# PDPA for API Providers
## (Data Owners & Custodians)

ดำรงศักดิ์ นภารัตน์
คณะอนุกรรมการส่งเสริมการคุ้มครองข้อมูลส่วนบุคคลมหาวิทยาลัยเชียงใหม่
Email: damrongsak.naparat@cmu.ac.th, dpo@cmu.ac.th
Website: https://privacy.cmu.ac.th

# Data Governance

*“การกำหนดสิทธิ หน้าที่และความรับผิดชอบของ**ผู้มีส่วนได้ส่วนเสีย**ในการ **บริหารจัดการข้อมูลทุกขั้นตอน** เพื่อให้การได้มาและการนำไปใช้ข้อมูลของหน่วยงาน **ถูกต้อง ครบถ้วน เป็นปัจจุบัน รักษาความเป็นส่วนบุคคล** และสามารถ**เชื่อมโยงได้**อย่างมีประสิทธิภาพ และ **มั่นคงปลอดภัย**”*

# จัดทำนโยบายและแนวปฏิบัติเพื่อกำกับข้อมูล


| Data Security | Data Privacy | Data Quality |
| --- | --- | --- |
| • Confidential<br>• Integrity<br>• Availability | • การขอความยินยอม<br>• เปิดเผยตามฐานกฎหมาย 7 ฐาน<br>• เปิดเผยเท่าที่จำเป็น | • ถูกต้อง<br>• ครบถ้วน<br>• เป็นปัจจุบัน<br>• มีมาตรฐาน<br>• ตอบสอบความต้องการการใช้งาน |

# 1. แยก Personal Data and Non-Personal Data

- มี Data Catalogue
- อาจจะต้องแยก API สำหรับ Personal Data and Non-Personal Data ออกจากกัน

# จัดทำ Meta Data

1. เลขที่ชุดข้อมูล (Dataset ID)
2. ชื่อชุดข้อมูล (Dataset Name)
3. เจ้าของข้อมูล (Data Owner)
4. ผู้สนับสนุนหรือผู้ร่วมดำเนินการ (Data Custodian/Supporter)
5. คำสำคัญ (Keyword)
6. คำอธิบาย (Description)
7. ขอบเขตข้อมูล (Data Scope)
8. แหล่งอ้างอิง/ที่มาของข้อมูล (Reference/Data Source)

# ตัวอย่างชุดข้อมูล

- ข้อมูลบัตรประชาชน
  - ชื่อ-นามสกุล (ไทย + อังกฤษ)
  - เพศ
  - วันเกิด
  - หมายเลขบัตรประชาชน
  - ที่อยู่ตามทะเบียนบ้าน
  - วันออกบัตร
  - วันหมดอายุ
- ข้อมูลสำหรับติดต่อ
  - ที่อยู่ปัจจุบัน
  - เบอร์โทรศัพท์
  - Email
- บัญชีธนาคาร
  - ชื่อ-นามสกุล
  - ธนาคาร/สาขา
  - หมายเลขบัญชีธนาคาร
- เลขประจำตัวผู้เสียภาษี
  - ชื่อ-นามสกุล
  - หมายเลขบัตรประชาชน
  - เลขประจำตัวผู้เสียภาษี
- ข้อมูลสุขภาพ
  - ส่วนสูง
  - น้ำหนัก
  - กรุ๊ปเลือด
  - ความดัน
  - โรคประจำตัว
  - ประวัติการรักษา
- ศาสนา
- ประวัติอาชญากรรม
- ความพิการ

# 2. กำหนดวัตถุประสงค์และฐานกฎหมายในการประมวลผลให้ชัดเจน

1. เพื่อจัดทำเอกสารประวัติศาสตร์/วิจัย/สถิติ (Research)
2. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือ สุขภาพ (Vital Interest)
3. เพื่อการปฏิบัติตามสัญญา (Contract)
4. เพื่อประโยชน์สาธารณะของผู้ควบคุมส่วนบุคคล (Public Interest)
5. เพื่อประโยชน์อันชอบธรรมของผู้ควบคุมข้อมูลส่วนบุคคล (Legitimate Interest)
6. เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล
7. นอกเหนือจากข้อยกเว้นข้างต้น ต้องขอ ***"ความยินยอม"*** (Consent)

1. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือ สุขภาพ
2. เป็นการดำเนินการโดยชอบตามกฎหมายของ มูลนิธิ สมาคม องค์กรไม่แสวงหากำไรที่มีวัตถุประสงค์จำเพาะ (เช่น การเมือง ศาสนา)
3. เป็นข้อมูลที่เปิดเผยต่อสาธารณะโดยความยินยอมของเจ้าของข้อมูล
4. เป็นการจำเป็นเพื่อการดำเนินการก่อตั้งสิทธิเรียกร้องตามกฎหมาย
5. เป็นการปฏิบัติตามกฎหมาย

****ข้อมูลอ่อนไหว (ม. 26)***

# 3. เก็บ ส่งต่อ หรือให้ใช้เท่าที่จำเป็น (Data Minimisation)

- ข้อมูลที่ให้ผ่าน API ยึดหลัก “ให้เท่าที่จำเป็น” เพื่อให้เพียงพอต่อ “วัตถุประสงค์” ของการประมวลผลครั้งนั้นเท่านั้น

