ประกาศการท่าเรือแห่งประเทศไทย

เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคลของการท่าเรือแห่งประเทศไทย

เพื่อเป็นการคุ้มครองข้อมูลส่วนบุคคลให้กับผู้ใช้บริการ ผู้ติดต่องาน และพนักงานของการท่าเรือแห่งประเทศไทย รวมทั้งเป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และกฎหมายอื่นที่เกี่ยวข้อง อาศัยอำนาจตามความในมาตรา ๓๒ (๒) แห่งพระราชบัญญัติการท่าเรือแห่งประเทศไทย พ.ศ. ๒๔๙๔ ผู้อำนวยการการท่าเรือแห่งประเทศไทย จึงให้ดำเนินการดังนี้

ข้อ ๑ ให้การดำเนินงานของการท่าเรือแห่งประเทศไทยในส่วนของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ซึ่งรวมถึงข้อมูลส่วนบุคคลอ่อนไหว เป็นไปตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลของการท่าเรือแห่งประเทศไทย (Data Privacy Policy of the Port Authority of Thailand) และแนวปฏิบัติสำหรับการดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของการท่าเรือแห่งประเทศไทย ที่แนบท้ายประกาศนี้

ข้อ ๒ แจ้งเตือนให้เจ้าของข้อมูลส่วนบุคคลรับทราบการติดตั้งกล้องวงจรปิดภายในพื้นที่ต่าง ๆ ของการท่าเรือแห่งประเทศไทย รวมถึงสื่อสารคำประกาศเกี่ยวกับความเป็นส่วนตัวในการใช้กล้องวงจรปิด (CCTV Privacy Notice) เพื่อให้เจ้าของข้อมูลส่วนบุคคลรับทราบได้อย่างชัดเจน

ข้อ ๓ สื่อสารให้เจ้าของข้อมูลส่วนบุคคลรับทราบถึงนโยบายคุกกี้สำหรับการเข้าใช้บริการผ่านช่องทางเว็บไซต์ของการท่าเรือแห่งประเทศไทย

ข้อ ๔ ให้หน่วยงานต่าง ๆ ของการท่าเรือแห่งประเทศไทย กำหนดมาตรการหรือแนวทางปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม และสอดคล้องตามนโยบายและแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลของการท่าเรือแห่งประเทศไทย

ข้อ ๕ ให้ผู้อำนวยการกองกฎหมาย ในฐานะเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของการท่าเรือแห่งประเทศไทย ตรวจสอบดูแลให้การดำเนินงานด้านข้อมูลส่วนบุคคลเป็นไปด้วยความเรียบร้อย และไม่ขัดต่อกฎหมายหรือระเบียบที่เกี่ยวข้อง

ข้อ ๖ เจ้าของข้อมูลส่วนบุคคลที่ต้องการติดต่อการท่าเรือแห่งประเทศไทย สามารถติดต่อได้ที่

๖.๑ ผู้ควบคุมข้อมูลส่วนบุคคล : การท่าเรือแห่งประเทศไทย

เลขที่ ๔๔๔ ถนนท่าเรือ แขวงคลองเตย เขตคลองเตย กรุงเทพมหานคร ๑๐๑๑๐

/ ๒ ...

๖.๒ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO) : ผู้อำนวยการกองกฎหมาย การท่าเรือแห่งประเทศไทย

เลขที่ ๔๔๔ ถนนท่าเรือ แขวงคลองเตย เขตคลองเตย กรุงเทพมหานคร ๑๐๑๑๐

อีเมล dpo@port.co.th

จึงประกาศมาเพื่อทราบโดยทั่วกัน

ประกาศ ณ วันที่ ๒๖ กรกฎาคม พ.ศ. ๒๕๖๕

(นายเกรียงไกร ไชยศิริวงศ์สุข)

ผู้อำนวยการการท่าเรือแห่งประเทศไทย

เรียน หัวหน้าหน่วยงานในสังกัด กทท.
เพื่อโปรดทราบและแจ้งพนักงานในสังกัดทราบ

(นายเจษฎา โปตระนันท์)
ผู้ช่วยผู้อำนวยการกองทรัพยากรบุคคล
๓ ส.ค. ๒๕๖๕

สำเนาถูกต้อง

(นายเจษฎา โปตระนันท์)
ผู้ช่วยผู้อำนวยการกองทรัพยากรบุคคล
๓ ส.ค. ๒๕๖๕

แนวปฏิบัติสำหรับการดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคล
เพื่อให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล
ของ การท่าเรือแห่งประเทศไทย

