PDPA กับการใช้ข้อมูลของนักศึกษาแพทย์ในการบริหารและวิจัย

นพ.นวนรรน ธีระอัมพรพันธุ์

คณะแพทยศาสตร์โรงพยาบาลรามาธิบดี มหาวิทยาลัยมหิดล

23 เมษายน 2567

www.SlideShare.net/Nawanan

BY NC

Disclaimer: เป็นความเห็นทางวิชาการส่วนบุคคล ไม่ใช่ความเห็นทางการของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (กคส.) หรือสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) และไม่ผูกพันการทำหน้าที่ของวิทยากรในบทบาทใดในปัจจุบันหรืออนาคต

ข้อมูลส่วนบุคคลกับงานด้านแพทยศาสตรศึกษา

- ข้อมูลส่วนบุคคลของใคร?
  - นักศึกษา
  - อาจารย์
  - นักการศึกษา/เจ้าหน้าที่
  - ผู้ป่วย
  - นักศึกษาในฐานะ Research Subject

ข้อมูลส่วนบุคคลกับงานด้านแพทยศาสตรศึกษา

- ใช้ข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ใดในงานด้านแพทยศาสตรศึกษา?
  - เพื่อการเรียนการสอน/การให้บริการการศึกษา
  - เพื่อดูแล well-being ของนักศึกษา
  - เพื่อบริหารจัดการพันธกิจด้านการศึกษา เช่น บริหารโครงการ ขับเคลื่อน กำกับ ติดตาม ประเมินผล แก้ไขปัญหา วิเคราะห์ วางแผน พัฒนาคุณภาพ ประกันคุณภาพ บริหารความเสี่ยง จัดการภาระงาน พัฒนาบุคลากร กำหนดทิศทาง นโยบาย ยุทธศาสตร์ และแผนงาน
  - เพื่อใช้อ้างอิงกรณีที่มีประเด็นทางกฎหมาย
  - เพื่อการวิจัย

Security & Privacy

http://en.wikipedia.org/wiki/A._S._Bradford_House

Security & Privacy

- Privacy: "The ability of an individual or group to seclude themselves or information about themselves and thereby reveal themselves selectively." (Wikipedia)
- Information Security: "Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction" (Wikipedia)

หลักการสำคัญของ Information Security

Confidentiality

- การรักษาความลับของข้อมูล

Integrity

- การรักษาความครบถ้วนและความถูกต้องของข้อมูล
- ปราศจากการเปลี่ยนแปลงแก้ไข ทำให้สูญหาย ทำให้เสียหาย หรือถูกทำลายโดยมิชอบ

Availability

- การรักษาสภาพพร้อมใช้งาน

Thailand Data Protection Guidelines 3.0

แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

Final Version 3.0

ธันวาคม 2563

สนับสนุนโดย

TDPG 3.0

https://www.law.chula.ac.th/wp-content/uploads/2020/12/TDPG3.0-C5-20201208.pdf

คณะนิติศาสตร์
จุฬาลงกรณ์มหาวิทยาลัย

เหตุผลในการประกาศใช้
พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

<u>หมายเหตุ</u> :- เหตุผลในการประกาศใช้พระราชบัญญัติฉบับนี้ คือ เนื่องจากปัจจุบันมีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมากจนสร้างความเดือดร้อนรำคาญหรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าว ทำได้โดยง่าย สะดวก และรวดเร็ว ก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวม สมควรกำหนดให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปขึ้น เพื่อกำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป จึงจำเป็นต้องตราพระราชบัญญัตินี้

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- **หมวด 1 คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล**
- **หมวด 2 การคุ้มครองข้อมูลส่วนบุคคล**
  - ส่วนที่ 1 บททั่วไป
  - ส่วนที่ 2 การเก็บรวบรวมข้อมูลส่วนบุคคล
  - ส่วนที่ 3 การใช้หรือเปิดเผยข้อมูลส่วนบุคคล
- **หมวด 3 สิทธิของเจ้าของข้อมูลส่วนบุคคล**
- **หมวด 4 สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล**
- **หมวด 5 การร้องเรียน**
- **หมวด 6 ความรับผิดทางแพ่ง**
- **หมวด 7 บทกำหนดโทษ**
  - ส่วนที่ 1 โทษอาญา
  - ส่วนที่ 2 โทษทางปกครอง
- **บทเฉพาะกาล**

เรื่องที่ควรทราบ เกี่ยวกับ PDPA

1. PDPA ไม่ได้มา “ยกเลิก” กฎหมายอื่นที่เกี่ยวข้องกับข้อมูลส่วนบุคคล เพียงแต่กำหนดหลักการเพิ่มเติม เงื่อนไขและหน้าที่ที่ต้องปฏิบัติ และสิทธิที่เจ้าของข้อมูลส่วนบุคคลมี

พรบ.สุขภาพแห่งชาติ พ.ศ. 2550

มาตรา 7 ข้อมูลด้านสุขภาพของบุคคล เป็นความลับส่วนบุคคล ผู้ใดจะนำไป**เปิดเผย**ในประการที่น่าจะทำให้บุคคลนั้น**เสียหาย**ไม่ได้ เว้นแต่การเปิดเผยนั้น**เป็นไปตามความประสงค์**ของบุคคลนั้นโดยตรง หรือมี**กฎหมายเฉพาะบัญญัติ**ให้ต้องเปิดเผย แต่ไม่ว่าในกรณีใด ๆ ผู้ใดจะอาศัยอำนาจหรือสิทธิตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการหรือกฎหมายอื่นเพื่อขอเอกสารเกี่ยวกับข้อมูลด้านสุขภาพของบุคคลที่ไม่ใช่ของตนไม่ได้

พรบ.ข้อมูลข่าวสารของราชการ พ.ศ. 2540

“เปิดเผยเป็นหลัก ปกปิดเป็นข้อยกเว้น”

มาตรา 15 ข้อมูลข่าวสารของราชการที่มีลักษณะอย่างหนึ่งอย่างใดดังต่อไปนี้ หน่วยงานของรัฐหรือเจ้าหน้าที่ของรัฐอาจมีคำสั่งมิให้เปิดเผยก็ได้ โดยคำนึงถึงการปฏิบัติหน้าที่ตามกฎหมาย...ประกอบกัน...

(5) รายงานการแพทย์หรือข้อมูลข่าวสารส่วนบุคคลซึ่งการเปิดเผยจะเป็นการรุกล้ำสิทธิส่วนบุคคลโดยไม่สมควร

(6) ข้อมูลข่าวสารของราชการที่มีกฎหมายคุ้มครองมิให้เปิดเผย...

