CHECKLIST การดำเนินการให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) สำหรับหน่วยงานของมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร

๑. DPO (Data Protection Officer)

- ☐ **แต่งตั้ง DPO และประกาศการแต่งตั้งในองค์กรให้รับทราบ**
- ☐ **DPO ทราบหน้าที่และแนวทางปฏิบัติที่มหาวิทยาลัยฯ กำหนด**
- ☐ **DPO รับการอบรมให้มีความรู้ความเข้าใจใน PDPA**
- ☐ **DPO ศึกษานโยบายด้านข้อมูลส่วนบุคคลทุกฉบับที่ประกาศโดยมหาวิทยาลัยฯ**
- ☐ DPO จัดอบรมบุคลากรในบริษัทให้มีความเข้าใจในเรื่อง PDPA เพื่อให้เกิดการปฏิบัติงานที่ถูกต้อง
- ☐ DPO จัดทำแนวปฏิบัติตาม มหาวิทยาลัย ฯ Data Governance Policy
- ☐ จัดสรรบุคคลากรในการบริหารจัดการและรองรับกระบวนการ PDPA compliance
- ☐ แจ้งรายชื่อ DPO ให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ทราบ
- ☐ DPO จัดทำประกาศ หรือแนวปฏิบัติที่ป้องกันไม่ให้บุคลากรในองค์กรเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ เช่น การเปิดเผยต่อบุคคลภายนอก
- ☐ DPO กำหนดขั้นตอนการปฏิบัติงาน (Work Procedures) เช่น การจัดการเรื่องคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล การเตรียมเอกสารหลักฐานในกรณีต้องประสานงานกับ สคส. ฯลฯ

๒. Privacy Notice

- ☐ **ปรับใช้ Privacy Notice แต่ละประเภทที่ประกาศโดยมหาวิทยาลัยฯ ให้เข้ากับบริบทของมหาวิทยาลัยฯ (โดยดูจาก ROPA เนื่องจากมหาวิทยาลัยอาจมีบางกิจกรรมที่ดำเนินการนอกเหนือจากที่ปรากฏใน Privacy Notice ที่ มหาวิทยาลัยฯ ประกาศ)**
- ☐ **ใส่ชื่อ DPO และช่องทางติดต่อไปใน Privacy Notice**
- ☐ **วาง Privacy Notice บน Platform ที่ต้องการแจ้งให้เจ้าของข้อมูลส่วนบุคคล (Data Subject) ทราบ เช่น**
  - **Privacy Notice สำหรับนักศึกษา วางบน Website หรือ Application ที่มีการเก็บและใช้ข้อมูลส่วนบุคคล (ถ้ามี)**
  - **Privacy Notice สำหรับอาจารย์ วางบนระบบบริหารจัดการทรัพยากรบุคคล (HRM)**
  - **Privacy Notice สำหรับบุคลากร วางบนระบบบริหารจัดการทรัพยากรบุคคล (HRM)**
  - **Privacy Notice สำหรับ CCTV (ถ้ามี)**
- ☐ **กำหนดวันในการนำ Privacy Notice ลงบน Platform ที่เลือกเพื่อเป็นการแจ้งเจ้าของข้อมูลส่วนบุคคล**

๓. COOKIE CONSENT (ถ้าไม่เก็บ ให้ข้ามไปข้ออื่น)

- ☐ **ศึกษานโยบายของมหาวิทยาลัยฯ เรื่องการเก็บ Cookie**
- ☐ **ใส่ Pop-Up บนเว็บไซต์ให้ผู้เยี่ยมชมเว็บไซต์สามารถตั้งค่าไม่ยอมรับ Cookie บางส่วนได้ โดยระบบต้องตั้งค่า Default ว่าผู้เยี่ยมชมเว็บไซต์ไม่ยอมรับ Cookie ที่ไม่สอดคล้องกับวัตถุประสงค์หลักของเว็บไซต์ จนว่าผู้เยี่ยมชมเว็บไซต์จะมาเปลี่ยนว่าเป็นยอมรับ**
- ☐ **มีระบบจัดการ Cookie เพื่อดำเนินการให้เป็นไปตามการตั้งค่าความยินยอมของผู้เยี่ยมชมเว็บไซต์**
- ☐ **ถ้ามีการใช้ Application ที่ Tracking ข้อมูลส่วนบุคคล ให้มีระบบจัดการให้ผู้ใช้งานสามารถตั้งค่าการอนุญาต/ ไม่อนุญาตให้ Tracking ข้อมูลส่วนบุคคล**

