การคุ้มครองข้อมูลส่วนบุคคล

สำหรับผู้ใช้งานระบบทะเบียนการศึกษา

ดร. พฤษภ์ บุญมา
รองผู้อำนวยการสำนักทะเบียนและประมวลผล
และอาจารย์ประจำภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเชียงใหม่

การคุ้มครองข้อมูลส่วนบุคคล

- การคุ้มครองข้อมูลส่วนบุคคล
- พรบ. คุ้มครองข้อมูลส่วนบุคคล พศ. 2562
- กรณีตัวอย่าง การละเมิดข้อมูลส่วนบุคคล

การคุ้มครองข้อมูลส่วนบุคคล

- การคุ้มครองข้อมูลส่วนบุคคล
- พรบ. คุ้มครองข้อมูลส่วนบุคคล พศ. 2562
- กรณีตัวอย่าง การละเมิดข้อมูลส่วนบุคคล

การคุ้มครองข้อมูลส่วนบุคคล

- ข้อมูลส่วนบุคคลคือข้อมูลที่สามารถระบุตัวบุคคลได้ ไม่ว่าทางตรงหรือทางอ้อม
  - ทำให้บุคคลอาจจะได้รับการปฏิบัติที่ไม่เท่าเทียม หรือไม่เป็นธรรม
- หน่วยงานที่รวบรวมข้อมูลมีภาระตามกฎหมายที่จะต้องปกป้องข้อมูลส่วนบุคคล
  - ไม่เก็บได้ ดีที่สุด

https://pxhere.com/en/photo/1449185

https://news.siamphone.com/news-43468.html

ทำไมเราต้องคุ้มครองข้อมูลส่วนบุคคล

- Accountability
  - เพราะเป็นความรับผิดชอบของเรา
- Public Trust
  - เพราะสาธารณชนจะได้เชื่อใจเรา
- Security Processing
  - เพราะเราจะได้มั่นใจได้ว่าเราทำงานอย่างปลอดภัย

วัตถุประสงค์ของการคุ้มครองข้อมูลส่วนบุคคล

- เพื่อปกป้องสิทธิส่วนบุคคลพื้นฐาน
- เพื่อให้เกิดประมวลผลและการไหลของข้อมูลที่ถูกต้อง

- การคุ้มครองข้อมูลส่วนบุคคลช่วยให้องค์กรสามารถแบ่งปันข้อมูลส่วนบุคคลได้อย่างปลอดภัย เป็นธรรม และ ได้สัดส่วน

สิทธิ์ของเจ้าของข้อมูลส่วนบุคคล

- เจ้าของข้อมูลมีสิทธิ์ในข้อมูลของตนเอง ถึงแม้ว่าตนเองไม่ได้เป็นผู้มอบข้อมูลให้
- ครอบคลุมถึงการรวบรวม เก็บ ใช้ และเปิดเผยข้อมูล
- เก็บเท่าที่จำเป็น ต้องทราบวัตถุประสงค์ ถ้ามีการเปลี่ยนวัตถุประสงค์ ต้องแจ้งใหม่

https://pdpa.pro/blogs/rights-of-data-subject-pdpa

การประมวลผลข้อมูลส่วนบุคคล

รวบรวม (Collect)

- ฐานทางกฎหมาย
- ความยินยอม
- วัตถุประสงค์จำกัด
- ใช้ข้อมูลน้อยที่สุด

จัดเก็บ (Storage)

- รูปแบบการจัดเก็บ
- Physical/Electronic
- ใครเข้าถึงได้บ้าง

ใช้ (Access)

- ใช้ภายใน/ภายนอกองค์กร
- ใครเข้าถึงได้บ้าง
- ตรงกับวัตถุประสงค์ไหม

เปิดเผย (Disclose)

- ใครเข้าถึงได้บ้าง
- การทำให้ไม่เป็นข้อมูลส่วนบุคคล

ส่งต่อ (Transfer)

- โอนไปต่างประเทศ
- โอนไปองค์กรอื่น
- วิธีการโอนปลอดภัยหรือไม่

สำรอง (Archive)

- สำรองกี่ชุด
- อายุของการสำรอง

ทำลาย (Dispose)

- ลบจริงไหม?
- ลบหมดไหม?

