

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เรื่อง หลักเกณฑ์ในการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคล เป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้

พ.ศ. ๒๕๖๗

โดยที่มาตรา ๓๓ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ กำหนดให้ เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ซึ่งคณะกรรมการ คุ้มครองข้อมูลส่วนบุคคลอาจกำหนดหลักเกณฑ์ในการดำเนินการดังกล่าวก็ได้ เพื่อให้เกิดความชัดเจน ในการดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคล

อาศัยอำนาจตามความในมาตรา ๑๖ (๔) ประกอบมาตรา ๓๓ วรรคห้า แห่งพระราชบัญญัติ คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์ ในการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของ ข้อมูลส่วนบุคคลได้ พ.ศ. ๒๕๖๗”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนดเก้าสิบวันนับแต่วันประกาศในราชกิจจานุเบกษา เป็นต้นไป

ข้อ ๓ เมื่อเจ้าของข้อมูลส่วนบุคคลใช้สิทธิตามมาตรา ๓๓ แห่งพระราชบัญญัติคุ้มครอง ข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ และไม่ใช้กรณีที่ ได้รับยกเว้นการใช้บังคับตามมาตรา ๓๓ วรรคสอง ให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามที่ เจ้าของข้อมูลส่วนบุคคลร้องขอโดยไม่ชักช้า แต่ต้องไม่เกินเก้าสิบวันนับแต่วันที่รับคำขอ

การดำเนินการตามวรรคหนึ่ง จะต้องดำเนินการให้ครอบคลุมถึงข้อมูลส่วนบุคคลที่ทำสำเนา หรือสำรองไว้ด้วย (ถ้ามี) และจะต้องทำให้แน่ใจว่าไม่มีผู้ใดสามารถกระทำการด้วยวิธีการใด ๆ ที่อาจ คาดหมายได้ตามสมควร เพื่อกู้คืนข้อมูลส่วนบุคคลหรือทำให้ข้อมูลนั้นย้อนกลับมาสามารถระบุตัวบุคคล ที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ไม่ว่าทางตรงหรือทางอ้อม

ในกรณีที่เจ้าของข้อมูลส่วนบุคคลใช้สิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ เพียงอย่างเดียวหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลอาจดำเนินการลบหรือทำลาย หรือทำให้ข้อมูล ส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ด้วยวิธีการอย่างอื่น

ตามประกาศนี้ ซึ่งอาจแตกต่างจากที่เจ้าของข้อมูลส่วนบุคคลร้องขอก็ได้ โดยผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่แจ้งให้เจ้าของข้อมูลส่วนบุคคลที่ใช้สิทธิทราบด้วย เว้นแต่จะเป็นกรณีตามข้อ ๗

ข้อ ๔ ในการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ตามข้อ ๓ หากไม่สามารถดำเนินการดังกล่าวได้ตามระยะเวลาที่กำหนดในข้อ ๓ เช่น กรณีข้อมูลส่วนบุคคลที่อยู่ในรูปแบบอิเล็กทรอนิกส์ ยังคงถูกเก็บบันทึกไว้ชั่วคราวระหว่างที่รอให้ถูกบันทึกทับหรือแทนที่โดยข้อมูลอื่น (to be overwritten by other data) เนื่องจากเหตุผลทางเทคนิค ผู้ควบคุมข้อมูลส่วนบุคคลต้องทำให้ข้อมูลส่วนบุคคลนั้นอยู่ในรูปแบบที่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลดังกล่าวเป็นไปได้ยาก จนกว่าจะดำเนินการตามข้อ ๓ แล้วเสร็จ โดยต้องจัดให้มีมาตรการเชิงองค์กร (organizational measures) และมาตรการเชิงเทคนิค (technical measures) ที่เหมาะสม ซึ่งอาจรวมถึงมาตรการทางกายภาพ (physical measures) ที่จำเป็นด้วย โดยคำนึงถึงปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน ลักษณะหรือประเภทของข้อมูลส่วนบุคคล ลักษณะ ประเภท หรือสถานะของเจ้าของข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน ทั้งนี้ เพื่อให้เป็นไปตามหลักเกณฑ์ ดังต่อไปนี้

