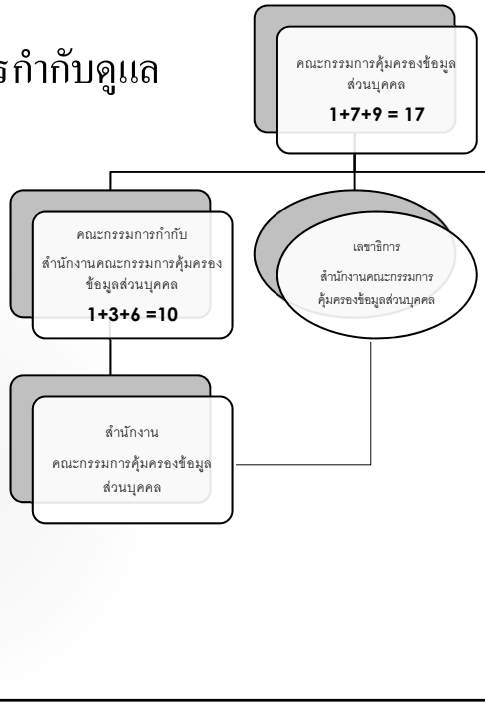
Not only respects Human Rights' Protection under Constitution

But

Reveals Consumer Protection Scheme by
Supervising Service Providers ("Controller" and "Processor")
and
Protecting Rights of Consumer ("Data Subject")

32

โครงสร้างการกำกับดูแล



33

สาระสำคัญของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ขอบเขตการบังคับใช้
ใช้บังคับแก่การเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลฯ ที่เกิดขึ้นในราชอาณาจักร
ครอบคลุมถึงกรณีผู้ควบคุมและผู้ประมวลผลอยู่นอกราชอาณาจักร หากมีกิจกรรมดังนี้
(1) เสนอขายสินค้าหรือบริการแก่เจ้าของข้อมูลซึ่งอยู่ในราชอาณาจักรไม่ว่าจะมีการชำระเงินหรือไม่
(2) การเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลที่เกิดขึ้นในราชอาณาจักร (GDPR Article 3 Territorial scope)

ระยะเวลาบังคับใช้
พ้น 1 ปี นับแต่วันประกาศในราชกิจจาฯ
ยกเว้นหมวดคณะกรรมการ และสำนักงานมีผลทันที

คำนิยาม
ข้อมูลส่วนบุคคล ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้ไม่สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ
ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

บทเฉพาะกาล
ให้ข้อมูลเดิมที่เก็บอยู่ก่อนวันที่กฎหมายใช้บังคับ ยังใช้หรือเปิดเผยได้ตามวัตถุประสงค์เดิมที่ได้แจ้งไว้ต่อเจ้าของข้อมูล และต้องกำหนดวิธีการยกเลิกความยินยอมให้สามารถแจ้งยกเลิกความยินยอมได้โดยง่าย

แจ้งให้ทราบ
ต้องแจ้งเจ้าของข้อมูลทราบถึงวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผย

ความยินยอม
ต้องขอความยินยอม โดยต้องมีความชัดเจน ไม่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลเข้าใจผิด
การขอความยินยอม ต้องทำเป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ เว้นแต่โดยสภาพไม่อาจขอความยินยอมด้วยวิธีการดังกล่าวได้
การถอนความยินยอม เจ้าของข้อมูลถอนความยินยอม เมื่อใดก็ได้ (เว้นแต่มีข้อจำกัด ตามที่กฎหมายกำหนด)

การเก็บข้อมูล ม.22-23
ให้เก็บได้เท่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูล

34

สาระสำคัญของ PDPA

ข้อยกเว้นการบังคับใช้ ม.4

พระราชบัญญัตินี้ ไม่ใช้บังคับแก่

(1) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของบุคคลที่ทำการเก็บ รวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์ส่วนตัวของบุคคลหรือเพื่อกิจกรรมในครอบครัวของบุคคลเท่านั้น

(2) การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงปลอดภัยของรัฐ ซึ่งรวมถึงความมั่นคงทางการคลังของรัฐ หรือการรักษาความปลอดภัยของประชาชน รวมทั้งหน้าที่เกี่ยวกับการป้องกันและปราบปรามการฟอกเงินหรือนิติวิทยาศาสตร์ หรือการรักษาความมั่นคงปลอดภัยไซเบอร์

(3) บุคคลหรือนิติบุคคลซึ่งใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวมไว้เฉพาะเพื่อกิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพหรือเป็นประโยชน์สาธารณะเท่านั้น

(4) สภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมาธิการ ซึ่งเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในการพิจารณาตามหน้าที่และอำนาจ