REG Registration Office Chiang Mai University

การประมวลผลข้อมูลส่วนบุคคล

การเข้าถึงข้อมูลโดยผู้ใช้งานระบบทะเบียนฯ

รวบรวม (Collect)

- ฐานทางกฎหมาย
- ความยินยอม
- วัตถุประสงค์จำกัด
- ใช้ข้อมูลน้อยที่สุด

จัดเก็บ (Storage)

- รูปแบบการจัดเก็บ
- Physical/Electronic
- ใครเข้าถึงได้บ้าง

ใช้ (Access)

- ใช้ภายใน/ภายนอกองค์กร
- ใครเข้าถึงได้บ้าง
- ตรงกับวัตถุประสงค์ไหม

เปิดเผย (Disclose)

- ใครเข้าถึงได้บ้าง
- การทำให้ไม่เป็นข้อมูลส่วนบุคคล

ส่งต่อ (Transfer)

- โอนไปต่างประเทศ
- โอนไปองค์กรอื่น
- วิธีการโอนปลอดภัยหรือไม่

สำรอง (Archive)

- สำรองกี่ชุด
- อายุของการสำรอง

ทำลาย (Dispose)

- ลบจริงไหม?
- ลบหมดไหม?

การจัดการข้อมูลส่วนบุคคลของนักศึกษา เป็นสิ่งที่บุคลากรทุกคนของมหาวิทยาลัย ต้องร่วมกันรับผิดชอบ

หลักการปกป้องข้อมูลส่วนบุคคล

- ปฏิบัติตามกรอบกฎหมาย เป็นธรรม และโปร่งใส
- มีวัตถุประสงค์ที่จำกัด
- ใช้ข้อมูลให้น้อยที่สุด
- คงความถูกต้องของข้อมูล
- จำกัดระยะเวลาการจัดเก็บข้อมูลเท่าที่จำเป็น
- รักษาความปลอดภัยของข้อมูล
- กำหนดความรับผิดชอบ

ปฏิบัติตามกรอบกฎหมาย เป็นธรรม และโปร่งใส

- การประมวลผลข้อมูลต้องมีฐานทางกฎหมาย
  - เรามีความชอบธรรมทางกฎหมายอย่างไร จึงสามารถรวบรวม ใช้ เก็บ เปิดเผย และ ทำลายข้อมูลเหล่านี้
- ในการใช้ฐานทางกฎหมาย ต้องใช้อย่างเป็นธรรม
  - เราใช้ความได้เปรียบทางกฎหมาย (เช่น การเป็นคณะ ภาควิชา) เอาเปรียบผู้อื่นอยู่หรือไม่
- การประมวลผลต้องทำอย่างโปร่งใส
  - ถ้ามีคนถามเราว่า เราประมวลผลข้อมูลอย่างไร เราตอบได้หรือไม่
- **ข้อมูลที่ได้รับจากสทป. ถ้าจะเปิดเผย หรือ ส่งต่อ ท่านมีฐานทางกฎหมายรองรับหรือไม่ ?**

มีวัตถุประสงค์ที่จำกัด

- การรวบรวม ใช้ เก็บ เปิดเผย หรือ ทำลายข้อมูลส่วนบุคคล ต้องทำตามวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลไว้ก่อน หรือ ขณะที่รวบรวม
  - ไม่ว่ารวบรวมโดยตรง หรือ รวบรวมจากช่องทางอื่น
- ในกรณีที่จะดำเนินการนอกเหนือจากวัตถุประสงค์ที่ได้แจ้งไว้ จะต้อง
  - แจ้งวัตถุประสงค์ใหม่ให้แก่เจ้าของข้อมูล และได้รับความยินยอม
  - มีฐานการประมวลผลตามกฎหมายอื่น ๆ
- **สทป. ได้แจ้งวัตถุประสงค์การประมวลผลข้อมูลกับนักศึกษาใหม่ทุกคน ว่าเป็นการทำเพื่อประมวลผลทางการศึกษา ถ้าส่วนงาน ต้องการเอาไปทำอย่างอื่น (เช่น การทำวิจัย ทุน) จะต้องทำการแจ้งวัตถุประสงค์ใหม่เสมอ**

ใช้ข้อมูลให้น้อยที่สุด

- การรวบรวมข้อมูล ให้รวบรวมเท่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมาย อย่าคิดว่า เก็บมาไว้ก่อน เผื่อได้ใช้ทีหลัง
- ให้มีการตรวจสอบเพื่อดำเนินการลบ หรือ ทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บ
- น้อย หมายถึงเช่น
  - field นี้ไม่ต้องเก็บได้ไหม? จำเป็นต้องเก็บทุกคนไหม? ต้องเก็บไว้ตลอดกาลไหม?
- **เมื่อท่านได้รับข้อมูลจากสทป. ท่านต้องรับผิดชอบในข้อมูลนั้นด้วย ถ้าท่านไม่ได้ใช้งาน ก็ไม่ควรจะดึงข้อมูลไป ซึ่งจะเป็นการเพิ่มภาระความรับผิดชอบที่ไม่จำเป็น**