# 4. รักษาความปลอดภัยการส่งข้อมูลผ่าน API และการจัดเก็บข้อมูล

- มีมาตรการรักษาความปลอดภัยในการส่งผ่านข้อมูลผ่าน API
- มีมาตรการรักษาความปลอดภัยเพื่อเก็บรักษาข้อมูลที่ได้รับจาก API
- มาตรการเช่น
  - การเข้ารหัสข้อมูล (data encryption)
  - การเลือกช่องทางการส่งที่ปลอดภัย (secured channel)
  - การยืนยันตัวตน (authentication)
  - การจำกัดการเข้าถึง (authorization and access control)

# 5. พึงระลึกว่าเจ้าของข้อมูลมีสิทธิ์ตามกฎหมาย ไม่ว่าข้อมูลจะถูกส่งต่อไปยังปลายทางใดก็ตาม

- สิทธิในการได้รับแจ้งข้อมูล (Right to be Informed)
- สิทธิในการเข้าถึง (Right of Access)
- สิทธิในการขอแก้ไขเพิ่มเติม (Right to Rectification)
- สิทธิในการโอนย้ายข้อมูล (Right to Data Portability)
- สิทธิในการขอลบหรือทำให้ข้อมูลการเป็นนิรนาม (Right to Erasure)
- สิทธิในการขอระงับการประมวลผล (Right to Restriction)
- สิทธิในการคัดค้าน (Right to Object)

# 6. การจัดการ “ความยินยอม” (consent management)

- มีการขอ “ความยินยอม” อย่างถูกต้อง
- มีกลไกเพื่อจัดการข้อมูลที่ได้รับจากการให้ความยินยอม (โดยเฉพาะเมื่อมีการถอนความยินยอม)

# 7. โอนย้ายข้อมูลด้วยความระมัดระวัง

- การโอนย้ายให้ให้บริการข้อมูลไปยังองค์กรอื่นต้องมีทำสัญญาเป็นลายลักษณ์อักษร
- ตรวจสอบให้มั่นใจว่าองค์กรที่รับข้อมูลต่อมีมาตรการในการประมวลผลข้อมูลที่สอดคล้องกับ พ.ร.บ. PDPA
- หากรับข้อมูลจากประเทศที่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคล เช่น GDPR ต้องประมวลผลข้อมูลส่วนบุคคลนั้นให้เป็นไปตามที่กฎหมายนั้นกำหนด

# 8. ทำ RoPA และ Data Catalogue

- ทำ  RoPA ของการประมวลผลข้อมูลส่วนบุคคลที่ให้บริการผ่าน APIs
- ทำ Data Catalogue เพื่อทำให้สามารถระบุ Personal Data (non-sensitive vs sensitive) และ Non-Personal Data ได้

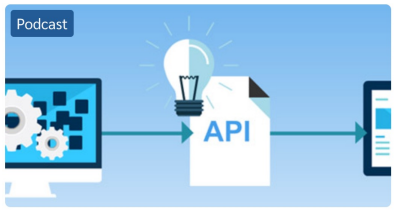
# Summary

1. แยก Personal Data และ  Non-Personal Data
2. กำหนดวัตถุประสงค์และฐานกฎหมายในการประมวลผลให้ชัดเจน
3. เก็บ ส่งต่อ หรือให้ใช้เท่าที่จำเป็น (Data Minimisation)
4. รักษาความปลอดภัยการส่งข้อมูลผ่าน API และการจัดเก็บข้อมูล
5. เจ้าของข้อมูลมีสิทธิ์ตามกฎหมายไม่ว่าข้อมูลจะถูกส่งต่อไปยังปลายทางใดก็ตาม และ Data Owner ยังมีความรับผิดรับชอบ
6. การจัดการ “ความยินยอม”
7. โอนย้ายข้อมูลด้วยความระมัดระวัง
8. ทำ RoPA และ Data Catalogue

# https://privacy.cmu.ac.th



## องค์ความรู้

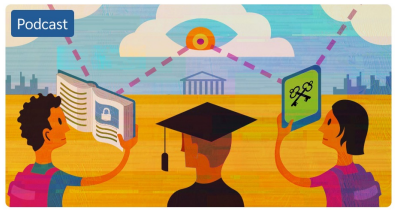



**การคุ้มครองข้อมูลส่วนบุคคลเมื่อส่งข้อมูลผ่าน APIs**

07/07/2023

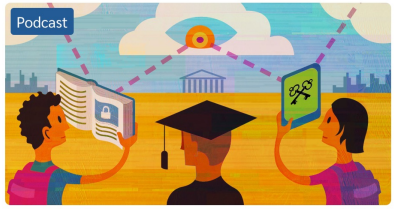

**การคุ้มครองข้อมูลส่วนบุคคลของศิษย์เก่า**

05/07/2023




**การคุ้มครองข้อมูลส่วนบุคคลของนักศึกษามหาวิทยาลัยเชียงใหม่ (ตอนที่ 2)**

27/06/2023




**การคุ้มครองข้อมูลส่วนบุคคลของนักศึกษามหาวิทยาลัยเชียงใหม่ (ตอนที่ 1)**

18/06/2023


**Record of Processing Activities (RoPA) เครื่องมือชั้นเยี่ยมสำหรับ PDPA**

11/06/2023


**10 ประเด็นควรระวังสำหรับ... ให้ละเมิด พ.ร.บ. ข้อ... 2562 (PDPA)**

Thai