(๑) ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้องไม่มีเจตนาที่จะเข้าถึง หรือนำข้อมูลส่วนบุคคลดังกล่าวมาใช้หรือเปิดเผยอีกต่อไป แม้จะยังมีข้อมูลดังกล่าวอยู่ก็ตาม

(๒) ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้องไม่สามารถนำข้อมูลส่วนบุคคลดังกล่าวมาใช้หรือเปิดเผย เพื่อให้บริการหรือมีผลต่อการตัดสินใจหรือดำเนินการใด ๆ เกี่ยวกับเจ้าของข้อมูลส่วนบุคคล หรือในลักษณะที่จะส่งผลกระทบต่อบุคคลในทางใดทางหนึ่งได้

(๓) ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้องต้องป้องกันมิให้ผู้ใดสามารถเข้าถึง ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลดังกล่าวได้

(๔) ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้องต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลดังกล่าวอย่างเหมาะสมตามระดับความเสี่ยง

(๕) ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้องจะต้องทำการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ตามประกาศนี้ เมื่อสามารถกระทำได้โดยไม่ชักช้า

ข้อ ๕ ความในข้อ ๓ มิให้นำมาใช้บังคับกับข้อมูลส่วนบุคคลที่ไม่อาจลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ เนื่องจากเหตุผลความจำเป็นอย่างยิ่ง เช่น กรณีที่การลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้นั้น อาจส่งผลกระทบต่อสิทธิในข้อมูลส่วนบุคคลหรือประโยชน์ของบุคคลอื่น ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่

แจ้งให้เจ้าของข้อมูลส่วนบุคคลที่ใช้สิทธิทราบพร้อมชี้แจงหรือแสดงให้เห็นถึงเหตุผลความจำเป็นที่สำคัญดังกล่าวแก่เจ้าของข้อมูลส่วนบุคคลด้วย

ข้อ ๖ ในการทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ หรือการทำให้เป็นข้อมูลนิรนาม (anonymization) ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการให้เป็นไปตามหลักเกณฑ์ ดังต่อไปนี้

(๑) จะต้องมีการลบหรือทำให้ปราศจากข้อมูลใด ๆ ที่เป็นตัวระบุทางตรง (direct identifiers) ของเจ้าของข้อมูลส่วนบุคคลในข้อมูลส่วนบุคคลดังกล่าว (de-identification) ซึ่งรวมถึงข้อมูลดังต่อไปนี้

(ก) ชื่อตัว ชื่อรอง หรือชื่อสกุลของบุคคล

(ข) เลขประจำตัวประชาชน เลขที่หนังสือเดินทาง เลขประจำตัวผู้เสียภาษีของบุคคล เลขที่บัตรประกันสังคม ตลอดจนเลขที่ หมายเลข หรือรหัสของบัตรประจำตัวอื่นใดของบุคคล

(ค) เลขที่ หมายเลข หรือรหัสสมาชิก ลูกค้า ผู้รับบริการ หรือบุคลากร ตลอดจนเลขที่ หมายเลข หรือรหัสของบัญชี สัญญา หรือสิ่งอื่นใดที่เป็นของเฉพาะตัวของบุคคล

(ง) หมายเลขโทรศัพท์ หมายเลขโทรสาร หรือหมายเลขติดต่อเฉพาะตัวของบุคคล

(จ) ที่อยู่ไปรษณีย์อิเล็กทรอนิกส์ (e-mail address) เฉพาะตัวของบุคคล

(ฉ) หมายเลขทะเบียนรถของบุคคล

(ช) ภาพใบหน้าของบุคคลที่ทำให้สามารถระบุตัวบุคคลได้

(ซ) ข้อมูลชีวภาพ (biometric data) ของบุคคลที่ทำให้สามารถระบุตัวบุคคลได้

(ฌ) ชื่อหรือรหัสบัญชีผู้ใช้งานในระบบสารสนเทศ แอปพลิเคชัน หรือบริการต่าง ๆ ที่เป็นของเฉพาะตัวของบุคคล