คงความถูกต้องของข้อมูล

- ทำให้ข้อมูลส่วนบุคคลที่รวบรวม ใช้ เก็บ หรือ เปิดเผย ต้องทำให้ถูกต้อง เป็นปัจจุบัน สมบูรณ์ และ ชัดเจน
- ความถูกต้อง เช่น
  - ถูกต้อง (Correctness) = ชื่อเขาถูกไหม
  - เป็นปัจจุบัน (Updated) = เขาเปลี่ยนชื่อแล้ว ข้อมูลเปลี่ยนตามยัง?
  - สมบูรณ์ (Completeness) = เขาแจ้งข้อมูลมาสามตัว เราเก็บกี่ตัว?
  - ชัดเจน (Explicit) = ข้อมูลที่แสดง คนสองคนอ่านแล้วเข้าใจตรงกันไหม?
- **ข้อมูลของสทป. มีการเปลี่ยนแปลงอยู่ตลอดเวลา ข้อมูลที่ท่านใช้ เป็นข้อมูลที่ปรับปรุงล่าสุดแล้วหรือไม่?**

จำกัดระยะเวลาการจัดเก็บข้อมูลเท่าที่จำเป็น

- ถูกเก็บรักษาในรูปแบบที่สามารถระบุตัวตนของเจ้าของข้อมูลส่วนบุคคลไม่นานกว่าที่จำเป็นสำหรับวัตถุประสงค์ที่ข้อมูลส่วนบุคคล
  - ต้องมีการบันทึกเป็นลายลักษณ์อักษรว่า ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล อย่างชัดเจน
- ถ้าจะเก็บไว้นานกว่านั้นต้อง
  - ทำให้อยู่ในรูปที่ไม่สามารถระบุตัวตนได้ (Anonymized)
  - มีฐานทางกฎหมายมารองรับ
- **ข้อมูลที่ได้รับจากสทป. ถ้าหมดวัตถุประสงค์ในการใช้งาน ก็ควรทำลายเสีย เพื่อจะได้ไม่เป็นภาระ อย่างไรสทป. ก็เก็บข้อมูลต้นฉบับไว้ให้ท่านอยู่แล้ว**

ความปลอดภัยของข้อมูล

- ความปลอดภัยของข้อมูลไม่ใช่เรื่องของฝ่าย IT หรือ สทป. เท่านั้น
- มีมาตรการรักษาความมั่นคงปลอดภัย เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ
  - Clear desk and clear screen policy
  - การสำรองข้อมูลเป็นเรื่องของทุกคน ไม่ใช่เฉพาะฝ่าย IT
  - การแชร์ข้อมูล ต้องแชร์อย่างระมัดระวัง อย่าแชร์ไฟล์แบบ Public เด็ดขาด!!!!!!
- **ท่านและสทป. มีความรับผิดชอบร่วมกัน ที่จะต้องดูแลข้อมูลส่วนบุคคลของนักศึกษาให้มีความปลอดภัย**

กำหนดความรับผิดชอบ

- ต้องมีการกำหนดความรับผิดชอบในขั้นตอนต่าง ๆ อย่างชัดเจน
- แปลว่า
  - ต้องรู้ว่าใครมีหน้าที่รับผิดชอบ
  - ต้องรู้ว่าเรามีหน้าที่รับผิดชอบอะไร ทำอะไรได้บ้าง ทำอะไรไม่ได้บ้าง
  - ต้องรู้ว่าสิ่งที่ทำ ทำเกินกว่าหน้าที่รับผิดชอบหรือไม่
  - ต้องรู้ว่าสิ่งที่ทำ ทำตรงกับหน้าที่รับผิดชอบหรือไม่
- **ท่านทราบหรือไม่ว่า ในหน่วยงานท่าน มีใครเข้าถึงข้อมูลในระบบ สทป. ได้บ้าง?**

การคุ้มครองข้อมูลส่วนบุคคล

- การคุ้มครองข้อมูลส่วนบุคคล
- พรบ. คุ้มครองข้อมูลส่วนบุคคล พศ. 2562
- กรณีตัวอย่าง การละเมิดข้อมูลส่วนบุคคล

