ประกาศสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ

เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล
ของสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ

โดยที่เป็นการสมควรกำหนดให้มีประกาศสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ เพื่อจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยสำหรับการป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบด้วยกฎหมาย ตามมาตรา ๓๗ (๑) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ซึ่งกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

อาศัยอำนาจตามความในมาตรา ๕๓ แห่งพระราชบัญญัติประกอบรัฐธรรมนูญว่าด้วยคณะกรรมการสิทธิมนุษยชนแห่งชาติ พ.ศ. ๒๕๖๐ ประกอบกับมาตรา ๓๗ (๑) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕ ประกาศ ณ วันที่ ๑๐ มิถุนายน พ.ศ. ๒๕๖๕ สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ (สำนักงาน กสม.) จึงออกประกาศไว้ ดังนี้

ข้อ ๑ วัตถุประสงค์

สำนักงาน กสม. ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ได้มีประกาศ เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคลของสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ เพื่อกำหนดแนวทางในการบริหารจัดการข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติให้เป็นไปในทิศทางเดียวกัน และช่วยให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เป็นไปโดยถูกต้องตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ซึ่งครอบคลุมถึงการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่กำหนดไว้อย่างกว้าง ในการนี้ จึงได้จัดทำมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลฉบับนี้ขึ้น เพื่อกำหนดรายละเอียดโดยมีเนื้อหาที่ครอบคลุมและสอดคล้องตามมาตรฐานขั้นต่ำที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

ข้อ ๒ บททั่วไป

สำนักงาน กสม. ต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัย สำหรับการป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ไม่ว่าข้อมูลส่วนบุคคลดังกล่าวจะอยู่ในรูปแบบเอกสารหรือรูปแบบอิเล็กทรอนิกส์ หรือรูปแบบอื่นใด โดยคำนึงถึงระดับความเสี่ยงตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตลอดจนโอกาสเกิดและผลกระทบจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล รวมถึงการดำเนินการเกี่ยวกับความเสี่ยงในการรักษาความมั่นคงปลอดภัย

ทั้งนี้ มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม ต้องคำนึงถึงความสามารถในการธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) สภาพความพร้อม (Availability) การดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัย และความเหมาะสมตามระดับความเสี่ยง

ข้อ ๓ มาตรการรักษาความมั่นคงปลอดภัยเชิงองค์กร (Organizational measures)

มาตรการรักษาความมั่นคงปลอดภัยเชิงองค์กร ประกอบไปด้วยการควบคุมการเข้าถึงข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศที่สำคัญที่มีการพิสูจน์และยืนยันตัวตน การอนุญาตหรือการกำหนดสิทธิในการเข้าถึงและใช้งานที่เหมาะสม โดยคำนึงถึงหลักการให้สิทธิเท่าที่จำเป็นและการให้สิทธิที่น้อยที่สุดเท่าที่จำเป็น โดยกำหนดให้มีมาตรการ ดังนี้

๓.๑ <u>การควบคุมการเข้าถึงข้อมูลส่วนบุคคล (Access Control)</u>

(๑) สำนักงาน กสม. ต้องกำหนดความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผย รวมทั้งการล่วงรู้ไม่ว่าด้วยประการใด ๆ การทำสำเนาข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศที่สำคัญโดยไม่ได้รับอนุญาต ปราศจากอำนาจหรือโดยมิชอบด้วยกฎหมาย ตลอดจนเพื่อป้องกันการทำสำเนา การนำอุปกรณ์ที่ใช้สำหรับจัดเก็บหรือประมวลผลข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศไปโดยปราศจากมูลเหตุอันจะอ้างกฎหมายได้

