

ประกาศตำรวจภูธรภาค ๔
เรื่อง นโยบายด้านการคุ้มครองข้อมูลส่วนบุคคล

เพื่อให้การปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานในสังกัดตำรวจภูธรภาค ๔ เป็นไปตามนโยบาย กฎหมาย ระเบียบ และคำสั่งที่เกี่ยวข้อง ให้สามารถนำไปปฏิบัติได้อย่างมีประสิทธิภาพ และเป็นรูปธรรม อาศัยอำนาจตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ มาตรา ๔ วรรคสาม บัญญัติให้ผู้ควบคุมข้อมูลส่วนบุคคลของหน่วยงานของรัฐต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐาน นั้น ตำรวจภูธรภาค ๔ จึงออกประกาศนโยบายด้านการคุ้มครองข้อมูลส่วนบุคคล ดังต่อไปนี้

ข้อ ๑ ประกาศฉบับนี้เรียกว่า “ประกาศตำรวจภูธรภาค ๔ เรื่อง นโยบายด้านการคุ้มครองข้อมูลส่วนบุคคล”

ข้อ ๒ ประกาศนี้ให้มีผลบังคับใช้ตั้งแต่วันประกาศเป็นต้นไป

ข้อ ๓ ให้ยกเลิก “ประกาศตำรวจภูธรภาค ๔ เรื่อง นโยบายด้านแนวทางการคุ้มครองข้อมูลส่วนบุคคล ประกาศ ณ วันที่ ๒๕ มิถุนายน พ.ศ.๒๕๖๘”

ข้อ ๔ วัตถุประสงค์และขอบเขตของประกาศ

๔.๑ การจัดทำนโยบายด้านแนวทางการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพ และเพื่อให้มีมาตรการเยียวยาเจ้าของข้อมูลส่วนบุคคลจากการถูกละเมิดสิทธิในข้อมูลส่วนบุคคลที่มีประสิทธิภาพ

๔.๒ กำหนดขอบเขตของการปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลโดยอ้างอิงประกาศของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และให้มีการปรับปรุงอย่างต่อเนื่อง

๔.๓ ประกาศนี้ ต้องเผยแพร่ให้ข้าราชการตำรวจได้รับทราบ และต้องถือปฏิบัติตามอย่างเคร่งครัด

๔.๔ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ทั้งข้าราชการตำรวจและบุคคลภายนอกที่ปฏิบัติงานให้หน่วยงาน ตระหนักถึงความสำคัญของข้อมูลส่วนบุคคล เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

ข้อ ๕ ในประกาศฉบับนี้

“คณะกรรมการ” หมายความว่า คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตำรวจภูธรภาค ๔ ตามคำสั่ง ตำรวจภูธรภาค ๔ เรื่อง “แต่งตั้งคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของตำรวจภูธรภาค ๔”

“เจ้าของข้อมูล” หมายความว่า ข้าราชการตำรวจ ลูกจ้าง และบุคคลผู้เป็นเจ้าของข้อมูลส่วนบุคคล หรือผู้มีสิทธิโดยชอบด้วยกฎหมาย

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคล ซึ่งสามารถทำให้ระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรม

“ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า หัวหน้าส่วนราชการผู้มีหน้าที่และอำนาจระดับกองบังคับการในการตัดสินใจเกี่ยวกับการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของแต่ละส่วนราชการหรือหน่วยงานในสังกัดตำรวจภูธรภาค ๔

“เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล” หมายความว่า เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของตำรวจภูธรภาค ๔ ซึ่งถูกแต่งตั้งโดยผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้มีอำนาจหน้าที่ตรวจสอบการดำเนินงานของผู้ควบควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคล ประสานงานและให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล กรณีที่มีปัญหาเกี่ยวกับการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

“ผู้ประมวลผลข้อมูลส่วนบุคคล” หมายความว่า ผู้ดำเนินการเกี่ยวกับการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมาย หรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคล

ข้อ ๖ มาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคล

แนวปฏิบัติสำหรับการดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคล กำหนดกรอบการทำงานเป็นขั้นตอนการปฏิบัติของผู้ควบคุมข้อมูลส่วนบุคคล ต้องปฏิบัติตาม มาตรา ๓๗ และผู้ประมวลผลข้อมูลส่วนบุคคลต้องปฏิบัติตามมาตรา ๔๐ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ ซึ่งผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคล ต้องจัดให้มีมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลให้ครอบคลุมอย่างน้อย ๓ ประเด็น คือ ๑) การธำรงไว้ซึ่งความลับ (confidentiality) ๒) ความถูกต้อง ครบถ้วน (integrity) และ ๓) สภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ โดยอย่างน้อยควรประกอบด้วยการดำเนินการ ๓ มาตรการ ดังต่อไปนี้

๖.๑ มาตรการป้องกันด้านการบริหารจัดการ (administrative safeguard)

๖.๑.๑ มีการออกระเบียบ วิธีปฏิบัติ สำหรับควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย เช่น กำหนดให้มีบันทึกการเข้า-ออกพื้นที่ กำหนดให้เจ้าหน้าที่รักษาความปลอดภัยตรวจสอบผู้มีสิทธิผ่านเข้า-ออก มีการกำหนดรายชื่อผู้มีสิทธิเข้าถึง ทั้งนี้ความเข้มข้นของมาตรการ ให้เป็นไปตามระดับความเสี่ยงหรือความเสียหายที่อาจเกิดขึ้นหากข้อมูลส่วนบุคคลรั่วไหล ถูกแก้ไข ถูกคัดลอก หรือถูกทำลายโดยมิชอบ

๖.๑.๒ มีการกำหนดเกี่ยวกับการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้งาน (user responsibilities) แบ่งเป็น รูปแบบต่าง ๆ เช่น สิทธิในการเข้าดู แก้ไขเพิ่มเติม เปิดเผยและเผยแพร่ การตรวจสอบคุณภาพข้อมูล ตลอดจนการลบทำลาย

๖.๒ มาตรการป้องกันด้านเทคนิค (technical safeguard)

๖.๒.๑ การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

๖.๒.๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาต ตามระดับสิทธิการใช้งาน ได้แก่ การนำเข้า เปลี่ยนแปลง แก้ไข เปิดเผย ตลอดจนการลบทำลาย

๖.๒.๓ จัดให้มีระบบสำรองและกู้คืนข้อมูล เพื่อให้ระบบ และ/หรือบริการต่าง ๆ ยังสามารถดำเนินการได้อย่างต่อเนื่อง

๖.๓ มาตรการป้องกันทางกายภาพ (physical safeguard) ในเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล (access control)

๖.๓.๑ มีการควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย เช่น มีบันทึกการเข้า-ออกพื้นที่ มีเจ้าหน้าที่รักษาความปลอดภัยของพื้นที่ มีระบบกล้องวงจรปิดติดตั้ง มีการล้อมรั้วและล็อคประตูทุกครั้ง มีระบบบัตรผ่านเฉพาะผู้มีสิทธิเข้า-ออก ทั้งนี้ความเข้มข้นของมาตรการ ให้เป็นไปตามระดับความเสี่ยงหรือความเสียหายที่อาจเกิดขึ้นหากข้อมูลส่วนบุคคลรั่วไหล ถูกแก้ไข ถูกคัดลอก หรือถูกทำลาย โดยมิชอบ

๖.๓.๒ กำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลส่วนบุคคล การลักขโมยอุปกรณ์จัดเก็บ หรือประมวลผลข้อมูลส่วนบุคคล การลักลอบนำอุปกรณ์เข้า-ออก

ข้อ ๗ วิธีการปฏิบัติ

ตำรวจภูธรภาค ๔ เป็นหน่วยงานภาครัฐขนาดใหญ่ และมีความซับซ้อนเกี่ยวข้องกับข้อมูลส่วนบุคคลจำนวนมาก การเก็บรวบรวมข้อมูลส่วนบุคคลของแต่ละหน่วยให้เก็บรวบรวมข้อมูลส่วนบุคคลที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล จึงให้ผู้ควบคุมข้อมูลส่วนบุคคล ดำเนินการตามลำดับความสำคัญให้สอดคล้องกับข้อมูลส่วนบุคคลของหน่วย ดังนี้