กฎหมายเฉพาะ

- **พรบ.โรคติดต่อ พ.ศ. 2558**

มาตรา ๑๐ ในกรณีที่ข้อมูลจากการเฝ้าระวัง การสอบสวนโรค หรือการแจ้งหรือรายงานตามพระราชบัญญัตินี้ ซึ่งมีการพาดพิงถึงตัวบุคคลทั้งที่ระบุตัวได้หรือไม่สามารถระบุตัวได้ จะต้องเก็บเป็นความลับและประมวลผลโดยไม่เปิดเผยชื่อ ทั้งนี้ การประมวลผลดังกล่าวจะต้องเหมาะสมและตรงกับวัตถุประสงค์ในการป้องกันและควบคุมโรค

เจ้าพนักงานควบคุมโรคติดต่ออาจเปิดเผยข้อมูลตามวรรคหนึ่งบางส่วนที่เกี่ยวกับการรักษา การป้องกัน การควบคุมโรคติดต่ออันตราย หรือการเกิดโรคระบาด ซึ่งมีผลกระทบต่อสุขภาพของประชาชน โดยได้รับคำยินยอมจากเจ้าของข้อมูลหรือตามหลักเกณฑ์ วิธีการ และเงื่อนไขที่คณะกรรมการประกาศกำหนด

เรื่องที่ควรทราบ เกี่ยวกับ PDPA

2. ข้อยกเว้นการบังคับใช้ PDPA

(1) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของ**บุคคลที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคล<u>เพื่อประโยชน์ส่วนตนหรือเพื่อกิจกรรมในครอบครัวของบุคคลนั้น</u>เท่านั้น**

(2) การดำเนินการของ**หน่วยงานของรัฐที่มีหน้าที่ใน<u>การรักษาความมั่นคงของรัฐ</u>** ซึ่งรวมถึงความมั่นคงทางการคลังของรัฐ หรือการรักษาความปลอดภัยของประชาชน รวมทั้งหน้าที่เกี่ยวกับการป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ หรือการรักษาความมั่นคงปลอดภัยไซเบอร์

(3) การใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำการ**เก็บรวบรวมไว้เฉพาะเพื่อ<u>กิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรม</u>อันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพหรือเป็นประโยชน์สาธารณะเท่านั้น**

(4) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลในการพิจารณาตามหน้าที่และอำนาจของสภาผู้แทนราษฎร วุฒิสภา รัฐสภา หรือคณะกรรมาธิการ

(5) การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา

(6) การดำเนินการของบริษัทข้อมูลเครดิตและสมาชิก

Reference: PDPA ม.4

เรื่องที่ควรทราบ เกี่ยวกับ PDPA

3. PDPA วางหลักการทั่วไปของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล

กระบวนการเกี่ยวกับข้อมูลส่วนบุคคล

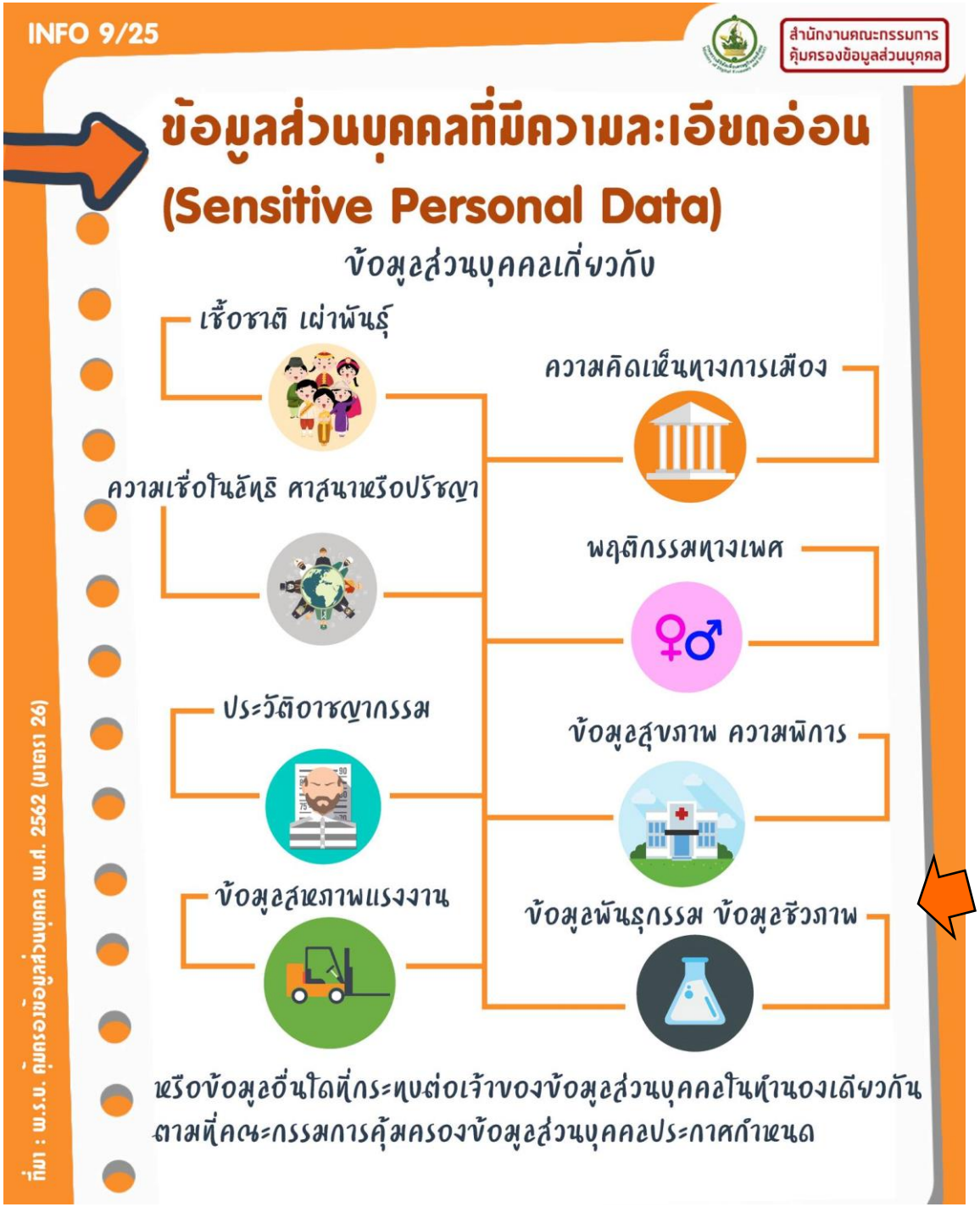
เก็บรวบรวม (Collection) → ใช้ (Use) → เปิดเผย (Disclosure)

ประมวลผล (Processing) = เก็บรวบรวม + ใช้ + เปิดเผย (+ จัดเก็บ/เก็บรักษา + วิเคราะห์ + แสดงผล + ทำรายงาน + แก้ไข + ลบ/ทำลาย ฯลฯ)

เรื่องที่ควรทราบ เกี่ยวกับ PDPA

4. ข้อมูลส่วนบุคคล (Personal Data) คือ ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ แบ่งเป็น 2 ประเภท

- ข้อมูลส่วนบุคคลทั่วไป (General/Non-Sensitive Personal Data)
- ข้อมูลส่วนบุคคลอ่อนไหว/ละเอียดอ่อน (Sensitive Personal Data)