(๒) สำนักดิจิทัลสิทธิมนุษยชนต้องบริหารจัดการและกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศที่อยู่ในระบบสารสนเทศของผู้ใช้งาน (User Responsibilities) ในรูปแบบต่าง ๆ เช่น สิทธิการเข้าถึง แก้ไข เปิดเผย การล่วงรู้ไม่ว่าด้วยประการใด ๆ ตลอดจนการลบและทำลาย รวมทั้งการเข้าถึงพื้นที่ที่สามารถเข้าถึงอุปกรณ์ทั้งหมดที่เกี่ยวข้อง เป็นต้น และต้องจัดให้มีการทบทวนปรับปรุงบริหารจัดการและกำหนดสิทธิให้เป็นปัจจุบันอยู่เสมอ

(๓) สำนักดิจิทัลสิทธิมนุษยชนต้องจัดให้มีกระบวนการในการพิสูจน์และยืนยันตัวตน สำหรับการเข้าถึงและใช้งานระบบสารสนเทศที่มีการเข้าถึงข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศและการเก็บรวบรวมข้อมูลการขอสิทธิในการเข้าถึงและใช้งานระบบสารสนเทศ

(๔) สำนักดิจิทัลสิทธิมนุษยชนต้องจัดให้มีการตรวจสอบยืนยันตัวตนและควบคุมบุคคลภายนอกที่เข้าปฏิบัติงานในพื้นที่ห้องเครื่องคอมพิวเตอร์แม่ข่าย ตลอดจนพื้นที่อื่นใดที่จัดเก็บอุปกรณ์ที่ใช้สำหรับจัดเก็บหรือประมวลผลข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศ

๓.๒ <u>การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)</u>

สำนักดิจิทัลสิทธิมนุษยชนต้องจัดให้มีมาตรการในการลงทะเบียนและการถอนสิทธิผู้ใช้งานตลอดจนการจัดการสิทธิการเข้าถึงของผู้ใช้งาน การบริหารจัดการสิทธิการเข้าถึงตามสิทธิการบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน และการถอดถอนหรือปรับปรุงสิทธิการเข้าถึงข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศ เพื่อควบคุมการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข เปิดเผย การล่วงรู้ไม่ว่าด้วยประการใด ๆ ตลอดจนการลบและทำลายข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศ

๓.๓ มาตรการรักษาความมั่นคงปลอดภัยตามกฎหมาย (Legal Measures for Private Security)

กรณีที่มีกฎหมายอื่นกำหนดให้สำนักงาน กสม. ต้องกำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลนั้น ให้สำนักงาน กสม. ดำเนินการตามที่กฎหมายอื่นกำหนด แต่ต้องมีมาตรฐานไม่ต่ำกว่ากฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

ข้อ ๔ มาตรการรักษาความมั่นคงปลอดภัยเชิงเทคนิค (Technical Measures)

มาตรการรักษาความมั่นคงปลอดภัยเชิงเทคนิคสำหรับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์ ที่ครอบคลุมส่วนประกอบของระบบสารสนเทศที่เกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลอย่างเหมาะสมตามระดับความเสี่ยง โดยคำนึงถึงหลักการป้องกันเชิงลึก (Defense in Depth) ที่ประกอบด้วยมาตรการป้องกันหลายชั้น (Multiple – Layered of Security Controls) เพื่อลดความเสี่ยงในบางสถานการณ์ โดยกำหนดให้มีมาตรการ ดังนี้

๔.๑ สำนักดิจิทัลสิทธิมนุษยชนต้องจัดให้มีวิธีการเพื่อสามารถตรวจสอบย้อนกลับเกี่ยวกับการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศ

๔.๒ สำนักดิจิทัลสิทธิมนุษยชนต้องจัดให้มีกระบวนการบริหารจัดการสิทธิการเข้าถึงของผู้ใช้งาน (User Access Management) เพื่อควบคุมการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข เปิดเผย การล่วงรู้ไม่ว่าด้วยประการใด ๆ ตลอดจนการลบและทำลายข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศ

๔.๓ สำนักดิจิทัลสิทธิมนุษยชนต้องจัดให้มีระบบสำรองและกู้คืนข้อมูล เพื่อให้ระบบสารสนเทศหรือบริการต่าง ๆ ยังดำเนินการได้อย่างต่อเนื่อง

