กรมการแพทย์แผนไทยและการแพทย์ทางเลือก
Department of Thai Traditional and Alternative Medicine

แผนปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2569

กรมการแพทย์แผนไทยและการแพทย์ทางเลือก

DTAM next

แผนปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล

ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

แผนปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๙
กรมการแพทย์แผนไทยและการแพทย์ทางเลือก

ที่ปรึกษา

นายแพทย์พงศธร พอกเพิ่มดี อธิบดีกรมการแพทย์แผนไทยและการแพทย์ทางเลือก

นายสมศักดิ์ กรีชัย รองอธิบดีกรมการแพทย์แผนไทยและการแพทย์ทางเลือก

นางสาวนริศรา งามสอาด รักษาราชการแทนผู้อำนวยการกองวิชาการและแผนงาน

บรรณาธิการ

นายจักรกฤษณ์ สิงห์บุตร เภสัชกรชำนาญการ กองวิชาการและแผนงาน

นางสาวสุวิมล สุมลตรี แพทย์แผนไทยชำนาญการ กองวิชาการและแผนงาน

ออกแบบปกและเล่ม

นายธนาวัฒน์ พลศิลป์ เจ้าหน้าที่วิเคราะห์นโยบายและแผน กองวิชาการและแผนงาน

รวบรวมและจัดทำโดย

กลุ่มงานบริหารจัดการข้อมูลขนาดใหญ่ กองวิชาการและแผนงาน
กรมการแพทย์แผนไทยและการแพทย์ทางเลือก

Website

http://www.dtam.moph.go.th

บทสรุปผู้บริหาร

แผนปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๙ ของกรมการแพทย์แผนไทยและการแพทย์ทางเลือก จัดทำขึ้นเพื่อให้การดำเนินงานสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และแผนแม่บทการส่งเสริมและการคุ้มครองข้อมูลส่วนบุคคลของประเทศ พ.ศ. ๒๕๖๗-๒๕๗๐ โดยกรมให้ความสำคัญกับการบริหารจัดการข้อมูลที่มีความอ่อนไหวสูง เช่น ข้อมูลด้านสุขภาพของผู้รับบริการ และข้อมูลของบุคลากร เพื่อให้ได้รับความคุ้มครองตามมาตรฐานสากล

เพื่อให้บรรลุวัตถุประสงค์ดังกล่าว แผนปฏิบัติการฉบับนี้ได้กำหนดสาระสำคัญครอบคลุมการดำเนินงาน ๑๐ มิติหลัก ดังต่อไปนี้

มิติที่ ๑ การกำกับดูแล (Oversight): มุ่งเน้นการวางรากฐานทางกฎหมายและจริยธรรมให้แก่องค์กร โดยมีการจัดทำตัวชี้วัด (KPI) และประเมินประสิทธิภาพการทำงานของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) อย่างน้อยปีละ ๑ ครั้ง รวมถึงนำผลการวัดประสิทธิภาพมาวางแผนพัฒนาปรับปรุงกระบวนการให้ดียิ่งขึ้น

มิติที่ ๒ นโยบายและแนวปฏิบัติ (Policies and procedures): จัดทำนโยบายเป็นลายลักษณ์อักษรเพื่อใช้เป็นคู่มือมาตรฐานในการปฏิบัติงานของบุคลากรทุกระดับ โดยมีเป้าหมายทบทวนนโยบายและแนวปฏิบัติให้ทันสมัยสอดคล้องกับกฎหมายอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

มิติที่ ๓ การอบรมและการสร้างความตระหนัก (Training and awareness): ปลูกฝังความรู้ความเข้าใจให้บุคลากรเพื่อลดความเสี่ยงจากข้อผิดพลาดของมนุษย์ (Human Error) โดยตั้งเป้าหมายให้บุคลากร ๑๐๐% เข้ารับการอบรมด้าน PDPA และต้องผ่านเกณฑ์ทดสอบหลังการอบรมไม่น้อยกว่า ๙๐%

มิติที่ ๔ สิทธิของเจ้าของข้อมูล (Individual's rights): วางกลไกที่โปร่งใสให้เจ้าของข้อมูลสามารถเข้าถึง แก้ไข หรือลบข้อมูลของตนเองได้อย่างอิสระ โดยตั้งเป้าหมายดำเนินการตอบสนองต่อคำร้องขอใช้สิทธิให้เสร็จสิ้นภายในระยะเวลา ๓๐ วัน ตามกฎหมายให้ได้ ๑๐๐%

มิติที่ ๕ ประกาศความเป็นส่วนตัว (Transparency): สื่อสารรายละเอียดการจัดเก็บ วัตถุประสงค์และการส่งหรือโอนข้อมูลให้เจ้าของข้อมูลทราบอย่างชัดเจนและโปร่งใส โดย Privacy Notice ต้องครอบคลุมทุกกิจกรรมในบันทึก ROPA และมีเป้าหมายให้เจ้าของข้อมูลรับทราบประกาศไม่น้อยกว่า ๙๐%

มิติที่ ๖ การจัดทำบันทึกรายกิจกรรมและการกำหนดฐานทางกฎหมาย (ROPA & lawful basis): จัดทำระบบบันทึกรายการกิจกรรม (ROPA) เพื่อตรวจสอบวงจรชีวิตของข้อมูลและยืนยันฐานทางกฎหมาย รวมถึงเพิ่มขั้นตอนตรวจสอบผู้มีอำนาจกระทำการแทนผู้เยาว์ และระบุวิธีการถอนความยินยอมอย่างชัดเจน

มิติที่ ๗ สัญญาและการส่งหรือโอนข้อมูล (Contracts and data sharing): จัดทำข้อตกลงการประมวลผลข้อมูล (DPA) แบบมาตรฐานกับผู้ประมวลผลข้อมูลส่วนบุคคลให้ครบถ้วน ๑๐๐% และมีการตรวจสอบการปฏิบัติตามสัญญาของผู้ประมวลผลข้อมูลอย่างน้อยปีละ ๑ ครั้ง

มิติที่ ๘ การบริหารจัดการความเสี่ยง (Risks): วิเคราะห์ผลกระทบ (DPIA) และควบคุมความเสี่ยงไม่ให้เกิดผลกระทบต่อสิทธิของเจ้าของข้อมูล โดยมีเป้าหมายให้ความเสี่ยงทั้งหมดที่ระบุไว้มีมาตรการจัดการรองรับ ๑๐๐% และรักษาความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

มิติที่ ๙ การรักษาความมั่นคงปลอดภัยของข้อมูล (Data security): วางมาตรการรักษาความลับ ความถูกต้อง และสภาพพร้อมใช้งานของข้อมูล โดยกำหนดวิธีทำลายข้อมูลอย่างถูกต้องตามมาตรฐาน และมีการจัดเก็บ Log (Audit trails) การเข้าถึง แก้ไข และลบข้อมูลไว้ ๑๐๐%

มิติที่ ๑๐ การรับมือต่อเหตุการละเมิดข้อมูล (Breach response and monitor): วางขั้นตอนรับมือเหตุละเมิด โดยมีเป้าหมายรายงานต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ภายใน ๗๒ ชั่วโมง ให้ได้ ๑๐๐% พร้อมทั้งวิเคราะห์แนวโน้มเพื่อออกมาตรการป้องกันไม่ให้เกิดเหตุการณ์ละเมิดซ้ำ

โดยสรุป การขับเคลื่อนแผนปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๙ ฉบับนี้ จะเป็นกลไกสำคัญในการยกระดับมาตรฐานการกำกับดูแลข้อมูลของกรมการแพทย์แผนไทยและการแพทย์ทางเลือกให้มีความมั่นคงปลอดภัยและสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ รวมถึงแผนแม่บทระดับประเทศ การดำเนินการอย่างเคร่งครัดและวัดผลได้จริงในทั้ง ๑๐ มิติ จะช่วยลดความเสี่ยงทางกฎหมาย พร้อมทั้งสร้างความโปร่งใสและธรรมาภิบาลในการบริหารจัดการข้อมูลที่มีความอ่อนไหวสูง โดยเฉพาะข้อมูลด้านสุขภาพของผู้รับบริการและข้อมูลบุคลากร ท้ายที่สุดแผนปฏิบัติการนี้ช่วยคุ้มครองสิทธิขั้นพื้นฐานของเจ้าของข้อมูล และเสริมสร้างความเชื่อมั่นจากประชาชนต่อการให้บริการด้านสาธารณสุข การศึกษาวิจัย และการส่งเสริมภูมิปัญญาการแพทย์แผนไทยของกรมอย่างยั่งยืนต่อไป

(นายพงศธร พอกเพิ่มดี)
อธิบดีกรมการแพทย์แผนไทยและการแพทย์ทางเลือก

แผนปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๙
กรมการแพทย์แผนไทยและการแพทย์ทางเลือก

๑. บทนำ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มีผลบังคับใช้ทุกมาตราตั้งแต่วันที่ ๑ มิถุนายน พ.ศ. ๒๕๖๕ โดยมีวัตถุประสงค์เพื่อให้มีการคุ้มครองข้อมูลส่วนบุคคลและให้มีมาตรการเยียวยาเจ้าของข้อมูลส่วนบุคคลจากการถูกละเมิดสิทธิในข้อมูลส่วนบุคคลที่มีประสิทธิภาพ หลักการสำคัญของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลเท่าที่จำเป็นตามวัตถุประสงค์อันชอบด้วยกฎหมายโดยต้องรักษาความมั่นคงปลอดภัยของข้อมูล และเจ้าของข้อมูลส่วนบุคคลมีสิทธิได้รับการแจ้งให้ทราบรายละเอียดในการเก็บรวบรวม การขอเข้าถึง การขอให้โอนการคัดค้านการเก็บรวบรวม ใช้หรือเปิดเผย การขอให้ลบหรือทำลาย หรือทำให้เป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้การขอระงับการใช้และการขอให้แก้ไขข้อมูลส่วนบุคคล

ทั้งนี้ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการให้ถูกต้องตามแนวทางที่กฎหมายกำหนดไว้ หากเกิดความเสียหายจากการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล จะมีความรับผิดทางแพ่ง รับโทษทางอาญาหรือทางปกครองแล้วแต่กรณี โดยมีโทษทางอาญาสูงสุด คือ จำคุกไม่เกิน ๑ ปี หรือปรับไม่เกิน ๑ ล้านบาท หรือทั้งจำทั้งปรับ และมีโทษทางปกครองสูงสุด ๕ ล้านบาท ส่งผลให้ทุกภาคส่วนต้องทำการปรับตัว ในส่วนของประชาชนต้องสร้างความตระหนักรู้ และความเข้าใจด้านการใช้สิทธิตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ในส่วนของภาคเอกชนและองค์กรต่าง ๆ ต้องกำหนดนโยบาย แนวทางดำเนินการ หรือแนวปฏิบัติ เพื่อให้การดำเนินการด้านการคุ้มครองข้อมูลส่วนบุคคลมีความสอดคล้องกับกฎหมายดังกล่าว

๒. ความสอดคล้องกับแผนแม่บทการส่งเสริมและการคุ้มครองข้อมูลส่วนบุคคลของประเทศ พ.ศ.๒๕๖๗-๒๕๗๐