กฎหมายกับการคุ้มครองข้อมูลส่วนบุคคล

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พศ. 2562 (PDPA)
  - ระงับใช้บางมาตราจนถึงกลางปี 2565
- กำหนดบทบาทของผู้ที่เกี่ยวข้องกับข้อมูลอย่างชัดเจน

ผู้ควบคุมข้อมูลส่วนบุคคล (DATA CONTROLLER)

- บุคคลธรรมดา นิติบุคคล หน่วยงานของรัฐ หรือ องค์กรใด ที่กำหนด วัตถุประสงค์ (Purpose) และ วิธีการประมวลผล (Mean) ข้อมูลส่วนบุคคล
  - มีอำนาจตัดสินใจว่า จะรวบรวมข้อมูลอะไร เพื่อวัตถุประสงค์ใด ประมวลผลด้วยวิธีการใด
- ในบริบทของมหาวิทยาลัยเชียงใหม่ ผู้ควบข้อมูลส่วนบุคคล คือ มหาวิทยาลัย ซึ่งกำหนดวัตถุประสงค์และวิธีการประมวลผลในประกาศข้อบังคับ และ แนวปฏิบัติต่าง ๆ
  - แล้วพนักงานละ?

ผู้ประมวลข้อมูลส่วนบุคคล (DATA PROCESSOR)

- บุคคล หรือ นิติบุคคลซึ่งดำเนินการเกี่ยวกับข้อมูลส่วนบุคคล ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล
  - ต้องไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล
  - ปฏิบัติหน้าที่ตามสัญญาจ้างที่มีวัตถุประสงค์เพื่อการประมวลผลตามที่ได้รับการว่าจ้าง
- โดยทั่วไป จะหมายถึง Outsource นอกหน่วยงาน

พนักงานเป็นผู้ควบคุมฯ หรือ ผู้ประมวลผลฯ ?

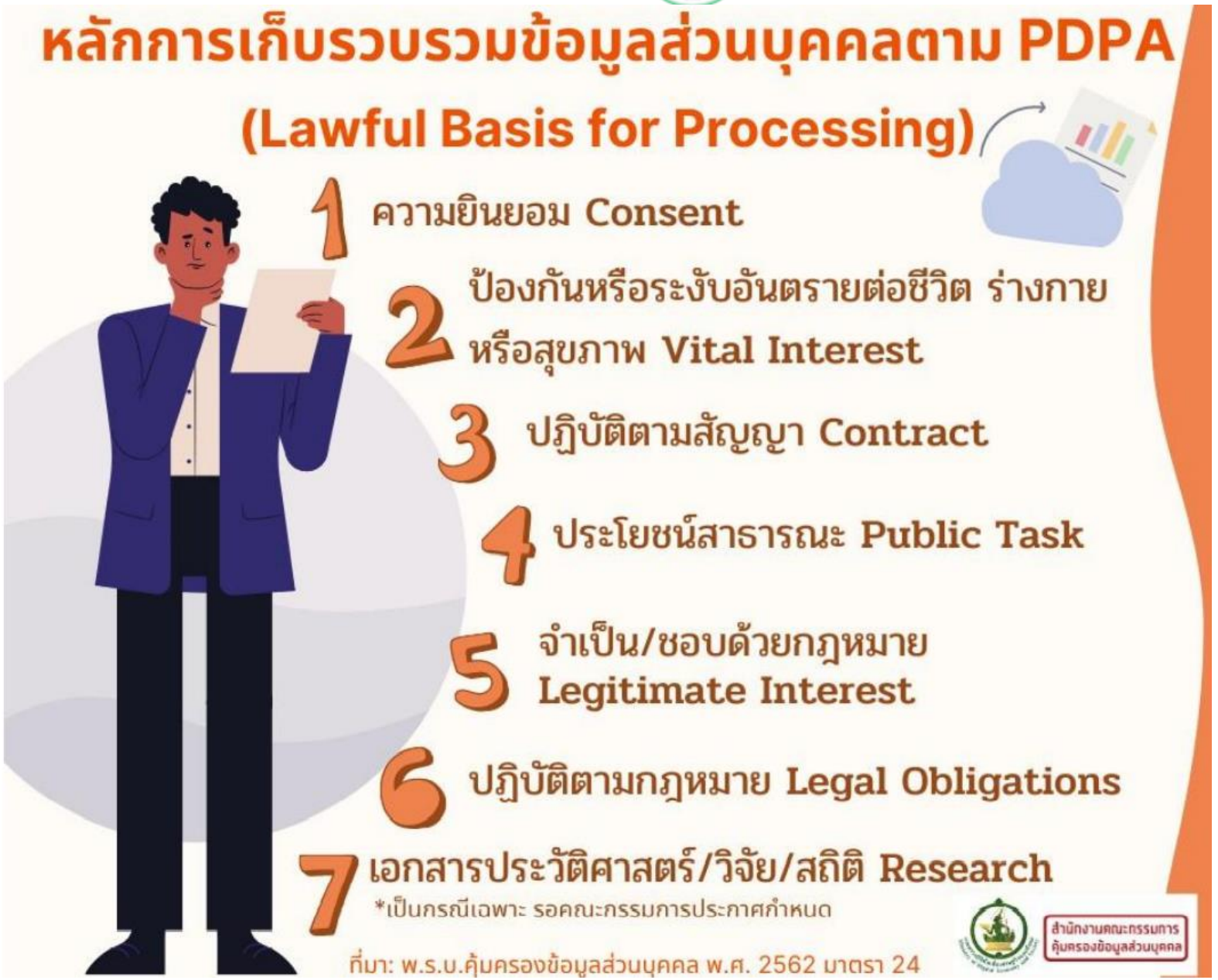
- มหาวิทยาลัย ซึ่งเป็นนิติบุคคล เป็นผู้ควบคุมข้อมูลส่วนบุคคล ไม่ใช่ผู้บริหาร พนักงาน หรือหน่วยงานใดหน่วยงานหนึ่ง
- สถานะ หน้าที่ และ ความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคลเป็นไปตามที่กฎหมายกำหนด ไม่สามารถปฏิเสธหรือมอบหมายได้
- พนักงานมหาวิทยาลัย ถือว่าเป็นส่วนหนึ่งของมหาวิทยาลัย จึงเป็นผู้ควบคุมข้อมูลส่วนบุคคลไปด้วย (UK Information Commissioner)
  - การจำแนกระหว่างผู้ควบคุมฯ กับ ผู้ประมวลผลฯ ไม่ได้จำแนกแค่หน้าที่ (Function) แต่รวมถึงความรับผิดชอบ (Responsibility)

หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล

- หน้าที่ในการแจ้งข้อมูลเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล
- หน้าที่ตอบสนองต่อคำขอใช้สิทธิ์ของเจ้าของข้อมูลส่วนบุคคล
- หน้าที่จัดให้มีมาตรการด้านความมั่นคงปลอดภัยที่เหมาะสม
- หน้าที่แจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
- หน้าที่จัดทำบันทึกรายการกิจกรรมการประมวลผล (ROPA)

ฐานในการเก็บรวมรวมข้อมูลตาม PDPA

- ฐานความยินยอมควรเป็นฐานสุดท้ายที่เลือกใช้ เพราะมีขั้นตอนการปฏิบัติที่ซับซ้อนกว่าฐานอื่น



การละเมิดข้อมูลส่วนบุคคล (DATA BREACH)

- การละเมิดข้อมูลส่วนบุคคล หมายถึงกรณีดังต่อไปนี้
  - การเสียซึ่งความลับ (Confidentiality)
  - การเสียซึ่งความสมบูรณ์ (Integrity)
  - การเสียซึ่งการเข้าถึง (Availability)
- ไม่ว่าในกรณีใด ก็ถือว่าเป็น Data Breach ทั้งหมด ไม่ใช่เฉพาะกรณีข้อมูลรั่วเท่านั้น

กฎหมายกับการคุ้มครองข้อมูลส่วนบุคคล

- เก็บเท่าที่จำเป็นต้องใช้ ถ้าไม่ใช้ ให้ทำลายทันที
- พยายามหาฐานการประมวลผลอื่นที่ไม่ใช่ฐานความยินยอม
  - ถ้าไม่มี ให้ถามตัวเองอีกรอบว่า จำเป็นต้องเก็บข้อมูลชุดนั้นไหม
- มีการกำหนดขั้นตอน บุคคล วิธีการ ต่าง ๆ ให้ชัดเจน
  - การกำกับดูแลข้อมูลที่ดี จะช่วยให้สามารถดำเนินการตาม PDPA ได้ง่าย
- เมื่อเกิด Data Breach จะต้องแจ้งผู้ที่เกี่ยวข้อง และ เจ้าของข้อมูลทันที