Sensitive Personal Data

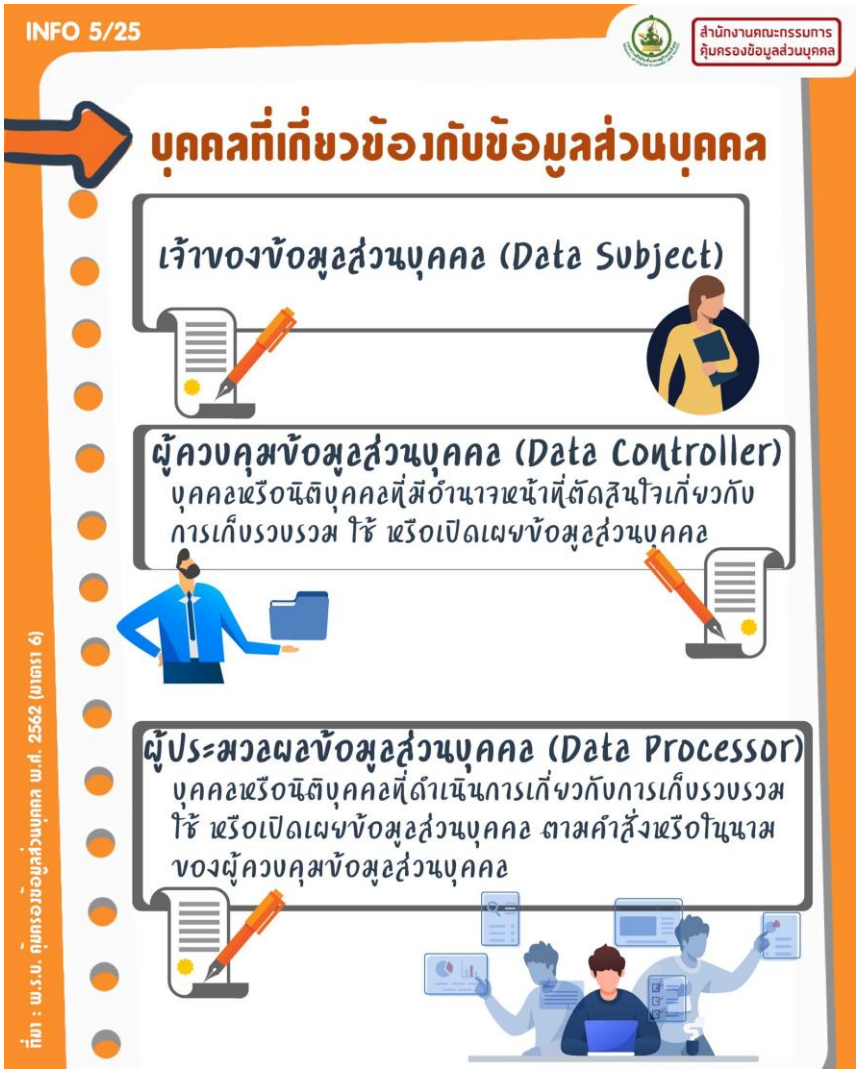
"ข้อมูลชีวภาพ" ตาม PDPA คือ Biometric Data (ที่ถูก คือ ข้อมูลชีวมาตร/ชีวมิติ) ใน พ.ร.บ. ใช้คำผิด แต่คำอธิบายในมาตรา 26 วรรคสอง ของ พ.ร.บ. ทำให้เข้าใจได้ว่าหมายถึง Biometric Data

Reference: PDPA ม.26

เรื่องที่ควรทราบ เกี่ยวกับ PDPA

5. ใครเป็นใคร ใน PDPA

- Data Subject (เจ้าของข้อมูลส่วนบุคคล)
- Controller (ผู้ควบคุมข้อมูลส่วนบุคคล)
  - มีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
  - เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในกิจการของตน
- Processor (ผู้ประมวลผลข้อมูลส่วนบุคคล)
  - ทำตามสั่ง/ในนามของ Controller



เรื่องที่ควรทราบ เกี่ยวกับ PDPA

6. PDPA กำหนดว่า การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล จะต้องทำ **“เท่าที่จำเป็น”** (ตามหลักการ Data Minimization)

- การเก็บรวบรวม ใช้ หรือเปิดเผย**เกินความจำเป็น เป็นความเสี่ยง** ของทั้ง controller และ data subject
- แต่ไม่ได้แปลว่าถ้าจำเป็นแล้วจะเก็บรวบรวม ใช้ หรือเปิดเผยไม่ได้
- “จำเป็น” -> มี **“ฐานทางกฎหมาย”** (lawful basis) 1 ใน 7 ฐาน ซึ่งไม่ใช่ว่าต้องขอความยินยอมก่อนเสมอไป ความยินยอมเป็นเพียง **“ฐานทางกฎหมาย” (lawful basis)** เดียวจากทั้งหมด 7 ฐาน เท่านั้น โดยแต่ละฐานจะมีเงื่อนไขและสถานการณ์ที่ควรนำมาใช้แตกต่างกัน

ฐานทางกฎหมายใน PDPA (กรณีไม่ใช่ข้อมูลส่วนบุคคลที่ sensitive)

1. การจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือการศึกษาวิจัยหรือสถิติ (Archiving, Research or Statistics)
2. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล (Vital Interest)
3. เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลฯ เป็นคู่สัญญา หรือเพื่อใช้ในการดำเนินการตามคำขอก่อนเข้าทำสัญญา (Contractual Performance)
4. เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะ หรือในการใช้อำนาจรัฐ (Public Task)
5. เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมาย เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลฯ (Legitimate Interests)
6. เป็นการปฏิบัติตามกฎหมาย (Legal Obligation)
7. ได้รับความยินยอม (Consent)

Reference: PDPA ม.24

ฐานการประมวลผลข้อมูล

Lawful Basis in PDPA

สำหรับข้อมูลส่วนบุคคลที่
ไม่ใช่ Sensitive Personal Data

Reference: PDPA ม.24

Legitimate Interests

- “เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมาย เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลฯ”
- การประเมิน Legitimate Interests Assessment (LIA) (3-part test) (From UK Information Commissioner’s Office [ICO])
  - **The purpose test** (identify the legitimate interest)
  - **The necessity test** (consider if the processing is necessary)
  - **The balancing test** (consider the individual’s interests)

https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/

LIA Part 1: The Purpose Test (Identify the Legitimate Interest)

1. How do we do the purpose test?

You need to identify your purpose and decide whether it counts as a legitimate interest. Be as specific as possible, as this helps you when it comes to the necessity and balancing tests.

You should ask:

- Why do you want to process the data?
- What benefit do you expect to get from the processing?
- Do any third parties benefit from the processing?
- Are there any wider public benefits to the processing?
- How important are those benefits?
- What would the impact be if you couldn't go ahead?
- What is the intended outcome for individuals?
- Are you complying with other relevant laws?
- Are you complying with industry guidelines or codes of practice?
- Are there any ethical issues with the processing?

https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/

LIA Part 1: The Purpose Test (Identify the Legitimate Interest)

Example

Lenders share data with Credit Reference Agencies (CRAs) about the payments made by an individual on an account. That data is then shared with any other lender that the individual makes an application to, so they can assess the individual's ability and inclination to repay a loan.

- The lender wants to accurately assess the likelihood that they will get back the money they lend out.
- The benefit is to minimise the risk of bad debts and ensure that the lender makes sustainable lending decisions to achieve a reasonable overall rate of return.
- It is also in the interests of the individual making the application that lenders make responsible lending decisions and don't allow them to become overburdened with debt they can't afford.
- Finally, it is in the interests of the public that lenders can make accurate risk assessments when making lending decisions. Without this, lenders may be less willing to lend, or at least lend at a reasonable interest rate.
- These benefits are vital to the proper functioning of the credit system.
- The intended outcome for the individual is that they will either be granted or refused credit on the basis of their ability to repay.
- The lenders comply with relevant consumer credit laws and standards.

The lenders have demonstrated a clear and specific legitimate interest, and have a good foundation for demonstrating necessity and objectively considering the balance of interests.

https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/

LIA Part 2: The Necessity Test (Consider if the Processing is Necessary)

2. How do we do the necessity test?

You must consider carefully whether the processing is actually necessary for the purpose you have identified in step one.

You need to ask:

- Will the processing actually help you achieve your purpose?
- Is the processing proportionate to that purpose, or could it be seen as using a sledgehammer to crack a nut?
- Can you achieve your purpose without processing the data, or by processing less data?
- Can you achieve your purpose by processing the data in another more obvious or less intrusive way?

Be honest in your consideration of whether the processing is necessary. If on the face of it there are potentially other less intrusive alternatives you need to be clear in your LIA why these are not reasonable alternatives.