๒.๑ องค์ประกอบของแผนแม่บทการส่งเสริมและการคุ้มครองข้อมูลส่วนบุคคลของประเทศ พ.ศ. ๒๕๖๗ - ๒๕๗๐

๑. มาตรการหรือแนวทางการดำเนินงานด้านการส่งเสริมและการคุ้มครองข้อมูลส่วนบุคคลที่สอดคล้องกับนโยบาย ยุทธศาสตร์ชาติและแผนระดับชาติที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

๒. มาตรการหรือแนวทางการส่งเสริมและสนับสนุนการเกิดทักษะการเรียนรู้ ความเข้าใจเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลให้แก่หน่วยงานภาครัฐ ภาคเอกชน และภาคประชาชน

๓. มาตรการหรือแนวทางการแก้ไขปัญหา อุปสรรคในการปฏิบัติตามนโยบาย ยุทธศาสตร์ชาติและแผนระดับชาติที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

๔. มาตรการหรือแนวทางการส่งเสริมและสนับสนุนการวิจัย เพื่อพัฒนาเทคโนโลยีที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

๒.๒ เป้าหมาย

๒.๒.๑ เป้าหมายร่วมกันของประเทศ

๑. สัดส่วนของหน่วยงานที่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ เพิ่มมากขึ้น

๒. สัดส่วนของการละเมิดข้อมูลส่วนบุคคลลดลง

๓. มีการปรับปรุง พัฒนากฎหมาย PDPA ให้ทันกับสถานการณ์ปัจจุบัน

๔. ประเทศไทยมีบริการกลางด้าน PDPA E-Service

๕. ประเทศไทยมีอันดับความสามารถในการแข่งขันทาง Data Privacy/Personal Data Protection/Trusted Data ที่ดีขึ้น

๒.๒.๒ ค่าเป้าหมายและตัวชี้วัด

- ค่าเป้าหมาย

๑. สัดส่วนของหน่วยงานเป้าหมายที่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มีจำนวน ๑๐๐%

๒. สัดส่วนการละเมิดข้อมูลส่วนบุคคลร้ายแรงลดลง ๒๐% ของปีฐาน

๓. มีการปรับปรุงเพิ่มประสิทธิภาพและพัฒนากฎหมาย PDPA

๔. ประเทศไทยมีบริการกลางด้าน PDPA E-Service อย่างน้อย ๑๑ บริการหลักตามกลุ่มอุตสาหกรรมเป้าหมายหลัก

๕. ประเทศไทยมีอันดับความสามารถในการแข่งขันทางด้าน Data Privacy/ Personal Data Protection/Trusted Data อยู่ใน ๓๐ อันดับแรกของการจัดอันดับนานาชาติ

- ตัวชี้วัด

๑. สัดส่วนหน่วยงานที่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๒. สัดส่วนการละเมิดข้อมูลส่วนบุคคล

๓. มีการประเมิน และการปรับปรุงพัฒนากฎหมาย PDPA

๔. จำนวนบริการกลางด้าน PDPA E-Service

๕. อันดับความสามารถในการแข่งขันทางดิจิทัล และหรือ Data Privacy/Personal Data Protection/Trusted Data ของการจัดอันดับนานาชาติ

๒.๓ ยุทธศาสตร์

๑. การเพิ่มประสิทธิภาพการบังคับใช้กฎหมาย PDPA Effective and Balanced Enforcement พัฒนามาตรฐาน หลักเกณฑ์ กฎเกณฑ์ เครื่องมือตัวชี้วัด และการกำกับดูแลความเป็นส่วนตัวของข้อมูล (Data Privacy Governance) รวมทั้งการปรับปรุงกฎหมายเพื่อเพิ่มความเข้มแข็งให้แก่การคุ้มครองข้อมูลส่วนบุคคล และส่งเสริมการดำเนินการต่าง ๆ ภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ เพิ่มขีดความสามารถในการแข่งขันของประเทศ

๒. การพัฒนากำลังคนและสร้างความเชื่อมั่น PDPA Knowledge and Trust Enhancement เสริมสร้างกำลังคน สร้างความรู้ ความเข้าใจ ความตระหนักรู้ ความเชื่อมั่นเท่าทันการเปลี่ยนแปลงด้านข้อมูลส่วนบุคคลอย่างเท่าเทียม ด้วยกลไกการให้ความรู้แบบมุ่งเป้า การรับรองด้านทักษะ การประชาสัมพันธ์ การป้องกัน และรูปแบบการแก้ปัญหา รวมทั้งความพร้อมต่อการเปลี่ยนแปลงด้านข้อมูลส่วนบุคคล

๓. การส่งเสริมเศรษฐกิจและสังคมดิจิทัล PDPA Digital Economy and Society Promotion เสริมสร้างความร่วมมือในประเทศ และต่างประเทศ เพื่อให้เกิดการมีส่วนร่วมในการขับเคลื่อนของทุกภาคส่วนในการสร้างและส่งเสริมเศรษฐกิจและสังคมดิจิทัล รวมทั้งเพิ่มขีดความสามารถด้านการคุ้มครองข้อมูลส่วนบุคคลของประเทศรวมทั้งสร้างเครือข่ายที่ยั่งยืน

๔. การสนับสนุนระบบนิเวศวิจัยและส่งเสริมการใช้เทคโนโลยี PDPA R&D and Technology Adoption สร้างกลไกและระบบนิเวศการวิจัย และระบบนิเวศที่เอื้ออำนวยต่อการใช้ PDPA

Preserving Solutions แบบมุ่งเป้า และเพื่อเพิ่มขีดความสามารถในการแข่งขันเพื่อให้เกิดมูลค่าทางเศรษฐกิจ รวมถึงลดความเสี่ยงในมิติต่าง ๆ

๒.๔ ประเด็นยุทธศาสตร์ภายใต้ แผนแม่บทการส่งเสริมและการคุ้มครองข้อมูลส่วนบุคคลของประเทศ พ.ศ.๒๕๖๗-๒๕๗๐

จากเป้าหมายดังกล่าว นำมาสู่การกำหนดยุทธศาสตร์ได้ ๔ ยุทธศาสตร์ ดังต่อไปนี้

ยุทธศาสตร์ที่ ๑ การเพิ่มประสิทธิภาพการบังคับใช้กฎหมาย (PDPA Effective and Balanced Enforcement)

- **ประเด็นยุทธศาสตร์** มุ่งเน้นการพัฒนามาตรฐาน หลักเกณฑ์ กฎเกณฑ์ เครื่องมือ ตัวชี้วัด และการกำกับดูแลความเป็นส่วนตัวของข้อมูล (Data Privacy Governance) รวมทั้งปรับปรุงกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลเพื่อเป็นการเพิ่มความเข้มแข็งให้แก่การคุ้มครองข้อมูลส่วนบุคคล ส่งเสริม

การดำเนินการต่าง ๆ ภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ซึ่งจะช่วยในการเพิ่มขีดความสามารถในการแข่งขันของประเทศ

- **ตัวชี้วัด**

๑. หน่วยงานภาครัฐและบริษัทในตลาดหลักทรัพย์จำนวน ๑๐๐% ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ได้ในระดับ ๕ ของ Privacy Maturity Model ภายในปี พ.ศ. ๒๕๗๐

๒. วิสาหกิจขนาดกลาง และขนาดย่อม (SME) ที่อยู่ในกลุ่มธุรกิจที่ต้องปฏิบัติงานเกี่ยวกับข้อมูลส่วนบุคคล ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ได้ในระดับ ๓ ของ Privacy Maturity Model ภายในปี พ.ศ. ๒๕๗๐

๓. มีการตรวจสอบการดำเนินการตาม พ.ร.บ. PDPA ของบริษัทต่างประเทศที่ได้จดแจ้งตามกฎหมายแพลตฟอร์มดิจิทัล

๔. มีแนวปฏิบัติที่จำเป็นครบ ๑๐๐% ของกลุ่มอุตสาหกรรม เป้าหมายภายในปี พ.ศ. ๒๕๗๐

๕. ร้อยละ ๕๐ ของหน่วยงานที่ปฏิบัติตาม PDPA ได้ในระดับ ๕ ได้เครื่องหมายรับรอง Trust Mark

๖. มีกลไก เครื่องมือในการตรวจสอบการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และประเมินความเสี่ยงสำหรับภาคเอกชนและหน่วยงานภาครัฐ อาทิ องค์กรปกครองส่วนท้องถิ่น มีการประเมิน และปรับปรุงพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ภายในปี พ.ศ. ๒๕๖๘

- **กลยุทธ์/มาตรการ**

๑. พัฒนาและส่งเสริมมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลเชิงรุกในภาครัฐและภาคเอกชนที่ทัดเทียมสากล แข่งขันได้ สร้างความเชื่อมั่นและสร้างความยั่งยืนทางข้อมูลส่วนบุคคล

๒. ส่งเสริมให้มีการกำกับ การเฝ้าระวัง การตรวจสอบการบังคับใช้กฎหมายอย่างเป็นธรรม มีประสิทธิภาพ โปร่งใส และตรวจสอบได้

๓. ใช้ข้อมูลที่ได้จากการรวบรวมและจากการวิจัยในการสร้าง/ทบทวนงานด้านกฎหมาย มาตรฐาน กฎเกณฑ์ แนวปฏิบัติที่เหมาะสมในแต่ละกลุ่มอุตสาหกรรมเป้าหมาย

- **หน่วยงาน**

๑. สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

๒. สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

๓. สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

๔. สภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย

๕. สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

๖. กรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์

๗. กระทรวงการคลัง

๘. กระทรวงสาธารณสุข

๙. สมาคมหอการค้าไทย สมาคมการค้า สมาพันธ์เอสเอ็มอีไทย

๑๐. สำนักงานคณะกรรมการส่งเสริมการลงทุน

๑๑. สถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน)

๑๒. กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม

๑๓. กระทรวงพาณิชย์

๑๔. กระทรวงการต่างประเทศ

๑๕. หน่วยงานกำกับดูแล* (Regulators)

๑๖. สถาบันวิจัย สถาบันการศึกษา

๑๗. หน่วยงานที่ลงนาม MOU

๑๘. หน่วยงานความร่วมมือต่างประเทศ

ยุทธศาสตร์ที่ ๒ การพัฒนากำลังคนและสร้างความเชื่อมั่น (PDPA Knowledge and Trust Enhancement)

- ประเด็นยุทธศาสตร์ มุ่งเน้นการเสริมสร้างกำลังคน สร้างความรู้ ความเข้าใจ ความตระหนักรู้ ความเชื่อมั่นเท่าทันการเปลี่ยนแปลงด้านข้อมูลส่วนบุคคลอย่างเท่าเทียม ด้วยกลไกการให้ความรู้แบบมุ่งเป้า การรับรองด้านทักษะ การประชาสัมพันธ์ การป้องกัน และรูปแบบการแก้ปัญหา รวมทั้งความพร้อมต่อการเปลี่ยนแปลงด้านข้อมูลส่วนบุคคล เป็นยุทธศาสตร์ที่สำคัญในการขับเคลื่อนการดำเนินงานด้านการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย จำเป็นต้องอาศัยความร่วมมือจากทุกภาคส่วนและดำเนินการอย่างจริงจังและต่อเนื่อง เพื่อให้ประชาชน รัฐและเอกชนสามารถใช้ประโยชน์จากเทคโนโลยีดิจิทัลได้อย่างปลอดภัยและมีประสิทธิภาพ