การคุ้มครองข้อมูลส่วนบุคคล

- การคุ้มครองข้อมูลส่วนบุคคล
- พรบ. คุ้มครองข้อมูลส่วนบุคคล พศ. 2562
- กรณีตัวอย่าง การละเมิดข้อมูลส่วนบุคคล

แนวปฏิบัติหลังเกิดการละเมิดข้อมูลส่วนบุคคล

- องค์กรสำรวจความเสียหาย และ ผลกระทบต่อเจ้าของข้อมูล (ทุกสถานการณ์)
- องค์กรทำการกู้ข้อมูล และ คืนการให้บริการ (ทุกสถานการณ์)
- องค์กรทำการบันทึกเหตุการณ์ (Incident Report) และแนวทางการแก้ไขในอนาคต (ทุกสถานการณ์)
- องค์กรแจ้งหน่วยงานกำกับดูแลถึงเหตุการณ์ และวิธีแก้ไข (เหตุการณ์มีความรุนแรงน้อย)
- องค์กรแจ้งเจ้าของข้อมูล (เหตุการณ์มีความรุนแรงมาก)

RANSOMWARE 1

- สทป. ถูกโจมตีโดย Ransomware ข้อมูลบางส่วนของ สทป. ซึ่งมีการ Backup และ เข้ารหัส ถูกล๊อคโดย Ransomware จากการตรวจสอบพบว่า ไม่มีการส่งข้อมูลดังกล่าวออกไปนอก สทป.
  - ข้อมูลมีการ Backup และสามารถกู้ได้อย่างรวดเร็ว จึงไม่มีการสูญเสียการเข้าถึงข้อมูล (Availability)
  - ข้อมูลมีการเข้ารหัส จึงสามารถป้องกันการเข้าถึงข้อมูลได้ (Confidentiality/Integrity)
- สทป. จัดทำเอกสารภายในเพื่อป้องกันเหตุการณ์เดียวกันในอนาคต ไม่ต้องแจ้งเจ้าของข้อมูล หรือ หน่วยงานกำกับ

RANSOMWARE 2

- สทป. ถูกโจมตีโดย Ransomware ข้อมูลบางส่วนของ สทป. ซึ่งไม่มีการ Backup ถูกล๊อคโดย Ransomware จากการตรวจสอบพบว่า ไม่มีการส่งข้อมูลดังกล่าวออกไปนอก สทป.
  - สทป. ใช้เวลา 4-5 วันในการกู้ข้อมูลกลับ จาก Paper Backup (คีย์มือเข้าไปใหม่) ได้บางส่วน (Integrity) และไม่สามารถให้บริการได้ในช่วงเวลาดังกล่าว (Availability)
  - ข้อมูลไม่มีการไหลออกนอกสทป. (Confidentiality)
- สทป. จัดทำเอกสารภายในเพื่อป้องกันเหตุการณ์เดียวกันในอนาคต แจ้งหน่วยงานกำกับ แต่ ไม่ต้องแจ้งเจ้าของข้อมูล

RANSOMWARE 3

- สทป. ถูกโจมตีโดย Ransomware ข้อมูลบางส่วนของ สทป. ซึ่งมีการ Backup ถูกล๊อคโดย Ransomware จากการตรวจสอบพบว่ามีการส่งข้อมูลดังกล่าวออกไปนอก สทป. รวมถึงเลขประจำตัวนักศึกษา และข้อมูลการลงทะเบียน
  - ข้อมูลมีการ Backup จึงไม่มีการสูญเสียข้อมูล (Availability)
  - ข้อมูลไม่มีการเข้ารหัส จึงไม่สามารถป้องกันการเข้าถึงข้อมูลได้ และข้อมูลอาจถูกแก้ไข (Confidentiality/Integrity)
- สทป. จัดทำเอกสารภายในเพื่อป้องกันเหตุการณ์เดียวกันในอนาคต แจ้งหน่วยงานกับกับ และเจ้าของข้อมูล

EXFILTRATION ATTACK 1 (ขโมยข้อมูล)