๔. DIRECT MARKETING OPT-OUT (ถ้าไม่มี ให้ข้ามไปข้ออื่น)

- ☐ **พัฒนาระบบการส่งอีเมล/ข้อความ และ พัฒนา Landing Page หรือช่องทางสำหรับเก็บข้อมูลการยกเลิกความยินยอมการรับ Direct Marketing (หรือที่เรียกว่า Direct Marketing Opt-out)**
- ☐ **รวบรวมรายชื่อนักศึกษา อาจารย์ และบุคลากร ที่จะทำการส่งข้อความไปให้ นักศึกษา อาจารย์ และบุคลากร เหล่านั้นยกเลิกความยินยอมการรับ Direct Marketing**
- ☐ **ปรับข้อความ Direct Marketing ที่มหาวิทยาลัยฯ กำหนดมาให้เข้ากับบริบทของมหาวิทยาลัยฯ และเลือกช่องทาง/ Platform ในการส่งข้อความ เช่น Email หรือ SMS**
- ☐ **มีกระบวนการจัดการความยินยอมของคนที่แจ้งยกเลิกความยินยอม โปรดดู Consent Management ข้างล่าง**

CHECKLIST การดำเนินการให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) สำหรับหน่วยงานของมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร

๕. Consent Management

๕.๑ การจัดการสำหรับ Consent มาตรฐานที่อนุมัติโดยมหาวิทยาลัย ฯ

- ☐ **ปรับใช้ฟอร์ม Consent ให้เข้ากับบริบทของมหาวิทยาลัย เช่น ใส่ชื่อหน่วยงาน ใส่เบอร์ติดต่อของหน่วยงาน ฯลฯ**
- ☐ **กำหนดวันในการนำฟอร์ม Consent ไปใช้กับนักศึกษา อาจารย์ และบุคลากร**
- ☐ **นำ Consent ไปวางใน ช่องทาง/ Platform ที่ต้องการขอความยินยอมตามบริบทของมหาวิทยาลัยฯ เช่น เป็น Hard Copy หรือลงใน Application หรือเว็บไซต์ ฯลฯ**
- ☐ **ในกรณีที่เป็น Hard Copy กำหนดวิธีการบันทึกข้อมูลลงระบบเพื่อการจัดการบริหาร Consent แบบอิเล็กทรอนิกส์ต่อไป เช่น การที่นักศึกษา อาจารย์ และบุคลากร ถอนความยินยอม**
- ☐ **กำหนดวิธีการจัดการความยินยอมและหลักปฏิบัติที่ชัดเจน สำหรับแต่ละวิธีการ (Paper, Manual Key-in, eConsent Management Platform)**
- ☐ หากเลือกวิธีการจัดการความยินยอมด้วยการพัฒนาระบบ eConsent Management, DPO จัดให้มีการอบรมเรื่องเทคนิคการสื่อสารกับลูกค้าเพื่อขอความยินยอม
- ☐ ประเมินความพร้อมของมหาวิทยาลัยและบุคลากรหน้างาน (First Line Operation)

๕.๒ การจัดการสำหรับ Direct Marketing Opt-Out

- ☐ **กำหนดวิธีการจัดการและกำหนดผู้รับผิดชอบบันทึกข้อมูลลงระบบเพื่อการจัดการบริหาร Consent แบบอิเล็กทรอนิกส์ กรณี นักศึกษา อาจารย์ และบุคลากร ตอบว่าขอยกเลิกการรับ Direct Marketing**
- ☐ **กำหนดหลักปฏิบัติและประกาศให้บุคลากรที่เกี่ยวข้องทราบว่า**
  - **มหาวิทยาลัยต้องไม่ส่งข้อความ Direct Marketing Opt-Out Message ไปให้นักศึกษา อาจารย์ และบุคลากรใหม่ที่กรอกข้อมูลใน Broad Consent แล้ว (เช่น หากวันที่ ๑ พฤษภาคม ๒๕๖๕ เป็นวันแรกที่บริษัทเริ่มใช้ Broad Consent กับนักศึกษา อาจารย์ และบุคลากร ดังนั้น กลุ่มนักศึกษา อาจารย์ และบุคลากร ที่จะได้รับข้อความ Direct Marketing Opt-Out คือรายชื่อนักศึกษา อาจารย์ และบุคลากร ก่อนที่มีอยู่ก่อนวันที่ ๑ มีนาคม ๒๕๖๕)**
  - **มหาวิทยาลัยสามารถส่ง Direct Marketing ไปหานักศึกษา อาจารย์ และบุคลากร ได้ หากนักศึกษา อาจารย์ และบุคลากร ที่ไม่ตอบอะไรกลับมาหลังจากได้รับข้อความ Direct Marketing Opt-Out แล้ว**