- ตัวชี้วัด

๑. มีมาตรฐานหลักสูตรอบรมสำหรับกลุ่ม DPO, CIO ของหน่วยงานที่เป็น Data Controller/Processor ที่สามารถวัด/ประเมินผลได้ และมีระบบการรับรอง (Certification)

๒. ประชาชนมีความเชื่อมั่นในการใช้บริการที่ต้องมีการใช้ข้อมูลส่วนบุคคลไม่น้อยกว่าร้อยละ ๘๐

๓. คะแนนเฉลี่ยการรู้เท่าทันสื่อสารสนเทศและการเข้าใจดิจิทัลในด้านการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยมีอันดับที่ดีขึ้น

๔. จำนวนข้อหารือที่มีผลกระทบสูงจากภาคเอกชน และภาครัฐมีสัดส่วนที่ลดลงจากปีฐาน

๕. มีหลักสูตร DPO,CIOในฐานข้อมูลกลางเพิ่มขึ้น

๖. มีข้อมูล DPO ในฐานข้อมูลกลางเพิ่มขึ้น

- กลยุทธ์/มาตรการ

๑. สร้างความรู้ และความตระหนักแก่ภาคประชาชน ภาคเอกชน ภาครัฐให้สามารถเข้าถึง เข้าใจอย่างเท่าทัน เท่าเทียม และเป็นการเรียนรู้ตลอดชีวิต

๒. ผลิต และพัฒนาหลักสูตรและบุคลากรด้านข้อมูลส่วนบุคคล Data Privacy, Personal Data Protection ให้เพียงพอ ตรงความต้องการ และเท่าทันการเปลี่ยนแปลงของเทคโนโลยี

๓. สร้างเครือข่ายการประชาสัมพันธ์ในรูปแบบต่าง ๆ ทั้ง Online และ Offline ที่ทันสมัย เข้าถึงกลุ่มเป้าหมายที่แตกต่างกันทั้งพื้นที่และบริบท

๔. พัฒนากลใกรูปแบบบการเรียนรู้ผ่าน PDPA Center ที่ยั่งยืนและเข้าถึงประชาชนแต่ละช่วงวัยและกลุ่มอุตสาหกรรมเป้าหมายหลัก

- หน่วยงาน

๑. สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

๒. สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

๓. สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัย ไซเบอร์เบอร์แห่งชาติ

๔. กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม

๕. กระทรวงศึกษาธิการ

๖. กระทรวงมหาดไทย

๗.สมาคมหอการค้าไทย สมาคมการค้า สมาพันธ์เอสเอ็มอีไทย

๘. สมาคมผู้สื่อข่าวออนไลน์ สมาคมนักข่าวแห่งประเทศไทย

๙. Platform ด้านสื่อดิจิทัลออนไลน์

๑๐. สถาบันคุณวุฒิวิชาชีพ (องค์การมหาชน)

๑๑. สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ

๑๒. สำนักงานคณะกรรมการพัฒนาระบบราชการ

๑๓. สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

๑๔. สำนักงานคณะกรรมการพัฒนาระบบราชการ

๑๕. สำนักงานคณะกรรมการข้าราชการพลเรือน

๑๖. สำนักงบประมาณ

๑๗. สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ

๑๘. เครือข่ายการศึกษา

ยุทธศาสตร์ที่ ๓ การส่งเสริมเศรษฐกิจและสังคมดิจิทัล (PDPA Digital Economy and Society Promotion)

- ประเด็นยุทธศาสตร์ เสริมสร้างความร่วมมือในประเทศ และต่างประเทศ เพื่อให้เกิดการมีส่วนร่วมในการขับเคลื่อนของทุกภาคส่วนในการสร้างและส่งเสริมเศรษฐกิจและสังคมดิจิทัล รวมทั้งเพิ่มขีดความสามารถด้านการคุ้มครองข้อมูลส่วนบุคคลของประเทศ รวมทั้งสร้างเครือข่ายที่ยั่งยืน

- ตัวชี้วัด

๑. ประเทศไทยมีคะแนนด้านความสามารถด้านการคุ้มครองข้อมูลส่วนบุคคลของประเทศ (Privacy Index) ในด้าน Data Privacy/ Personal Data Protection/ Trusted Data อยู่ในกลุ่ม ๓๐ อันดับแรกของการจัดอันดับนานาชาติ

๒. มูลค่าการลงทุนในอุตสาหกรรมดังที่มีการที่มีการใช้ส่านบุตรอย่างมีธรรมาภิบาลเพิ่มมากขึ้น ร้อยละ ๕ จากปีฐาน

๓. จำนวนกรณีการละเมิดการคุ้มครองข้อมูลส่วนบุคคลลดลดลงร้อยละ ๕ จากปีฐาน

- กลยุทธ์/มาตรการ

๑. พัฒนาคะแนนด้านตัวชี้วัดความสามารถด้านการคุ้มครองข้อมูลส่วนบุคคลของประเทศ (Privacy Index) และทำการสำรวจความพร้อมของประเทศร่วมกับหน่วยงานรัฐและภาคอุตสาหกรรม

๒. สร้างเครือข่ายกับหน่วยงานกำกับดูแล (Regulators), ภาคอุตสาหกรรมในการที่จะดำเนินการสำรวจ/ตรวจ/ประเมิน ด้านการคุ้มครองข้อมูลส่วนบุคคลในระดับอุตสาหกรรม โดยการใช้ Priacy Maturity Model who Privacy Maturity Assessment Framework

๓. มีการดำเนินการความร่วมมือสร้างเครือข่าย และกำหนดแผนการดำเนินงานร่วมกับหน่วยงานกำกับดูแลด้านการคุ้มครองข้อมูลูส่วนบุคคล และหน่วยงานด้านส่งเสริมงานด้านข้อมูลส่วนบุคคลระหว่างประเทศ รวมทั้งภาคอุตสาหกรรมในประเทศและต่างประเทศ

๔. เร่งสร้างมูลค่าเพิ่มอุตสาหกรรมดิจิทัลที่รักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้ก้าวสู่อุตสาหกรรมใหม่ที่แข่งขันได้ในตลาดโลก

- หน่วยงาน

๑. สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
๒. สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
๓. สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
๔. สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
๕. กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม
๖. กระทรวงศึกษาธิการ
๗. กระทรวงการคลัง
๘. กระทรวงสาธารณสุข
๙. สมาคมหอการค้าไทย สมาคมการค้า สมาพันธ์เอสเอ็มอีไทย
๑๐. สำนักงานคณะกรรมการส่งเสริมการลงทุน
๑๑. ภาคอุตสาหกรรม
๑๒. สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
๑๓. สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
๑๔. สำนักงานคณะกรรมการกำกับหลักทรัพย์ตลาดหลักทรัพย์
๑๕. สถาบันคุณวุฒิวิชาชีพ (องค์การมหาชน)
๑๖. กระทรวงพาณิชย์
๑๗. กระทรวงการต่างประเทศ
๑๘. กรมเจรจาการค้าระหว่างประเทศ

ยุทธศาสตร์ที่ ๔ การสนับสนุนระบบนิเวศวิจัยและส่งเสริมการใช้เทคโนโลยี (PDPA R&D and Technology Adoption)

- ประเด็นยุทธศาสตร์ สร้างกลไกระบบนิเวศวิจัย และระบบนิเวศที่เอื้ออำนวยต่อการใช้ PDPA Preserving Solutions แบบมุ่งเป้า และเพื่อเพิ่มขีดความสามารถในการแข่งขันเพื่อให้เกิดมูลค่าทางเศรษฐกิจรวมถึงการลดความเสี่ยงในด้านต่าง ๆ ซึ่งถือว่าเป็นกำลังสำคัญต่อการขับเคลื่อนนวัตกรรมด้านการคุ้มครองข้อมูลส่วนบุคคล นอกจากนี้การเปิดโอกาสให้นักวิจัยและผู้ประกอบการสามารถสร้าง

นวัตกรรมที่ใช้ข้อมูลส่วนบุคคลได้อย่างปลอดภัยและเป็นธรรม โดยไม่ถูกขัดขวางจากนโยบายกฎหมาย จะทำให้ประเทศไทยมีศักยภาพในการแข่งขันระดับนานาชาติเห็นขึ้น

- ตัวชี้วัด

๑. จำนวน Sandbox ที่ดำเนินการร่วมกับหน่วยงานภาคอุตสาหกรรม ปีละ ๑ sandbox

๒. มีเครือข่ายความร่วมมือทางวิชาการ งานวิจัยและนวัตกรรม ระหว่างกระทรวงต่าง ๆ และเชื่อมโยงกับภาคเอกชน รวมทั้งระดับนานาชาติ

๓. จำนวนบริการ (PDPA Service) ในระบบบริการกลางเพิ่มขึ้นอย่างน้อย ๒ บริการต่อปี

๔. มีภาครัฐ ภาคอุตสาหกรรม ประยุกต์ใช้ระบบ/เครื่องมือต่าง ๆ ในสัดส่วนร้อยละ ๒๕ จากปีฐาน

๕. มีเครื่องมือในด้านการสนับสนุนการพัฒนาระบบเชื่อมต่อบริการระหว่างระบบบริการกลาง กับระบบบริการของเอกชน อย่างน้อย ๒ เครื่องมือ/ปี

๖. มีการจัดงาน PDPA Summit ระดับนานาชาติ

- กลยุทธ์/มาตรการ

๑. สร้างกลไกในการพัฒนาระบบนิเวศวิจัยและนวัตกรรมทางด้าน privacy-preserving solution เช่น Privacy Enhancing Technologies (PET), Data Privacy และ Data security เชื่อมโยงหน่วยงานในประเทศ และประสานสู่นานาชาติ

๒. สร้างระบบกลางข้อมูลด้าน Data Privacy/ Personal Data Protection/ Trusted Data สำหรับการใช้ การเชื่อมโยง การทำงานวิจัย และสร้างนวัตกรรมที่เกี่ยวข้อง รวมทั้งเชื่อมต่อกับระบบบริการของเอกชนได้อย่างมีประสิทธิภาพ

๓. ยกระดับมาตรฐานระบบบริการกลาง PDPA Services ให้สามารถแข่งขันในระดับสากลได้

๔. ส่งเสริมให้มีการทำงานร่วมกันกับภาครัฐ ภาคอุตสาหกรรม ทั้งในและต่างประเทศ ในรูปแบบต่าง ๆ ที่ตรงกับความต้องการของหน่วยงานนั้น ๆ เพื่อช่วยให้การประยุกต์ใช้บริการอย่างกว้างขวาง และยกระดับความสามารถในการแข่งขันได้อย่างยั่งยืน รวมทั้งร่วมจัดงาน PDPA Summit

- หน่วยงาน

๑. สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

๒. สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

๓. สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

๔. สภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย

๕. สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

๖. กรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์

๗. กระทรวงการคลัง

๘. กระทรวงสาธารณสุข

๙. สมาคมหอการค้าไทย สมาคมการค้า สมาพันธ์เอสเอ็มอีไทย

๑๐. สำนักงานคณะกรรมการส่งเสริมการลงทุน

๑๑. สถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน)