If you find it difficult to explain how the processing helps achieve your objective, or there are many alternative methods which simply aren't your chosen business model, you may need to go back to step one and be more specific about your purpose. A clearly defined purpose should make the necessity test easier to navigate.

https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/

LIA Part 3: The Balancing Test (Consider the Individual's Interests)

3. How do we do the balancing test?

You need to consider the interests and fundamental rights and freedoms of the individual, and whether these override the legitimate interests you have identified.

There is no exhaustive list of what you should take into account when conducting the balancing test. However you should as a minimum consider:

- the **nature of the personal data** you want to process;
- the **reasonable expectations** of the individual; and
- the **likely impact** of the processing on the individual and whether any safeguards can be put in place to mitigate negative impacts.

https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/

LIA: Considering All 3 Parts

How do we decide the outcome?

You need to weigh up all the factors identified during your LIA for and against the processing, and decide whether you still think your interests should take priority over any risk to individuals. This is not a mathematical exercise and there is an element of subjectivity involved, but you should be as objective as possible.

You must be confident that you can show why the benefits of the processing justify any risks you have identified. The more significant the risks, the more compelling your justification must be.

Sometimes the outcome very obviously weighs in one direction in which case making the decision should be straightforward.

https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/

INFO 10/25

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Personal Data)

เช่น เชื้อชาติ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ

จะชอบด้วยกฎหมาย เมื่อทำตามหลักการหนึ่งหลักการใด ดังนี้

1. **Explicit Consent** ได้รับความยินยอมโดยชัดแจ้ง
2. **Vital Interest** ป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล ซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้
3. **Social Protection & Non-Profit** การดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไร

4. **Manifestly Made Public** ข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล
5. **Legal Claims** จำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

ที่มา : พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (มาตรา 26)

ฐานการประมวลผลข้อมูล

Lawful Basis in PDPA

สำหรับ Sensitive Personal Data

Reference: PDPA ม.26

ฐานการประมวลผลข้อมูล

Lawful Basis in PDPA

สำหรับ Sensitive Personal Data

Reference: PDPA ม.26

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- **ข้อยกเว้นการเก็บรวบรวมข้อมูลส่วนบุคคลที่เป็น Sensitive Data โดยไม่ได้รับความยินยอมโดยชัดแจ้ง (มาตรา 26)**
  - **(1) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคลซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ ไม่ว่าด้วยเหตุใดก็ตาม**
  - (2) เป็นการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงานให้แก่สมาชิก ผู้ซึ่งเคยเป็นสมาชิก หรือผู้ซึ่งมีการติดต่ออย่างสม่ำเสมอกับมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรตามวัตถุประสงค์ดังกล่าวโดยไม่ได้เปิดเผยข้อมูลส่วนบุคคลนั้นออกไปภายนอกมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรนั้น

Reference: PDPA ม.26

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- **ข้อยกเว้นการเก็บรวบรวมข้อมูลส่วนบุคคลที่เป็น Sensitive Data โดยไม่ได้รับความยินยอมโดยชัดแจ้ง (มาตรา 26)**
  - (3) เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล
  - (4) เป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

Reference: PDPA ม.26

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- **ข้อยกเว้นการเก็บรวบรวมข้อมูลส่วนบุคคลที่เป็น Sensitive Data โดยไม่ได้รับความยินยอมโดยชัดแจ้ง (มาตรา 26)**
  - (5) เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ
    - (ก) เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์ ทั้งนี้ ในกรณีที่ไม่ใช่การปฏิบัติตามกฎหมายและข้อมูลส่วนบุคคลนั้นอยู่ในความรับผิดชอบของผู้ประกอบอาชีพหรือวิชาชีพหรือผู้มีหน้าที่รักษาข้อมูลส่วนบุคคลนั้นไว้เป็นความลับตามกฎหมาย ต้องเป็นการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ประกอบวิชาชีพทางการแพทย์

Reference: PDPA ม.26

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- **ข้อยกเว้นการเก็บรวบรวมข้อมูลส่วนบุคคลที่เป็น Sensitive Data โดยไม่ได้รับความยินยอมโดยชัดแจ้ง (มาตรา 26)**
  - (5) เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ
    - (ข) ประโยชน์สาธารณะด้านการสาธารณสุข เช่น การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์ ซึ่งได้จัดให้มีมาตรการที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ

Reference: PDPA ม.26

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- **ข้อยกเว้นการเก็บรวบรวมข้อมูลส่วนบุคคลที่เป็น Sensitive Data โดยไม่ได้รับความยินยอมโดยชัดแจ้ง (มาตรา 26)**
  - (5) เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ
    - (ค) การคุ้มครองแรงงาน การประกันสังคม หลักประกันสุขภาพแห่งชาติ สวัสดิการเกี่ยวกับการรักษาพยาบาลของผู้มีสิทธิตามกฎหมาย การคุ้มครองผู้ประสบภัยจากรถ หรือการคุ้มครองทางสังคม ซึ่งการเก็บรวบรวมข้อมูลส่วนบุคคลเป็นสิ่งจำเป็นในการปฏิบัติตามสิทธิหรือหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลหรือเจ้าของข้อมูลส่วนบุคคล โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

Reference: PDPA ม.26

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- **ข้อยกเว้นการเก็บรวบรวมข้อมูลส่วนบุคคลที่เป็น Sensitive Data โดยไม่ได้รับความยินยอมโดยชัดแจ้ง (มาตรา 26)**
  - (5) เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ
    - (ง) การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่น ทั้งนี้ ต้องกระทำเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวเพียงเท่าที่จำเป็นเท่านั้น และได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคลตามที่คณะกรรมการประกาศกำหนด
    - (จ) ประโยชน์สาธารณะที่สำคัญ โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

Reference: PDPA ม.26

เรื่องที่ควรทราบ เกี่ยวกับ PDPA

7. ใน PDPA เราไม่ใช้ "ความยินยอม" (consent) เป็น "เหตุผลแรก" (ฐานแรก) ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล แต่เราจะพิจารณาว่ามีฐานทางกฎหมายอื่นที่เข้าได้ก่อนหรือไม่ หากไม่มี จึงค่อยใช้ "ฐานความยินยอม" (Consent should be the last resort.)

- **เหตุผล** ฐานความยินยอมตาม PDPA ใช้เมื่อเจ้าของข้อมูลฯ มีความเป็นอิสระในการตัดสินใจ (ไม่ได้ถูกผูกมัดด้วยเงื่อนไขอื่น อยู่ก่อน) และ PDPA วางหลักการเรื่อง consent ที่มีเงื่อนไขค่อนข้างเยอะ เพื่อรองรับหลักการความเป็นอิสระในการตัดสินใจ

- **หมายเหตุ** การไม่ใช้ฐานความยินยอมใน PDPA หมายถึงเฉพาะเรื่องการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล แต่ไม่รวมกรณีการให้บริการหรือการขอความยินยอมอื่น ๆ นอกเหนือจากเรื่องข้อมูลส่วนบุคคล เช่น โรงพยาบาล/แพทย์ ขอ consent ในการลงทะเบียนผู้ป่วย/เข้ารักษา/admit/ทำหัตถการ หรือการทำวิจัย ซึ่งเป็นไปตามหลักเกณฑ์จริยธรรมในเรื่องนั้น ๆ และนโยบายขององค์กร

