**ประกาศสำนักงานสภาความมั่นคงแห่งชาติ**

**เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของสำนักงานสภาความมั่นคงแห่งชาติ**

---

โดยที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕ กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ดังนั้น เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลของสำนักงานสภาความมั่นคงแห่งชาติ เป็นไปอย่างเหมาะสมและมีประสิทธิภาพ รวมทั้งสอดคล้องกับแนวปฏิบัติตามกรอบธรรมาภิบาลข้อมูลของสำนักงานสภาความมั่นคงแห่งชาติ

อาศัยอำนาจตามความในมาตรา ๓๗ (๑) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และข้อ ๔ ของประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕ ประกอบกับมาตรา ๒๒ แห่งพระราชบัญญัติสภาความมั่นคงแห่งชาติ พ.ศ. ๒๕๕๙ เลขาธิการสภาความมั่นคงแห่งชาติจึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสำนักงานสภาความมั่นคงแห่งชาติ เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของสำนักงานสภาความมั่นคงแห่งชาติ”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“สำนักงาน” หมายความว่า สำนักงานสภาความมั่นคงแห่งชาติ

“หน่วยงาน” หมายความว่า สำนัก กอง หรือกลุ่มที่จัดตั้งขึ้นเป็นหน่วยงานภายใต้กฎกระทรวงแบ่งส่วนราชการสำนักงานสภาความมั่นคงแห่งชาติ สำนักนายกรัฐมนตรี พ.ศ. ๒๕๖๓ หรือหน่วยงานอื่นใดภายใต้คำสั่งสำนักงานสภาความมั่นคงแห่งชาติ

“เจ้าหน้าที่” หมายความว่า ข้าราชการ ลูกจ้างประจำ พนักงานราชการ พนักงานจ้างเหมาบริการ หรือบุคลากรอื่นใดของสำนักงานสภาความมั่นคงแห่งชาติ

“ความมั่นคงปลอดภัย” หมายความว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

“เจ้าของข้อมูลส่วนบุคคล” หมายความว่า บุคคลธรรมดาซึ่งเป็นเจ้าของข้อมูลส่วนบุคคลที่สำนักงานสภาความมั่นคงแห่งชาติ เก็บรวบรวม ใช้ หรือเปิดเผย

/“ผู้ควบคุมข้อมูล...

“ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

“ผู้ประมวลผลข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

“การประมวลผลข้อมูลส่วนบุคคล” หมายความว่า การดำเนินการใด ๆ กับข้อมูลส่วนบุคคล เช่น เก็บรวบรวม บันทึก สำเนา จัดระเบียบ เก็บรักษา ปรับปรุง เปลี่ยนแปลง ใช้ กู้คืน เปิดเผย ส่งต่อ เผยแพร่ โอน รวม ลบ ทำลาย เป็นต้น

“การละเมิดข้อมูลส่วนบุคคล” หมายความว่า การละเมิดมาตรการรักษาความมั่นคงปลอดภัยที่ทำให้เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ไม่ว่าจะเกิดจากเจตนา ความจงใจ ความประมาทเลินเล่อ การกระทำโดยปราศจากอำนาจหรือโดยมิชอบ การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ภัยคุกคามทางไซเบอร์ ข้อผิดพลาดบกพร่องหรืออุบัติเหตุ หรือเหตุอื่นใด

ข้อ ๔ จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสม ซึ่งครอบคลุม ๓ ประเด็น ได้แก่ การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ โดยคำนึงถึงระดับความเสี่ยงตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตลอดจนโอกาสเกิดและผลกระทบจากเหตุการละเมิดข้อมูลส่วนบุคคล ประกอบด้วยการดำเนินการ ดังต่อไปนี้

๔.๑ **มาตรการเชิงองค์กร (organizational measures)**

๑) แจ้งมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลตามประกาศนี้ ให้แก่เจ้าหน้าที่ของสำนักงาน และ/หรือผู้มีส่วนได้เสียของสำนักงานทราบ รวมถึงสร้างเสริมความตระหนักรู้ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลให้กับเจ้าหน้าที่และให้ปฏิบัติตามมาตรการที่กำหนดอย่างเคร่งครัด

๒) มีการออกระเบียบ วิธีปฏิบัติ สำหรับควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย มีการกำหนดบันทึกการเข้าออกพื้นที่ ให้เจ้าหน้าที่รักษาความปลอดภัยตรวจสอบผู้มีสิทธิผ่านเข้าออก ทั้งนี้ความเข้มข้นของมาตรการ ให้เป็นไปตามระดับความเสี่ยง หรือความเสียหายที่อาจเกิดขึ้นหากข้อมูลส่วนบุคคลรั่วไหล ถูกแก้ไข ถูกคัดลอก หรือถูกทำลายโดยมิชอบ

๓) มีการกำหนดเกี่ยวกับการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้งาน (user responsibilities) แบ่งเป็นรูปแบบต่าง ๆ เช่น สิทธิในการเข้าถึง เก็บรวบรวม ใช้ เปลี่ยนแปลง แก้ไข เพิ่มเติม เปิดเผยและเผยแพร่ การตรวจสอบคุณภาพข้อมูล ตลอดจนการลบทำลาย

/๔) จัดให้มีวิธีการ...