- ระบบ Backup บน Cloud ของ สทป. ตั้งค่าผิดพลาด ทำให้บุคคลภายนอกสามารถเข้าถึงข้อมูลที่ถูกเข้ารหัสได้
  - ข้อมูลเป็นตัว Backup ดังนั้นจึงไม่กระทบต่อการให้บริการ (Availability)
  - ข้อมูลมีการเข้ารหัส จึงสามารถป้องกันการเข้าถึงข้อมูลได้ (Confidentiality/Integrity)
- สทป. จัดทำเอกสารภายในเพื่อป้องกันเหตุการณ์เดียวกันในอนาคต ไม่ต้องแจ้งเจ้าของข้อมูล หรือ หน่วยงานกำกับ

EXFILTRATION ATTACK 2 (ขโมยข้อมูล)

- ฐานข้อมูลของ สทป. ถูกแฮค ทำให้ข้อมูลการลงทะเบียนถูกขโมยออกไป และนำไปขายบนเว็บไซต์ใต้ดิน ไม่มีข้อมูลอ่อนไหวอยู่ในชุดข้อมูล และข้อมูลต้นฉบับไม่ถูกลบ และ ไม่ถูกแก้ไข
  - สทป. ไม่สูญเสียข้อมูล หรือ การเข้าถึงข้อมูล (Availability/Integrity)
  - บุคคลภายนอกสามารถเข้าถึงข้อมูลส่วนบุคคลได้ (Confidentiality)
- สทป. จัดทำเอกสารภายในเพื่อป้องกันเหตุการณ์เดียวกันในอนาคต แจ้งหน่วยงานกำกับ และเจ้าของข้อมูล

HUMAN RISK 1 (บุคลากร)

- เจ้าหน้าที่ของสทป. ได้รับมอบหมายให้ประมวลผลข้อมูลส่วนบุคคล จึงทำสำเนาข้อมูลบางส่วนจากฐานข้อมูลของ สทป. ไปไว้ในคอมพิวเตอร์ส่วนตัว ภายหลังเจ้าหน้าที่ได้ใช้ข้อมูลดังกล่าวเพื่อติดต่อเจ้าของข้อมูลเพื่อมาเรียนพิเศษกับตนเอง
  - องค์กรไม่สูญเสียข้อมูล หรือ การเข้าถึงข้อมูล (Availability)
  - ข้อมูลถูกใช้งานผิดวัตถุประสงค์ (Integrity)
  - บุคคลภายนอกเข้าถึงข้อมูลไม่ได้ (Confidentiality)
- สทป. จัดทำเอกสารภายในเพื่อป้องกันเหตุการณ์เดียวกันในอนาคต แจ้งหน่วยงานกำกับ แต่ไม่ต้องแจ้งเจ้าของข้อมูล

HUMAN RISK 2 (บุคลากร)

- สทป. ส่งข้อมูลนักศึกษาที่ต้องทำประกันให้กับบริษัทประกัน แต่ส่งข้อมูลศิษย์เก่าไปให้ด้วย เมื่อทราบว่าส่งข้อมูลผิด เจ้าหน้าที่ได้ติดต่อบริษัทประกันเพื่อลบข้อมูลส่วนเกินออก
  - องค์กรไม่สูญเสียข้อมูล หรือ การเข้าถึงข้อมูล (Availability)
  - ข้อมูลถูกใช้งานผิดวัตถุประสงค์ (Integrity)
  - บุคคลภายนอกเข้าถึงข้อมูลไม่ได้ (Confidentiality)
- สทป. จัดทำเอกสารภายในเพื่อป้องกันเหตุการณ์เดียวกันในอนาคต แจ้งหน่วยงานกำกับ แต่ไม่ต้องแจ้งเจ้าของข้อมูล

HUMAN RISK 3 (บุคลากร)

- สทป. ส่งเอกสารแจ้งรายชื่อผู้สมัครและข้อมูลการสมัครให้กับคณะ แต่ส่งผิดอีเมล ทำให้ข้อมูลดังกล่าวถูกส่งไปยังบุคคลที่สามที่ไม่เกี่ยวข้อง ซึ่งเจ้าหน้าที่ สทป. ได้ทำการติดต่อบุคคลดังกล่าว เพื่อขอให้ลบข้อมูล
  - องค์กรไม่สูญเสียข้อมูล หรือ การเข้าถึงข้อมูล (Availability)
  - ข้อมูลถูกใช้งานผิดวัตถุประสงค์ (Integrity)
  - บุคคลภายนอกเข้าถึงข้อมูลได้ (Confidentiality)
- สทป. จัดทำเอกสารภายในเพื่อป้องกันเหตุการณ์เดียวกันในอนาคต แจ้งหน่วยงานกำกับ และเจ้าของข้อมูล