เพื่อให้เป็นไปตามมาตรา ๓๗ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ เรื่อง หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล กทท. จึงกำหนดแนวปฏิบัติสำหรับการดำเนินการของ กทท. ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ดังนี้

๑. กระบวนการจัดทำมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม ตามมาตรา ๓๗ (๑)

วัตถุประสงค์ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

แนวทางการดำเนินงาน

จัดให้มีมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคล ครอบคลุมอย่างน้อย ๓ ประเด็น ดังนี้

- การธำรงไว้ซึ่งความลับ (confidentiality)
- ความถูกต้องครบถ้วน (integrity) และ
- สภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคล

และต้องประกอบด้วยมาตรการป้องกัน ๓ ด้าน คือ

- มาตรการป้องกันด้านการบริหารจัดการ (administrative safeguard)
- มาตรการป้องกันด้านเทคนิค (technical safeguard) และ
- มาตรการป้องกันทางกายภาพ (physical safeguard)

ขั้นตอนดำเนินงาน

๑.๑ การจัดทำมาตรการป้องกันด้านการบริหารจัดการ (administrative safeguard)

๑.๑.๑ จัดทำระเบียบ วิธีปฏิบัติ สำหรับควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

๑.๑.๒ ประเมินผลกระทบความเสี่ยงข้อมูลส่วนบุคคล (Data Protection Impact Assessment : DPIA) เพื่อกำหนดระดับความเสี่ยง หรือ ความเสียหายที่อาจเกิดขึ้นหากข้อมูลส่วนบุคคลรั่วไหล ถูกแก้ไข ถูกคัดลอก หรือ ถูกทำลาย โดยมิชอบ

๑.๑.๓ จัดทำแนวทางการอนุญาตหรือสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้งาน (user responsibilities) ในรูปแบบต่าง ๆ ตามระดับความเสี่ยงและผลกระทบที่อาจเกิดขึ้น กรณีข้อมูลส่วนบุคคลถูกละเมิด เช่น สิทธิในการเข้าดู แก้ไข เพิ่มเติม เปิดเผยและเผยแพร่ การตรวจสอบคุณภาพข้อมูล ตลอดจนการลบทำลาย

๑.๑.๔ ทบทวนมาตรการป้องกันด้านการบริหารจัดการ อย่างน้อยปีละ ๑ ครั้ง

๑.๒ การจัดมาตรการป้องกันด้านเทคนิค (technical safeguard)

๑.๒.๑ จัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล

๑.๒.๒ กำหนดวิธีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management) เพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาต ตามระดับสิทธิการใช้งาน ได้แก่ การนำเข้า เปลี่ยนแปลง แก้ไข เปิดเผย ตลอดจนการลบทำลาย

/๑.๒.๓ จัดให้...

๑.๒.๓ จัดให้มีระบบสำรองและกู้คืนข้อมูล เพื่อให้ระบบ และ/หรือ บริการต่าง ๆ ยังสามารถดำเนินการได้อย่างต่อเนื่อง

๑.๒.๔ ทบทวนมาตรการป้องกันด้านเทคนิค อย่างน้อยปีละ ๑ ครั้ง

๑.๓ การจัดทำมาตรการป้องกันทางกายภาพ (physical safeguard) สำหรับการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล (access control)

๑.๓.๑ กำหนดแนวทางและวิธีการควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

๑.๓.๒ กำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลส่วนบุคคล การลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล การลักลอบนำอุปกรณ์เข้าออก

๑.๓.๓ ทบทวนมาตรการป้องกันทางกายภาพเมื่อมีความจำเป็น หรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป เพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

๑.๔ รายงานผลการดำเนินงานต่อคณะกรรมการกำกับดูแลและขับเคลื่อนตามข้อกำหนดของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ของ กทท. และคณะกรรมการฝ่ายบริหาร กทท.