๗.๑ จัดให้ข้าราชการตำรวจมีความรู้ความเข้าใจ และความตระหนักรู้ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเท่าที่จำเป็น และปฏิบัติตามมาตรการต่างๆ ตามที่ตำรวจภูธรภาค ๔ และสำนักงานตำรวจแห่งชาติ กำหนด

๗.๒ สำรวจข้อมูลส่วนบุคคลของหน่วยด้วยแบบสอบถาม เพื่อสำรวจ การเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคล เนื่องจากแต่ละหน่วยมีอำนาจหน้าที่และความรับผิดชอบแตกต่างกัน

๗.๓ จัดทำประกาศความเป็นส่วนตัว หรือคำประกาศเกี่ยวกับความเป็นส่วนตัว (privacy notice) เพื่อแจ้งให้เจ้าของข้อมูลทราบถึงรายละเอียดก่อนหรือขณะเก็บรวบรวมข้อมูลส่วนบุคคล และจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคล (privacy policy) เพื่อประโยชน์ในการบริหารจัดการข้อมูล และแจ้งให้ข้าราชการตำรวจในสังกัดทราบถึงนโยบายและแนวปฏิบัติในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลภายในหน่วยงาน ให้สอดคล้องตาม มาตรา ๒๓ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒

๗.๔ จัดทำเอกสารอื่นใด นอกจากข้อ ๗.๓ ได้แก่ ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล ข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล การบันทึกรายการประมวลผลข้อมูลส่วนบุคคล นโยบายคุกกี้ เอกสารแสดงความยินยอม แบบคำร้องใช้สิทธิของเจ้าของข้อมูล หนังสือตอบกลับการใช้สิทธิของเจ้าของข้อมูล หนังสือแจ้งเหตุละเมิดข้อมูลส่วนบุคคล คำประกาศเกี่ยวกับความเป็นส่วนตัวในการใช้กล้องวงจรปิด นโยบายการใช้เทคโนโลยีปัญญาประดิษฐ์และเอกสารอื่นใด ให้ผู้ควบคุมข้อมูลส่วนบุคคลพิจารณาดำเนินการให้สอดคล้องกับข้อมูลส่วนบุคคลที่ดำเนินการเก็บ รวบรวม ใช้ หรือเปิดเผยแล้วแต่กรณี

๗.๕ จัดทำระเบียบ วิธีปฏิบัติ ประกาศ คำสั่ง หรือหนังสือกำชับ หนังสือสั่งการให้เป็นไปตามมาตรฐานด้านมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ตามข้อ ๖ เพื่อป้องกัน

ข้อมูลรั่วไหล นอกจากนี้ยังมีแนวทางการปฏิบัติและหลักเกณฑ์การประเมินความสอดคล้องด้านการคุ้มครองข้อมูลส่วนบุคคลด้านอื่นๆ ที่เกี่ยวข้อง ได้แก่ ด้านองค์กรและการกำกับดูแล ด้านนโยบายและแนวปฏิบัติ ด้านการอบรมและการสร้างความตระหนักรู้ ด้านสิทธิของเจ้าของข้อมูลส่วนบุคคล ด้านการเจ้งวัตถุประสงค์และความโปร่งใส ด้านการจัดทำบันทึกรายการและฐานทางกฎหมาย ด้านข้อตกลงการประมวลผลข้อมูลส่วนบุคคล และการแบ่งปันข้อมูลส่วนบุคคล ด้านความเสี่ยงและการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล

ข้อ ๘ หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคลและเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ ดังนี้

๘.๑ ผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่ จัดให้มีมาตรการรักษาความปลอดภัยที่เหมาะสมตามมาตรา ๓๗ บันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล โดยจะบันทึกเป็นหนังสือหรือระบบอิเล็กทรอนิกส์ ตามมาตรา ๓๙ และต้องจัดให้มีข้อตกลงประมวลผลข้อมูลส่วนบุคคล ตามมาตรา ๔๐

๘.๒ ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคล จัดให้มีมาตรการรักษาความปลอดภัยที่เหมาะสม จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล มาตรา ๔๐

