



มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ของกรมการปกครอง พ.ศ. ๒๕๖๗

โดยที่มาตรา ๓๗ (๑) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ กำหนดให้ ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมเพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้มีประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕ เพื่อกำหนดมาตรฐานขั้นต่ำในการคุ้มครองข้อมูลส่วนบุคคลในระยะแรกที่กฎหมายมีผลใช้บังคับแล้ว ดังนั้น เพื่อให้การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของกรมการปกครองสามารถดำเนินการให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕ กรมการปกครอง จึงออกมาตรการไว้ ดังต่อไปนี้

ข้อ ๑ ในมาตรการนี้

“เจ้าหน้าที่” หมายความว่า ข้าราชการ ลูกจ้างประจำ พนักงานราชการ ลูกจ้างเหมาบริการ และสมาชิกกองอาสารักษาดินแดน ในสังกัดกรมการปกครองไม่ว่าจะมีหน้าที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ได้มาหรือไม่ก็ตาม ทั้งนี้ ให้รวมถึงบุคคลอื่นใดซึ่งปฏิบัติหน้าที่หรือมีหน้าที่เก็บรักษาข้อมูลส่วนบุคคล ที่ได้มาตามกฎหมายในความรับผิดชอบกรมการปกครอง ด้วย

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

ข้อ ๒ เจ้าหน้าที่ต้องตระหนักรู้ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล และการรักษาความมั่นคงปลอดภัย (Privacy and Security Awareness) และการแจ้งนโยบาย แนวปฏิบัติ และมาตรการด้านการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยอย่างเหมาะสม โดยคำนึงถึงลักษณะ และวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูล ส่วนบุคคล ระดับความเสี่ยง และทรัพยากรที่ต้องใช้ให้สอดคล้องตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และตามประกาศนี้อย่างเคร่งครัด

ข้อ ๓ เจ้าหน้าที่อาจเลือกใช้มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ที่แตกต่างไปจากประกาศฉบับนี้ได้ หากมาตรฐานดังกล่าวมีมาตรการรักษาความมั่นคงปลอดภัยไม่ต่ำกว่าที่กำหนดในมาตรการนี้

หมวด ๑

มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

ข้อ ๔ เจ้าหน้าที่ต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลครอบคลุมถึงมาตรการป้องกันด้านการบริหารจัดการ (administrative safeguard) มาตรการป้องกันด้านเทคนิค (technical safeguard) และมาตรการป้องกันทางกายภาพ (physical safeguard) ในเรื่องการเข้าถึง หรือควบคุมการใช้งานข้อมูลส่วนบุคคล (access control) โดยอย่างน้อย ต้องประกอบด้วยการดำเนินการ ดังต่อไปนี้

- (๑) การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย
- (๒) การกำหนดเกี่ยวกับการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคล
- (๓) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาตแล้ว
- (๔) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งานของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคล โดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลส่วนบุคคล การลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล
- (๕) การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึงเปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

หมวด ๒

มาตรการการป้องกันรั่วไหลข้อมูลส่วนบุคคล

ข้อ ๕ ห้ามทำสำเนาเอกสารระบุตัวตนของผู้รับบริการโดยไม่จำเป็น เช่น บัตรประจำตัวประชาชน หรือ passport ไม่ว่าจะด้วยวิธีการ Xerox , Scan File , Email , Save File , Download , Print , ถ่ายรูปด้วยมือถือ เว้นแต่เป็นการการเก็บเข้าระบบหรือ Storage ของกรมการปกครอง ตามกระบวนการทำงานปกติ หรือเป็นไปตามหลักเกณฑ์ที่กรมการปกครองกำหนด

ข้อ ๖ ให้จัดทำใบรับส่งเอกสาร หรือ Checklist สำหรับการรับส่งเอกสารภายในและภายนอกองค์กรรวมถึงระบุประเภทเอกสารที่ต้องขอจากผู้รับบริการ ให้ผู้รับบริการลงนามต้องมีกระบวนการตรวจสอบความถูกต้อง และปิดผนึกให้เรียบร้อย เพื่อป้องกันการละเมิดหรือล่วงรู้ข้อมูลระหว่างทาง

ข้อ ๗ การจัดส่งเอกสารผ่านช่องทางต่างๆ ให้ดำเนินการ ดังนี้

- (๑) ใส่ซองปิดผนึก ระบุผู้รับให้ชัดเจน
- (๒) นำส่งด้วยตนเอง หรือผู้ได้รับมอบหมายจาก กรมการปกครอง โดยส่งถึงผู้รับบริการเท่านั้น เว้นแต่จะได้รับอนุญาตเป็นกรณี ๆ ไป
- (๓) กรณีผู้ให้บริการภายนอก ต้องเป็นผู้ที่ให้บริการที่ กรมการปกครอง กำหนดเท่านั้น
- (๔) กรณีส่งผ่านไปรษณีย์ ต้องส่งแบบปิดผนึก ระบุผู้รับอย่างเจาะจงและต้องมีมาตรการป้องกันการรั่วไหลของข้อมูลอื่นเพิ่มเติม เช่น การปิดบังข้อมูลสำคัญบางส่วนหรือให้ผู้ให้บริการส่งไปรษณีย์ที่กรมการปกครองกำหนดเท่านั้น
- (๕) ต้องมีการติดตามสถานการณ์จัดส่ง โดยเฉพาะกรณีที่เจ้าของข้อมูลมิได้เป็นผู้รับเอง
- (๖) ไม่ควรใช้ Line หรือ Email ส่วนตัว ในการปฏิบัติงานหรือการรับทำธุรกรรมใด ๆ ที่มีข้อมูลบุคคล และข้อมูลลับหรือลับมากของกรมการปกครอง

/ข้อ ๘ ให้จัดทำ...

ข้อ ๘ ให้จัดทำทะเบียนการให้ข้อมูลลับหรือลับมาก เพื่อให้สามารถระบุ ติดตาม ตรวจสอบ ข้อมูลผู้รับได้

ข้อ ๙ ให้ระบุชั้นความลับของเอกสาร ได้แก่ การจัดทำป้ายเพื่อระบุชั้นความลับที่เอกสาร เพิ่มและจัดเก็บให้สอดคล้องกับแนวทาง หรือมาตรการบริหารจัดการข้อมูลตามระดับชั้นความลับ

ข้อ ๑๐ ให้จัดทำทะเบียนบันทึก การทำลายเอกสาร และข้อมูลตามทะเบียนซึ่งอาจอยู่ใน รูปแบบเอกสารหรือไฟล์ทะเบียน

ข้อ ๑๑ วิธีการทำลายข้อมูลให้ดำเนินการ ดังนี้

(๑) การทำลายเอกสาร ให้ใช้เครื่องย่อยเอกสารชนิดที่ไม่สามารถนำกลับมาประกอบใหม่ หรือฉีกเอกสารก่อนหย่อนลงกล่อง

(๒) การลบข้อมูล หรือทำลายข้อมูลตามประเภทสื่อบันทึกข้อมูล จะต้องลบหรือทำลายข้อมูลนั้น ๆ ให้ไม่สามารถกู้คืนข้อมูลกลับมาใช้ได้อีก

ข้อ ๑๒ การบันทึกไฟล์งานให้บันทึกใน CLOUD DRIVE หรือระบบงานที่กรมการปกครอง จัดเตรียมไว้ให้เท่านั้น โดยจะต้องมีการดำเนินการจัดเก็บ ดังนี้

(๑) จัดเก็บโดยต้องมีการกำหนดวันที่บันทึกไฟล์

(๒) กำหนดสิทธิการเข้าถึงไฟล์ใน Folder หรือข้อมูลในระบบเฉพาะเจ้าหน้าที่ที่เกี่ยวข้อง

(๓) ต้องมีการเข้ารหัส (Encrypt) ด้วยสำหรับข้อมูลที่มีชั้นความลับ

ข้อ ๑๓ ในกรณีการส่งไฟล์ที่มีข้อมูลที่มีชั้นความลับ หรือลับมากระหว่างกันภายในองค์กร ให้ดำเนินการ ดังนี้

(๑) ให้จัดทำเป็น link และส่งให้ผู้ที่ต้องใช้ข้อมูลเข้ามาดูผ่าน link ดังกล่าว

(๒) หากไม่สามารถดำเนินการตาม (๑) ได้ และมีความจำเป็นจะต้องส่งเป็นไฟล์ให้ ดำเนินการ Encrypt ไฟล์ก่อนส่งทุกครั้ง โดยขอให้พิจารณาปิดบังข้อมูลบางส่วน และส่งเฉพาะบุคคลที่เกี่ยวข้องโดยตรงเท่านั้นกรณีเป็นผู้รับไฟล์ให้ปฏิบัติตามข้อ ๕ คือห้ามทำสำเนาหรือบันทึกข้อมูลเก็บไว้หลาย แห่งเกินความจำเป็น

ข้อ ๑๔ การใช้และลบบันทึกไฟล์ข้อมูลลับ ให้ดำเนินการ ดังนี้

(๑) กรณีมีความจำเป็นต้องใช้ข้อมูล ให้ย้ายไปเก็บอยู่ใน CLOUD DRIVE หรือ ระบบงานที่กรมการปกครองจัดเตรียมไว้ให้

(๒) กรณีต้องการเก็บไฟล์งานไว้ใช้อ้างอิงใน Folder ส่วนตัว ให้ดำเนินการนำข้อมูล ส่วนบุคคลออกก่อน และให้จัดเก็บได้ตามระยะเวลาที่ฝ่ายงานกำหนดหรือลบทิ้งเมื่อไม่ต้องใช้งานแล้ว

(๓) กรณีมีความจำเป็นต้องบันทึกไฟล์ที่มีข้อมูลส่วนบุคคล ออกมาใช้งาน บน Drive C , Drive D เช่น กรณีการทำงานบน Microsoft Office Online ให้ทำได้เฉพาะกับกรณีใช้เครื่อง คอมพิวเตอร์ของกรมการปกครองเท่านั้น

(๔) เมื่อทำงานเสร็จ และได้บันทึกไฟล์เข้าไปใน CLOUD DRIVE แล้วต้องลบไฟล์ ที่บันทึกไว้ในเครื่องคอมพิวเตอร์ทุกครั้งและหมั่นลบไฟล์ที่อยู่ในเครื่องทุกปี