(5) การพิจารณาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา

(6) การดำเนินกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

การยกเว้นทั้งหมดหรือแต่บางส่วน ในลักษณะใด กิจการใด หรือหน่วยงานใด ตามวรรคหนึ่ง หรือเพื่อประโยชน์สาธารณะอื่นใด ให้ตราเป็นพระราชกฤษฎีกา

ผู้ควบคุมข้อมูล ตาม (2) (3) (4) (5) และ (6) และที่ได้รับยกเว้นตามวรรคสอง ต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานด้วย

35

สาระสำคัญของ PDPA

ข้อยกเว้นการจัดเก็บข้อมูลโดยไม่ต้องได้รับความยินยอม ม.24

(1) เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ ตามที่คณะกรรมการประกาศกำหนด

(2) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

(3) เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

(4) เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล

(5) เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล

(6) เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

ข้อยกเว้นการจัดเก็บข้อมูล<u>จากแหล่งอื่น</u> ม.25

ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง เว้นแต่
(1) ได้แจ้งถึงการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นให้แก่เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า แต่ต้องไม่เกินสามสิบวันนับแต่วันที่เก็บรวบรวมและได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล
(2) เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26

36

สาระสำคัญของ PDPA

การเก็บข้อมูล Sensitive ม.26

ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

(1) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคลซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ ไม่ว่าด้วยเหตุใดก็ตาม

(2) เป็นการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไร ที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญาหรือสหภาพแรงงานให้แก่สมาชิก ผู้ซึ่งเคยเป็นสมาชิก หรือผู้ซึ่งมีการติดต่ออย่างสม่ำเสมอกับมูลนิธิสมาคม หรือองค์กรที่ไม่แสวงหากาไรตามวัตถุประสงค์ดังกล่าวโดยไม่ได้เปิดเผยข้อมูลส่วนบุคคลนั้นออกไปภายนอกมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากาไรนั้น

(3) เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล

(4) เป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

(5) เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลวัตถุประสงค์เกี่ยวกับ
- เวชศาสตร์ป้องกัน หรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง...
- ประโยชน์สาธารณะด้านการสาธารณสุข
- การคุ้มครองแรงงาน การประกันสังคม หลักประกันสุขภาพแห่งชาติ...
- การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่น
- ประโยชน์สาธารณะที่สำคัญ

กรณีประวัติอาชญากรรม ต้องกระทำภายใต้การควบคุมของหน่วยงานที่มีอำนาจหน้าที่ตามกฎหมาย

37

สาระสำคัญของ PDPA

การใช้ หรือ การเปิดเผยข้อมูล ม.27

ห้ามมิให้ใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอม

การใช้หรือเปิดเผยข้อมูลส่วนบุคคลนั้น จะต้องเป็นไปตามที่ให้ความยินยอม

การใช้หรือเปิดเผยในกรณียกเว้นตาม ม. 24 และ ม.26 จะต้องบันทึกการใช้และการเปิดเผยนั้นด้วย

การโอนข้อมูลไปต่างประเทศ ม.28

ต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ทั้งนี้ต้องเป็นไปตามหลักเกณฑ์ที่คณะกรรมการกำหนด

กำหนดข้อยกเว้น

(1) เป็นการปฏิบัติตามกฎหมาย

(2) ได้รับความยินยอมจากเจ้าของข้อมูล โดยได้แจ้งถึงมาตรฐานที่ไม่เพียงพอของปลายทางที่รับข้อมูลแล้ว

(3) เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลเป็นคู่สัญญาหรือเพื่อใช้ดำเนินการตามคำขอของเจ้าของข้อมูล ก่อนเข้าทำสัญญานั้น

(4) เป็นการทำตามสัญญาระหว่างผู้ควบคุมข้อมูลกับบุคคลหรือนิติบุคคลอื่น เมื่อเจ้าของข้อมูลไม่สามารถให้ความยินยอมในขณะนั้นได้

(5) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกายหรือสุขภาพของเจ้าของข้อมูลหรือบุคคลอื่น เมื่อเจ้าของข้อมูลส่วนบุคค]ไม่สามารถให้ความยินยอมในขณะนั้นได้

(6) เป็นการจำเป็นเพื่อดำเนินภารกิจเพื่อประโยชน์สาธารณะที่สำคัญ

(GDPR Article 45 Transfers on the basic of an adequacy decision safeguards)

