**สรุปรายการที่ต้องดำเนินการให้ครอบคลุมตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล**

**1. การดำเนินงานภาพรวมของมหาวิทยาลัย**

| ลำดับ | รายการ | กรอบเวลา | สถานะ | ผู้ดำเนินการ |
|---|---|---|---|---|
| 1 | การจัดทำบันทึกกิจกรรมการประมวลผลข้อมูล (Record of Processing Activities : ROPA) | ภายใน 1 มิ.ย. | -มีตัวอย่างแล้ว- หน่วยงานอยู่ระหว่างการจัดทำ | ผู้ควบคุมข้อมูลทุกหน่วยงาน |
| 2 | การจัดทำเอกสารแจ้งข้อมูลการประมวลผลข้อมูล (Privacy Notice) | ภายใน 1 มิ.ย. | -มีตัวอย่างแล้ว- หน่วยงานอยู่ระหว่างการจัดทำ | ผู้ควบคุมข้อมูลทุกหน่วยงาน |
| 3 | การขอความยินยอมในการประมวลผลข้อมูล (Data Processing Consent) | ภายใน 1 มิ.ย. | -มีตัวอย่างแล้ว- หน่วยงานอยู่ระหว่างการจัดทำ | ผู้ควบคุมข้อมูลทุกหน่วยงาน |
| 4 | การจัดทำ Cookie consent | ภายใน 1 มิ.ย. | -มีตัวอย่างแล้ว- หน่วยงานอยู่ระหว่างการจัดทำ | ผู้ควบคุมข้อมูลทุกหน่วยงาน |
| 5 | การจัดทำข้อตกลงระหว่าง ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูล (DPA: Data Processing Agreement) | ภายใน 1 มิ.ย. | -มีตัวอย่างแล้ว- หน่วยงานอยู่ระหว่างการจัดทำ | ผู้ควบคุมข้อมูลเฉพาะบางหน่วยงานที่มีการจ้างผู้ประมวลผลภายนอก |
| 6 | ข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (data sharing agreement) | ภายใน 1 มิ.ย. | -มีตัวอย่างแล้ว- หน่วยงานอยู่ระหว่างการจัดทำ | ผู้ควบคุมข้อมูลเฉพาะบางหน่วยงานที่มีแบ่งปันข้อมูลส่วนบุคคล |
| 7 | การจัดการทำข้อตกลงแลกเปลี่ยนข้อมูลภายในหน่วยงาน | ภายใน 1 มิ.ย. | -มีตัวอย่างแล้ว- หน่วยงานอยู่ระหว่างการจัดทำ | ผู้ควบคุมข้อมูลทุกหน่วยงาน |
| 8 | การอบรม (Training) สร้างความตระหนักรู้ (Awareness) และประเมินความสามารถบุคลากร (Assessment) ด้านการคุ้มครองข้อมูลส่วนบุคคล | ภายใน 1 มิ.ย. | อยู่ระหว่างดำเนินการ | คณะกรรมการประชาสัมพันธ์ข้อมูล |
| 9 | กำกับการเปิดเผย ส่ง หรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ (Cross-Border Data Transfer) | 1 เดือน | -มีตัวอย่างแล้ว- | ผู้ควบคุมข้อมูลส่วนบุคคลเฉพาะบางหน่วยงานที่มีการส่งข้อมูลไปตปท.<br>* CIA, COOP |

| ลำดับ | รายการ | กรอบเวลา | สถานะ | ผู้ดำเนินการ |
|---|---|---|---|---|
| 10 | DATA Life Cycle management | 3 เดือน | ดำเนินการจัดการข้อมูลตั้งแต่ต้นจนจบตามรอบกระบวนการ | ผู้ควบคุมข้อมูลทุกหน่วยงาน ดำเนินการ กับข้อมูลตามที่ระบุไว้ใน privacy notice |
| 11 | การจัดทำและประเมิน Risk Assessment | 3 เดือน | -มีตัวอย่างแล้ว- | ผู้ควบคุมข้อมูลทุกหน่วยงาน |
| 12 | การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment : DPIA) | 6 เดือน | -มีตัวอย่างแล้ว- | เฉพาะการประมวลผลข้อมูลที่มีผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลที่มีความเสี่ยงสูง, มีการประมวลผลข้อมูลที่อ่อนไหว *เช่น CCTV, ร.พ. |
| 13 | IT System Support PDPA | 1 ปี | (อยู่ระหว่างวิเคราะห์ข้อมูลการจัดหาเครื่องมือ) | DPO, คณะกรรมการ PDPA |
| 14 | การติดตาม (Monitor) และการตรวจสอบประเมินการดำเนินงานด้านการคุ้มครองข้อมูลส่วนบุคคล (Audit) | ทุกไตรมาส | ดำเนินการตามรอบประเมินที่กำหนด | คณะกรรมการ PDPA / คณะทำงาน Audit |