๔) จัดให้มีวิธีการเพื่อตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

๕) ในกรณีที่มีการฝ่าฝืนไม่ปฏิบัติตามมาตรการ เนื่องจากความบกพร่องของสำนักงาน และทำให้เกิดการละเมิดหรือการรั่วไหลของข้อมูลส่วนบุคคล สำนักงานจะแจ้งให้เจ้าของข้อมูลทราบถึงรายละเอียดของเหตุการณ์และแผนเยียวยาความเสียหายจากการละเมิดหรือรั่วไหลดังกล่าวโดยเร็ว อย่างไรก็ตาม สำนักงานจะไม่รับผิดชอบในความเสียหายใด ๆ อันเกิดจากการใช้ การเปิดเผย รวมถึงการประมาทเลินเล่อของเจ้าของข้อมูลหรือบุคคลอื่นที่ได้รับความยินยอมจากเจ้าของข้อมูล

๖) เมื่อพ้นระยะเวลาการใช้งานข้อมูลส่วนบุคคลหรือไม่มีความจำเป็นในการเก็บรักษาข้อมูลส่วนบุคคลอีกต่อไป สำนักงานจะลบหรือทำลายข้อมูลส่วนบุคคลออกจากระบบการจัดเก็บ เว้นแต่ในกรณีที่ต้องเก็บรักษาข้อมูลส่วนบุคคลไว้ตามที่กฎหมายกำหนด

๔.๒ **มาตรการเชิงเทคนิค (technical measures)**

๑) จัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล

๒) การบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาต ตามระดับสิทธิการบริหารจัดการข้อมูล ได้แก่ การนำเข้า เปลี่ยนแปลง แก้ไข เปิดเผย ตลอดจนการลบทำลาย

(๑) มีการควบคุมการเข้าถึงข้อมูลส่วนบุคคล และส่วนประกอบของระบบสารสนเทศที่สำคัญที่มีการพิสูจน์และยืนยันตัวตน และการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงและใช้งานที่เหมาะสม โดยคำนึงถึงหลักการให้สิทธิเท่าที่จำเป็น ตามหลักการให้สิทธิที่น้อยที่สุดเท่าที่จำเป็น

(๒) มีการบริหารจัดการการเข้าถึงของผู้ใช้งานที่เหมาะสม รวมถึงการลงทะเบียนและการถอนสิทธิผู้ใช้งาน การจัดการสิทธิการเข้าถึงของผู้ใช้งาน การบริหารจัดการสิทธิการเข้าถึงตามสิทธิการบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน ทั้งนี้ ต้องมีการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน อย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การเปลี่ยนตำแหน่ง โอนย้าย หรือการลาออก เพื่อการถอดถอนหรือปรับปรุงสิทธิการเข้าถึง

๓) จัดให้มีระบบสำรองและกู้คืนข้อมูล เพื่อให้ระบบสารสนเทศยังสามารถดำเนินการได้อย่างต่อเนื่อง

๔.๓ **มาตรการทางกายภาพ (physical measures)**

๑) มีการควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย เช่น มีบันทึกการเข้าออกพื้นที่ มีเจ้าหน้าที่รักษาความปลอดภัยของพื้นที่ มีระบบกล้องวงจรปิดติดตั้ง มีการล็อคประตูทุกครั้ง มีระบบบัตรผ่านเฉพาะ

ผู้มีสิทธิเข้าออก ทั้งนี้ ความเข้มข้นของมาตรการให้เป็นไปตามระดับความเสี่ยงหรือความเสียหายที่อาจเกิดขึ้นหากข้อมูลส่วนบุคคลรั่วไหล ถูกแก้ไข ถูกคัดลอก หรือถูกทำลายโดยมิชอบ

๒) กำหนดผู้ที่ได้รับอนุญาตให้เข้าถึงอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคลตามหน้าที่ความรับผิดชอบเท่าที่จำเป็น เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลส่วนบุคคล การลักลอบนำอุปกรณ์เข้าออก หรือการลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล

๓) การดำเนินการป้องกันและระมัดระวังไม่ให้ข้อมูลรั่วไหลหรือถูกละเมิด เช่น ไม่เปิดไฟล์ข้อมูลส่วนบุคคลในที่สาธารณะ ปิด/เก็บข้อมูลส่วนบุคคลให้มิดชิดเมื่อลุกออกจากโต๊ะ กรณีการใช้เครื่องคอมพิวเตอร์ร่วมกันต้องลบไฟล์ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลออกจากหน้าจอทุกครั้งและออกจากระบบ (Log out) ให้เรียบร้อย รวมถึงทำลายเอกสารข้อมูลส่วนบุคคลด้วยตนเองทุกครั้งโดยไม่ฝากบุคคลอื่นทำลายแทน เป็นต้น

ข้อ ๕ ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ต้องดำเนินการเพื่อป้องกันมิให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ โดยอย่างน้อยควรประกอบด้วยการดำเนินการ ดังต่อไปนี้

๕.๑ **การประเมินก่อนส่งมอบข้อมูล**

๑) ให้ดำเนินการตรวจสอบสิทธิ อำนาจหน้าที่ และฐานกฎหมายที่บุคคล และ/หรือนิติบุคคลรายอื่นนั้นใช้เพื่อร้องขอข้อมูลส่วนบุคคล

๒) ให้สอบถามวัตถุประสงค์ในการนำข้อมูลไปใช้งานเพื่อให้สามารถประเมินว่าควรสำเนาข้อมูลให้ในระดับรายละเอียดเท่าใด และจำเป็นต้องทราบข้อมูลที่ชี้จำเพาะบุคคลหรือไม่ หากแปลงข้อมูลที่ชี้จำเพาะบุคคลแทนด้วยรหัสใหม่ที่เป็นนิรนามจะเพียงพอต่อการนำไปใช้ประโยชน์หรือไม่

๕.๒ **เมื่อส่งมอบข้อมูล**

๑) จัดเตรียมข้อมูลใหม่จากข้อมูลดิบให้มีระดับรายละเอียดเท่าที่จำเป็นต่อจุดประสงค์การใช้งาน

๒) ส่งมอบข้อมูล พร้อมทำการบันทึกชื่อผู้ขอข้อมูล ข้อมูลสำหรับติดต่อ วัน-เดือน-ปีที่ให้ข้อมูล ฐานกฎหมายที่ใช้สำหรับเข้าถึงข้อมูลส่วนบุคคล ตลอดจนวัตถุประสงค์การนำไปใช้งาน

๓) แจ้งให้บุคคลหรือนิติบุคคลนั้นทราบว่าเมื่อรับข้อมูลไปแล้ว ผู้รับข้อมูลจะต้องดำเนินการตามหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลสำหรับข้อมูลชุดที่ร้องขอไปนั้นเช่นเดียวกัน ตามขอบเขตและวัตถุประสงค์การใช้งานที่แจ้งไว้

๕.๓ **หลังส่งมอบข้อมูล**

๑) ติดตามการใช้งานเป็นครั้งคราว เช่น ทุก ๓ เดือน ๖ เดือน หรือ ๑ ปี เพื่อบันทึกสถานะล่าสุดในการใช้งานข้อมูลนั้น หากไม่มีความจำเป็นใช้งานตามวัตถุประสงค์ที่แจ้งไว้เดิมควรแจ้งให้บุคคลหรือนิติบุคคลนั้นลบทำลายข้อมูล

/๒) กำหนดวิธีการ...

๒) กำหนดวิธีการในการปรับปรุงข้อมูลให้ทันสมัยต่อการใช้งานของผู้ใช้อยู่เสมอ เช่น มีโปรแกรมคอมพิวเตอร์สำหรับเชื่อมต่อปรับปรุงให้ข้อมูลต้นทางและปลายทางมีความทันสมัยเท่ากันโดยอัตโนมัติตลอดเวลา

ข้อ ๖ จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม โดยอย่างน้อยควรประกอบด้วยการดำเนินการ ดังต่อไปนี้

๖.๑ มีการติดตามเป็นระยะว่าข้อมูลส่วนบุคคลที่อยู่ในความดูแลของตนนั้น (ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล) มีรายการหรือมีชุดข้อมูลใดที่พ้นกำหนดระยะเวลาการเก็บรักษาหรือไม่ (ตามที่แจ้งเจ้าของข้อมูลส่วนบุคคลไว้ในประกาศความเป็นส่วนตัว (Privacy Notice) หรือ ตามที่ขอความยินยอมไว้) ทั้งนี้เพื่อดำเนินการลบทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ตามแต่กรณี