ข้อ ๕ มาตรการรักษาความมั่นคงปลอดภัยเชิงกายภาพ (Physical Safeguards)

มาตรการรักษาความมั่นคงปลอดภัยเชิงกายภาพสำหรับป้องกันข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศ ตลอดจนอาคารและอุปกรณ์ที่เกี่ยวข้องให้ได้รับความปลอดภัยจากการถูกทำลายทั้งจากภัยธรรมชาติและการกระทำโดยมิชอบด้วยกฎหมาย ที่ประกอบด้วยมาตรการการควบคุมการเข้าถึงสิ่งปลูกสร้าง อาคาร พื้นที่ปฏิบัติงาน ความมั่นคงปลอดภัยของพื้นที่ปฏิบัติงาน และการควบคุมการใช้อุปกรณ์และส่วนประกอบของระบบสารสนเทศ โดยกำหนดให้มีมาตรการ ดังนี้

๕.๑ สำนัก/หน่วย ที่เก็บรวบรวมข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศ ต้องควบคุมการเข้าถึงข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศในทุกรูปแบบ ทั้งข้อมูลเอกสารและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย เช่น การจัดทำบันทึกการเข้าออกพื้นที่สำหรับบุคคลที่ไม่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศ ติดตั้งระบบกล้องวงจรปิด จัดให้มีทางเข้าออกด้วยระบบที่สามารถตรวจสอบกำหนดสิทธิเฉพาะบุคคลในการผ่านเข้าออกได้โดยใช้บัตรผ่าน ลายนิ้วมือ หรือวิธีการอื่นใดในการยืนยันตัวตน เป็นต้น เพื่อตรวจสอบผู้มีสิทธิเข้าออกหรือตรวจสอบและเฝ้าระวังผู้เข้าออกพื้นที่ และการเก็บข้อมูลส่วนบุคคลที่เป็นเอกสารในที่เก็บที่ควบคุมการเข้าถึงได้

ทั้งนี้ ให้กำหนดแต่เฉพาะผู้ที่เกี่ยวข้องเท่านั้นที่เป็นผู้มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศ

ข้อ ๖ มาตรการเสริมสร้างความรู้ความเข้าใจในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล (Measures to Enhance Understanding of Personal Data Security)

สำนักงาน กสม. ต้องส่งเสริมให้บุคลากร พนักงาน ลูกจ้าง หรือบุคคลอื่นที่เป็นผู้ใช้งาน (User) หรือบุคคลอื่นใดที่เกี่ยวข้องกับการเข้าถึง เก็บรวบรวม ใช้ เปลี่ยนแปลง แก้ไข ลบ การล่วงรู้ไม่ว่าด้วยประการใด ๆ หรือการเปิดเผยข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศ มีความรู้ความเข้าใจและตระหนักรู้ถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และแจ้งให้บุคคลดังกล่าวทราบและถือปฏิบัติตามนโยบาย แนวปฏิบัติ และมาตรการที่เกี่ยวข้อง รวมทั้งกรณีที่มีการปรับปรุงแก้ไขนโยบาย แนวปฏิบัติ และมาตรการดังกล่าวด้วย โดยคำนึงถึงลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ระดับความเสี่ยง ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

ข้อ ๗ มาตรการจัดการความเสี่ยงในการคุ้มครองข้อมูลส่วนบุคคล (Risk Management Measures in Personal Data Protection)