๑๒. กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม

๑๓. กระทรวงพาณิชย์

๑๔. กระทรวงการต่างประเทศ

๑๕. หน่วยงานกำกับดูแล* (Regulators)
๑๖. สถาบันวิจัย สถาบันการศึกษา
๑๗. หน่วยงานที่ลงนาม MOU
๑๘. หน่วยงานความร่วมมือต่างประเทศ

๒. สาระสำคัญของแผนปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๙ กรมการแพทย์แผนไทยและการแพทย์ทางเลือก

กรมการแพทย์แผนไทยและการแพทย์ทางเลือกมีภารกิจสำคัญในการให้บริการด้านสาธารณสุข การศึกษาวิจัย และการส่งเสริมภูมิปัญญาการแพทย์แผนไทย ซึ่งมีความจำเป็นต้องเกี่ยวข้องกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลจำนวนมหาศาล ทั้งในส่วนของข้อมูลบุคลากร ข้อมูลผู้รับบริการ (คนไข้) และผู้มีส่วนได้ส่วนเสีย ข้อมูลเหล่านี้ถือเป็นสินทรัพย์ที่มีค่าและมีความอ่อนไหวสูง โดยเฉพาะข้อมูลด้านสุขภาพซึ่งจำเป็นต้องได้รับความคุ้มครองตามมาตรฐานสากล

เพื่อให้การดำเนินงานของกรมฯ สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) และแผนแม่บทการส่งเสริมและการคุ้มครองข้อมูลส่วนบุคคลของประเทศ พ.ศ.๒๕๖๗-๒๕๗๐ กรมจึงได้จัดทำแผนปฏิบัติการฉบับนี้ขึ้นโดยมีสาระสำคัญครอบคลุม ๑๐ มิติ ดังนี้

มิติที่ ๑ การกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคล (Oversight)
มิติที่ ๒ นโยบายและแนวปฏิบัติ (Policies and procedures)
มิติที่ ๓ การอบรมและการสร้างความตระหนัก (Training and awareness)
มิติที่ ๔ สิทธิของเจ้าของข้อมูลส่วนบุคคล (Individual’s rights)
มิติที่ ๕ ประกาศความเป็นส่วนตัว (Transparency)
มิติที่ ๖ การจัดทำบันทึกรายกิจกรรมการประมวลผลข้อมูลส่วนบุคคลและการกำหนดฐานทางกฎหมาย (ROPA & lawful basis)
มิติที่ ๗ สัญญาและการส่งหรือโอนข้อมูลส่วนบุคคล (Contracts and data sharing)
มิติที่ ๘ การบริหารจัดการความเสี่ยง (Risks)
มิติที่ ๙ การรักษาความมั่นคงปลอดภัยของข้อมูล (Data security)
มิติที่ ๑๐ การรับมือต่อเหตุการละเมิดข้อมูลส่วนบุคคล (Breach response and monitor)

๑. การกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคล (Oversight)

วัตถุประสงค์

การกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคลมีวัตถุประสงค์หลักเพื่อวางรากฐานทางกฎหมายและจริยธรรมให้แก่องค์กร โดยมุ่งเน้นการสร้างระบบการบริหารจัดการข้อมูลที่สอดคล้องกับมาตรฐานพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ เพื่อให้การเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคลเป็นไปอย่างจำกัดเท่าที่จำเป็นและมีฐานทางกฎหมายรองรับอย่างชัดเจน ทั้งนี้เพื่อเป็นการคุ้มครองสิทธิและเสรีภาพขั้นพื้นฐานของเจ้าของข้อมูล มิให้ถูกละเมิดหรือนำข้อมูลไปใช้ในทางมิชอบ

แนวทางการปฏิบัติ

๑. จัดทำตัวชี้วัด (KPI) เช่น การจัดการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล การแก้ไข Data breach การปฏิบัติตามกฎหมายและประกาศฯ ด้านการคุ้มครองข้อมูลส่วนบุคคล เป็นต้น เพื่อวัดผลประสิทธิภาพในการปฏิบัติงานของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

๒. ประเมินวัดผลประสิทธิภาพในการปฏิบัติงานของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) อย่างต่อเนื่องเป็นประจำ (อย่างน้อยปีละ ๑ ครั้ง)

๓. จัดให้มีการทบทวนผลจากการวัดประสิทธิภาพ เพื่อนำมาวางแผนพัฒนาปรับปรุงกระบวนการ เพิ่มเติมเครื่องมือ หรือทรัพยากรอื่น ๆ ที่จำเป็นให้กับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

๔. มีการนำเสนอแผนพัฒนาปรับปรุงกระบวนการให้บริหารรับทราบและอนุมัติ

๕. มีการติดตามแผนพัฒนาปรับปรุงกระบวนการอย่างต่อเนื่อง

เป้าหมาย และตัวชี้วัด ค่าเป้าหมาย

เป้าประสงค์	ตัวชี้วัด	ค่าเป้าหมาย ปี ๒๕๖๙
การจัดการสิทธิเจ้าของข้อมูล	ร้อยละของคำร้องขอใช้สิทธิที่ดำเนินการเสร็จสิ้นภายในระยะเวลาที่กฎหมายกำหนด (๓๐ วัน)	๑๐๐%
การตอบสนองต่อเหตุละเมิด	ระยะเวลาที่ใช้ในการรายงานเหตุละเมิดต่อคณะกรรมการฯ นับแต่ทราบเหตุ (ต้องไม่เกิน ๗๒ ชั่วโมง)	๑๐๐% ของเหตุที่พบ
การปฏิบัติตามกฎหมาย	จำนวนข้อผิดพลาดหรือข้อร้องเรียนจากหน่วยงานกำกับดูแล (สคส.)	๐ รายการ
การประเมินประสิทธิภาพ	ผลคะแนนการประเมินการปฏิบัติงานของ DPO โดยผู้บริหารหรือคณะกรรมการ	ไม่น้อยกว่า ๘๐% (ระดับดีมาก)
การพัฒนาและปรับปรุง	จำนวนแผนพัฒนา/ปรับปรุงกระบวนการที่ได้รับการอนุมัติและนำไปปฏิบัติจริง	อย่างน้อย ๑ แผน/ปี

๒. นโยบายและแนวปฏิบัติ (Policies and procedures)

วัตถุประสงค์

การกำหนดนโยบายและแนวปฏิบัติมีวัตถุประสงค์หลัก เพื่อบริหารจัดการข้อมูลส่วนบุคคลให้มีความชัดเจนและเป็นลายลักษณ์อักษร เพื่อใช้เป็นคู่มือมาตรฐานให้แก่บุคลากรทุกระดับในการปฏิบัติหน้าที่ได้อย่างถูกต้องตามที่กฎหมายกำหนด โดยมุ่งเน้นการสร้างกระบวนการจัดการข้อมูลที่มีธรรมาภิบาลตั้งแต่ขั้นตอนการเก็บรวบรวม การจัดเก็บรักษา การนำไปใช้ประโยชน์ ตลอดจนการทำลายข้อมูลเมื่อสิ้นสุดความจำเป็น ทั้งนี้เพื่อให้มั่นใจว่ากิจกรรมการประมวลผลข้อมูลส่วนบุคคลทั้งหมดขององค์กรตั้งอยู่บนฐานทางกฎหมายที่เหมาะสม มีการแจ้งวัตถุประสงค์ที่โปร่งใส และมีการขอความยินยอมอย่างถูกต้องในกรณีที่จำเป็นนอกจากนี้ แนวปฏิบัติที่ชัดเจนยังมีเป้าหมายเพื่อเป็นเกราะป้องกันทางกฎหมายและลดความเสี่ยงจากการตีความที่ผิดพลาด โดยการระบุขั้นตอนการทำงานอย่างเป็นลำดับขั้น ซึ่งครอบคลุมถึงมาตรการรักษาความมั่นคงปลอดภัยเชิงเทคนิคและเชิงบริหารจัดการ เพื่อป้องกันการเข้าถึงข้อมูลโดยมิชอบและการรั่วไหลของข้อมูลส่วนบุคคล ขณะเดียวกันยังเป็นการวางรากฐานในการตอบสนองต่อเหตุการละเมิดและข้อร้องเรียนจากเจ้าของข้อมูลได้อย่างมีประสิทธิภาพและทันท่วงที

แนวทางการปฏิบัติ

๑. จัดให้มีการทบทวนนโยบายและกระบวนการคุ้มครองข้อมูลส่วนบุคคลอย่างน้อยปีละ ๑ ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงที่สำคัญ

๒. จัดให้มีการทบทวนผลจากการวัดประสิทธิภาพ เพื่อนำมาปรับปรุงนโยบายและกระบวนการด้านการคุ้มครองข้อมูลส่วนบุคคลให้มีประสิทธิภาพมากขึ้น ตามแนวทางปฏิบัติที่ดีด้านการคุ้มครองข้อมูลส่วนบุคคล

เป้าหมาย และตัวชี้วัด ค่าเป้าหมาย

เป้าประสงค์	ตัวชี้วัด	ค่าเป้าหมาย ปี ๒๕๖๙
การรักษาความทันสมัยของนโยบาย	จำนวนครั้งที่มีการทบทวนนโยบายและแนวปฏิบัติ (Privacy Policy/Manual) ให้สอดคล้องกับกฎหมายปัจจุบัน	**อย่างน้อย ๑ ครั้ง/ปี** (หรือทุกครั้งที่มีการเปลี่ยนแปลง)
การทบทวนกระบวนการทำงาน	ร้อยละของกระบวนการคุ้มครองข้อมูลส่วนบุคคลที่ได้รับการตรวจสอบและปรับปรุง (Update) ตามบันทึกรายการประมวลผล (ROPA)	**๑๐๐%** ของกระบวนการหลัก
การนำผลประเมินมาปรับปรุง	จำนวนข้อเสนอแนะจากการวัดประสิทธิภาพ (KPIs เดิม) ที่ถูกนำมาปรับปรุงนโยบาย/กระบวนการอย่างเป็นรูปธรรม	**๑๐๐%** ของข้อเสนอแนะที่สำคัญ
ความสอดคล้องกับแนวปฏิบัติที่ดี	ระดับความสำเร็จในการปรับปรุงกระบวนการให้สอดคล้องกับมาตรฐานสากล หรือแนวทางที่ สคส. ประกาศเพิ่มเติม	**ระดับดีเยี่ยม** (ไม่มีข้อบกพร่องรุนแรง)

๓. การอบรมและการสร้างความตระหนัก (Training and awareness)