Consent ใน PDPA

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- **ความยินยอม (มาตรา 19)**
  - ผู้ควบคุมข้อมูลส่วนบุคคลจะกระทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไม่ได้หากเจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอมไว้ก่อนหรือในขณะนั้น เว้นแต่บทบัญญัติแห่ง พ.ร.บ.นี้ หรือกฎหมายอื่นบัญญัติให้กระทำได้
  - การขอความยินยอมต้องทำโดยชัดแจ้ง เป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ เว้นแต่โดยสภาพไม่อาจขอความยินยอมด้วยวิธีการดังกล่าวได้
  - ในการขอความยินยอม... ต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไปด้วย และการขอความยินยอมนั้นต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน มีแบบหรือข้อความที่เข้าถึงได้ง่ายและเข้าใจได้ รวมทั้งใช้ภาษาที่อ่านง่าย และไม่เป็นการหลอกลวงหรือทำให้เข้าใจผิดในวัตถุประสงค์ดังกล่าว...
  - ในการขอความยินยอม...ผู้ควบคุมข้อมูลส่วนบุคคลต้องคำนึงอย่างถึงที่สุดในความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคลในการให้ความยินยอม ทั้งนี้ ในการเข้าทำสัญญาซึ่งรวมถึงการให้บริการใด ๆ ต้องไม่มีเงื่อนไขในการให้ความยินยอมเพื่อเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ไม่มีความจำเป็นหรือเกี่ยวข้องสำหรับการเข้าทำสัญญาซึ่งรวมถึงการให้บริการนั้น ๆ

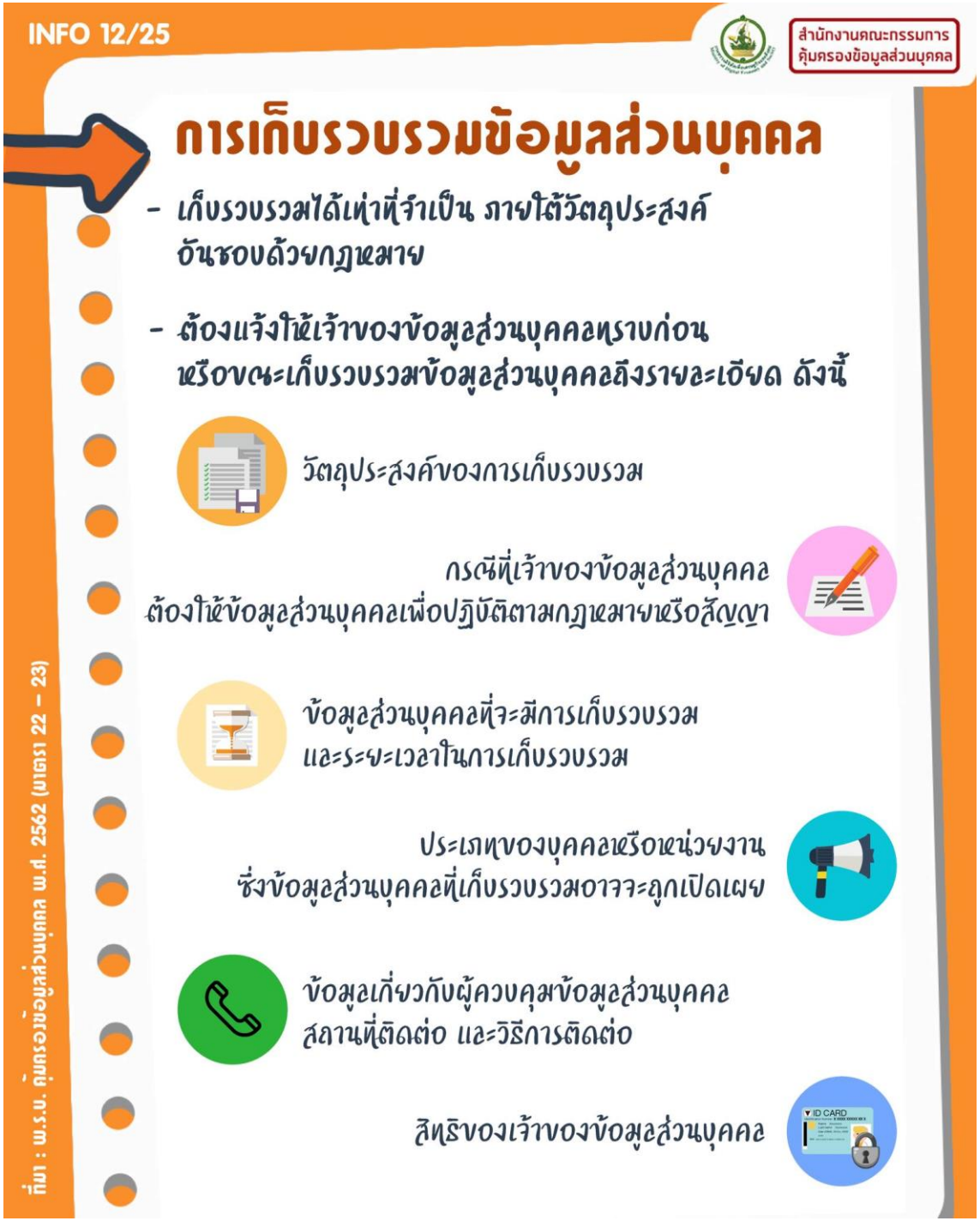
พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- **ความยินยอม (มาตรา 19)**
  - เจ้าของข้อมูลส่วนบุคคลจะถอนความยินยอมเสียเมื่อใดก็ได้โดยจะต้องถอนความยินยอมได้ง่ายเช่นเดียวกับการให้ความยินยอม เว้นแต่มีข้อจำกัดสิทธิในการถอนความยินยอมโดยกฎหมายหรือสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคล ทั้งนี้ การถอนความยินยอมย่อมไม่ส่งผลกระทบต่อการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมไปแล้วโดยชอบตามที่กำหนดไว้ในหมวดนี้
  - ในกรณีที่การถอนความยินยอมส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลในเรื่องใด ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงผลกระทบจากการถอนความยินยอมนั้น
  - การขอความยินยอมที่ไม่เป็นไปตามที่กำหนด ไม่มีผลผูกพันเจ้าของข้อมูลส่วนบุคคล และไม่ทำให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้

เรื่องที่ควรทราบ เกี่ยวกับ PDPA

8. เมื่อมีเหตุผลความจำเป็น (ฐานทางกฎหมาย) ที่จะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลแล้ว controller ต้อง

- แจ้ง Privacy Notice แก่เจ้าของข้อมูลฯ ก่อนหรือในขณะเก็บรวบรวมข้อมูล
- ใช้ตามวัตถุประสงค์เท่าที่ได้แจ้งไป (ไม่พูดอย่าง ทำอย่าง)
- ถ้าจะเอาข้อมูลที่มีอยู่ไปใช้ในวัตถุประสงค์อื่น ต้องวนลูปกลับไปวิเคราะห์ฐานทางกฎหมาย และแจ้ง Privacy Notice ใหม่



การแจ้งวัตถุประสงค์และรายละเอียดให้เจ้าของข้อมูลส่วนบุคคลทราบ (Privacy Notice)

เรื่องที่ควรทราบ เกี่ยวกับ PDPA

9. ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล controller มีหน้าที่

- ดูแล Security ให้ดี
- มีมาตรการป้องกันไม่ให้ผู้อื่นใช้หรือเปิดเผยข้อมูลโดยมิชอบ
- ลบหรือทำลายข้อมูล เมื่อหมดความจำเป็นในการเก็บ (Data Retention Policy)
- แจ้งเหตุการละเมิดข้อมูล (Breach Notification) ให้ สคส. หรือ data subject ทราบ
- จัดทำบันทึกรายการ (Record of Processing Activities: ROPA) ไว้ให้ตรวจสอบ
- พิจารณาเงื่อนไขการส่งหรือโอนข้อมูลไปต่างประเทศให้สอดคล้องกับ PDPA
- พิจารณาเงื่อนไขการเก็บรวบรวมข้อมูลจากแหล่งอื่น (นอกจาก subject) ให้ถูกต้อง
- ทำสัญญา/ข้อตกลง เป็นคำสั่งที่กำหนดเงื่อนไขการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลของ processor ที่ประมวลผลข้อมูลตามคำสั่งหรือในนามของ controller
- แต่งตั้ง DPO หากเข้าหลักเกณฑ์ (เช่น process sensitive data หรือประมวลผลข้อมูลจำนวนมาก)