๖.๒ กรณีเจ้าของข้อมูลส่วนบุคคลขอใช้สิทธิให้ลบทำลายข้อมูล (หรือขอถอนความยินยอม) ต่อผู้ควบคุมข้อมูลส่วนบุคคล และผู้ควบคุมข้อมูลส่วนบุคคลใช้ฐานความยินยอมในการเก็บรวบรวมข้อมูลส่วนบุคคล เช่นนี้ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการลบทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ตามแต่กรณี

๖.๓ การลบทำลายข้อมูลหรือการทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ อาจยกเว้นไม่กระทำก็ได้ในกรณีผู้ควบคุมข้อมูลส่วนบุคคลมีเหตุผลความจำเป็นที่เหนือกว่าสิทธิของเจ้าของข้อมูล เช่น

๑) เพื่อวัตถุประสงค์การจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ การศึกษาวิจัยหรือสถิติ

๒) เพื่อการสร้างประโยชน์สาธารณะตามหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลรายนั้น

๓) เพื่อประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพหรือระบบและการให้บริการด้านสังคมสงเคราะห์

๔) การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์หรือเครื่องมือแพทย์

ข้อ ๗ มีการระบุความเสี่ยงที่สำคัญที่อาจเกิดขึ้นกับทรัพย์สินสารสนเทศที่สำคัญ การป้องกันความเสี่ยงที่อาจเกิดขึ้น การตรวจสอบและเฝ้าระวังภัยคุกคามและเหตุการละเมิดข้อมูลส่วนบุคคล และการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามและเหตุการละเมิดข้อมูลส่วนบุคคล และกำหนดหน้าที่รับผิดชอบให้แก่ผู้แทนสำนักงานในการดำเนินการเมื่อเกิดเหตุการละเมิด ประกอบด้วย

/๗.๑ การละเมิดข้อมูล...

๗.๑ การละเมิดข้อมูลส่วนบุคคลแต่ละเหตุอาจเกี่ยวข้องกับการละเมิดประเภทใดประเภทหนึ่งหรือหลายประเภท ดังต่อไปนี้

๑) การละเมิดความลับของข้อมูลส่วนบุคคล (Confidentiality Breach) ซึ่งมีการเข้าถึง หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ หรือเกิดจากข้อผิดพลาดบกพร่องหรืออุบัติเหตุ

๒) การละเมิดความถูกต้องครบถ้วนของข้อมูลส่วนบุคคล (Integrity Breach) ซึ่งมีการเปลี่ยนแปลง แก้ไขข้อมูลส่วนบุคคลให้ไม่ถูกต้อง ไม่สมบูรณ์ หรือไม่ครบถ้วน โดยปราศจากอำนาจหรือโดยมิชอบ หรือเกิดจากข้อผิดพลาดบกพร่องหรืออุบัติเหตุ

๓) การละเมิดความพร้อมใช้งานของข้อมูลส่วนบุคคล (Availability Breach) ซึ่งทำให้ไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้ หรือมีการทำลายข้อมูลส่วนบุคคลทำให้ข้อมูลส่วนบุคคลไม่อยู่ในสภาพที่พร้อมใช้งานได้ตามปกติ

๗.๒ มีการประเมินความเสี่ยงของการละเมิดข้อมูลส่วนบุคคลว่าการละเมิดข้อมูลส่วนบุคคลนั้นมีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลเพียงใด จำเป็นต้องแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลหรือเจ้าของข้อมูลส่วนบุคคลหรือไม่ ซึ่งอาจพิจารณาจากปัจจัย ดังต่อไปนี้

๑) ลักษณะและประเภทของการละเมิดข้อมูลส่วนบุคคล

๒) ลักษณะหรือประเภทของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด

๓) ปริมาณของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด ซึ่งอาจพิจารณาจากจำนวนเจ้าของข้อมูลส่วนบุคคลหรือจำนวนรายการ (records) ของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด

๔) ลักษณะ ประเภท หรือสถานะของเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ

๕) ความร้ายแรงของผลกระทบและความเสียหายที่เกิดขึ้นหรืออาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคลจากการละเมิดข้อมูลส่วนบุคคล และประสิทธิผลของมาตรการที่ใช้ หรือจะใช้เพื่อป้องกันระงับหรือแก้ไขเหตุการละเมิดข้อมูลส่วนบุคคล หรือเยียวยาความเสียหายต่อการบรรเทาผลกระทบและความเสียหายที่เกิดขึ้นหรืออาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคล

๖) ผลกระทบในวงกว้างต่อการดำเนินการตามภารกิจของสำนักงานหรือต่อสาธารณะจากเหตุการละเมิดข้อมูลส่วนบุคคล

๗) ลักษณะของระบบการจัดเก็บข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด และมาตรการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้อง

ทั้งนี้ หลักเกณฑ์ในการพิจารณาประเมินความเสี่ยงจะต้องพิจารณาจากข้อเท็จจริงตามปัจจัยที่เกี่ยวข้องเป็นกรณี ๆ ไป

๗.๓ การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และการแจ้งเหตุแก่เจ้าของข้อมูลส่วนบุคคล ประกอบด้วยการดำเนินการ ดังต่อไปนี้

/๑) กำหนดเจ้าหน้าที่...