วัตถุประสงค์

การดำเนินงานด้านการอบรมและการสร้างความตระหนักมีวัตถุประสงค์ประการสำคัญ เพื่อปลูกฝังความรู้ความเข้าใจที่ถูกต้องให้แก่บุคลากรทุกระดับ เกี่ยวกับหลักการและเจตนารมณ์ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ โดยมุ่งเน้นให้บุคลากรมีความสามารถในการจำแนกประเภทข้อมูลส่วนบุคคล และเข้าใจถึงบทบาทหน้าที่ความรับผิดชอบของตนในฐานะผู้ปฏิบัติงานที่ต้องเกี่ยวข้องกับข้อมูลส่วนบุคคลในทุกมิติ ทั้งนี้เพื่อให้เกิดความตระหนักถึงคุณค่าและศักดิ์ศรีความเป็นมนุษย์ของเจ้าของข้อมูล และสามารถนำหลักเกณฑ์ตามกฎหมายไปประยุกต์ใช้ในการปฏิบัติงานจริงได้อย่างถูกต้องแม่นยำ และเป็นไปในทิศทางเดียวกันทั่วทั้งองค์กร นอกจากด้านวิชาการแล้ว กระบวนการสร้างความตระหนักรู้ยังมีเป้าหมายเพื่อเสริมสร้างทักษะในการเฝ้าระวังและการตอบสนองต่อภัยคุกคามทางไซเบอร์ที่อาจนำไปสู่การรั่วไหลของข้อมูล โดยมุ่งหวังให้บุคลากรเกิดความระมัดระวังในการใช้งานระบบสารสนเทศและมีจิตสำนึกในการรักษาความลับของข้อมูลเป็นสำคัญ การอบรมอย่างต่อเนื่องจะช่วยลดความเสี่ยงที่เกิดจากความประมาทเลินเล่อหรือความรู้เท่าไม่ถึงการณ์ (Human Error) ซึ่งเป็นสาเหตุหลักของการละเมิดข้อมูลส่วนบุคคลในปัจจุบัน

แนวทางการปฏิบัติ

๑. จัดให้มีการทบทวนการอบรมและสร้างความตระหนักเรื่องการปกป้องข้อมูลส่วนบุคคลให้มีความถูกต้อง สอดคล้องกับนโยบายและกลยุทธ์ขององค์กรในการคุ้มครองข้อมูลส่วนบุคคล รวมถึงพระราชบัญญัติและประกาศฯ ด้านการคุ้มครองข้อมูลส่วนบุคคล

๒. องค์กรมีการทบทวนการอบรมและสร้างความตระหนักเรื่องการปกป้องข้อมูลส่วนบุคคลอยู่เป็นประจำ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงของนโยบายและกระบวนการด้านการคุ้มครองข้อมูลส่วนบุคคล

๓. จัดให้มีการประเมินการจัดอบรมและการสร้างความตระหนักเรื่องปกป้องข้อมูลส่วนบุคคล เช่น มีแบบทดสอบหลังจากการอบรม เป็นต้น โดยใช้ผลประเมินเป็นตัวชี้วัด (KPI) ถึงประสิทธิภาพของการจัดอบรมและการสร้างความตระหนัก

๔. ประเมินการจัดอบรมและการสร้างความตระหนักเรื่องการปกป้องข้อมูลส่วนบุคคลทุกครั้ง

๕. พิจารณาภัยคุกคามใหม่ ๆ ที่อาจเกิดขึ้น เพื่อนำไปปรับปรุงและพัฒนาเนื้อหาที่ใช้ในการฝึกอบรมและการสร้างความตระหนักเรื่องปกป้องข้อมูลส่วนบุคคล

๖. จัดให้มีการปรับปรุงและพัฒนาเนื้อหาที่ใช้ในการฝึกอบรมและการสร้างความตระหนักเรื่องการปกป้องข้อมูลส่วนบุคคล เมื่อมีพระราชบัญญัติและประกาศฯ ด้านการคุ้มครองข้อมูลส่วนบุคคลใหม่

เป้าหมาย และตัวชี้วัด ค่าเป้าหมาย

เป้าประสงค์	ตัวชี้วัด	ค่าเป้าหมาย ปี ๒๕๖๙
การครอบคลุมของการอบรม	ร้อยละของพนักงานทั้งหมดที่เข้ารับการอบรมด้าน PDPA และการรักษาความมั่นคงปลอดภัยข้อมูล	๑๐๐%
ประสิทธิภาพการเรียนรู้	ร้อยละของเจ้าหน้าที่ที่ผ่านเกณฑ์การทดสอบหลังการอบรม (Post-test) ตามคะแนนที่กำหนด (เช่น ๘๐%)	ไม่น้อยกว่า ๙๐%
ความทันสมัยของเนื้อหา	จำนวนครั้งในการปรับปรุงเนื้อหาหลักสูตรให้สอดคล้องกับกฎหมายใหม่ ภัยคุกคามใหม่ หรือนโยบายที่เปลี่ยนไป	อย่างน้อย ๑ ครั้ง/ปี (หรือเมื่อมีการเปลี่ยนแปลงสำคัญ)
ความถี่ในการสร้างความตระหนักรู้	จำนวนกิจกรรมสร้างความตระหนักรู้ (เช่น Newsletter, Infographic, หรือ Mini-quiz) นอกเหนือจากการอบรมใหญ่	อย่างน้อย ๑ ครั้ง/ไตรมาส
การประเมินผลความพึงพอใจ	คะแนนเฉลี่ยความพึงพอใจต่อหลักสูตรและวิทยากรจากผู้เข้ารับการอบรม	อย่างน้อย ๑ ครั้ง/ไตรมาส

๔. สิทธิของเจ้าของข้อมูลส่วนบุคคล (Individual's rights)

วัตถุประสงค์

การคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล มุ่งเน้นการวางกลไกที่เอื้ออำนวยให้เจ้าของข้อมูลสามารถตรวจสอบ ติดตาม และจัดการข้อมูลของตนเองได้อย่างอิสระและเป็นธรรม ไม่ว่าจะเป็นสิทธิในการเข้าถึงข้อมูล สิทธิในการแก้ไขข้อมูลให้ถูกต้อง สิทธิในการคัดค้านการประมวลผล หรือสิทธิในการขอให้ลบทำลายข้อมูลเมื่อสิ้นสุดความจำเป็น ทั้งนี้เพื่อให้มั่นใจว่าองค์กรปฏิบัติหน้าที่ในฐานะผู้ควบคุมข้อมูลด้วยความเคารพในความเป็นส่วนตัวและศักดิ์ศรีความเป็นมนุษย์ สอดคล้องตามเจตนารมณ์ของกฎหมายที่ต้องการป้องกันการนำข้อมูลไปใช้ในลักษณะที่ละเมิดต่อเจ้าของข้อมูลโดยมิชอบ

นอกจากนี้ การบริหารจัดการสิทธิยังมีวัตถุประสงค์เพื่อสร้างระบบการสื่อสารที่โปร่งใสและเข้าถึงได้ง่าย ระหว่างองค์กรและเจ้าของข้อมูล โดยการกำหนดขั้นตอนและช่องทางการใช้สิทธิที่ชัดเจน ไม่ซับซ้อน

และมีการตอบสนองภายในระยะเวลาที่กฎหมายกำหนด กระบวนการดังกล่าวมีเป้าหมายเพื่อลดข้อพิพาทและสร้างความเข้าใจอันดีต่อกัน ซึ่งจะช่วยสร้างบรรยากาศแห่งความไว้วางใจในการให้บริการ

แนวทางการปฏิบัติ

๑. จัดทำตัวชี้วัด (KPI) เช่น % ในการจัดการคำขอใช้สิทธิจากเจ้าของข้อมูลส่วนบุคคลได้ตามเวลาเพื่อวัดผลประสิทธิภาพการจัดการคำขอใช้สิทธิ จากเจ้าของข้อมูลส่วนบุคคล

๒. ประเมินวัดผลการจัดการคำขอใช้สิทธิจากเจ้าของข้อมูลส่วนบุคคล อย่างต่อเนื่องเป็นประจำ (อย่างน้อยปีละ ๑ ครั้ง)

๓. ทบทวนผลจากการวัดประสิทธิภาพ เพื่อนำมาปรับปรุงนโยบายและกระบวนการการจัดการกับคำขอใชสิทธิจากเจ้าของข้อมูลส่วนบุคคลให้มีประสิทธิภาพมากขึ้น

เป้าหมาย และตัวชี้วัด ค่าเป้าหมาย

เป้าประสงค์	ตัวชี้วัด	ค่าเป้าหมาย ปี ๒๕๖๙
ประสิทธิภาพการตอบสนองสิทธิ	ร้อยละของคำขอใช้สิทธิที่ดำเนินการเสร็จสิ้นภายในระยะเวลาที่กฎหมายกำหนด (ไม่เกิน ๓๐ วัน)	๑๐๐%
ความถูกต้องในการดำเนินการ	ร้อยละของคำขอที่ดำเนินการได้ถูกต้องตามประเภทสิทธิที่ร้องขอ (เช่น การลบ, การแก้ไข, การขอเข้าถึง)	๑๐๐%
การติดตามและประเมินผล	จำนวนครั้งในการประเมินและสรุปรายงานผลการจัดการคำขอเสนอต่อผู้บริหาร	อย่างน้อย ๑ ครั้ง/ปี
การพัฒนากระบวนการ	จำนวนข้อบกพร่องหรือคอขวด ที่พบจากการทบทวนและได้รับการแก้ไข/ปรับปรุงนโยบาย	**ทุกประเด็นที่พบ** (ตามแผนปรับปรุง)
ความพึงพอใจของเจ้าของข้อมูล	คะแนนความพึงพอใจของเจ้าของข้อมูลส่วนบุคคลต่อขั้นตอนการใช้สิทธิ	ไม่น้อยกว่า ๘๐%

๕. ประกาศความเป็นส่วนตัว (Transparency)

วัตถุประสงค์

การจัดทำการประกาศความเป็นส่วนตัวมีวัตถุประสงค์หลักเพื่อสร้าง "ความโปร่งใส" (Transparency) ในทุกกระบวนการจัดการข้อมูลส่วนบุคคล โดยมุ่งเน้นการสื่อสารข้อมูลที่จำเป็นให้แก่เจ้าของข้อมูลได้รับทราบอย่างชัดเจน ครบถ้วน และเข้าใจง่าย ตั้งแต่ก่อนหรือในขณะเก็บรวบรวมข้อมูล ไม่ว่าจะเป็นรายละเอียดเกี่ยวกับประเภทของข้อมูลที่จัดเก็บ วัตถุประสงค์ในการนำไปใช้งาน ระยะเวลาในการจัดเก็บรักษา ตลอดจนการเปิดเผยข้อมูลแก่บุคคลที่สาม ทั้งนี้เพื่อให้เจ้าของข้อมูลสามารถตัดสินใจเกี่ยวกับการให้ข้อมูลของตนบนพื้นฐานของข้อมูลที่ถูกต้องและเพียงพอ สอดคล้องตามหลักการพื้นฐานของกฎหมายที่ต้องการให้การประมวลผลข้อมูลเป็นไปโดยชอบธรรมและสามารถตรวจสอบได้

นอกจากนี้ ประกาศความเป็นส่วนตัวยังมีเป้าหมายเพื่อเป็นเครื่องมือในการยืนยันสิทธิของเจ้าของข้อมูล และระบุช่องทางการติดต่อผู้ควบคุมข้อมูลหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) อย่างเป็นรูปธรรม เพื่อให้เจ้าของข้อมูลเกิดความมั่นใจว่าข้อมูลของตนจะถูกนำไปใช้ตามขอบเขตที่แจ้งไว้เท่านั้น และจะไม่ถูกนำไปใช้ในลักษณะที่เป็นการละเมิดความเป็นส่วนตัวหรือนอกเหนือจากความคาดหมาย

โดยชอบธรรม การประกาศนโยบายที่ชัดเจนยังช่วยลดความคลุมเครือและป้องกันข้อพิพาททางกฎหมายที่อาจเกิดขึ้นจากการสื่อสารที่คลาดเคลื่อน