(ญ) ข้อมูลอื่นใดที่เป็นสิ่งเฉพาะตัวของบุคคลที่ทำให้สามารถระบุตัวบุคคลได้โดยตรง

(๒) หลังจากการดำเนินการตาม (๑) จะต้องมีการพิจารณาดำเนินการเพิ่มเติมเพื่อให้แน่ใจว่าข้อมูลดังกล่าวเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ทางอ้อม โดยมีโอกาสในการระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ในระดับที่ต่ำเพียงพอ ทั้งนี้ เพื่อป้องกันการทำให้ข้อมูลนั้นย้อนกลับมาสามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ (re-identification) โดยอาจพิจารณาทำการแฝงข้อมูล (pseudonymization) หรือดำเนินการอย่างหนึ่งอย่างใดต่อข้อมูลทั้งหมดหรือบางส่วน เพื่อลดโอกาสในการระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลจากข้อมูลที่เป็นตัวระบุทางอ้อม (indirect identifiers) เช่น วันเดือนปีเกิด อายุ ตำแหน่งงาน สังกัด วันเดือนปีที่เข้ารับบริการ ที่อยู่สำหรับพักอาศัยหรือสถานที่ทำงาน เลขที่อยู่ไอพี (Internet Protocol address หรือ IP address) หรือข้อมูลอื่นใดที่มีลักษณะคล้ายกัน ให้อยู่ในระดับที่ต่ำเพียงพอ

ในการดำเนินการตาม (๒) ให้ผู้ควบคุมข้อมูลส่วนบุคคลพิจารณาดำเนินการโดยคำนึงถึงปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการ

ในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน ลักษณะหรือประเภทของข้อมูลส่วนบุคคล ลักษณะประเภท หรือสถานะของเจ้าของข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการ ตลอดจนความเสี่ยง แรงจูงใจ และความสามารถของบุคคลที่อาจประสงค์จะทำให้ข้อมูลนั้น ย้อนกลับมาสามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ (re-identification) ประกอบกัน

ข้อ ๗ ในกรณีที่เจ้าของข้อมูลส่วนบุคคลใช้สิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ เนื่องจากเป็นกรณีที่ข้อมูลส่วนบุคคลได้ถูกเก็บรวบรวม ใช้ หรือเปิดเผยโดยไม่ชอบด้วยกฎหมายตามมาตรา ๓๓ (๔) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และไม่ใช่วินิจฉัยที่ได้รับยกเว้นการใช้บังคับตามมาตรา ๓๓ วรรคสอง หรือกรณีอื่นที่ผู้ควบคุมข้อมูลส่วนบุคคลอาจปฏิเสธคำขอได้ตามกฎหมาย ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเท่านั้น โดยไม่อาจดำเนินการทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ตามข้อ ๖ แทนได้

ข้อ ๘ เมื่อผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ตามคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลแล้ว ให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งให้เจ้าของข้อมูลส่วนบุคคลที่ใช้สิทธิทราบ

ในกรณีที่การดำเนินการตามวรรคหนึ่ง เป็นการทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ตามข้อ ๖ ให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งรายละเอียดในการดำเนินการดังกล่าวให้เจ้าของข้อมูลส่วนบุคคลทราบตามสมควร เว้นแต่เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดนั้นอยู่แล้ว

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อาจดำเนินการตามคำขอใช้สิทธิตามวรรคหนึ่งได้ ให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งให้เจ้าของข้อมูลส่วนบุคคลที่ใช้สิทธิทราบพร้อมเหตุผล

ข้อ ๙ นอกจากการดำเนินการตามที่เจ้าของข้อมูลส่วนบุคคลใช้สิทธิตามมาตรา ๓๓ วรรคหนึ่ง แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลตามมาตรา ๓๗ (๓) ด้วย โดยให้นำข้อ ๓ วรรคสองและวรรคสาม ข้อ ๔ ข้อ ๕ และข้อ ๖ ของประกาศนี้มาใช้บังคับโดยอนุโลม

ข้อ ๑๐ ให้ประธานกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นผู้รักษาการตามประกาศนี้

ประกาศ ณ วันที่ ๓๑ กรกฎาคม พ.ศ. ๒๕๖๗

เจียรชัย ณ นคร

ประธานกรรมการคุ้มครองข้อมูลส่วนบุคคล