สำนักดิจิทัลสิทธิมนุษยชนต้องจัดให้มีมาตรการจัดการความเสี่ยงในการคุ้มครองข้อมูลส่วนบุคคล โดยดำเนินการระบุความเสี่ยงในการคุ้มครองข้อมูลส่วนบุคคลอันประกอบไปด้วยความเสี่ยงที่สำคัญที่อาจเกิดขึ้นกับทรัพย์สินสารสนเทศ (Information Assets) ที่สำคัญ เพื่อการป้องกันความเสี่ยงที่สำคัญที่อาจเกิดขึ้น และเพื่อการตรวจสอบและเฝ้าระวังภัยคุกคามและเหตุแห่งการละเมิดข้อมูลส่วนบุคคล เมื่อมีการตรวจพบเหตุอันเป็นภัยคุกคามและเหตุแห่งการละเมิดข้อมูลส่วนบุคคล ตลอดจนการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามและเหตุแห่งการละเมิดข้อมูลส่วนบุคคลด้วย ทั้งนี้ เท่าที่จำเป็น เหมาะสม และเป็นไปได้ตามประเภทและระดับความเสี่ยง และให้ดำเนินการแจ้งให้บุคลากร พนักงาน ลูกจ้าง หรือบุคคลอื่นที่เป็นผู้ใช้งาน (User) หรือบุคคลอื่นใดที่เกี่ยวข้องทราบ และดำเนินการตามมาตรการอย่างเคร่งครัด

ข้อ ๘ การทบทวนมาตรการรักษาความมั่นคงปลอดภัย (Review of Security Measures)

สำนักงาน กสม. ต้องจัดให้มีการทบทวนมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลอยู่เสมอ และในกรณีเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป เพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม โดยคำนึงถึงระดับความเสี่ยงตามปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกันที่มีลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน โดยกำหนดให้ต้องมีการทบทวนมาตรการรักษาความมั่นคงปลอดภัย ดังนี้

๘.๑ เมื่อมีเหตุละเมิดหรือกระทำการโดยมิชอบด้วยกฎหมายต่อข้อมูลส่วนบุคคล ให้ถือว่าสำนักงาน กสม. มีความจำเป็นต้องทบทวนมาตรการรักษาความมั่นคงปลอดภัย เว้นแต่เหตุหรือการกระทำนั้นไม่มีความเสี่ยงในการเกิดผลกระทบต่อสิทธิและเสรีภาพของบุคคล

๘.๒ เมื่อสำนักดิจิทัลสิทธิมนุษยชนเห็นว่า มีการเปลี่ยนแปลงที่มีนัยสำคัญทางเทคโนโลยีสารสนเทศที่มีความจำเป็นต้องทบทวนมาตรการรักษาความมั่นคงปลอดภัย

๘.๓ สำนักดิจิทัลสิทธิมนุษยชนต้องเสนอให้สำนักงาน กสม. ทบทวนมาตรการในการรักษาความมั่นคงปลอดภัย อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๙ มาตรการควบคุมผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processors Controlling Measures)

สำนักงาน กสม. ต้องจัดให้มีมาตรการในการควบคุมผู้ประมวลผลข้อมูลส่วนบุคคล เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศ หรือการกระทำที่มิชอบด้วยกฎหมาย และต้องปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลฉบับนี้ โดยกำหนดให้มีมาตรการ ดังนี้

๙.๑ สำนักงาน กสม. ต้องควบคุมบุคคลหรือนิติบุคคลที่เป็นผู้ให้บริการด้านการจัดเก็บข้อมูล ผู้พัฒนาระบบสารสนเทศ ผู้รับจ้างบันทึกข้อมูล หรือผู้เกี่ยวข้องภายนอก ที่มีสิทธิในการเข้าถึงข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศ รวมถึงผู้ใช้งานข้อมูลส่วนบุคคลที่สำนักงาน กสม. เป็นผู้ควบคุมข้อมูลส่วนบุคคล ให้เป็นไปตามมาตรการรักษาความมั่นคงปลอดภัยเชิงกายภาพ

๙.๒ สำนักงาน กสม. ต้องจัดให้มีข้อตกลงระหว่างสำนักงาน กสม. และผู้ประมวลผลข้อมูลส่วนบุคคลเป็นลายลักษณ์อักษร โดยต้องกำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้สำนักงาน กสม. ทราบถึงเหตุละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

ประกาศ ณ วันที่ ๑๗ มกราคม พ.ศ. ๒๕๖๗

พิทักษ์พล บุณยมาลิก

เลขาธิการคณะกรรมการสิทธิมนุษยชนแห่งชาติ