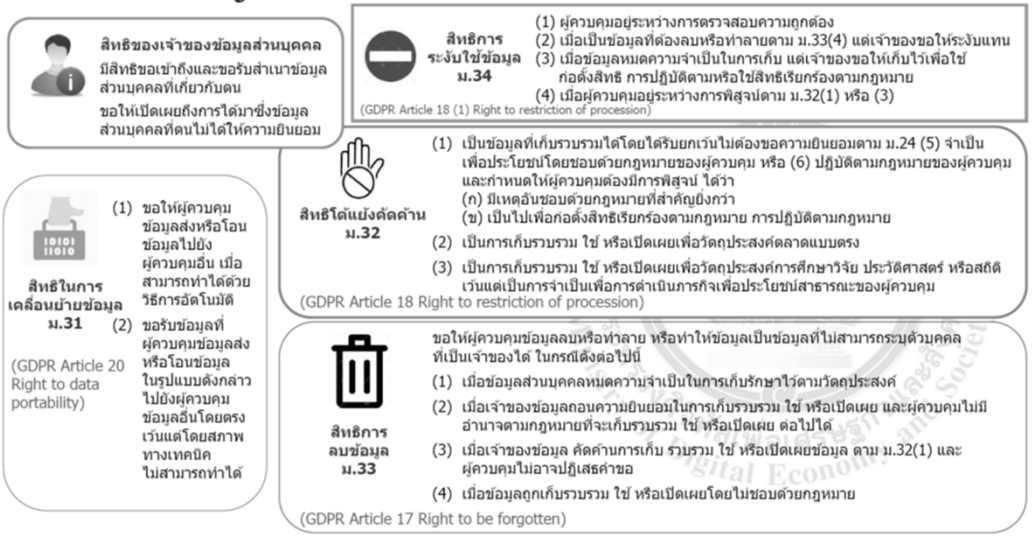
กรณีมีปัญหาเกี่ยวกับมาตรฐานที่เพียงพอของปลายทาง ให้คณะกรรมการกำหนดเป็นผู้วินิจฉัย (GDPR Article 46 Transfer subject to appropriate)

BCR ม.29

กำหนดหลักการ กฎเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลไปยังต่างประเทศและอยู่ในเครือกิจการหรือเครือธุรกิจเดียวกัน เพื่อการประกอบกิจการหรือธุรกิจร่วมกัน หากมีนโยบายที่ได้รับการตรวจสอบและรับรองจากสำนักงาน สามารถโอนข้อมูลไปยังต่างประเทศได้ (เป็นไปตามที่คณะกรรมการกำหนด (GDPR Article 47 Binding corporate rules)