แนวทางการปฏิบัติ

๑. เพิ่มรายละเอียดให้ Privacy notice ขององค์กรมีการแจ้งประเภทของบุคคลหรือหน่วยงานที่อาจได้รับข้อมูลส่วนบุคคล รวมถึงรายละเอียดเกี่ยวกับการส่งหรือโอนข้อมูลไปยังต่างประเทศ ตามมาตรา ๒๓ ข้อ ๔ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๒. เพิ่มขั้นตอนการทบทวน Privacy notice ที่แจ้งกับเจ้าของข้อมูลว่าสามารถครอบคลุมทุกกิจกรรมการประมวลผลทั้งหมดที่บันทึกไว้ในเอกสาร ROPA: Records of Processing Activities

๓. กระบวนการทบทวนต้องดำเนินการอยู่เป็นประจำ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

๔. จัดทำตัวชี้วัด เช่น % ในการรับทราบข้อมูลของ Privacy notice เป็นต้น เพื่อวัดผลประสิทธิภาพใน การแจ้ง Privacy notice

๕. ประเมินวัดผลประสิทธิภาพของการแจ้ง Privacy notice อย่างต่อเนื่องเป็นประจำ (อย่างน้อยปีละ ๑ ครั้ง)

๖. จัดให้มีการทบทวนผลจากการวัดประสิทธิภาพ เพื่อ นำมาปรับปรุงแนวทางการแจ้ง Privacy notice ให้มีประสิทธิภาพมากขึ้น เช่น การใช้เทคโนโลยีเข้ามาช่วยเหลือ เป็นต้น

เป้าหมาย และตัวชี้วัด ค่าเป้าหมาย

เป้าประสงค์	ตัวชี้วัด	ค่าเป้าหมาย ปี ๒๕๖๙
ความครบถ้วนตามกฎหมาย	ร้อยละของ Privacy Notice ที่มีการระบุประเภทผู้รับข้อมูลและรายละเอียดการโอนข้อมูลไปต่างประเทศครบถ้วน	๑๐๐%
ความสอดคล้องกับกิจกรรมจริง	ร้อยละของกิจกรรมการประมวลผลใน ROPA ที่มี Privacy Notice ครอบคลุมครบทุกกิจกรรม	๑๐๐%
การทบทวนตามรอบระยะเวลา	จำนวนครั้งในการทบทวนความล้าสมัยของ Privacy Notice และกระบวนการที่เกี่ยวข้อง	อย่างน้อย ๑ ครั้ง/ปี (หรือเมื่อมีการเปลี่ยนแปลง)
ประสิทธิภาพในการแจ้ง	ร้อยละของเจ้าของข้อมูลที่รับทราบ/เข้าถึง Privacy Notice (เช่น วัดจากอัตราการคลิกอ่าน หรือการเซ็นรับทราบ)	ไม่น้อยกว่า ๙๐%
การพัฒนากระบวนการด้วยเทคโนโลยี	จำนวนแนวทางหรือเทคโนโลยีใหม่ที่นำมาใช้เพื่อเพิ่มประสิทธิภาพในการแจ้ง (เช่น QR Code, Consent Portal, หรือ Automated Notice)	อย่างน้อย ๑ รายการ/ปี

๖. การจัดทำบันทึกรายกิจกรรมการประมวลผลข้อมูลส่วนบุคคลและการกำหนดฐานทางกฎหมาย (ROPA & lawful basis)

วัตถุประสงค์

การจัดทำบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (ROPA) มีวัตถุประสงค์หลักเพื่อสร้างระบบการบริหารจัดการข้อมูลที่สามารถตรวจสอบได้ โดยมุ่งหวังให้องค์กรมีคลังข้อมูลที่รวบรวมรายละเอียดของกิจกรรมการประมวลผลทั้งหมดอย่างเป็นระบบ ตั้งแต่แหล่งที่มาของข้อมูล ประเภทของข้อมูล วัตถุประสงค์ในการใช้งาน ไปจนถึงการส่งต่อหรือโอนข้อมูลไปยังบุคคลภายนอก บันทึกนี้เปรียบเสมือนแผนที่นำทางที่ช่วยให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถมองเห็นภาพรวมของวงจรชีวิตข้อมูล (Data Life Cycle) ภายในองค์กรได้อย่างชัดเจน ซึ่งเป็นเครื่องมือสำคัญในการเตรียมความพร้อมเพื่อรายงานต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเมื่อมีการร้องขอ หรือเมื่อเกิดเหตุการละเมิดข้อมูลส่วนบุคคล

ในส่วนของการกำหนดฐานทางกฎหมาย (Lawful Basis) นั้น มีวัตถุประสงค์เพื่อยืนยันว่าทุกกิจกรรมการประมวลผลข้อมูลส่วนบุคคลขององค์กรดำเนินไปโดยมีอำนาจหน้าที่หรือสิทธิรองรับตามกฎหมายอย่างถูกต้อง ไม่ว่าจะเป็นการใช้ฐานสัญญา ฐานความยินยอม ฐานประโยชน์โดยชอบด้วยกฎหมาย หรือฐานอื่นใดที่พระราชบัญญัติกำหนดไว้ การระบุฐานทางกฎหมายที่เหมาะสมสำหรับแต่ละกิจกรรมการประมวลผลมีเป้าหมายเพื่อป้องกันการใช้ดุลยพินิจโดยมิชอบ และเป็นการรับประกันว่าสิทธิของเจ้าของข้อมูลจะได้รับการคุ้มครองอย่างเหมาะสมตามเงื่อนไขของฐานทางกฎหมายนั้น ๆ ซึ่งจะช่วยลดความเสี่ยงจากการถูกฟ้องร้องหรือการเผชิญกับโทษปรับทางปกครองอันเนื่องมาจากการประมวลผลข้อมูลโดยปราศจากฐานทางกฎหมายรองรับ ทั้งนี้การจัดทำ ROPA ควบคู่ไปกับการระบุฐานทางกฎหมายที่ชัดเจน มีวัตถุประสงค์เพื่อยกระดับมาตรฐานธรรมาภิบาลข้อมูลขององค์กรให้มีความมั่นคงและโปร่งใส ช่วยให้องค์กรสามารถบริหารจัดการความเสี่ยงด้านความเป็นส่วนตัวได้อย่างมีประสิทธิภาพ

แนวทางการปฏิบัติ

๑. เพิ่มขั้นตอนที่ตรวจสอบผู้ที่มีอำนาจกระทำการแทนเจ้าของข้อมูลส่วนบุคคลที่เป็นผู้เยาว์หรือบุคคลไร้ความสามารถหรือเสมือนไร้ความว่าสามารถให้คำยินยอมแทนเจ้าของข้อมูลส่วนบุคคลได้ โดยจะต้องเป็นไปตามมาตรา ๒๐ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒

๒. เพิ่มวิธีการถอนความยินยอม ตามมาตรา ๑๙ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ในเอกสารหรือข้อความที่ขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

๓. จัดทำเอกสารหรือระบบ Dashboard ที่สามารถ ระบุ กิจกรรมที่มีการประมวลผลข้อมูล จำนวนข้อมูลส่วนบุคคลที่ใช้งานในแต่ละกิจกรรม จำนวนเจ้าของข้อมูลในแต่ละกิจกรรม

๔. จัดทำตัวชี้วัด เช่น % ความครบถ้วนของ ROPA, % ความถูกต้องของ ROPA เป็นต้น โดยใช้ข้อมูลจากเอกสารหรือ Dashboard ในการวัดผลประสิทธิภาพในการจัดการ ROPA

๕. ประเมินวัดผลประสิทธิภาพการจัดการ ROPA อย่างต่อเนื่องเป็นประจำ (อย่างน้อยปีละ ๑ ครั้ง)

๖. จัดให้มีการทบทวนผลจากการวัดประสิทธิภาพ เพื่อ นำปรับปรุงแก้ไขบันทึกรายการกิจกรรมการประมวลผลข้อมูลสวนบุคคล (ROPA: Records of Processing Activities) ให้มีความครบถ้วน ถูกต้อง

๗. จัดให้มีการดำเนินการปรับปรุงแก้ไขบันทึกรายการ กิจกรรมการประมวลผลข้อมูลส่วนบุคคล (ROPA: Records of Processing Activities) อย่างต่อเนื่อง เป็นประจำ (อย่างน้อยปีละ ๑ ครั้ง)

๘. จัดให้มีขั้นตอนการทบทวนเอกสารที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล (เช่น สัญญา, Privacy notice, ข้อตกลงการประมวลผล เป็นต้น) ว่าสามารถครอบคลุมทุกกิจกรรมการประมวลผลทั้งหมดที่บันทึกไว้ในเอกสาร ROPA: Records of Processing Activities

๙. กระบวนการทบทวนต้องดำเนินการอยู่เป็นประจำ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

เป้าหมาย และตัวชี้วัด ค่าเป้าหมาย

เป้าประสงค์	ตัวชี้วัด	ค่าเป้าหมาย ปี ๒๕๖๙
การจัดการความยินยอม	ร้อยละของจัดเก็บข้อมูลผู้เยาว์/บุคคลไร้ความสามารถ ที่มีระบบตรวจสอบอำนาจปกครองครบถ้วน	๑๐๐%
การให้สิทธิถอนความยินยอม	ร้อยละของแบบฟอร์มขอความยินยอมที่มีระบุ "วิธีการถอนความยินยอม" ไว้อย่างชัดเจน	๑๐๐%
ความสมบูรณ์ของบันทึกรายการ	ร้อยละความครบถ้วน และความถูกต้องของข้อมูลใน ROPA เมื่อเทียบกับกิจกรรมจริง	ไม่น้อยกว่า ๙๕%
การประเมินประสิทธิภาพ ROPA	จำนวนครั้งในการประเมินและสรุปผลประสิทธิภาพการจัดการ ROPA ประจำปี	อย่างน้อย ๑ ครั้ง/ปี
ความสอดคล้องของเอกสาร	ร้อยละของสัญญา (DPA), Notice และเอกสารอื่น ๆ ที่ครอบคลุมกิจกรรมทั้งหมดใน ROPA	๑๐๐%
การทบทวนและปรับปรุง	จำนวนครั้งที่มีการทบทวนเอกสารและกระบวนการตามรอบ หรือเมื่อมีการเปลี่ยนแปลงสำคัญ	อย่างน้อย ๑ ครั้ง/ปี

๗. สัญญาและการส่งหรือโอนข้อมูลส่วนบุคคล (Contracts and data sharing)