๑) กำหนดเจ้าหน้าที่ผู้รับผิดชอบกิจกรรม และวิธีการแจ้งเหตุละเมิดให้แก่ผู้แทนสำนักงานทราบอย่างชัดเจน เช่น การแจ้งทางอีเมล และแจ้งทางโทรศัพท์กรณีเป็นเหตุละเมิดที่มีความรุนแรงและเร่งด่วน

๒) กำหนดวิธีปฏิบัติให้ผู้แทนสำนักงานต้องดำเนินการแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบถึงเหตุละเมิดข้อมูลส่วนบุคคลได้ภายในเจ็ดสิบสองชั่วโมง นับแต่ทราบเหตุ กรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยเร็ว

๓) การแจ้งเหตุละเมิดอาจได้รับยกเว้นไม่ต้องดำเนินการก็ได้ หากการละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

ข้อ ๘ การดำเนินการใด ๆ ภายใต้มาตรการที่กำหนดไว้ในประกาศนี้ จะต้องคำนึงถึงความสามารถในการธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคลไว้ได้อย่างเหมาะสมตามระดับความเสี่ยง โดยคำนึงถึงปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน ลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้และความเป็นไปได้ในการดำเนินการประกอบกัน

ข้อ ๙ การเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์ ให้ปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยที่กำหนดไว้ในประกาศนี้ ทั้งนี้ รูปแบบอิเล็กทรอนิกส์ดังกล่าวจะครอบคลุมส่วนประกอบต่าง ๆ ของระบบสารสนเทศที่เกี่ยวข้องกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล เช่น ระบบและอุปกรณ์จัดเก็บข้อมูลส่วนบุคคล เครื่องคอมพิวเตอร์แม่ข่าย (servers) เครื่องคอมพิวเตอร์ลูกข่าย (clients) และอุปกรณ์ต่าง ๆ ที่ใช้ ระบบเครือข่าย ซอฟต์แวร์และแอปพลิเคชัน อย่างเหมาะสมตามระดับความเสี่ยง โดยคำนึงถึงหลักการป้องกันเชิงลึก (defense in depth) ที่ควรประกอบด้วยมาตรการป้องกันหลายชั้น (multiple layers of security controls) เพื่อลดความเสี่ยงในกรณีที่มาตรการบางมาตรการมีข้อจำกัดในการป้องกันความมั่นคงปลอดภัยในบางสถานการณ์

ข้อ ๑๐ จัดให้มีข้อตกลงระหว่างสำนักงานสภาความมั่นคงแห่งชาติในฐานะผู้ควบคุมข้อมูลส่วนบุคคลกับผู้ประมวลผลข้อมูลส่วนบุคคล สำนักงานจะกำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมเทียบเท่าหรือดีกว่ามาตรการตามประกาศนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้สำนักงานทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น ทั้งนี้ความเข้มข้นของมาตรการให้เป็นไปตามระดับความเสี่ยง หรือความเสียหายที่อาจเกิดขึ้นหากข้อมูลส่วนบุคคลรั่วไหล ถูกแก้ไข ถูกคัดลอกหรือถูกทำลายโดยมิชอบ

/ข้อ ๑๑ ทบทวน...

ข้อ ๑๑ ทบทวนมาตรการรักษาความมั่นคงปลอดภัยที่กำหนดไว้ในประกาศนี้ในกรณีมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป เพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม โดยคำนึงถึงระดับความเสี่ยงตามปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน ลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน เมื่อมีเหตุการละเมิดข้อมูลส่วนบุคคล ให้ถือว่าผู้ควบคุมข้อมูลส่วนบุคคลมีความจำเป็นต้องทบทวนมาตรการรักษาความมั่นคงปลอดภัย เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

จึงประกาศให้ทราบโดยทั่วกัน

ประกาศ ณ วันที่ ๒๔ พฤษภาคม พ.ศ. ๒๕๖๖

พลเอก
(สุพจน์ มาลานิยม)
เลขาธิการสภาความมั่นคงแห่งชาติ