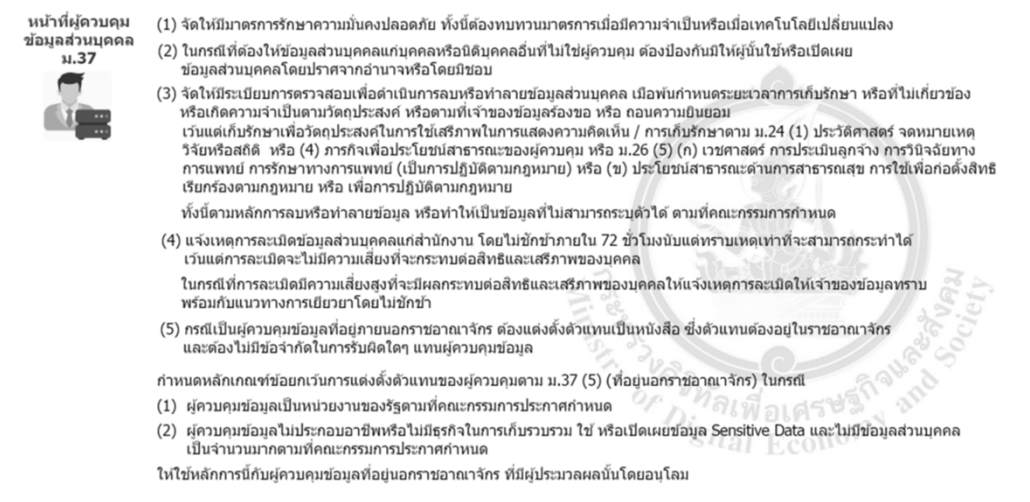
38

สาระสำคัญของ PDPA

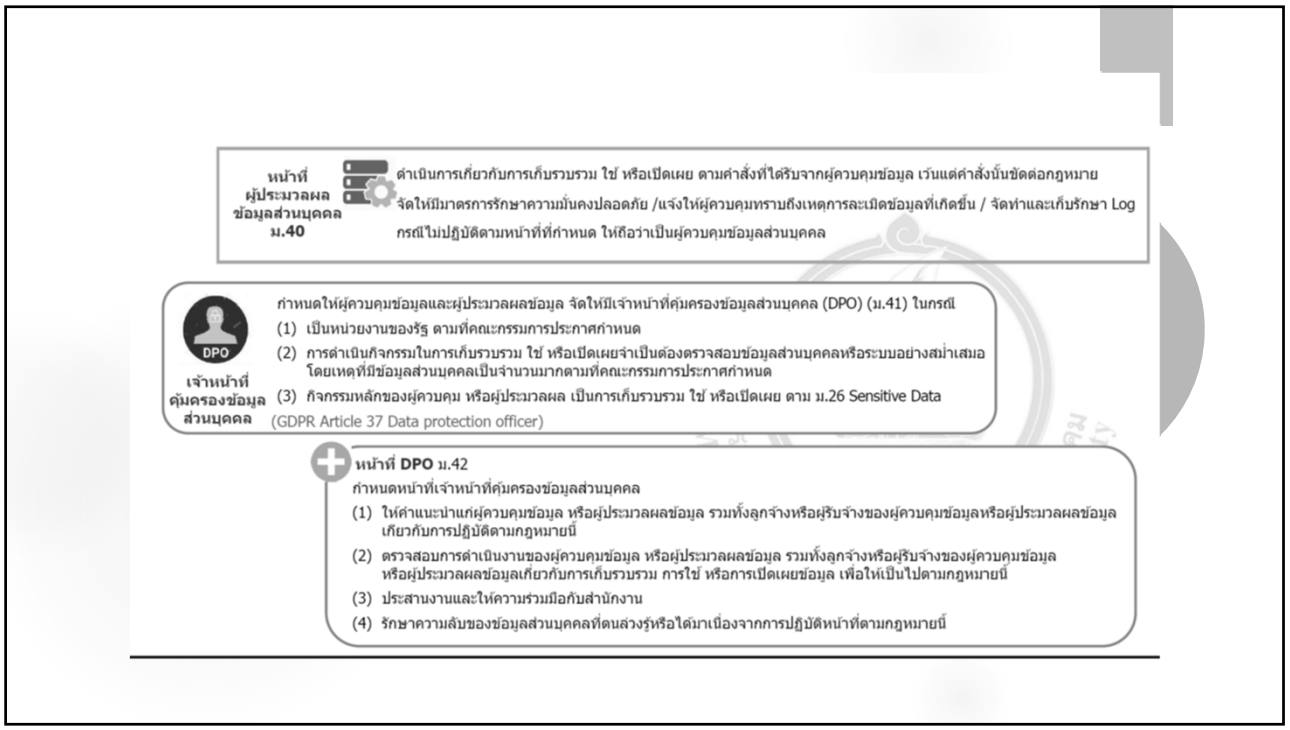


39

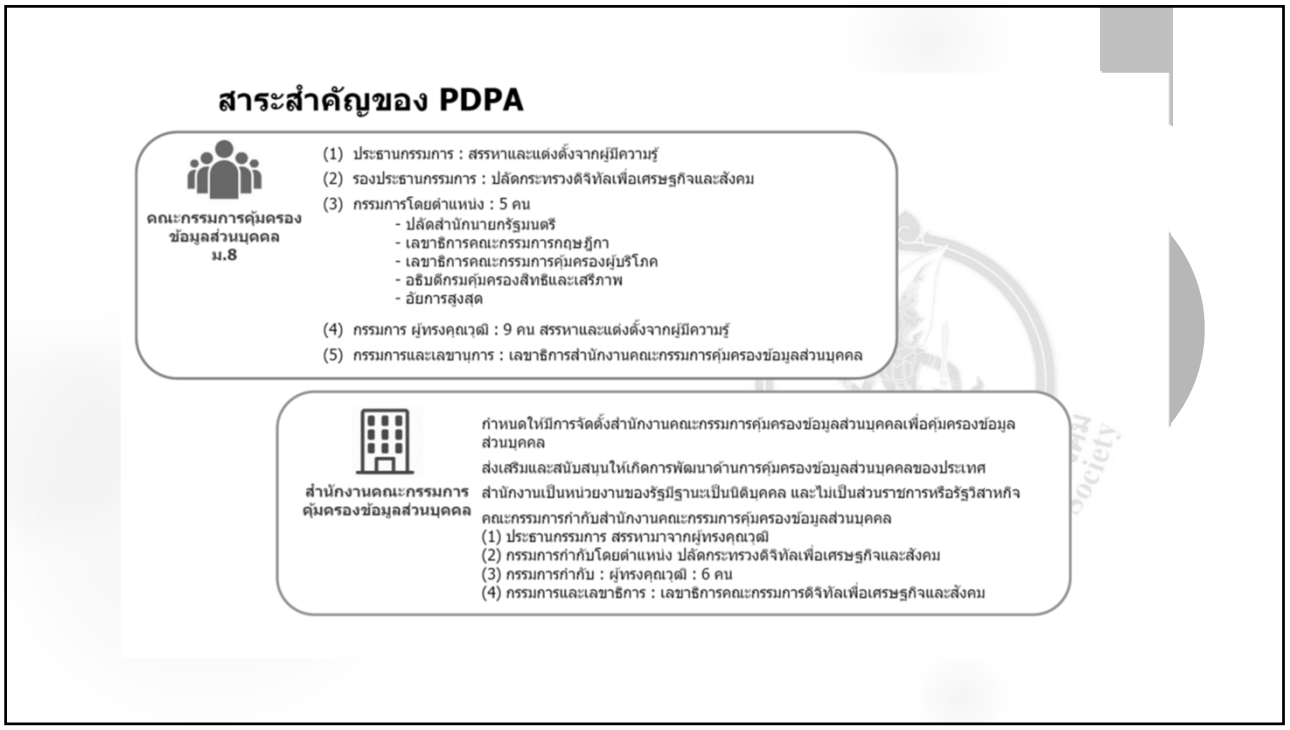
สาระสำคัญของ PDPA



40


หน้าที่ ผู้ประมวลผลข้อมูลส่วนบุคคล ม.40
ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผย ตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูล เว้นแต่คำสั่งนั้นขัดต่อกฎหมาย
จัดให้มีมาตรการรักษาความมั่นคงปลอดภัย /แจ้งให้ผู้ควบคุมทราบถึงเหตุการละเมิดข้อมูลที่เกิดขึ้น / จัดทำและเก็บรักษา Log
กรณีไม่ปฏิบัติตามหน้าที่ที่กำหนด ให้ถือว่าเป็นผู้ควบคุมข้อมูลส่วนบุคคล
DPO
เจ้าหน้าที่ คุ้มครองข้อมูลส่วนบุคคล
กำหนดให้ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) (ม.41) ในกรณี
(1) เป็นหน่วยงานของรัฐ ตามที่คณะกรรมการประกาศกำหนด
(2) การดำเนินกิจกรรมในการเก็บรวบรวม ใช้ หรือเปิดเผยจำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ โดยเหตุที่มีข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่คณะกรรมการประกาศกำหนด
(3) กิจกรรมหลักของผู้ควบคุม หรือผู้ประมวลผล เป็นการเก็บรวบรวม ใช้ หรือเปิดเผย ตาม ม.26 Sensitive Data
(GDPR Article 37 Data protection officer)
หน้าที่ DPO ม.42
กำหนดหน้าที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
(1) ให้คำแนะนำแก่ผู้ควบคุมข้อมูล หรือผู้ประมวลผลข้อมูล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูล เกี่ยวกับการปฏิบัติตามกฎหมายนี้
(2) ตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูล หรือผู้ประมวลผลข้อมูล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูล หรือผู้ประมวลผลข้อมูลเกี่ยวกับการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูล เพื่อให้เป็นไปตามกฎหมายนี้
(3) ประสานงานและให้ความร่วมมือกับสำนักงาน
(4) รักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่ตามกฎหมายนี้

41

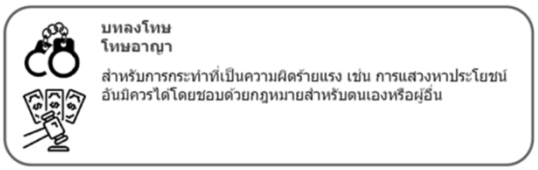

สาระสำคัญของ PDPA
คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ม.8
(1) ประธานกรรมการ : สรรหาและแต่งตั้งจากผู้มีความรู้
(2) รองประธานกรรมการ : ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
(3) กรรมการโดยตำแหน่ง : 5 คน
- ปลัดสำนักนายกรัฐมนตรี
- เลขาธิการคณะกรรมการกฤษฎีกา
- เลขาธิการคณะกรรมการคุ้มครองผู้บริโภค
- อธิบดีกรมคุ้มครองสิทธิและเสรีภาพ
- อัยการสูงสุด
(4) กรรมการ ผู้ทรงคุณวุฒิ : 9 คน สรรหาและแต่งตั้งจากผู้มีความรู้
(5) กรรมการและเลขานุการ : เลขาธิการสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
กำหนดให้มีการจัดตั้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเพื่อคุ้มครองข้อมูลส่วนบุคคล
ส่งเสริมและสนับสนุนให้เกิดการพัฒนาด้านการคุ้มครองข้อมูลส่วนบุคคลของประเทศ
สำนักงานเป็นหน่วยงานของรัฐมีฐานะเป็นนิติบุคคล และไม่เป็นส่วนราชการหรือรัฐวิสาหกิจ
คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
(1) ประธานกรรมการ สรรหามาจากผู้ทรงคุณวุฒิ
(2) กรรมการกำกับโดยตำแหน่ง ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
(3) กรรมการกำกับ : ผู้ทรงคุณวุฒิ : 6 คน
(4) กรรมการและเลขาธิการ : เลขาธิการคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคม

42

สาระสำคัญของ PDPA

43

สาระสำคัญของ PDPA



		บทลงโทษ		
		ปรับ	จำคุก	ทั้งสอง
ม.79 ผู้ควบคุมข้อมูลฝ่าฝืนหรือไม่ปฏิบัติตาม	ม.27 วรรคหนึ่ง (ใช้หรือเปิดเผยโดยไม่ได้รับความยินยอม)	<= 500,000	<=6 เดือน	✓ ยอมความได้
	ม.27 วรรคสอง (ได้รับข้อมูลตามวรรคหนึ่ง เปิดเผยนอกวัตถุประสงค์)			
	ม.28 (โอนข้อมูลไปต่างประเทศ) เกี่ยวกับข้อมูล ม.26 (Sensitive) โดยทำให้ผู้อื่นเกิดความเสียหาย			
	ม.27 วรรคสอง ใช้หรือเปิดเผยโดยไม่ได้รับความยินยอม หรือนอกวัตถุประสงค์หรือ ส่งหรือโอนข้อมูลส่วนบุคคลที่ Sensitive ไปต่างประเทศ เพื่อแสวงหาผลประโยชน์ที่มิควรได้	<=1,000,000	<=1 ปี	✓ ยอมความได้
ม.80 ผู้ใด	ล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ ตาม พ.ร.บ. นี้ ถ้านำไปเปิดเผยแก่ผู้อื่น	<=500,000	<=6 เดือน	✓
ม.81 นิติบุคคล	กระทำความผิดตาม พ.ร.บ. นี้ ถ้าการกระทำนั้นเกิดจากการสั่งการหรือการกระทำของกรรมการ หรือผู้จัดการ หรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น ผู้นั้นต้องรับโทษตามที่บัญญัติไว้ด้วย			

44

สาระสำคัญของ PDPA

บทลงโทษ
โทษปรับทางปกครอง

สำหรับความผิดที่เป็นการฝ่าฝืนหรือไม่ปฏิบัติตามหลักเกณฑ์ที่กำหนด เช่น การไม่ขอความยินยอมตามแบบหรือข้อความที่คณะกรรมการประกาศกำหนด ไม่ปฏิบัติตามคำสั่งของคณะกรรมการผู้เชี่ยวชาญ หรือไม่มาชี้แจงข้อเท็จจริง เป็นต้น

ม.82 ผู้ควบคุมข้อมูลไม่ปฏิบัติตาม	ม.23 ไม่แจ้งให้เจ้าของข้อมูลทราบถึงวัตถุประสงค์	<=1,000,000
	ม.30 วรรคสี่ ไม่ปฏิบัติตามเกณฑ์ในการให้เจ้าของเข้าถึงข้อมูล+รับสำเนา	
	ม.39 วรรคหนึ่ง บันทึกรายการให้เจ้าของข้อมูลและสำนักงานตรวจสอบ	
	ม.41 วรรคหนึ่ง จัดให้มี DPO หรือ ม.42 วรรคสอง สนับสนุน DPO หรือ วรรคสาม ไล่ DPO	
ม.83 ผู้ควบคุมข้อมูลฝ่าฝืนหรือไม่ปฏิบัติตาม	ม.21 เก็บ ใช้ รวบรวม เผยแพร่ต้องเป็นไปตามวัตถุประสงค์	<=3,000,000
	ม.22 เก็บ รวบรวม ให้เท่าที่จำเป็นตามที่กฎหมายกำหนด	
	ม.24 ข้อยกเว้นการเก็บจากเจ้าของข้อมูลโดยตรง	
	ม.25 วรรคหนึ่ง (ข้อยกเว้นการเก็บจากแหล่งอื่น)	
	ม.27 วรรคหนึ่งหรือวรรคสอง (ใช้เปิดเผยโดยไม่มีความยินยอม)	
	ม.28 โอนไปต่างประเทศ	
	ม.32 วรรคสอง (สิทธิคัดค้าน ใช้ เปิดเผย)	
	ม.37 หน้าที่ผู้ควบคุม	
	ขอความยินยอมโดยการหลอกลวง หรือใช้ผิดวัตถุประสงค์ (ม.21) ซึ่งได้นำมาใช้โดยอนุโลมตาม ม.25 วรรคสอง (แจ้งวัตถุประสงค์ใหม่)	
	ส่งหรือโอนข้อมูล ไม่เป็นไปตาม ม.29 วรรคหนึ่งหรือวรรคสาม (CBR)	

45

สาระสำคัญของ PDPA

บทลงโทษ
โทษปรับทางปกครอง

สำหรับความผิดที่เป็นการฝ่าฝืนหรือไม่ปฏิบัติตามหลักเกณฑ์ที่กำหนด เช่น การไม่ขอความยินยอมตามแบบหรือข้อความที่คณะกรรมการประกาศกำหนด ไม่ปฏิบัติตามคำสั่งของคณะกรรมการผู้เชี่ยวชาญ หรือไม่มาชี้แจงข้อเท็จจริง เป็นต้น

ม.84 ผู้ควบคุมข้อมูลฝ่าฝืน	ม.26 Sensitive วรรคหนึ่งหรือวรรคสอง (ใช้หรือเปิดเผยโดยไม่ได้รับความยินยอม)	<=5,000,000
	ม.27 วรรคหนึ่ง ใช้หรือเปิดเผยโดยไม่ได้รับความยินยอม หรือ วรรคสอง นอกเหนือวัตถุประสงค?	
	ม.28 ส่งหรือโอนข้อมูลไป ต.ป.ท. ซึ่งเป็นข้อมูล ม.26 Sensitive Data	
	ส่งหรือโอน ที่เป็นข้อมูล ม.26 Sensitive Data โดยไม่เป็นไปตาม ม.29 วรรคหนึ่งหรือวรรคสาม (CBR))	
ม.85 ผู้ประมวลผลข้อมูลไม่ปฏิบัติตาม	ม.41 วรรคหนึ่ง (DPO) หรือ ม.42 วรรคสองหรือวรรคสาม (การไล่ DPO)	<=1,000,000
ม.86 ผู้ประมวลผลข้อมูลไม่ปฏิบัติตาม	ม.40 หน้าที่ผู้ประมวลผล โดยไม่มีเหตุอันควร	<=3,000,000
	ส่งหรือโอนข้อมูลโดยไม่เป็นไปตาม ม.29 วรรคหนึ่งหรือวรรคสาม (CBR)	
	ม.37(5) ผู้ควบคุมต้องตั้ง DPO ซึ่งได้นำมาใช้บังคับโดยอนุโลมตาม ม.38 วรรคสอง (การตั้งตัวแทนในราชอาณาจักร)	
ม.87 ผู้ประมวลผลข้อมูล	ส่งหรือโอนข้อมูลไป ตปท. ตาม ม.26 Sensitive Data วรรคหนึ่งหรือวรรคสาม (ประวัติอาชญากรรม) โดยไม่เป็นไปตาม ม.29 วรรคหนึ่งหรือวรรคสาม (CBR)	<=5,000,000
ม.88 ตัวแทนผู้ควบคุมหรือตัวแทนผู้ประมวลผล	ไม่ปฏิบัติตาม ม.39 วรรคหนึ่ง (บันทึกรายการ) ซึ่งมาบังคับใช้โดยอนุโลมตาม ม.39 วรรคสอง (ตัวแทนผู้ควบคุม) และ ม.41 วรรคหนึ่ง (ตั้ง DPO) ซึ่งมาบังคับใช้โดยอนุโลมตาม ม.4 วรรคสี่ (การตั้งตัวแทนในราชอาณาจักร)	<=1,000,000
ม.89 ผู้ใด	ไม่ปฏิบัติตามคำสั่งของคณะกรรมการผู้เชี่ยวชาญ ตามมาตรา 75 หรือไม่ปฏิบัติตาม ม.76 วรรคหนึ่ง (แจ้งให้ส่งหนังสือ) หรือไม่อำนวยความสะดวกแก่ พนง.จนท. ตาม ม.76 วรรคสี่	<=500,000

46

บทเฉพาะกาล

- ในวาระเริ่มแรก ให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ประกอบด้วยกรรมการโดยตำแหน่ง ให้รองประธานทำหน้าที่ประธานเป็นการชั่วคราว

  ให้แต่งตั้งประธานกรรมการและกรรมการผู้ทรงคุณวุฒิให้แล้วเสร็จภายใน 90 วันนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ
- ให้ดำเนินการให้มีคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน 90 วันนับแต่วันที่มีการแต่งตั้งประธานกรรมการและกรรมการผู้ทรงคุณวุฒิในคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
- ให้ดำเนินการจัดตั้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลให้แล้วเสร็จภายใน 1 ปีนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ
- ให้สำนักงานปลัดกระทรวง D.E. ทำหน้าที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
- ให้รัฐมนตรี D.E. แต่งตั้งรองปลัดกระทรวง D.E. ทำหน้าที่เลขาธิการสำนักงานฯ เป็นการชั่วคราว และให้แต่งตั้งเลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลให้แล้วเสร็จภายใน 90 วัน นับแต่วันที่จัดตั้งสำนักงานฯ แล้วเสร็จ

