



ประกาศสำนักงานสถิติแห่งชาติ

เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๔

โดยที่มาตรา ๓ วรรคสอง แห่งพระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พ.ศ. ๒๕๖๓ กำหนดให้ผู้ควบคุมข้อมูล ซึ่งเป็นหน่วยงานหรือกิจการตามบัญชีท้ายพระราชกฤษฎีกาดังกล่าวต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กำหนด

อาศัยอำนาจตามความในมาตรา ๓ วรรคสอง แห่งพระราชกฤษฎีกากำหนดหน่วยงาน และกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พ.ศ. ๒๕๖๓ สำนักงานสถิติแห่งชาติ จึงออกประกาศไว้ ดังนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสำนักงานสถิติแห่งชาติ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๔”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันที่ประกาศเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“เจ้าหน้าที่” หมายความว่า ข้าราชการ ลูกจ้างประจำ พนักงานราชการ และลูกจ้างชั่วคราว ในสังกัดสำนักงานสถิติแห่งชาติ ไม่ว่าจะ มีหน้าที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ได้มา ตามกฎหมายว่าด้วยสถิติ และกฎหมายอื่นที่เกี่ยวข้องหรือไม่ก็ตาม ทั้งนี้ ให้รวมถึงบุคคลอื่นใดซึ่งปฏิบัติหน้าที่ หรือมีหน้าที่เก็บรักษาข้อมูลส่วนบุคคลที่ได้มาตามกฎหมายว่าด้วยสถิติ ด้วย

“ความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล” หมายความว่า การดำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ

ข้อ ๔ เจ้าหน้าที่ต้องตระหนักรู้ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล ตามประกาศนี้อย่างเคร่งครัด

ข้อ ๕ เจ้าหน้าที่ต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ครอบคลุมถึงมาตรการป้องกันด้านการบริหารจัดการ (administrative safeguard) มาตรการป้องกันด้านเทคนิค (technical safeguard) และมาตรการป้องกันทางกายภาพ (physical safeguard) ในเรื่อง การเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล (access control) โดยอย่างน้อย ต้องประกอบด้วย การดำเนินการ ดังต่อไปนี้

(๑) การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผล ข้อมูลส่วนบุคคลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

(๒) การกำหนดเกี่ยวกับการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคล

(๓) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุม การเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาตแล้ว

(๔) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งานของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคล โดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนา ข้อมูลส่วนบุคคล การลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล

(๕) การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ข้อ ๖ เจ้าหน้าที่อาจเลือกใช้มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ที่แตกต่างไปจากประกาศฉบับนี้ได้ หากมาตรฐานดังกล่าวมีมาตรการรักษาความมั่นคงปลอดภัยไม่ต่ำกว่าที่กำหนดในประกาศนี้

ข้อ ๗ ให้ผู้อำนวยการสำนักงานสถิติแห่งชาติ รักษาการตามประกาศนี้ และให้มีอำนาจตีความ และวินิจฉัยปัญหาอันเกิดจากการปฏิบัติตามประกาศนี้

ประกาศ ณ วันที่ ๒ กุมภาพันธ์ พ.ศ. ๒๕๖๔



(นางสาววันเพ็ญ พูลวงษ์)

ผู้อำนวยการสำนักงานสถิติแห่งชาติ