HUMAN RISK 4 (บุคลากร)

- เจ้าหน้าที่วางเอกสารรายชื่อนักศึกษาที่พ้นสภาพไว้บนโต๊ะทำงาน ซึ่งอยู่ใกล้กับหน้าต่างกระจก ทำให้บุคคลที่เดินผ่านไปผ่านมามองเห็นเอกสารที่วางบนโต๊ะได้
  - องค์กรไม่สูญเสียข้อมูล หรือ การเข้าถึงข้อมูล (Availability/Integrity)
  - บุคคลภายนอกเข้าถึงข้อมูลได้ (Confidentiality)
- สทป. จัดทำเอกสารภายในเพื่อป้องกันเหตุการณ์เดียวกันในอนาคต แจ้งหน่วยงานกำกับ และเจ้าของข้อมูล

HUMAN RISK 5 (บุคลากร)

- เจ้าหน้าที่ สทป. ทำการส่งเอกสารทางการศึกษาให้กับนักศึกษา แต่ใส่เอกสารสลับซองกัน ทำให้ผู้รับเอกสารไม่ได้รับเอกสารของตนเอง หลังจากที่ทราบว่าส่งผิด จึงได้ติดต่อผู้รับให้ทำการส่งเอกสารที่ส่งผิดกลับมา
  - องค์กรไม่สูญเสียข้อมูล หรือ การเข้าถึงข้อมูล (Availability/Integrity)
  - บุคคลภายนอกเข้าถึงข้อมูลได้ (Confidentiality)
- สทป. จัดทำเอกสารภายในเพื่อป้องกันเหตุการณ์เดียวกันในอนาคต แจ้งหน่วยงานกำกับ และเจ้าของข้อมูล

LOSS DEVICES/PAPER DOCUMENTS (หาย)

- เจ้าหน้าที่ สทป. ทำโทรศัพท์หาย ซึ่งโทรศัพท์ดังกล่าว มีโปรแกรมที่ใช้เข้าถึงอีเมลที่ใช้รับส่งเอกสารที่มีข้อมูลส่วนบุคคลอยู่ เจ้าหน้าที่คนดังกล่าวรู้ตัวหลังจากผ่านไปสองชั่วโมง จึงรีบโทรติดต่อไปยังโทรศัพท์ ผู้รับไม่ยอมคืนโทรศัพท์ เจ้าหน้าที่จึงทำการ Wipe-out ข้อมูลในโทรศัพท์
  - องค์กรไม่สูญเสียข้อมูล หรือ การเข้าถึงข้อมูล (Availability/Integrity)
  - บุคคลภายนอกเข้าถึงข้อมูลได้ (Confidentiality)
- สทป. จัดทำเอกสารภายในเพื่อป้องกันเหตุการณ์เดียวกันในอนาคต แจ้งหน่วยงานกำกับ และเจ้าของข้อมูล

LOSS DEVICES/PAPER DOCUMENTS (หาย)

- เจ้าหน้าที่ทำการสำเนาข้อมูลส่วนบุคคลในรูปแฟ้ม XLSX ใส่ใน Thumbdrive เพื่อนำไปทำงานที่บ้าน โดยมีการใส่ Password ในแฟ้มดังกล่าว ต่อมา เจ้าหน้าที่ได้ทำ Thumbdrive ดังกล่าวหายระหว่างไปรับลูกที่โรงเรียน และไม่สามารถหา Thumbdrive เจอได้
  - องค์กรไม่สูญเสียข้อมูล หรือ การเข้าถึงข้อมูล (Availability/Integrity)
  - บุคคลภายนอกเข้าถึงข้อมูลไม่ได้ (Confidentiality)
- สทป. จัดทำเอกสารภายในเพื่อป้องกันเหตุการณ์เดียวกันในอนาคต ไม่ต้องแจ้งหน่วยงานกำกับ และเจ้าของข้อมูล

สรุป

- การคุ้มครองข้อมูลส่วนบุคคลของนักศึกษา เป็นเรื่องของทุกคน ไม่ใช่เรื่องของเจ้าหน้าที่ IT หรือ สทป.
- การคุ้มครองข้อมูล ทำให้การทำงานลำบากขึ้นแน่ แต่ก็ทำให้ทำงานได้อย่างมั่นใจมากขึ้นด้วย
- อย่างไรก็ต้องทำงาน ทำอย่างไรให้ทำงานได้อย่างมั่นใจ
- ป้องกัน ดีกว่า แก้ไข