๕.๓ การจัดการสำหรับ Consent อื่น ๆ ที่มหาวิทยาลัย ฯ อาจจะมีขึ้นมาเฉพาะเรื่อง (หรือที่เรียกว่า Ad Hoc Consent)

- ☐ **ปรับใช้ฟอร์ม Adhoc Consent ให้เข้ากับบริบทของมหาวิทยาลัย เช่น ใส่ชื่อหน่วยงาน ใส่เบอร์ติดต่อของหน่วยงาน ฯลฯ พร้อมทั้งระบุวัตถุประสงค์ของการขอความยินยอม**
- ☐ **นำ Ad Hoc Consent ไปวางใน ช่องทาง/ Platform ที่ต้องการขอความยินยอมตามบริบทของมหาวิทยาลัย เช่น เป็น Hard Copy หรือลงใน Application หรือเว็บไซต์ ฯลฯ**
- ☐ **กำหนดวิธีการบันทึกข้อมูลลงระบบเพื่อการจัดการบริหาร Consent แบบอิเล็กทรอนิกส์ต่อไป เช่น การที่นักศึกษา อาจารย์ และบุคลากร ถอนความยินยอม**

๖. **ROPA (Records of Processing Activity)** (บันทึกรายการกิจกรรมข้อมูลส่วนบุคคล)

- ☐ กำหนดช่วงเวลาประจำสำหรับการทบทวน ROPA เดิมให้เป็นปัจจุบัน (update) อยู่เสมอ
- ☐ กำหนดผู้รับผิดชอบ เมื่อมีกิจกรรมใหม่ หรือมีการยกเลิกกิจกรรมใด ให้เป็นผู้ Update ใน ROPA เนื่องจากอาจถูกตรวจสอบได้โดยหน่วยงานผู้กำกับดูแล (สคส.)

๗. Data processing agreement

- ☐ **ระบุ Vendor ที่เข้าข่ายเป็น Data Processor แต่ยังไม่มี Data Processing Agreement ระหว่างกัน หรือมีสัญญาแต่ยังไม่ครอบคลุม**
- ☐ **เจรจาทำ Data Processing Agreement กับ Vendor ข้างต้น โดยใช้ Template สัญญา Data Processing Agreement ที่ มหาวิทยาลัย ฯ ประกาศ**
- ☐ กำหนดวิธีปฏิบัติและช่องทางการปรึกษากับฝ่ายกฎหมาย หากเกิดอุปสรรคในการเจรจาการทำสัญญาดังกล่าวในเชิงกฎหมาย
- ☐ ทุกครั้งที่มีการตกลงจ้าง Vendor ต้องพิจารณาว่า Vendor เข้าข่ายเป็น Data Processor หรือไม่ และถ้าหากเป็น Data Processor ให้ดำเนินการทำ Data Processing Agreement

CHECKLIST การดำเนินการให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) สำหรับหน่วยงานของมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร

๘. DPIA (Data Protection Impact Assessment) (การประเมินความเสี่ยงด้านผลกระทบเรื่องข้อมูลส่วนบุคคล)

- ☐ **ทราบนโยบายของ มหาวิทยาลัย ฯ เรื่องการทำ DPIA เพื่อพิจารณาว่ากิจกรรมใดเข้าข่ายต้องทำ DPIA**
- ☐ **ถ้ากิจกรรมนั้นเข้าข่ายต้องทำ DPIA ให้ใช้แบบฟอร์ม DPIA ที่ มหาวิทยาลัย ฯ กำหนดในการทำการประมิน**
- ☐ ดำเนินการระงับความเสี่ยง หรือเพิ่ม Security ตามผลประเมิน DPIA

๙. Data Security

- ☐ **ประเมินความเสี่ยงด้าน Security ตามนโยบายของ มหาวิทยาลัย ฯ**
- ☐ **กำหนดมาตรฐานขั้นต่ำด้าน Security ตามที่ระบุไว้ในกฎหมายลำดับรองของ PDPA เช่น การทำ Access Control และ Access Rights Management เป็นต้น**
- ☐ **ศึกษาระดับความเสี่ยงในการละเมิดข้อมูลส่วนบุคคลและกำหนดแผนในการปิดช่องโหว่ทั้งทางระบบและ Business processes**
- ☐ กำกับและติดตามผลประเมินความเสี่ยงอยู่เป็นประจำเพื่อพัฒนามาตรการด้าน Security ให้มีประสิทธิภาพยิ่งขึ้น

๑๐.Data Subject Rights

- ☐ **กำหนดวิธีการ และ พัฒนาระบบ/ช่องทางเพื่อรองรับการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล**
- ☐ **ระบุช่องทางการติดต่อกับ DPO ของหน่วยงาน ไปในฟอร์มการร้องขอสิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights Form) ที่ประกาศโดย มหาวิทยาลัย ฯ**
- ☐ **นำแบบฟอร์ม Data Subject Rights Form ไปวางไว้ในช่องทาง/ Platform ที่ให้เจ้าของข้อมูลส่วนบุคคลสามารถเข้าถึงได้ เช่น Website หรือ Application**
- ☐ อบรมหรือแจ้งบุคลากรที่เกี่ยวข้องกับการรับเรื่องร้องเรียนจากนักศึกษา อาจารย์ และบุคลากร ให้เข้าใจถึงแบบฟอร์ม สถานการณ์ที่นักศึกษา อาจารย์ และบุคลากร จะเรียกร้องสิทธิ และวิธีการในการให้ฟอร์มกับนักศึกษา อาจารย์ และบุคลากร
- ☐ เมื่อมีการเรียกร้องสิทธิ การพิจารณาอนุมัติตามคำร้องขอหรือการปฏิเสธคำร้องขอ ให้เป็นไปตามแนวปฏิบัติของ มหาวิทยาลัย ฯ
- ☐ บันทึกเหตุผลในการอนุมัติตามคำร้องขอหรือปฏิเสธคำร้องเป็นลายลักษณ์อักษรทุกครั้ง เพื่อเป็นหลักฐาน

๑๑.Data Breach Incident report

- ☐ **ประกาศนโยบาย กำหนดวิธีการและช่องทางสำหรับการแจ้ง DPO ในกรณีที่การละเมิดข้อมูลส่วนบุคคลเกิดขึ้น**
- ☐ **DPO ทราบกระบวนการ Data Breach Incident Report ที่ประกาศโดย มหาวิทยาลัย ฯ ที่ระบุถึงแนวทางการประเมินความเสี่ยง การแจ้งหน่วยงานกำกับดูแล และการแจ้งเจ้าของข้อมูลส่วนบุคคล (ถ้าความเสี่ยงระดับสูง)**
- ☐ เมื่อทราบถึงการละเมิดข้อมูลส่วนบุคคลเกิดขึ้น ให้แจ้ง DPO ทันที
- ☐ DPO ต้องดำเนินการตามกระบวนการ Data Breach Incident Report ที่ประกาศโดย มหาวิทยาลัย ฯ ที่ระบุถึงแนวทางการประเมินความเสี่ยง การแจ้งหน่วยงานกำกับดูแล และการแจ้งเจ้าของข้อมูลส่วนบุคคล (ถ้าความเสี่ยงระดับสูง)

๑๒.Cross-border Personal data Transfer (ถ้ามี)

- ☐ ตรวจสอบว่าบริษัทมีการโอนข้อมูลส่วนบุคคลไปยังหน่วยงานที่ตั้งอยู่ในต่างประเทศ
  - หากมี ได้มีการตรวจสอบเพิ่มเติมว่าประเทศดังกล่าวถูกรองรับโดยกฎหมาย PDPA ว่าเป็นประเทศที่อนุญาตให้โอนข้อมูลส่วนบุคคลไปได้
- ☐ ในกรณีที่หน่วยงานที่จะโอนข้อมูลส่วนบุคคลไปหานั้นตั้งอยู่ในประเทศที่ไม่อยู่ในรายชื่ออนุญาต บริษัทประกาศนโยบายและกำหนดวิธิปฏิบัติให้เป็นอย่างใดอย่างหนึ่งตามมาตรา ๒๘-๒๙ ของ พรบ. PDPA เช่น
  - ขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล
  - ทำสัญญาโอนข้อมูลส่วนบุคคลข้ามพรมแดนระหว่างกัน ตาม Template สัญญาที่ประกาศโดย มหาวิทยาลัย ฯ
  - โดยมีข้อยกเว้นว่า ถ้าหากการโอนข้อมูลส่วนบุคคลข้ามพรมแดนเป็นไปเพื่อการระงับอันตรายต่อชีวิตโดยที่เจ้าของข้อมูลไม่อาจให้ความยินยอมได้ หรือเป็นไปเพื่อการปฏิบัติตามสัญญาที่เจ้าของข้อมูลเป็นคู่สัญญา ได้มีการระบุและแจ้งผู้ปฏิบัติงานให้ทราบว่าสามารถโอนข้อมูลส่วนบุคคลข้ามพรมแดนได้