วัตถุประสงค์

การจัดการสัญญาและข้อตกลงเกี่ยวกับการส่งหรือโอนข้อมูลส่วนบุคคล มีเป้าหมายสำคัญเพื่อสร้างกรอบความรับผิดชอบที่ชัดเจนระหว่างองค์กรและบุคคลภายนอก ไม่ว่าจะเป็นผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) โดยมุ่งเน้นการจัดทำข้อตกลงประมวลผลข้อมูล (Data Processing Agreement) เพื่อกำกับดูแลให้การนำข้อมูลไปใช้เป็นไปตามขอบเขตและวัตถุประสงค์ที่กำหนดไว้เท่านั้น ทั้งนี้เพื่อป้องกันการนำข้อมูลส่วนบุคคลไปใช้ในทางมิชอบ หรือการเปิดเผยข้อมูลโดยปราศจากอำนาจหน้าที่ ซึ่งเป็นกลไกสำคัญในการรักษาความปลอดภัยของข้อมูลตลอดห่วงโซ่การดำเนินงานขององค์กร ในส่วนของการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ องค์กรมีวัตถุประสงค์เพื่อให้มั่นใจว่าข้อมูลส่วนบุคคลของเจ้าของข้อมูลจะยังคงได้รับความคุ้มครองในระดับที่เพียงพอ ตามมาตรฐานที่กฎหมายกำหนด โดยการวางมาตรการรองรับที่เหมาะสม เช่น การจัดทำข้อสัญญามาตรฐาน เพื่อเป็นการบริหารจัดการความเสี่ยงด้านกฎหมายข้ามพรมแดน และคุ้มครองสิทธิของเจ้าของข้อมูลมิให้ด้อยไปกว่าเกณฑ์ที่กำหนดไว้ในประเทศไทย

แนวทางการปฏิบัติ

๑. องค์กรมีการจัดทำบันทึกการใช้หรือเปิดเผยข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่น (ทั้งที่มีการขอความยินยอมและได้รับข้อยกเว้น) ตาม มาตรา ๒๗ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒

๒. องคกรมีการทำสัญญาการประมวลผลข้อมูลส่วนบุคคลครอบคลุมทุกผู้ประมวลผลข้อมูลส่วนบุคคล

๓. องคกรมีแบบ (Template) ข้อตกลงการ ประมวลผลข้อมูลส่วนบุคคลโดยมีเนื้อหาเกี่ยวกับหน้าที่และความรับผิดชอบของผู้ประมวลข้อมูลส่วนบุคคล กิจกรรมที่เกี่ยวข้องกับการประมวลผลข้อมูล ข้อกำหนดเชิงเทคนิคและมาตรการรักษา ความปลอดภัยของข้อมูล เป็นต้น ตามมาตรา ๔๐ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๔. องคกรมีเอกสารหรือ Dashboard ที่แสดงจำนวนข้อตกลง สัญญา สถานะ และระยะเวลาผูกพัน ของทุกคู่สัญญาเพื่อนำไปใช้เป็นตัวชี้วัดประสิทธิภาพของกระบวนการ

๕. องค์กรมีการจัดทำตัวชี้วัด เช่น ความสามารถใน การปฏิบัติตามสัญญาของผู้ประมวลผลข้อมูลส่วนบุคคล เป็นต้น เพื่อวัดประสิทธิภาพของกระบวนการที่เกี่ยวข้องกับสัญญาการประมวลผลข้อมูลส่วนบุคคล และดำเนินการวัดผลเป็นประจำ อย่างน้อยปีละ ๑ ครั้ง

๖. องคกรมีการตรวจสอบการปฏิบัติตามสัญญาการประมวลผลข้อมูลส่วนบุคคลกับผู้ประมวลผลข้อมูล อย่างน้อยปีละ ๑ ครั้ง

๗. องคกรมีนำผลจากการตรวจสอบการปฏิบัติตาม สัญญาการประมวลผลมาใช้ในการปรับปรุงแก้ไข ข้อตกลง สัญญากับผู้ประมวลผลข้อมูลส่วนบุคคลอย่างต่อเนื่องสัญญากับผู้ประมวลผลข้อมูลส่วนบุคคลอย่างต่อเนื่องหรืออย่างน้อย ปีละ ๑ ครั้ง

เป้าหมาย และตัวชี้วัด ค่าเป้าหมาย

เป้าประสงค์	ตัวชี้วัด	ค่าเป้าหมาย ปี ๒๕๖๙
การบันทึกการใช้/เปิดเผย	ร้อยละของรายการใช้หรือเปิดเผยข้อมูลไปยัง Controller อื่น ที่มีการบันทึกลงในระบบ/สมุดทะเบียนครบถ้วน	๑๐๐%
การทำสัญญาประมวลผล	ร้อยละของผู้ประมวลผลข้อมูล (Processors) ทั้งหมดที่มีการลงนามในสัญญา DPA ครบถ้วน	๑๐๐%
มาตรฐานสัญญา	ร้อยละของสัญญา DPA ที่ใช้ Template มาตรฐาน (มีเนื้อหาครบตามมาตรา ๔๐ หน้าที่, มาตรการเทคนิค, Security)	๑๐๐%
การติดตามสถานะ	มีระบบ Dashboard แสดงสถานะสัญญา ระยะเวลาผูกพัน และจำนวนคู่สัญญาที่ใช้งานได้จริง	มีระบบพร้อมใช้งาน ๑๐๐%
การตรวจสอบผู้ประมวลผล	ร้อยละของผู้ประมวลผลข้อมูลที่ถูกตรวจสอบการปฏิบัติตามสัญญา (Site Audit หรือ Self-Assessment)	**๑๐๐%** (อย่างน้อย ๑ ครั้ง/ปี)

เป้าประสงค์	ตัวชี้วัด	ค่าเป้าหมาย ปี ๒๕๖๙
การปฏิบัติตามสัญญา	คะแนนเฉลี่ยความสามารถในการปฏิบัติตามสัญญาของผู้ประมวลผลข้อมูล (วัดจากผล Audit)	**ไม่น้อยกว่า ๘๕%**
การพัฒนาและแก้ไข	ร้อยละของข้อตรวจพบจากผล Audit ที่ได้รับการนำไปปรับปรุง/แก้ไขสัญญาหรือกระบวนการให้ดีขึ้น	**๑๐๐% ของประเด็นสำคัญ**

๘. การบริหารจัดการความเสี่ยง (Risks)

วัตถุประสงค์

การบริหารจัดการความเสี่ยงมีวัตถุประสงค์เพื่อวิเคราะห์โอกาสที่อาจเกิดผลกระทบเชิงลบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลอันเนื่องมาจากการประมวลผลข้อมูลขององค์กร โดยมุ่งเน้นการวางมาตรการควบคุมและลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ทั้งในมิติของความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งานของข้อมูล (Availability) เพื่อให้มั่นใจว่ากิจกรรมการดำเนินงานขององค์กรจะไม่ก่อให้เกิดความเสียหายแก่เจ้าของข้อมูล และเป็นไปตามหลักการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment - DPIA) ตามที่กฎหมายและมาตรฐานสากลพึงมี

นอกจากนี้ การบริหารจัดการความเสี่ยงยังมีเป้าหมายเพื่อเสริมสร้างความมั่นคงปลอดภัยในโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและระเบียบปฏิบัติงานภายใน โดยการคาดการณ์สถานการณ์ความไม่แน่นอนที่อาจนำไปสู่การรั่วไหลหรือการละเมิดข้อมูลส่วนบุคคล ซึ่งช่วยให้องค์กรสามารถจัดสรรทรัพยากรและงบประมาณในการป้องกันภัยคุกคามได้อย่างตรงจุดและมีประสิทธิภาพสูงสุด กระบวนการนี้ยังเป็นกลไกสำคัญในการสร้าง "ความยืดหยุ่นทางธุรกิจ" ที่ช่วยให้องค์กรสามารถตอบสนองและฟื้นฟูระบบได้ทันท่วงทีหากเกิดเหตุการณ์ที่ไม่คาดคิด ลดทอนผลกระทบต่อภาพลักษณ์และลดความเสี่ยงจากการถูกลงโทษทางกฎหมายทั้งในทางแพ่ง ทางอาญา และทางปกครอง

แนวทางการปฏิบัติ

๑. เพิ่มกระบวนการจัดทำมาตรการเพื่อลดความเสี่ยงที่ระบุในทะเบียนการจัดการความเสี่ยง (Risk register)

๒. เพิ่มกระบวนการในการติดตามความเสี่ยงที่ถูกระบุว่าสามารถลดความเสี่ยงได้อยู่ในระดับที่องค์กรยอมรับได้อย่างต่อเนื่อง

๓. มีการกำหนดรอบในการประเมินความเสี่ยงด้านข้อมูลส่วนบุคคลอย่างน้อยปีละ ๑ ครั้ง หรือทุกครั้ง ที่มีการเปลี่ยนแปลง

๔. จัดทำตัวชี้วัดและดำเนินการวัดผลกระบวนการ จัดการความเสี่ยงด้านข้อมูลส่วนบุคคลว่าสามารถระบุ จัดการและลดความเสี่ยงได้อย่างมีประสิทธิภาพ

๕. กำหนดให้มีการดำเนินการอย่างสม่ำเสมออย่างน้อย ปีละ ๑ ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงที่สำคัญ

๖. จัดให้มีการนำผลที่ได้จากวัดประสิทธิภาพของกระบวนการจัดการความเสี่ยงด้านข้อมูลส่วนบุคคลมาปรับปรุงขั้นตอนหรือเพิ่มเติมเทคโนโลยี ในการระบุจัดการและลดความเสี่ยง โดยมีการดำเนินการอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

เป้าหมาย และตัวชี้วัด ค่าเป้าหมาย

เป้าประสงค์	ตัวชี้วัด	ค่าเป้าหมาย ปี ๒๕๖๙
การระบุและลดความเสี่ยง	ร้อยละของความเสี่ยงที่ระบุใน Risk Register ที่มีมาตรการจัดการรองรับชัดเจน	๑๐๐%
การรักษาความเสี่ยงให้อยู่ในระดับที่ยอมรับได้	ร้อยละของความเสี่ยงที่ถูกประเมินซ้ำแล้วพบว่าอยู่ในระดับ "ยอมรับได้" หลังใช้มาตรการลดความเสี่ยง	ไม่น้อยกว่า ๙๐%
ความสม่ำเสมอในการประเมิน	จำนวนครั้งในการประเมินความเสี่ยงด้านข้อมูลส่วนบุคคล (DPIA หรือ Risk Assessment) ประจำปี	อย่างน้อย ๑ ครั้ง/ปี (หรือทุกครั้งที่เปลี่ยนระบบ)
ประสิทธิภาพการลดความเสี่ยง	อัตราการลดลงของระดับความเสี่ยง (Risk Score) ก่อนและหลังการดำเนินมาตรการปรับปรุง	ลดลงอย่างน้อย ๑ ระดับ (เช่น จากสูงเป็นกลาง)
การพัฒนาและปรับปรุงด้วยเทคโนโลยี	ร้อยละของข้อเสนอแนะจากการวัดผลที่ได้รับการนำไปปรับปรุงกระบวนการหรือเพิ่มเทคโนโลยีจัดการความเสี่ยง	๑๐๐%

๙. การรักษาความมั่นคงปลอดภัยของข้อมูล (Data security)

วัตถุประสงค์

การรักษาความมั่นคงปลอดภัยของข้อมูล มุ่งเน้นการปฏิบัติตามมาตรฐานขั้นต่ำที่กฎหมายกำหนดเพื่อรักษาไว้ซึ่งความลับ (Confidentiality) ของข้อมูลมิให้ถูกเข้าถึงโดยผู้ไม่มีสิทธิ ความถูกต้องครบถ้วน (Integrity) มิให้ข้อมูลถูกแก้ไขเปลี่ยนแปลงโดยมิชอบ และ สภาพพร้อมใช้งาน (Availability) เพื่อให้มั่นใจว่าข้อมูลจะสามารถเข้าถึงได้ตามความจำเป็นและสิทธิของเจ้าของข้อมูล ทั้งนี้เพื่อป้องกันและลดโอกาสในการเกิดเหตุละเมิดข้อมูลส่วนบุคคล ซึ่งอาจส่งผลกระทบต่อสิทธิ เสรีภาพ และความเชื่อมั่นของเจ้าของข้อมูลในวงกว้าง