47

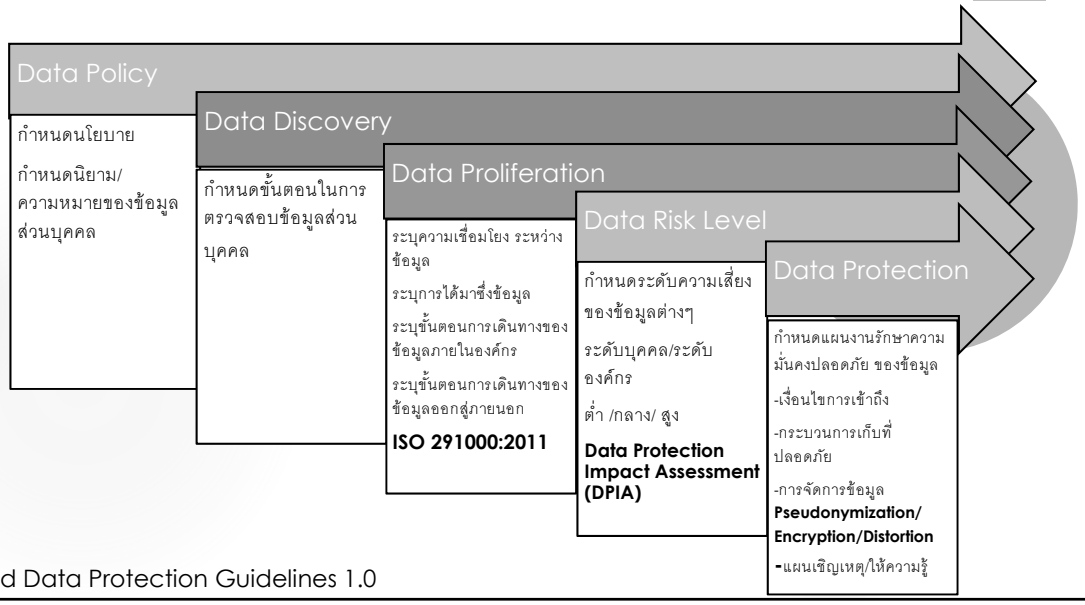
What shall be done with existing Personal Data

Section 95:

- **For existing <u>Personal Data collected before enforcement of the law</u>,**
- **Controller is capable "to collect" and "to use" the existing data only under former objectives providing that:**
- **The Controller must grant the Data Subject convenient procedure on revocation of his consent and**
- **inform the Data Subject who denies collecting and using of his own data to utilize such procedure easily.**

48

การเตรียมความพร้อมขององค์กร



ที่มา. Thailand Data Protection Guidelines 1.0

49

PDPA Overview

Scope of Obligations — Enforced to both Public and Private Sector; Shall be Principle law for Personal Protection; Except some activities; Extra territorial

Definitions

Personal Data refers to data about an individual who can be identify or identifiable from that data but not including data of the deceased

Covers electronic & non-electronic data

Not define Data Subject or Data Owner

Data Controller having the power and duties to make decisions regarding the collection, use, or disclosure of the Personal Data

Data Processor under the instruction of or in the name of Data Controller

Consent shall be requested from data subject for the collection, use, or disclosure of personal data

Purpose Limitation Collection of personal data may be made to the extent necessary under the lawful objective of personal data controller

Complaints shall be submitted to the Expert committee

Entry into force

Coming into force 1 year after its publication except Committee and Office shall effect next day publication

Data obtained before the date of coming into force

Data controller can use personal data in accordance with the objectives already notified to the data subject prior to the enforcement of this Act, and must be defined method for cancel consent

The PDPA does not cover — Any individual acting in a personal use or for his family activities

Transfer/ Crossborder Limitation prescribes the rules on sending or transfer of personal data abroad

Limiting Collection, Use, Disclosure

shall not collect personal data without the consent of the data subject

provides exceptions for some cases where personal data can be collected without the consent of data subject

shall inform the data subject of the period of retention of personal data

shall not collect sensitive personal data or any other data as prescribed by the committee

Data subject right

to rectify : can request their data be updated or made complete.

to forgotten : right to withdraw his or her consent or delete or destroy the data when Data controller fails to comply with the rules under this Act.

to data portability : can request a copy of their data in digital format.

50

Key Considerations of the PDPA

Penalties

<= 5,000,000

The PDPA Penalties & fines apply to both Controllers and Processors

Explicit consent

Must be provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

Limiting Collection, Use, Disclosure

collect, use or disclose personal data about an individual for the purposes that a reasonable person would consider appropriate in the circumstances and for which the individual has given consent.

Breach notification within 72 hours

Reported within 72 hours of first having become aware of the breach.

Right to be forgotten

data subject to have the data controller erase his / her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data.

Right to access and portability

Data subjects can request confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, in an electronic format (if practicable).

Appointed Data Protection Officers

Appointed in certain cases (public authorities, when monitoring of data subjects on a large scale and when processing special categories of data). To facilitate the need for a organisation to demonstrate their compliance to the PDPA

51

52