Data Controller Responsibilities

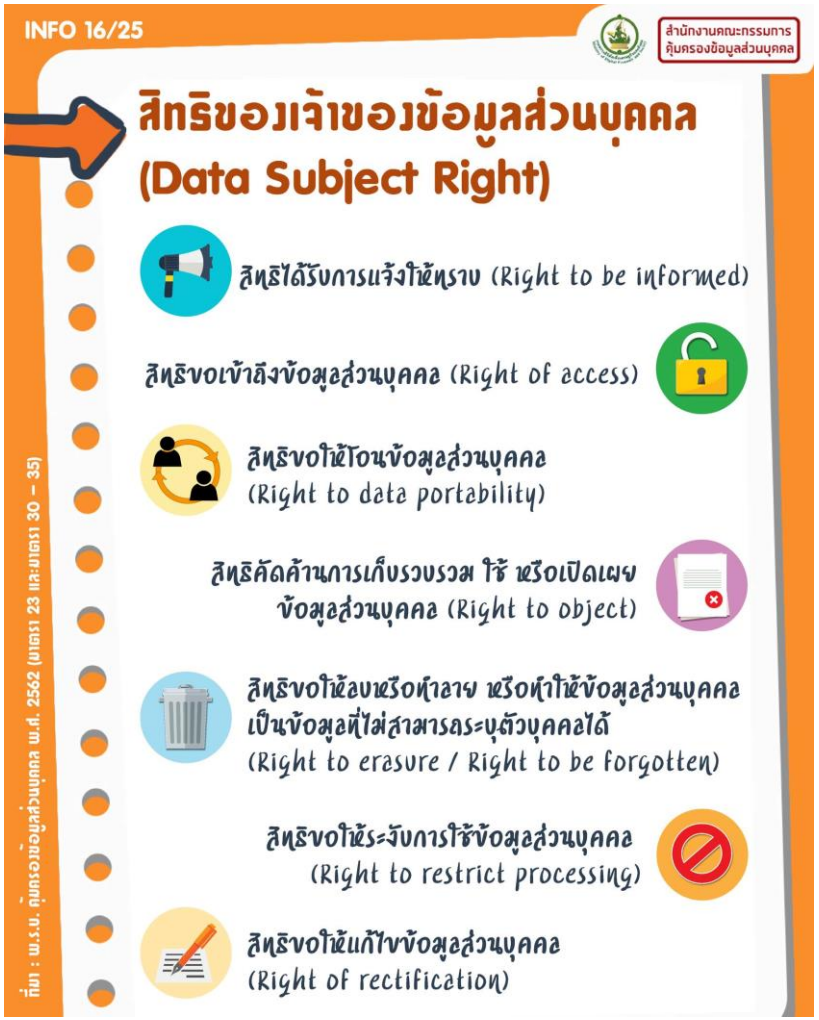
1. Security
2. Preventing Unauthorized Processing
3. Data Retention
4. Breach Notification
5. Record of Processing Activities (ROPA)
6. International Data Transfer
7. Secondary Data Collection
8. Data Processing Agreement (DPA)
9. Data Protection Officer (DPO)

เรื่องที่ควรทราบ เกี่ยวกับ PDPA

10. Controller ต้องจัดให้มีช่องทางให้เจ้าของข้อมูลฯ ขอใช้สิทธิต่าง ๆ ได้

สิทธิของเจ้าของข้อมูลส่วนบุคคล

- Right to Be Informed (Privacy Notice)
- Right of Access
- Right to Data Portability
- Right to Object
- Right to be Forgotten
- Right to Restrict Processing
- Right of Rectification

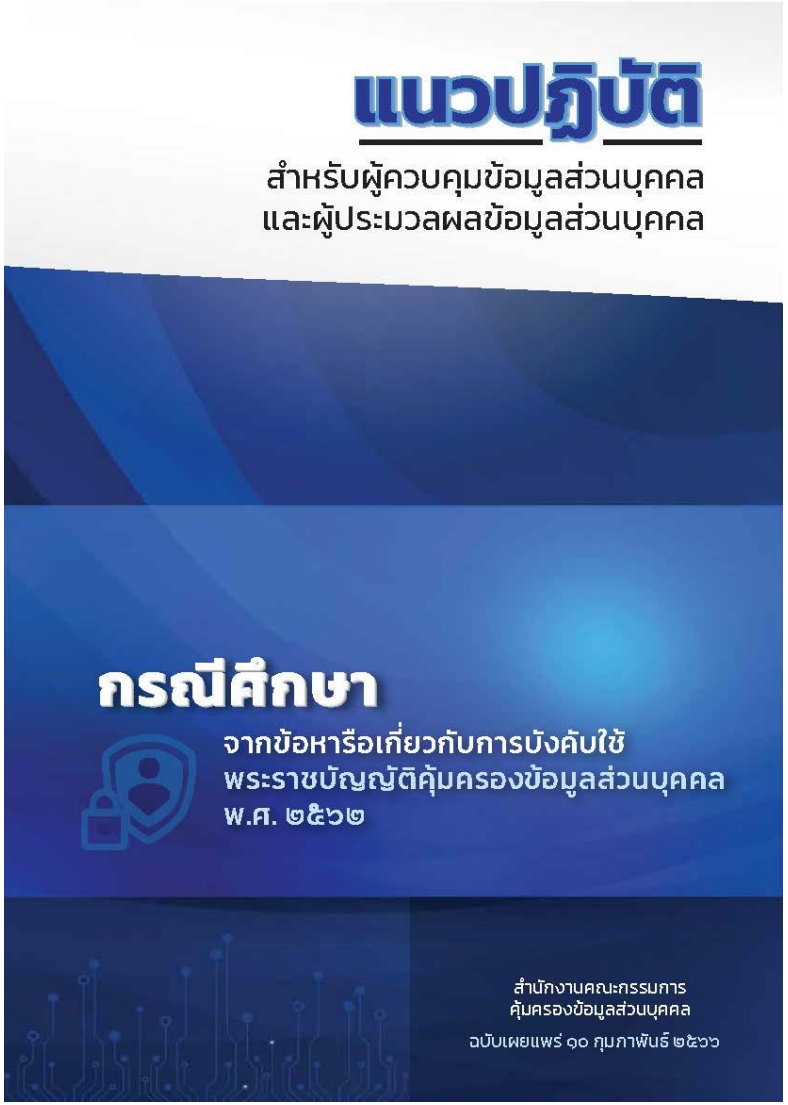


เรื่องที่ควรทราบ เกี่ยวกับ PDPA

(แถม) ข้อมูลที่เก็บรวบรวมไว้แล้วก่อนกฎหมายบังคับใช้ สามารถใช้ต่อไปได้ตามวัตถุประสงค์เดิม