นอกจากนี้ การวางมาตรการรักษาความมั่นคงปลอดภัยยังมีวัตถุประสงค์เพื่อยกระดับโครงสร้างพื้นฐานด้านดิจิทัลขององค์กร ผ่านการบูรณาการมาตรการเชิงเทคนิคและมาตรการเชิงบริหารจัดการที่เหมาะสมกับระดับความเสี่ยง ไม่ว่าจะเป็นการใช้เทคโนโลยีการเข้ารหัสข้อมูล การควบคุมการเข้าถึงตามหลักการให้สิทธิเท่าที่จำเป็น และการจัดให้มีระบบการตรวจสอบย้อนหลังที่โปร่งใส ซึ่งกระบวนการเหล่านี้มีเป้าหมายเพื่อสร้างความเชื่อมั่นว่า องค์กรมีระบบการจัดการที่รัดกุมเพียงพอต่อการรับมือกับภัยคุกคามรูปแบบใหม่ ๆ และสามารถระงับเหตุหรือบรรเทาความเสียหายได้อย่างทันท่วงทีหากเกิดการบุกรุกระบบ

แนวทางการปฏิบัติ

๑. กำหนดวิธีในการลบหรือทำลายข้อมูลที่อยู่ในรูปของเอกสารหรือบนสื่ออิเล็กทรอนิกส์ตามประกาศฯ เรื่อง หลักเกณฑ์ในการลบหรือทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ พ.ศ.๒๕๖๗ ซึ่งระบุไว้ในนโยบายความมั่นคงปลอดภัย สารสนเทศ และได้มีการแจ้งให้ผู้ที่มีส่วนเกี่ยวข้องรับทราบเป็นที่เรียบร้อยแล้ว

๒. เพิ่มการจัดเก็บล็อก (Log) เพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง แก้ไข หรือลบข้อมูลส่วนบุคคล (Audit trails) สำหรับการเข้าถึงระบบ

๓. จัดให้มีการทบทวนนโยบายและกระบวนการด้านมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศอยู่เป็นประจำ อย่างน้อยปีละ ๑ ครั้งหรือเมื่อมีการเปลี่ยนแปลงด้านบุคลากร กฎหมาย หรือเหตุการณ์ภายนอกอื่น ๆ ที่มีผลกระทบต่อนโยบาย

๔. จัดทำตัวชี้วัด เช่น จำนวนเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่เกิดขึ้น เป็นต้น เพื่อวัดผลประสิทธิภาพกระบวนมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศทั้งหมด โดยทำอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง

๕. นำผลการวัดผลประสิทธิภาพหรือผลการทดสอบ มาปรับปรุงมาตรการรักษาความมั่นคงปลอดภัย สารสนเทศที่ยังไม่สามารถดำเนินการได้ตามตัวชี้วัดอยู่อย่างน้อยปีละ ๑ ครั้ง

เป้าหมาย และตัวชี้วัด ค่าเป้าหมาย

เป้าประสงค์	ตัวชี้วัด	ค่าเป้าหมาย ปี ๒๕๖๙
การทำลายข้อมูลตามมาตรฐาน	ร้อยละของกิจกรรมการลบ/ทำลายข้อมูลที่ดำเนินการถูกต้องตามประกาศฯ พ.ศ. ๒๕๖๗ และนโยบายที่กำหนด	๑๐๐%
การตรวจสอบย้อนหลัง	ร้อยละของระบบสารสนเทศที่จัดเก็บข้อมูลส่วนบุคคลที่มีการบันทึก Log การเข้าถึง/แก้ไข/ลบ อย่างครบถ้วน	๑๐๐%
การรักษาความทันสมัยของนโยบาย	จำนวนครั้งในการทบทวนนโยบายความมั่นคงปลอดภัยสารสนเทศ	อย่างน้อย ๑ ครั้ง/ปี
ประสิทธิภาพการป้องกัน	จำนวนเหตุการณ์ข้อมูลรั่วไหลหรือการเข้าถึงโดยมิชอบ ที่มีสาเหตุจากระบบ	๐ รายการ
การแก้ไขและปรับปรุง	ร้อยละของข้อบกพร่องจากการทดสอบ/วัดผล ที่ได้รับการปรับปรุงแก้ไขตามแผนงาน	๑๐๐%

๑๐.การรับมือต่อเหตุการละเมิดข้อมูลส่วนบุคคล (Breach response and monitor)

วัตถุประสงค์

การจัดการและตอบสนองต่อเหตุการณ์ละเมิดข้อมูลส่วน มุ่งเน้นการวางขั้นตอนการทำงานที่เป็นลำดับชัดเจน ตั้งแต่การตรวจสอบยืนยันเหตุการณ์ การประเมินระดับความรุนแรงของความเสี่ยง ไปจนถึงการแจ้งเหตุละเมิดต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายในระยะเวลา ๗๒ ชั่วโมง ตามที่กฎหมายกำหนด รวมถึงการแจ้งให้เจ้าของข้อมูลทราบในกรณีที่มีความเสี่ยงสูง ทั้งนี้เพื่อเป็นการแสดงออกถึงความรับผิดชอบและความโปร่งใสขององค์กรในการคุ้มครองสิทธิของบุคคลอย่างสูงสุด

ในด้านการเฝ้าระวัง (Monitoring) นั้น เพื่อสร้างระบบการตรวจตราเชิงรุกที่สามารถตรวจพบความผิดปกติหรือสัญญาณบ่งชี้ถึงภัยคุกคามได้ก่อนที่จะเกิดความเสียหายในวงกว้าง โดยการใช้เครื่องมือทางเทคโนโลยีและกระบวนการตรวจสอบสม่ำเสมอเพื่อประเมินความมั่นคงปลอดภัยของระบบสารสนเทศ การเฝ้าระวังอย่างต่อเนื่องไม่เพียงแต่ช่วยให้องค์กรสามารถตอบสนองต่อเหตุการณ์ได้ทันท่วงที แต่ยังเป็นแหล่งข้อมูลสำคัญในการวิเคราะห์หาสาเหตุที่แท้จริง เพื่อนำไปสู่การปรับปรุงมาตรการป้องกันและอุดช่องโหว่

ของระบบในอนาคต ลดโอกาสการเกิดเหตุซ้ำซ้อน และสร้างความยืดหยุ่นให้แก่โครงสร้างพื้นฐานด้านข้อมูลขององค์กร

แนวทางการปฏิบัติ

๑. จัดทำตัวชี้วัด เช่น จำนวนเหตุการละเมิดข้อมูลส่วนบุคคลภายในระยะเวลา ๑ ปี ระยะเวลาที่ใช้ในการรับมือและรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการละเมิดข้อมูลส่วนบุคคล เป็นต้น เพื่อวัดผลประสิทธิภาพในการรับมือและรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการละเมิดข้อมูลส่วนบุคคล อย่างน้อยปีละ ๑ ครั้ง

๒. นำผลการวัดประสิทธิภาพในการรับมือและรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการละเมิดข้อมูลส่วนบุคคลมาพัฒนาปรับปรุงแผนรับมือต่อเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการละเมิดข้อมูลส่วนบุคคล อย่างน้อยปีละ ๑ ครั้ง

๓. จัดใหมีการวิเคราะห์แนวโน้มของเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้นในรอบระยะเวลาที่ผ่านมา เพื่อใช้ในการออกมาตรการในการป้องกันไม่ให้เกิดเหตุการละเมิดซ้ำ

๔. ออกมาตรการป้องกันไม่ให้เกิดเหตุการละเมิดข้อมูลส่วนบุคคลซ้ำ หลังการวิเคราะห์แนวโน้มของเหตุการละเมิดข้อมูลส่วนบุคคล

เป้าหมาย และตัวชี้วัด ค่าเป้าหมาย

เป้าประสงค์	ตัวชี้วัด	ค่าเป้าหมาย ปี ๒๕๖๙
ความรวดเร็วในการรายงานเหตุ	ร้อยละของเหตุละเมิดที่ได้รับการรายงานต่อคณะกรรมการฯ (สคส.) ภายใน ๗๒ ชม. นับแต่ทราบเหตุ	๑๐๐%
ประสิทธิภาพการรับมือ	ระยะเวลาเฉลี่ยในการระงับเหตุ หลังได้รับแจ้งเหตุ	ภายใน ๒๔ ชม.
การป้องกันการเกิดเหตุซ้ำ	อัตราการเกิดเหตุละเมิดซ้ำในลักษณะเดิมหลังจากออกมาตรการป้องกันแล้ว	๐%
การวิเคราะห์แนวโน้ม	จำนวนรายงานวิเคราะห์แนวโน้มและสาเหตุของเหตุละเมิด เพื่อเสนอผู้บริหาร	อย่างน้อย ๒ ครั้ง/ปี
การพัฒนาแผนรับมือ	จำนวนครั้งที่มีการปรับปรุง "แผนรับมือเหตุละเมิด" ตามผลการวัดประสิทธิภาพ	อย่างน้อย ๑ ครั้ง/ปี

บรรณานุกรม

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์ในการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ พ.ศ. ๒๕๖๗ https://ratchakitcha.soc.go.th/documents/๓๙๒๑๘.pdf

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง ๒๕๖๒ มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ.๒๕๖๕ https://ratchakitcha.soc.go.th/documents/๑๗๒๑๑๓๒๖.pdf

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา ๔๑ (๒) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พ.ศ.๒๕๖๖ https://ratchakitcha.soc.go.th/documents/๑๔๐D๒๒๖S๐๐๐๐๐๐๐๐๐๑๒๐๐.pdf

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่เป็นหน่วยงานของรัฐซึ่งต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๖ https://ratchakitcha.soc.go.th/documents/๑๔๐D๑๗๔S๐๐๐๐๐๐๐๐๐๖๔๐๐.pdf

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕ https://ratchakitcha.soc.go.th/documents/๑๗๒๓๓๔๖๐.pdf

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕ https://ratchakitcha.soc.go.th/documents/๑๗๒๑๑๓๒๕.pdf

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
https://ratchakitcha.soc.go.th/documents/๑๗๐๘๒๓๐๗.pdf

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล. (๒๕๖๗) แผนแม่บทการส่งเสริมและการคุ้มครองข้อมูลส่วนบุคคลของประเทศ พ.ศ. ๒๕๖๗ - ๒๕๗๐. ประกาศ ณ วันที่ ๕ เมษายน พ.ศ. ๒๕๖๗ ราชกิจจานุเบกษา เล่ม ๑๔๑ ตอนพิเศษ ๑๑๘ ง หน้า ๓๔-๗๑ (ฉบับวันที่ ๒๙ เมษายน ๒๕๖๗) กรุงเทพฯ: กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล. (๒๕๖๘) รายงานผลการประเมินแบบสอบถาม Privacy Maturity Model ในรูปแบบประเมินตนเอง (Self assessment): กรมการแพทย์แผนไทยและการแพทย์ทางเลือก กระทรวงสาธารณสุข กรุงเทพฯ: สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล