ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

อาศัยอำนาจตามความในมาตรา ๑๖ (๔) ประกอบมาตรา ๓๗ (๔) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล จึงออกประกาศไว้ดังต่อไปนี้

ข้อ ๑ ประกาศฉบับนี้เรียกว่า “ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“การละเมิดข้อมูลส่วนบุคคล” หมายความว่า การละเมิดมาตรการรักษาความมั่นคงปลอดภัยที่ทำให้เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ไม่ว่าจะเกิดจากเจตนา ความจงใจ ความประมาทเลินเล่อ การกระทำโดยปราศจากอำนาจหรือโดยมิชอบ การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ภัยคุกคามทางไซเบอร์ ข้อผิดพลาดบกพร่องหรืออุบัติเหตุ หรือเหตุอื่นใด

“สำนักงาน” หมายความว่า สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

“คณะกรรมการ” หมายความว่า คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ข้อ ๔ เหตุการละเมิดข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องแจ้งแก่สำนักงานหรือเจ้าของข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ประกอบด้วยเหตุที่เกิดจากการละเมิดมาตรการรักษาความมั่นคงปลอดภัย ที่ทำให้เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ไม่ว่าจะเกิดจากเจตนา ความจงใจ ความประมาทเลินเล่อ การกระทำโดยปราศจากอำนาจหรือโดยมิชอบ การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ภัยคุกคามทางไซเบอร์ ข้อผิดพลาดบกพร่องหรืออุบัติเหตุ หรือเหตุอื่นใด ซึ่งอาจเกิดจากการกระทำของผู้ควบคุมข้อมูลส่วนบุคคลนั้นเอง ผู้ประมวลผลข้อมูลส่วนบุคคลที่ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคลนั้น ตลอดจนพนักงาน ลูกจ้าง ผู้รับจ้าง ตัวแทน หรือบุคคลที่เกี่ยวข้องของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลดังกล่าว หรือบุคคลอื่น หรือเหตุปัจจัยอื่น โดยเหตุการละเมิดข้อมูลส่วนบุคคลแต่ละเหตุอาจเกี่ยวข้องกับการละเมิดประเภทใดประเภทหนึ่งหรือหลายประเภท ดังต่อไปนี้

(๑) การละเมิดความลับของข้อมูลส่วนบุคคล (Confidentiality Breach) ซึ่งมีการเข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ หรือเกิดจากข้อผิดพลาดบกพร่องหรืออุบัติเหตุ

(๒) การละเมิดความถูกต้องครบถ้วนของข้อมูลส่วนบุคคล (Integrity Breach) ซึ่งมีการเปลี่ยนแปลง แก้ไขข้อมูลส่วนบุคคลให้ไม่ถูกต้อง ไม่สมบูรณ์ หรือไม่ครบถ้วน โดยปราศจากอำนาจหรือโดยมิชอบ หรือเกิดจากข้อผิดพลาดบกพร่องหรืออุบัติเหตุ

(๓) การละเมิดความพร้อมใช้งานของข้อมูลส่วนบุคคล (Availability Breach) ซึ่งทำให้ไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้ หรือมีการทำลายข้อมูลส่วนบุคคล ทำให้ข้อมูลส่วนบุคคลไม่อยู่ในสภาพที่พร้อมใช้งานได้ตามปกติ

ข้อ ๕ เมื่อผู้ควบคุมข้อมูลส่วนบุคคลได้รับแจ้งข้อมูลในเบื้องต้นจากผู้ใด ไม่ว่าโดยทางวาจา เป็นหนังสือ หรือวิธีการอื่นทางอิเล็กทรอนิกส์ หรือผู้ควบคุมข้อมูลส่วนบุคคลทราบเอง ว่ามีหรือน่าจะมีเหตุการละเมิดข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการ ดังต่อไปนี้

(๑) ประเมินความน่าเชื่อถือของข้อมูลดังกล่าว และตรวจสอบข้อเท็จจริงเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลในเบื้องต้นโดยไม่ชักช้าเท่าที่จะสามารถกระทำได้ ว่ามีเหตุอันควรเชื่อได้ว่ามีการละเมิดข้อมูลส่วนบุคคลหรือไม่ โดยผู้ควบคุมข้อมูลส่วนบุคคลพึงดำเนินการตรวจสอบมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ทั้งมาตรการเชิงองค์กร (organizational measures) และมาตรการเชิงเทคนิค (technical measures) ซึ่งอาจรวมถึงมาตรการทางกายภาพ (physical measures) ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลดังกล่าว ทั้งในส่วนที่เกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคลนั้นเอง ผู้ประมวลผลข้อมูลส่วนบุคคลที่ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคลนั้น ตลอดจนพนักงาน ลูกจ้าง ผู้รับจ้าง ตัวแทน หรือบุคคลที่เกี่ยวข้องของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลดังกล่าว เพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถยืนยันได้ว่ามีการละเมิดข้อมูลส่วนบุคคลเกิดขึ้นหรือไม่ ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคลต้องพิจารณารายละเอียดจากข้อเท็จจริงที่เกี่ยวข้อง รวมทั้งประเมินความเสี่ยงที่การละเมิดข้อมูลส่วนบุคคลดังกล่าวจะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

(๒) หากระหว่างการตรวจสอบข้อเท็จจริงเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลตาม (๑) พบว่ามีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการด้วยตนเองหรือสั่งการให้ผู้ประมวลผลข้อมูลส่วนบุคคลหรือผู้เกี่ยวข้องดำเนินการป้องกัน ระงับ หรือแก้ไขเพื่อให้การละเมิดข้อมูลส่วนบุคคลสิ้นสุดหรือไม่ให้การละเมิดข้อมูลส่วนบุคคลส่งผลกระทบเพิ่มเติม โดยทันทีเท่าที่จะสามารถกระทำได้ ทั้งนี้ อาจใช้มาตรการทางบุคลากร กระบวนการ หรือเทคโนโลยีที่จำเป็นและเหมาะสม

(๓) เมื่อพิจารณาจากข้อเท็จจริงตาม (๑) แล้วเห็นว่า มีเหตุอันควรเชื่อว่ามีการละเมิดข้อมูลส่วนบุคคลจริง ให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งเหตุการละเมิดแก่สำนักงานโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

(๔) ในกรณีที่การละเมิดข้อมูลส่วนบุคคลดังกล่าวมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย

(๕) ดำเนินการตามมาตรการที่จำเป็นและเหมาะสมเพื่อระงับ ตอบสนอง แก้ไข หรือฟื้นฟูสภาพจากเหตุการละเมิดข้อมูลส่วนบุคคลดังกล่าว รวมทั้งป้องกันและลดผลกระทบจากการเกิดเหตุการละเมิดข้อมูลส่วนบุคคลในลักษณะเดียวกันในอนาคต ซึ่งรวมถึงการทบทวนมาตรการรักษาความมั่นคงปลอดภัยเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม โดยคำนึงถึงระดับความเสี่ยงตามปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน ลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

ข้อ ๖ ในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงาน ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลเป็นลายลักษณ์อักษร หรือแจ้งผ่านโดยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใดตามที่สำนักงานกำหนด โดยในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลต้องระบุสาระสำคัญดังต่อไปนี้เท่าที่จะสามารถกระทำได้

(๑) ข้อมูลโดยสังเขปเท่าที่จะสามารถระบุได้เกี่ยวกับลักษณะและประเภทของการละเมิดข้อมูลส่วนบุคคล โดยอาจบรรยายถึงลักษณะและจำนวนเจ้าของข้อมูลส่วนบุคคลหรือลักษณะและจำนวนรายการ (records) ของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด

(๒) ชื่อ สถานที่ติดต่อ และวิธีการติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในกรณีที่มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือชื่อ สถานที่ติดต่อ และวิธีการติดต่อของบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลมอบหมายให้ทำหน้าที่ประสานงานและให้ข้อมูลเพิ่มเติม

(๓) ข้อมูลเกี่ยวกับผลกระทบที่อาจเกิดขึ้นจากเหตุการละเมิดข้อมูลส่วนบุคคล

(๔) ข้อมูลเกี่ยวกับมาตรการที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือจะใช้เพื่อป้องกัน ระงับ หรือแก้ไขเหตุการละเมิดข้อมูลส่วนบุคคล หรือเยียวยาความเสียหาย โดยอาจใช้มาตรการทางบุคลากร กระบวนการ หรือเทคโนโลยี หรือมาตรการอื่นใดที่จำเป็นและเหมาะสม

ข้อ ๗ ในกรณีที่มีเหตุจำเป็นที่ทำให้แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลล่าช้ากว่าเจ็ดสิบสองชั่วโมงนับแต่ทราบเหตุ ไม่ว่าจะเกิดจากการตรวจสอบข้อมูลในเบื้องต้น การดำเนินการป้องกัน ระงับ หรือแก้ไขเหตุการละเมิดข้อมูลส่วนบุคคลที่จำเป็น หรือมีเหตุจำเป็นอื่นอันไม่อาจก้าวล่วงได้ ผู้ควบคุมข้อมูลส่วนบุคคลอาจขอให้สำนักงานพิจารณายกเว้นความผิดจากการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลล่าช้าได้ โดยให้ผู้ควบคุมข้อมูลส่วนบุคคลชี้แจงเหตุผลความจำเป็นและรายละเอียดที่เกี่ยวข้องเพื่อแสดงให้เห็นว่ามีเหตุจำเป็นที่ไม่อาจหลีกเลี่ยงได้ที่ทำให้แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลล่าช้า โดยจะต้องแจ้งแก่สำนักงานโดยเร็ว ทั้งนี้ ต้องไม่เกินสิบห้าวันนับแต่ทราบเหตุ

สำนักงานอาจแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลชี้แจงเหตุผลหรือข้อเท็จจริงเพิ่มเติมภายหลังได้ และหากสำนักงานพิจารณาแล้วเห็นควรให้ยกเว้นความผิดจากการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลล่าช้า เนื่องจากมีเหตุจำเป็น ให้ถือว่าผู้ควบคุมข้อมูลส่วนบุคคลได้รับยกเว้นการดำเนินการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานตามกำหนดเวลาในมาตรา ๓๗ (๔)

การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานไม่เป็นเหตุยกเว้นหน้าที่หรือความรับผิดของผู้ควบคุมข้อมูลส่วนบุคคลตามกฎหมายเฉพาะที่เกี่ยวข้องกับกิจการนั้นหรือกฎหมายอื่น

ข้อ ๘ ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลมีข้อตกลงกับผู้ประมวลผลข้อมูลส่วนบุคคลเพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรือมอบหมายหรือสั่งการให้ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของตนเอง ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องระบุไว้ในข้อตกลงหรือในสัญญาที่เกี่ยวข้องให้ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่ผู้ควบคุมข้อมูลส่วนบุคคลโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมงนับแต่ผู้ประมวลผลข้อมูลส่วนบุคคลทราบเหตุเท่าที่จะสามารถกระทำได้เช่นกัน

ข้อ ๙ ผู้ควบคุมข้อมูลส่วนบุคคลอาจยกข้อยกเว้นการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานเพื่อประกอบการพิจารณาได้ หากผู้ควบคุมข้อมูลส่วนบุคคลพิสูจน์ได้ว่าเหตุการละเมิดข้อมูลส่วนบุคคลนั้น ไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ซึ่งรวมถึงกรณีที่ข้อมูลส่วนบุคคลตามเหตุการละเมิดข้อมูลส่วนบุคคลนั้น เป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ หรือข้อมูลส่วนบุคคลนั้นไม่อยู่ในสภาพที่ใช้งานได้เนื่องจากมีมาตรการทางเทคโนโลยีที่เพียงพอ หรือเหตุอื่นใดที่เชื่อถือได้

ในการยกข้อยกเว้นดังกล่าว ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ให้ข้อมูลหรือส่งเอกสารหรือหลักฐานเกี่ยวกับเหตุที่ควรได้รับการยกเว้น ซึ่งรวมถึงรายละเอียดเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลหรือข้อมูลอื่นใด ให้สำนักงานพิจารณา

ข้อ ๑๐ เมื่อมีเหตุการละเมิดข้อมูลส่วนบุคคลและผู้ควบคุมข้อมูลส่วนบุคคลได้แจ้งเหตุการละเมิดแก่สำนักงานแล้วหรืออยู่ระหว่างการเตรียมการเพื่อแจ้งสำนักงาน หากผู้ควบคุมข้อมูลส่วนบุคคลได้ตรวจสอบข้อเท็จจริงแล้วพบว่า การละเมิดข้อมูลส่วนบุคคลดังกล่าวมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลพร้อมสาระสำคัญดังต่อไปนี้ให้เจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบทราบเท่าที่จะสามารถกระทำได้โดยไม่ชักช้า

(๑) ข้อมูลโดยสังเขปเกี่ยวกับลักษณะของการละเมิดข้อมูลส่วนบุคคล

(๒) ชื่อ สถานที่ติดต่อ และวิธีการติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลมอบหมายให้ทำหน้าที่ประสานงาน

(๓) ข้อมูลเกี่ยวกับผลกระทบที่อาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคลจากเหตุการละเมิดข้อมูลส่วนบุคคล