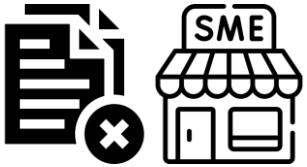
- ถ้าใช้ฐานความยินยอม ต้องมีช่องทางให้ data subject ถอนความยินยอมได้
- ข้อมูลที่เก็บรวบรวมหลังจากวันที่กฎหมายบังคับใช้แล้ว ต้องดำเนินการตาม PDPA เต็มรูป
- ถ้านำข้อมูลที่เก็บรวบรวมไว้ก่อนแล้วไปใช้ในวัตถุประสงค์อื่น (repurpose) ต้องดำเนินการตาม PDPA เต็มรูป

ตัวอย่างการปรับใช้กฎหมายในการตอบข้อหารือ



https://www.pdpc.or.th/consultation/

กฎหมายลำดับรองตาม PDPA ที่ประกาศแล้ว



- **ประกาศ กคส. เรื่อง การยกเว้นการบันทึกรายการของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็ก พ.ศ. 2565**
  - ประกาศในราชกิจจานุเบกษาเมื่อ 20 มิ.ย. 2565 มีผลใช้บังคับตั้งแต่วันถัดจากวันประกาศฯ

- **ประกาศ กคส. เรื่อง หลักเกณฑ์และวิธีการในการจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล พ.ศ. 2565**
  - ประกาศในราชกิจจานุเบกษาเมื่อ 20 มิ.ย. 2565 มีผลใช้บังคับเมื่อพ้นกำหนด 180 วันนับแต่วันประกาศฯ

- **ประกาศ กคส. เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565**
  - ประกาศในราชกิจจานุเบกษาเมื่อ 20 มิ.ย. 2565 มีผลใช้บังคับตั้งแต่วันถัดจากวันประกาศฯ

- **ประกาศ กคส. เรื่อง หลักเกณฑ์การพิจารณาออกคำสั่งลงโทษปรับทางปกครองของคณะกรรมการผู้เชี่ยวชาญ พ.ศ. 2565**
  - ประกาศในราชกิจจานุเบกษาเมื่อ 20 มิ.ย. 2565 มีผลใช้บังคับตั้งแต่วันถัดจากวันประกาศฯ

Image Source: Flaticon.com

กฎหมายลำดับรองตาม PDPA ที่ประกาศแล้ว

- **ระเบียบ กคส. ว่าด้วยการยื่น การไม่รับเรื่อง การยุติเรื่อง การพิจารณา และระยะเวลาในการพิจารณาคำร้องเรียน พ.ศ. 2565**
  - ประกาศในราชกิจจานุเบกษาเมื่อ 11 ก.ค. 2565 มีผลใช้บังคับตั้งแต่วันถัดจากวันประกาศฯ
- **ประกาศ กคส. เรื่อง คุณสมบัติและลักษณะต้องห้าม วาระการดำรงตำแหน่ง การพ้นจากตำแหน่ง และการดำเนินงานอื่นของคณะกรรมการผู้เชี่ยวชาญ พ.ศ. 2565**
  - ประกาศในราชกิจจานุเบกษาเมื่อ 11 ก.ค. 2565 มีผลใช้บังคับตั้งแต่วันถัดจากวันประกาศฯ
- **ประกาศ กคส. เรื่อง หลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2565**
  - ประกาศในราชกิจจานุเบกษาเมื่อ 12 ก.ย. 2565 มีผลใช้บังคับตั้งแต่วันถัดจากวันประกาศฯ
- **ประกาศ กคส. เรื่อง กำหนดแบบบัตรประจำตัวของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2565**
  - ประกาศในราชกิจจานุเบกษาเมื่อ 12 ก.ย. 2565 มีผลใช้บังคับตั้งแต่วันถัดจากวันประกาศฯ
- **ประกาศ กคส. เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565**
  - ประกาศในราชกิจจานุเบกษาเมื่อ 15 ธ.ค. 2565 มีผลใช้บังคับตั้งแต่วันประกาศฯ

Image Source: Flaticon.com

กฎหมายลำดับรองตาม PDPA ที่ประกาศแล้ว

- **ประกาศ กคส. เรื่อง หลักเกณฑ์และวิธีการในการจัดทำคำสั่งของคณะกรรมการผู้เชี่ยวชาญตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2566**
  - ประกาศในราชกิจจานุเบกษาเมื่อ 21 มิ.ย. 2566 มีผลใช้บังคับตั้งแต่วันถัดจากวันประกาศฯ

- **ประกาศ กคส. เรื่อง ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่เป็นหน่วยงานของรัฐ ซึ่งต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2566**
  - ประกาศในราชกิจจานุเบกษาเมื่อ 18 ก.ค. 2566 มีผลใช้บังคับเมื่อพ้นกำหนด 90 วันนับแต่วันประกาศฯ

- **พรฎ.กำหนดลักษณะ กิจการ หรือหน่วยงานที่ได้รับการยกเว้นไม่ให้นำพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บางส่วนมาใช้บังคับ พ.ศ. 2566**
  - ประกาศในราชกิจจานุเบกษาเมื่อ 17 ส.ค. 2566 มีผลใช้บังคับเมื่อพ้นกำหนด 150 วันนับแต่วันประกาศฯ

- **ประกาศ กคส. เรื่อง การจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา 41 (2) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2566**
  - ประกาศในราชกิจจานุเบกษาเมื่อ 14 ก.ย. 2566 มีผลใช้บังคับเมื่อพ้นกำหนด 90 วันนับแต่วันประกาศฯ

Image Source: Flaticon.com

กฎหมายลำดับรองตาม PDPA ที่ประกาศแล้ว

- **ประกาศ กคส. เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งได้รับการยกเว้นไม่ให้นำพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาใช้บังคับ พ.ศ. 2566**
  - ประกาศในราชกิจจานุเบกษาเมื่อ 8 ธ.ค. 2566 มีผลใช้บังคับเมื่อพ้นกำหนด 90 วันนับแต่วันประกาศฯ

- **ประกาศ กคส. เรื่อง มาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล สำหรับการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ พ.ศ. 2566**
  - ประกาศในราชกิจจานุเบกษาเมื่อ 8 ธ.ค. 2566 มีผลใช้บังคับเมื่อพ้นกำหนด 90 วันนับแต่วันประกาศฯ

Section 28

- **ประกาศ กคส. เรื่อง หลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศตามมาตรา 28 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2566**
  - ประกาศในราชกิจจานุเบกษาเมื่อ 25 ธ.ค. 2566 มีผลใช้บังคับเมื่อพ้นกำหนด 90 วันนับแต่วันประกาศฯ

Image Source: Flaticon.com

กฎหมายลำดับรองตาม PDPA ที่ประกาศแล้ว

Section 29

- **ประกาศ กคส. เรื่อง หลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศตามมาตรา 29 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2566**
  - ประกาศในราชกิจจานุเบกษาเมื่อ 25 ธ.ค. 2566 มีผลใช้บังคับเมื่อพ้นกำหนด 90 วันนับแต่วันประกาศฯ

- **ประกาศ กคส. เรื่อง มาตรการที่เหมาะสมสำหรับการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการศึกษาวิจัยหรือสถิติตามมาตรา 24 (1) และการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่นตามมาตรา 26 (5) (ง) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2566**
  - ประกาศในราชกิจจานุเบกษาเมื่อ 8 ม.ค. 2567 มีผลใช้บังคับเมื่อพ้นกำหนด 90 วันนับแต่วันประกาศฯ

- **ประกาศ กคส. เรื่อง หลักเกณฑ์เกี่ยวกับมาตรการคุ้มครองสำหรับการเก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรมที่มิได้กระทำภายใต้การควบคุมของหน่วยงานที่มีอำนาจหน้าที่ตามกฎหมาย พ.ศ. 2566**
  - ประกาศในราชกิจจานุเบกษาเมื่อ 8 ม.ค. 2567 มีผลใช้บังคับเมื่อพ้นกำหนด 90 วันนับแต่วันประกาศฯ

