



ประกาศศูนย์พิสูจน์หลักฐาน ๒
เรื่อง นโยบายด้านแนวทางการคุ้มครองข้อมูลส่วนบุคคล

โดยที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ มาตรา ๔ วรรคสาม บัญญัติให้ผู้ควบคุมข้อมูลส่วนบุคคลของหน่วยงานของรัฐต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐาน นั้น

เพื่อให้การปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานในศูนย์พิสูจน์หลักฐาน ๒ เป็นไปตามนโยบาย กฎหมาย ระเบียบ และคำสั่งที่เกี่ยวข้อง ให้สามารถนำไปปฏิบัติได้ ศูนย์พิสูจน์หลักฐาน ๒ จึงออกประกาศนโยบายด้านแนวทางการคุ้มครองข้อมูลส่วนบุคคล ดังต่อไปนี้

ข้อ ๑ วัตถุประสงค์และขอบเขตของประกาศ

๑.๑ การจัดทำนโยบายด้านแนวทางการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพ และเพื่อให้มีมาตรการเยียวยาเจ้าของข้อมูลส่วนบุคคลจากการถูกละเมิดสิทธิในข้อมูลส่วนบุคคลที่มีประสิทธิภาพ

๑.๒ กำหนดขอบเขตของการปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลโดยอ้างอิงประกาศของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และให้มีการปรับปรุงอย่างต่อเนื่อง

๑.๓ ประกาศนี้ ต้องเผยแพร่ให้ข้าราชการตำรวจได้รับทราบ และต้องถือปฏิบัติตามอย่างเคร่งครัด

๑.๔ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ทั้งข้าราชการตำรวจและบุคคลภายนอก ที่ปฏิบัติงานให้ศูนย์พิสูจน์หลักฐาน ๒ ตระหนักถึงความสำคัญของข้อมูลส่วนบุคคล เกี่ยวกับการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

๑.๕ ประกาศนี้ต้องมีการแก้ไขให้ถูกต้องโดยทบทวนปรับปรุงให้เป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๒ ประกาศนี้ให้มีผลบังคับใช้ตั้งแต่วันที่นี้เป็นต้นไป

ข้อ ๓ มาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคล

แนวปฏิบัติสำหรับการดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคล กำหนดกรอบการทำงานเป็นขั้นตอนการปฏิบัติของผู้ควบคุมข้อมูล ตามมาตรา ๓๗ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ ซึ่งผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลให้ครอบคลุมอย่างน้อย ๓ ประเด็น คือ ๑) การธำรงไว้ซึ่งความลับ (Confidentiality) ๒) ความถูกต้องครบถ้วน (Integrity) และ ๓) สภาพพร้อมใช้งาน (Availability) ของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อป้องกันการสูญหายเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ โดยอย่างน้อยควรประกอบด้วยการดำเนินการ ๓ มาตรการ ดังต่อไปนี้

๓.๑ มาตรการป้องกันด้านการบริหารจัดการ (Administrative Safeguard)

๓.๑.๑ มีการออกระเบียบ วิธีปฏิบัติ สำหรับควบคุมการเข้าถึงข้อมูลส่วนบุคคล และอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย เช่น กำหนดให้มีบันทึกการเข้าออกพื้นที่ กำหนดให้เจ้าหน้าที่รักษาความปลอดภัยตรวจสอบผู้มีสิทธิผ่าน เข้า-ออก มีการกำหนดรายชื่อผู้มีสิทธิเข้าถึง ทั้งนี้ความเข้มข้นของมาตรการ ให้เป็นไปตามระดับความเสี่ยงหรือความเสียหายที่อาจเกิดขึ้นหากข้อมูลส่วนบุคคลรั่วไหล ถูกแก้ไข ถูกคัดลอก หรือถูกทำลาย โดยมิชอบ

๓.๑.๒ มีการกำหนดเกี่ยวกับการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้งาน (User Responsibilities) แบ่งเป็น รูปแบบต่าง ๆ เช่น สิทธิในการเข้าสู่ แก้ไข เพิ่มเติมเปิดเผยและเผยแพร่ การตรวจสอบคุณภาพข้อมูล ตลอดจนการลบทำลาย

๓.๒ มาตรการป้องกันด้านเทคนิค (Technical Safeguard)

๓.๒.๑ การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล

๓.๒.๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) เพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาต ตามระดับสิทธิการใช้งาน ได้แก่ การนำเข้า เปลี่ยนแปลง แก้ไข เปิดเผย ตลอดจนการลบทำลาย

๓.๒.๓ จัดให้มีระบบสำรองและกู้คืนข้อมูล เพื่อให้ระบบ และ/หรือบริการต่างๆ ยังสามารถดำเนินการได้อย่างต่อเนื่อง

๓.๓ มาตรการป้องกันทางกายภาพ (Physical Safeguard) ในเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล (Access Control)

๓.๓.๑ มีการควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย เช่น มีบันทึกการเข้า-ออก พื้นที่มีเจ้าหน้าที่รักษาความปลอดภัยของพื้นที่ มีระบบกล้องวงจรปิดติดตั้ง มีการล้อมรั้วและล็อกประตูทุกครั้ง มีระบบบัตรผ่านเฉพาะผู้มีสิทธิเข้าออก ทั้งนี้ความเข้มข้นของมาตรการ ให้เป็นไปตามระดับความเสี่ยง หรือความเสียหายที่อาจเกิดขึ้นหากข้อมูลส่วนบุคคลรั่วไหล ถูกแก้ไข ถูกคัดลอก หรือ ถูกทำลายโดยมิชอบ

