ประกาศสำนักงานการปฏิรูปที่ดินเพื่อเกษตรกรรม
เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

โดยสำนักงานการปฏิรูปที่ดินเพื่อเกษตรกรรม (ส.ป.ก.) เป็นหน่วยงานของรัฐตามบัญชีท้ายพระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พ.ศ.๒๕๖๓ ซึ่งต้องจัดให้มีมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลเป็นไปตามประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ.๒๕๖๓ เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลของ ส.ป.ก. เป็นไปอย่างมีประสิทธิภาพสามารถปฏิบัติได้อย่างเป็นรูปธรรม

อาศัยอำนาจตามความในมาตรา ๓ วรรคสอง แห่งพระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พ.ศ. ๒๕๖๓ เลขาธิการ ส.ป.ก. จึงออกประกาศไว้ ดังนี้

(๑) การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

(ก) ควบคุมการเข้าถึงข้อมูลส่วนบุคคลไว้ให้เฉพาะเจ้าหน้าที่ที่มีความจำเป็นต้องใช้ข้อมูลในการปฏิบัติงานในหน้าที่ในแต่ละลำดับชั้น และจัดให้มีการบันทึกและทำสำรองข้อมูลของการเข้าถึงหรือการเข้าใช้งานในระยะเวลาที่เหมาะสมหรือตามระยะเวลาที่กฎหมายกำหนด นอกจากนี้ ในบางกรณีอาจจะใช้การเข้ารหัส เพื่อรักษาความมั่นคงปลอดภัยในการส่งผ่านข้อมูล

(ข) กำหนดให้มีมาตรการที่เหมาะสมสำหรับการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลโดยเฉพาะ เพื่อป้องกันข้อมูลส่วนบุคคลที่อาจส่งผลกระทบต่อความรู้สึก ความเชื่อ ความสงบเรียบร้อยและศีลธรรมอันดีของประชาชนซึ่งเป็นผู้ใช้บริการของ ส.ป.ก. หรืออาจก่อให้เกิดความเสียหาย หรือมีผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลโดยชัดเจน เช่น เลขประจำตัวประชาชน เป็นต้น

(ค) ส.ป.ก. ใช้อุปกรณ์ในการจัดเก็บข้อมูลและอุปกรณ์รักษาความปลอดภัยที่มีประสิทธิภาพรวมถึงการเข้ารหัสข้อมูลเพื่อให้ข้อมูลส่วนบุคคลมีความปลอดภัย

(๒) การกำหนดเกี่ยวกับการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคล

ส.ป.ก. กำหนดเกี่ยวกับการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคล ดังนี้

(ก) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น เพิ่มข้อมูล ลบข้อมูล แก้ไขข้อมูลอ่านข้อมูลอย่างเดียว เป็นต้น

(ข) กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) ที่ได้กำหนดไว้

(ค) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษร และได้รับการพิจารณาอนุญาตจากผู้อำนวยการหรือผู้ดูแลระบบที่ได้รับมอบหมาย

(๓) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาตแล้ว

ส.ป.ก. มีการกำหนดขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งาน (user registration) ดังนี้

(ก) จัดทำแบบฟอร์มขอใช้ระบบสารสนเทศ และให้ผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์มเพื่อตรวจสอบสิทธิและดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน

(ข) มีการระบุเลขประจำตัวประชาชน ชื่อ นามสกุล ของผู้ใช้งาน

(ค) มีการระบุ ตำแหน่ง หน่วยงานในสังกัด และหมายเลขโทรศัพท์ติดต่อ

(ง) มีการลงนามของผู้บังคับบัญชาของผู้ใช้งาน

(จ) มีการตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

(ฉ) มีการบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศ

(ช) มีหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ และตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย เกษียณอายุราชการ หรือสิ้นสุดการจ้าง เป็นต้น

(ซ) มีกระบวนการทบทวนสิทธิการเข้าถึงข้อมูลของผู้ใช้ระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น มีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย เกษียณอายุราชการ หรือสิ้นสุดการจ้าง เป็นต้น

(๔) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลส่วนบุคคล การลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล

ส.ป.ก. กำหนดการเข้าถึงข้อมูลส่วนบุคคลไว้ให้เฉพาะเจ้าหน้าที่โดยแบ่งเป็นระดับชั้นในการเข้าถึงข้อมูล และไม่อนุญาตให้บุคคลอื่นเข้าถึงหรือใช้ข้อมูลที่ ส.ป.ก. มีการจัดเก็บรวบรวมข้อมูลเกี่ยวกับข้อมูลส่วนบุคคล เว้นแต่ ได้รับความยินยอมจากเจ้าของข้อมูลโดยทำหนังสือให้ความยินยอมเปิดเผยข้อมูลส่วนบุคคลเป็นลายลักษณ์อักษร หรือกรณีที่มีการบังคับให้เปิดเผยข้อมูลส่วนบุคคลตามกฎหมายที่กำหนดเพื่อประโยชน์แก่การสอบสวนของพนักงานสอบสวน หรือการพิจารณาพิพากษาคดีของศาลตามหมายศาล หรือคำสั่งศาล ส.ป.ก. มีหน้าที่จะต้องปฏิบัติตาม

(๕) การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ส.ป.ก. มีวิธีการจัดเก็บ Log File ในระบบสารสนเทศเพื่อใช้ในการตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคลโดยอัตโนมัติ ที่สามารถเชื่อมโยงกับข้อมูลที่ระบุตัวบุคคลผู้ใช้งานได้ เช่น Username ของผู้ใช้งาน เวลา วันที่ รายการข้อมูลที่ถูกเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูล ข้อมูลหมายเลขไอพี (IP Address) ระบบสารสนเทศที่เข้าออกก่อนและหลัง เป็นต้น ทั้งนี้ เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ.๒๕๖๐ มาตรา ๒๖ ที่กำหนดให้ผู้ให้บริการต้องเก็บข้อมูลจราจรคอมพิวเตอร์ไว้ไม่น้อยกว่า ๙๐ วัน นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็น พนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ไว้เกิน ๙๐ วัน แต่ไม่เกิน ๒ ปี เป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้

(๖) ส.ป.ก. กำหนดให้เจ้าหน้าที่ทุกคนที่เกี่ยวข้อง ต้องให้ความสำคัญและรับผิดชอบในการจัดเก็บและคุ้มครองข้อมูลส่วนบุคคล และปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่ประกาศไว้อย่างเคร่งครัด

(๗) ส.ป.ก. เสริมสร้างความตระหนักรู้ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลให้แก่ข้าราชการ พนักงานราชการ ลูกจ้างชั่วคราว และเจ้าหน้าที่ของ ส.ป.ก. ด้วยการเผยแพร่ข้อมูลข่าวสารให้ความรู้ จัดสัมมนา หรือฝึกอบรมในเรื่องดังกล่าวให้แก่บุคลากรในองค์กรเป็นประจำ

(๘) บรรดาประกาศ หนังสือเวียน หรือข้อสั่งการใดที่ขัดหรือแย้งกับประกาศนี้ ให้ใช้ตามประกาศนี้

(๙) ประกาศนี้ให้มีผลบังคับตั้งแต่บัดนี้เป็นต้นไป เว้นแต่จะมีประกาศเปลี่ยนแปลง

ประกาศ ณ วันที่ ๑๖ เมษายน พ.ศ. ๒๕๖๔

(นายวิณะโรจน์ ทรัพย์ส่งสุข)
เลขาธิการสำนักงานการปฏิรูปที่ดินเพื่อเกษตรกรรม