๘.๓ ผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคล จะจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของหน่วยก็ได้ โดยให้พิจารณาตามแต่ละกรณีของมาตรา ๔๑ ทั้งนี้ในส่วนของตำรวจภูธรภาค ๔ มีหัวหน้าส่วนราชการผู้มีหน้าที่ และอำนาจระดับกองบังคับการเป็นคณะกรรมการ ควรจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เนื่องจากเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล มีหน้าที่ให้คำแนะนำ และตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ประสานงานและให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และรักษาความลับของข้อมูลส่วนบุคคล ตามมาตรา ๔๒

ข้อ ๙ การแจ้งเหตุละเมิด และรายงานเรื่องร้องทุกข์ร้องเรียน

ให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งเหตุละเมิดข้อมูลส่วนบุคคลแก่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของตำรวจภูธรภาค ๔ และของสำนักงานตำรวจแห่งชาติ โดยไม่ชักช้าภายในยี่สิบสี่ชั่วโมงนับแต่ทราบเหตุ และ แจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล โดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถทำได้ ตามมาตรา ๓๗ (๔) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒

สำหรับกรณีการรายงานเรื่องร้องเรียนด้านการคุ้มครองข้อมูลส่วนบุคคลของข้าราชการตำรวจ หรือหน่วยงาน ทั้งจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และหน่วยงานที่เกี่ยวข้อง และกรณีการแจ้งร้องทุกข์ในความผิดที่มีบทกำหนดโทษทางอาญา (ตามมาตรา ๗๙ มาตรา ๘๐ และมาตรา ๘๑) ให้หัวหน้าส่วนราชการระดับกองบังคับการ รายงานผลการดำเนินการให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตำรวจภูธรภาค ๔ ทราบ ภายในระยะเวลาที่กำหนด นับแต่วันที่ได้รับเรื่อง

ข้อ ๑๐ ประกาศตำรวจภูธรภาค ๔ เรื่อง นโยบายด้านการคุ้มครองข้อมูลส่วนบุคคล นี้เป็นมาตรการในการคุ้มครองข้อมูลส่วนบุคคลของตำรวจภูธรภาค ๔ ซึ่งข้าราชการตำรวจ รวมทั้งลูกจ้าง และหน่วยงานภายนอก จะต้องปฏิบัติตามอย่างเคร่งครัด โดยที่ผู้ควบคุมข้อมูลส่วนบุคคลอาจเลือกใช้มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่แตกต่างไปจากประกาศฉบับนี้ได้ หากมาตรฐานดังกล่าวมีมาตรการรักษาความมั่นคงปลอดภัยไม่ต่ำกว่าที่กำหนดในประกาศนี้

ข้อ ๑๑ ประกาศตำรวจภูธรภาค ๔ เรื่อง นโยบายด้านการคุ้มครองข้อมูลส่วนบุคคล นี้ ให้ส่วนราชการระดับกองบังคับการในฐานะผู้ควบคุมข้อมูลส่วนบุคคลของแต่ละหน่วยเป็นผู้รับผิดชอบ หากเกิดปัญหาในการปฏิบัติให้รายงานปัญหาต่อ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของตำรวจภูธรภาค ๔ ได้รับทราบ

ข้อ ๑๒ มอบหมายให้กองบังคับการอำนวยการ ตำรวจภูธรภาค ๔ เป็นผู้ดำเนินการออกประกาศในครั้งต่อไป และมอบหมายให้กองบังคับการกฎหมายและคดี ตำรวจภูธรภาค ๔ ดำเนินการในส่วนที่เกี่ยวข้องด้านกฎหมายนโยบายด้านการคุ้มครองข้อมูลส่วนบุคคลนี้

ข้อ ๑๓ แนวทางในการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลตามประกาศตำรวจภูธรภาค ๔ ฉบับนี้ ให้เป็นไปตามที่ผู้บัญชาการตำรวจภูธรภาค ๔ กำหนด

ประกาศ ณ วันที่ ๑๖ มกราคม พ.ศ.๒๕๖๙

พลตำรวจโท

(สันติ ชัยนิรามัย)

ผู้บัญชาการตำรวจภูธรภาค ๔