**2. สรุปรายการที่ต้องดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)**

**(ตามแนวปฏิบัติผู้คุ้มครองข้อมูลส่วนบุคคล)**

| ลำดับ | รายการ | กรอบเวลา |
|---|---|---|
| 1 | **มาตรการป้องกันด้านการบริหารจัดการ**<br>• ให้มีการกำหนดเกี่ยวกับการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้งาน (user responsibilities) | ภายใน 1 มิ.ย. |
| 2 | **มาตรการป้องกันด้านเทคนิค (technical safeguard)**<br>• จัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล | ภายใน 1 มิ.ย. |
| 3 | • การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาต ตามระดับสิทธิการใช้งาน เช่น การนำเข้า เปลี่ยนแปลง แก้ไข เปิดเผย ตลอดจนการลบทำลาย | ภายใน 1 มิ.ย. |
| 4 | • จัดให้มีระบบสำรองและกู้คืนข้อมูล (ในส่วนของผู้ควบคุมข้อมูลประจำหน่วยงาน) | ภายใน 1 มิ.ย. |
| 5 | **มาตรการป้องกันทางกายภาพ (physical safeguard)**<br>• มีการล้อมรั้วและล็อคประตูทุกครั้ง ล็อคตู้เอกสารข้อมูลส่วนบุคคล | ภายใน 1 มิ.ย. |
| 6 | • กำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต | ภายใน 1 มิ.ย. |
| 7 | **การส่งมอบข้อมูล**<br>- **การประเมินก่อนส่งมอบข้อมูล**<br>• ให้ดำเนินการตรวจสอบสิทธิ อำนาจหน้าที่ และฐานกฎหมายที่บุคคล และ/หรือ นิติบุคคลรายอื่นนั้น ใช้เพื่อร้องขอข้อมูลส่วนบุคคล | 1 เดือน |
| 8 | • ให้สอบถามวัตถุประสงค์ในการนำข้อมูลไปใช้งานเพื่อให้สามารถประเมินว่าควรสำเนาข้อมูลให้ในระดับรายละเอียดเท่าใด | 1 เดือน |
| 9 | - **เมื่อส่งมอบข้อมูล**<br>• จัดเตรียมข้อมูลใหม่จากข้อมูลดิบให้มีระดับรายละเอียดเท่าที่จำเป็นต่อจุดประสงค์การใช้งาน | 1 เดือน |
| 10 | • ส่งมอบข้อมูล พร้อมทำการบันทึกชื่อผู้ขอข้อมูล ข้อมูลสำหรับติดต่อ วัน-เดือน-ปี ที่ให้ข้อมูล ฐานกฎหมายที่ใช้สำหรับเข้าถึงข้อมูลส่วนบุคคล ตลอดจนวัตถุประสงค์การนำไปใช้งาน | 1 เดือน |
| 11 | • แจ้งให้บุคคล หรือ นิติบุคคลนั้น ทราบว่าเมื่อรับข้อมูลไปแล้ว ผู้รับข้อมูลจะต้องดำเนินการตามหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลสำหรับข้อมูลชุดที่ร้องขอไปนั้นเช่นเดียวกัน ตามขอบเขตและวัตถุประสงค์การใช้งานที่แจ้งไว้ | 1 เดือน |
| 12 | - **หลังส่งมอบข้อมูล**<br>• ติดตามการใช้งานเป็นครั้งคราว เช่น ทุก 3 เดือน 6 เดือน หรือ 1 ปี เพื่อบันทึกสถานะล่าสุดในการใช้งานข้อมูลนั้น หากไม่มีความจำเป็นใช้งานตามวัตถุประสงค์ที่แจ้งไว้เดิม ควรแจ้งให้บุคคลหรือ นิติบุคคลนั้น ลบทำลายข้อมูล | 3 เดือน |

| ลำดับ | รายการ | กรอบเวลา |
|---|---|---|
| 13 | • กำหนดวิธีการในการปรับปรุงข้อมูลให้ทันสมัยต่อการใช้งานของผู้ใช้อยู่เสมอ เช่น มีโปรแกรมคอมพิวเตอร์สำหรับเชื่อมต่อปรับปรุงให้ข้อมูลต้นทางและปลายทางมีความทันสมัยเท่ากันโดยอัตโนมัติตลอดเวลา | 1 ปี |
| 14 | **การทำลายข้อมูล**<br>• ติดตามรายการข้อมูลที่ต้องทำลาย เมื่อพ้นกำหนดระยะเวลาการเก็บรักษา | ตามระยะเวลาที่ระบุใน privacy notice |