(๔) แนวทางการเยียวยาความเสียหายของเจ้าของข้อมูลส่วนบุคคล และข้อมูลโดยสังเขปเกี่ยวกับมาตรการที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือจะใช้เพื่อป้องกัน ระงับ หรือแก้ไขเหตุการละเมิดข้อมูลส่วนบุคคล โดยอาจใช้มาตรการทางบุคลากร กระบวนการ หรือเทคโนโลยี หรือมาตรการอื่นใดที่จำเป็นและเหมาะสม รวมถึงข้อแนะนำเกี่ยวกับมาตรการที่เจ้าของข้อมูลส่วนบุคคลอาจดำเนินการเพิ่มเติมเพื่อป้องกัน ระงับ หรือแก้ไขเหตุการละเมิดข้อมูลส่วนบุคคล หรือเยียวยาความเสียหาย

ข้อ ๑๑ ในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบทราบ หากโดยสภาพไม่สามารถดำเนินการแจ้งเป็นรายบุคคลเป็นหนังสือหรือโดยวิธีการทางอิเล็กทรอนิกส์ได้เนื่องจากไม่มีวิธีการติดต่อ หรือโดยเหตุจำเป็นอื่นใด ผู้ควบคุมข้อมูลส่วนบุคคลอาจแจ้งเหตุการละเมิดแก่เจ้าของข้อมูลส่วนบุคคลเป็นกลุ่ม หรือแจ้งเป็นการทั่วไปผ่านสื่อสาธารณะ สื่อสังคมออนไลน์ หรือโดยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใดที่เจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบหรือบุคคลทั่วไปสามารถเข้าถึงการแจ้งดังกล่าวได้

การแจ้งเหตุการละเมิดแก่เจ้าของข้อมูลส่วนบุคคลเป็นกลุ่ม หรือแจ้งเป็นการทั่วไป จะต้องไม่ก่อให้เกิดความเสียหายหรือผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล

ข้อ ๑๒ ในการประเมินความเสี่ยงสำหรับการละเมิดข้อมูลส่วนบุคคล ว่ามีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลเพียงใด ผู้ควบคุมข้อมูลส่วนบุคคลอาจพิจารณาจากปัจจัยดังต่อไปนี้

(๑) ลักษณะและประเภทของการละเมิดข้อมูลส่วนบุคคล

(๒) ลักษณะหรือประเภทของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด

(๓) ปริมาณของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด ซึ่งอาจพิจารณาจากจำนวนเจ้าของข้อมูลส่วนบุคคลหรือจำนวนรายการ (records) ของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด

(๔) ลักษณะ ประเภท หรือสถานะของเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ รวมถึงข้อเท็จจริงว่าเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ ประกอบด้วยผู้เยาว์ ผู้พิการ ผู้ไร้ความสามารถ ผู้เสมือนไร้ความสามารถ หรือบุคคลเปราะบาง (vulnerable persons) ที่ขาดความสามารถในการปกป้องสิทธิและประโยชน์ของตนเนื่องจากข้อจำกัดต่าง ๆ ด้วยหรือไม่ เพียงใด

(๕) ความร้ายแรงของผลกระทบและความเสียหายที่เกิดขึ้นหรืออาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคลจากการละเมิดข้อมูลส่วนบุคคล และประสิทธิผลของมาตรการที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือจะใช้เพื่อป้องกัน ระงับ หรือแก้ไขเหตุการละเมิดข้อมูลส่วนบุคคล หรือเยียวยาความเสียหายต่อการบรรเทาผลกระทบและความเสียหายที่เกิดขึ้นหรืออาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคล

(๖) ผลกระทบในวงกว้างต่อธุรกิจหรือการดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคลหรือต่อสาธารณะจากเหตุการละเมิดข้อมูลส่วนบุคคล

(๗) ลักษณะของระบบการจัดเก็บข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด และมาตรการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ทั้งที่เป็นมาตรการเชิงองค์กร (organizational measures) และมาตรการเชิงเทคนิค (technical measures) รวมถึงมาตรการทางกายภาพ (physical measures)

(๘) สถานะทางกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลว่าเป็นบุคคลธรรมดาหรือนิติบุคคล รวมทั้งขนาดและลักษณะของกิจการของผู้ควบคุมข้อมูลส่วนบุคคล

ข้อ ๑๓ ให้ประธานกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นผู้รักษาการตามประกาศนี้

ประกาศ ณ วันที่ ๖ ธันวาคม พ.ศ. ๒๕๖๕
เธียรชัย ณ นคร
ประธานกรรมการคุ้มครองข้อมูลส่วนบุคคล