๓.๓.๒ กำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การเปิดเผย การลวงรู้ หรือการลักลอบ ทำสำเนาข้อมูลส่วนบุคคล การลักขโมยอุปกรณ์จัดเก็บ หรือประมวลผลข้อมูลส่วนบุคคล การลักลอบนำอุปกรณ์เข้าออก

ข้อ ๔ วิธีการปฏิบัติ

ศูนย์พิสูจน์หลักฐาน ๒ เป็นหน่วยงานภาครัฐขนาดใหญ่ และมีความซับซ้อนเกี่ยวข้องกับข้อมูลส่วนบุคคลจำนวนมาก การเก็บรวบรวมข้อมูลส่วนบุคคลของแต่ละหน่วยให้เก็บรวบรวมข้อมูลส่วนบุคคลที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล ดังนี้

๔.๑ ให้ข้าราชการตำรวจมีความรู้ความเข้าใจ และความตระหนักรู้ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒

๔.๒ ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดทำประกาศความเป็นส่วนตัว หรือ คำประกาศเกี่ยวกับความเป็นส่วนตัว (Privacy Notice) เพื่อแจ้งให้เจ้าของข้อมูลทราบถึงรายละเอียดก่อน หรือขณะเก็บรวบรวมข้อมูลส่วนบุคคล ตามมาตรา ๒๓ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒

๔.๓ จัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) เพื่อประโยชน์ในการบริหารจัดการข้อมูล และแจ้งให้ข้าราชการตำรวจในสังกัดได้ทราบถึงนโยบายและ แนวทางหรือกำหนดวิธีในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของบุคคลภายในหน่วยงาน

๔.๔ ผู้บังคับบัญชาจะต้องออกระเบียบ วิธีปฏิบัติ ประกาศ คำสั่ง หรือหนังสือสั่งการเกี่ยวกับมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคล ตามข้อ ๓ เพื่อป้องกันมิให้ข้อมูลส่วนบุคคลรั่วไหล รายละเอียดวิธีปฏิบัติ ด้านการคุ้มครองข้อมูลส่วนบุคคลให้เป็นไปตามเอกสารแนบท้ายประกาศนี้

ข้อ ๕ นโยบายด้านการคุ้มครองข้อมูลส่วนบุคคลนี้ เป็นมาตรการในการคุ้มครองข้อมูลส่วนบุคคลของศูนย์พิสูจน์หลักฐาน ๒ ซึ่งข้าราชการตำรวจ รวมทั้งลูกจ้าง และหน่วยงานภายนอกจะต้องปฏิบัติตามอย่างเคร่งครัด โดยที่ผู้ควบคุมข้อมูลส่วนบุคคลอาจเลือกใช้มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่แตกต่างไปจากประกาศฉบับนี้ได้ หากมาตรฐานดังกล่าวมีมาตรการรักษาความมั่นคงปลอดภัยไม่ต่ำกว่าที่กำหนดในประกาศนี้ และควรให้หน่วยที่มีอำนาจตีความและวินิจฉัยปัญหา อันเกิดจากการปฏิบัติตามประกาศนี้

ข้อ ๖ ทุกหน่วยงานต้องจัดให้มีคำประกาศเกี่ยวกับความเป็นส่วนตัว เพื่อแจ้งให้เจ้าของข้อมูลทราบ และควรมีนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) เพื่อประโยชน์ในการ บริหารจัดการข้อมูล และแจ้งให้ข้าราชการตำรวจในสังกัดได้ทราบถึงนโยบายด้านแนวทางการคุ้มครองข้อมูลส่วนบุคคล

ข้อ ๗ นโยบายด้านแนวทางการคุ้มครองข้อมูลส่วนบุคคลให้ผู้ควบคุมข้อมูลส่วนบุคคลของแต่ละหน่วยเป็นผู้รับผิดชอบ

ข้อ ๘ ให้ผู้ควบคุมข้อมูลส่วนบุคคลของหน่วยงานนั้นแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่
สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้าภายใน ๗๒ ชั่วโมงนับแต่ทราบเหตุ

ข้อ ๙ การออกนโยบายด้านแนวทางการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความ
ปลอดภัยครั้งต่อไป มอบหมายให้ ฝ่ายอำนวยการ ศูนย์พิสูจน์หลักฐาน ๒ เป็นผู้ดำเนินการ

ประกาศ ณ วันที่ ๑๖ ธันวาคม พ.ศ. ๒๕๖๘

พลตำรวจตรีหญิง



(อติมา ธรรมเมศรานนท์)

ผู้บังคับการศูนย์พิสูจน์หลักฐาน ๒

เอกสารประกอบการเตรียมความพร้อม
พ.ร.บ.ข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒

- เอกสาร ๑ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒
- เอกสาร ๒ พระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ พ.ศ.๒๕๖๓
- เอกสาร ๓ พระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ พ.ศ.๒๕๖๔
- เอกสาร ๔ แนวความคิดในการเตรียมความพร้อมจากหน่วยงานภาครัฐ
๓ หน่วยงาน
- ๔.๑ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)
 - ๔.๒ คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
 - ๔.๓ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)
- เอกสาร ๕ คู่มือการเตรียมความพร้อมเอกสารแม่แบบ (template) สำหรับการดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ของหน่วยงานในสังกัด ตร. ตามมาตรา ๓๗ แห่ง พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒
- เอกสาร ๖ ชุดเอกสารแม่แบบ (template) สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)
- เอกสาร ๗ แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Thailand Data Protection Guidelines ๓.๐ (Version ๓.๐ Extension)) เมษายน ๒๕๖๔ คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