Image Source: Flaticon.com

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

โดยที่เป็นการสมควรกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ โดยให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลในระยะแรกที่กฎหมายมีผลใช้บังคับมีความเหมาะสม

อาศัยอำนาจตามความในมาตรา ๑๖ (๔) และมาตรา ๓๗ (๑) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า "ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕"

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ในประกาศนี้

"ความมั่นคงปลอดภัย" หมายความว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

ข้อ ๔ ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ โดยมาตรการรักษาความมั่นคงปลอดภัยดังกล่าว อย่างน้อยต้องมีการดำเนินการ ดังต่อไปนี้

(๑) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องครอบคลุมการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ไม่ว่าข้อมูลส่วนบุคคลดังกล่าวจะอยู่ในรูปแบบเอกสารหรือในรูปแบบอิเล็กทรอนิกส์ หรือรูปแบบอื่นใดก็ตาม

(๒) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องประกอบด้วยมาตรการเชิงองค์กร (organizational measures) และมาตรการเชิงเทคนิค (technical measures) ที่เหมาะสม ซึ่งอาจรวมถึงมาตรการทางกายภาพ (physical measures) ที่จำเป็นด้วย โดยคำนึงถึงระดับความเสี่ยงตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตลอดจนโอกาสเกิดและผลกระทบจากเหตุการละเมิดข้อมูลส่วนบุคคล

(๓) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องคำนึงถึงการดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัย ตั้งแต่การระบุความเสี่ยงที่สำคัญที่อาจจะเกิดขึ้นกับทรัพย์สินสารสนเทศ

(information assets) ที่สำคัญ การป้องกันความเสี่ยงที่สำคัญที่อาจจะเกิดขึ้น การตรวจสอบและเฝ้าระวังภัยคุกคามและเหตุการละเมิดข้อมูลส่วนบุคคล การเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามและเหตุการละเมิดข้อมูลส่วนบุคคล และการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามหรือเหตุการละเมิดข้อมูลส่วนบุคคลด้วย ทั้งนี้ เท่าที่จำเป็นเหมาะสม และเป็นไปได้ตามระดับความเสี่ยง

(๔) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องคำนึงถึงความสามารถในการธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคลไว้ได้อย่างเหมาะสมตามระดับความเสี่ยง โดยคำนึงถึงปัจจัยทางเทคโนโลยี บริบทสภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน ลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

(๕) สำหรับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์ มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องครอบคลุมส่วนประกอบต่าง ๆ ของระบบสารสนเทศที่เกี่ยวข้องกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล เช่น ระบบและอุปกรณ์จัดเก็บข้อมูลส่วนบุคคล เครื่องคอมพิวเตอร์แม่ข่าย (servers) เครื่องคอมพิวเตอร์ลูกข่าย (clients) และอุปกรณ์ต่าง ๆ ที่ใช้ ระบบเครือข่าย ซอฟต์แวร์และแอปพลิเคชัน อย่างเหมาะสมตามระดับความเสี่ยง โดยคำนึงถึงหลักการป้องกันเชิงลึก (defense in depth) ที่ควรประกอบด้วยมาตรการป้องกันหลายชั้น (multiple layers of security controls) เพื่อลดความเสี่ยงในกรณีที่มาตรการบางมาตรการมีข้อจำกัดในการป้องกันความมั่นคงปลอดภัยในบางสถานการณ์

(๖) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว ในส่วนที่เกี่ยวกับการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคล อย่างน้อยต้องประกอบด้วยการดำเนินการดังต่อไปนี้อย่างเหมาะสมตามระดับความเสี่ยง โดยคำนึงถึงความจำเป็นในการเข้าถึงและใช้งานตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล การรักษาความมั่นคงปลอดภัยตามระดับความเสี่ยง ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

(ก) การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศที่สำคัญ (access control) ที่มีการพิสูจน์และยืนยันตัวตน (identity proofing and authentication) และการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงและใช้งาน (authorization) ที่เหมาะสม โดยคำนึงถึงหลักการให้สิทธิเท่าที่จำเป็น (need-to-know basis) ตามหลักการให้สิทธิที่น้อยที่สุดเท่าที่จำเป็น (principle of least privilege)

(ข) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) ที่เหมาะสม ซึ่งอาจรวมถึงการลงทะเบียนและการถอนสิทธิผู้ใช้งาน (user registration and de-registration) การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (user access provisioning) การบริหารจัดการสิทธิการเข้าถึง

ตามสิทธิ (management of privileged access rights) การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (management of secret authentication information of users) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access rights) และการถอดถอนหรือปรับปรุงสิทธิการเข้าถึง (removal or adjustment of access rights)

(ค) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ซึ่งรวมถึงกรณีที่เป็นการกระทำนอกเหนือบทบาทหน้าที่ที่ได้รับมอบหมาย ตลอดจนการลักลอบทำสำเนาข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และการลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล

(ง) การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง แก้ไข หรือลบข้อมูลส่วนบุคคล (audit trails) ที่เหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

(๗) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องรวมถึงการสร้างเสริมความตระหนักรู้ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัย (privacy and security awareness) และการแจ้งนโยบาย แนวปฏิบัติ และมาตรการด้านการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคลอย่างเหมาะสม ให้บุคลากร พนักงาน ลูกจ้าง หรือบุคคลอื่นที่เป็นผู้ใช้งาน (user) หรือเกี่ยวข้องกับการเข้าถึง เก็บรวบรวม ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคล ทราบและถือปฏิบัติ รวมทั้งกรณีที่มีการปรับปรุงแก้ไขนโยบาย แนวปฏิบัติ และมาตรการดังกล่าวด้วย โดยคำนึงถึงลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ระดับความเสี่ยง ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

ข้อ ๕ ผู้ควบคุมข้อมูลส่วนบุคคลต้องทบทวนมาตรการรักษาความมั่นคงปลอดภัยตามข้อ ๔ เมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม โดยคำนึงถึงระดับความเสี่ยงตามปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน ลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

เมื่อมีเหตุการละเมิดข้อมูลส่วนบุคคล ให้ถือว่าผู้ควบคุมข้อมูลส่วนบุคคลมีความจำเป็นต้องทบทวนมาตรการรักษาความมั่นคงปลอดภัยตามวรรคหนึ่ง เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

ข้อ ๖ ในการจัดให้มีข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล ให้ผู้ควบคุมข้อมูลส่วนบุคคลพิจารณากำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลจัดให้มี

มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น โดยมาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องเป็นไปตามมาตรฐานขั้นต่ำตามข้อ ๔ โดยคำนึงถึงระดับความเสี่ยงตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตลอดจนโอกาสเกิดและผลกระทบจากเหตุการละเมิดข้อมูลส่วนบุคคล

ข้อ ๗ ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ตามกฎหมายอื่นในการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามกฎหมายนั้น แต่มาตรการรักษาความมั่นคงปลอดภัยดังกล่าวของผู้ควบคุมข้อมูลส่วนบุคคลจะต้องเป็นไปตามมาตรฐานขั้นต่ำที่กำหนดในประกาศนี้ด้วย

ข้อ ๘ ให้ประธานกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นผู้รักษาการตามประกาศนี้

ประกาศ ณ วันที่ ๑๐ มิถุนายน พ.ศ. ๒๕๖๕
เธียรชัย ณ นคร
ประธานกรรมการคุ้มครองข้อมูลส่วนบุคคล