๒. กระบวนการป้องกันบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ กทท. ใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจ หรือโดยมิชอบ ในกรณีที่ กทท. ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลนั้น ตามมาตรา ๓๗ (๒)

วัตถุประสงค์ เพื่อป้องกันมิให้บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคลที่ กทท. ต้องให้ข้อมูลส่วนบุคคล ใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจ หรือโดยมิชอบ

ขั้นตอนการดำเนินงาน

๒.๑ การประเมินก่อนส่งมอบข้อมูล

๒.๑.๑ ตรวจสอบสิทธิ อำนาจหน้าที่ และฐานกฎหมายที่บุคคล และ/หรือ นิติบุคคลรายอื่นนั้น ใช้เพื่อร้องขอข้อมูลส่วนบุคคล

๒.๑.๒ สอบถามวัตถุประสงค์ในการนำข้อมูลไปใช้งาน เพื่อให้สามารถประเมินว่าควรสำเนาข้อมูลให้ในระดับรายละเอียดเท่าใด และจำเป็นต้องทราบข้อมูลที่ชี้จำเพาะบุคคลหรือไม่ หากแปลงข้อมูลที่ชี้จำเพาะบุคคลแทนด้วยรหัสใหม่ที่เป็นนิรนามจะเพียงต่อการนำไปใช้ประโยชน์หรือไม่

๒.๑.๓ กทท. จะแจ้งให้เจ้าของข้อมูลทราบก่อน กรณี กทท. พิจารณาว่า ข้อมูลส่วนบุคคลที่จะส่งมอบให้บุคคลและ/หรือนิติบุคคลอื่นที่ไม่ใช่ กทท. เป็นข้อมูลที่สมควรแจ้งให้เจ้าของข้อมูลรับทราบ

๒.๒ เมื่อส่งมอบข้อมูล

๒.๒.๑ จัดเตรียมข้อมูลใหม่จากข้อมูลดิบให้มีระดับรายละเอียดเท่าที่จำเป็นต่อวัตถุประสงค์การใช้งาน

๒.๒.๒ ส่งมอบข้อมูล พร้อมทำการบันทึกชื่อผู้ขอข้อมูล ข้อมูลสำหรับติดต่อ วัน-เดือน-ปี ที่ให้ข้อมูล ฐานกฎหมายที่ใช้สำหรับเข้าถึงข้อมูลส่วนบุคคล ตลอดจนวัตถุประสงค์การนำไปใช้งาน

๒.๒.๓ แจ้งให้บุคคล หรือ นิติบุคคลนั้น ทราบว่าเมื่อรับข้อมูลไปแล้ว ผู้รับข้อมูลจะต้องดำเนินการตามหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลสำหรับข้อมูลชุดที่ร้องขอไปนั้นเช่นเดียวกัน ตามขอบเขตและวัตถุประสงค์การใช้งานที่แจ้งไว้

/๒.๒.๔ บันทึก...

๒.๒.๔ บันทึกรายละเอียดการส่งมอบข้อมูลลงรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Data Processing Activity : ROPA)

๓. กระบวนการตรวจสอบการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม ตามมาตรา ๓๗ (๓)

วัตถุประสงค์ เพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคล เมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม เว้นแต่เก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็นการเก็บรักษาไว้เพื่อวัตถุประสงค์ตามมาตรา ๒๔ (๑) หรือ (๔) หรือมาตรา ๒๖ (๕) (ก) หรือ (ข) การใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย ทั้งนี้ ให้นำความใน มาตรา ๓๓ วรรคห้า มาใช้บังคับกับการลบหรือทำลายข้อมูลส่วนบุคคลโดยอนุโลม

ขั้นตอนการดำเนินงาน

๓.๑ การติดตามตรวจสอบ

๓.๑.๑ จัดทำรายงานการเก็บรวบรวมข้อมูลส่วนบุคคล (Data Inventory Timeline) ที่มีข้อมูลเวลาที่ได้รับข้อมูลส่วนบุคคลมาจากเจ้าของข้อมูล

๓.๑.๒ กำหนดระยะเวลาติดตามตรวจสอบอย่างสม่ำเสมอ (เช่น ทุกสัปดาห์ หรือ ทุกเดือน) ตามระดับความเสี่ยงหรือผลกระทบจากการละเมิดสิทธิของเจ้าของข้อมูล

๓.๑.๓ ตรวจสอบข้อมูลส่วนบุคคลที่อยู่ในความดูแลตน (ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล) มีรายการหรือมีชุดข้อมูลใดที่พ้นกำหนดระยะเวลาการเก็บรักษา ตามที่แจ้งเจ้าของข้อมูลส่วนบุคคลไว้ในนโยบายการคุ้มครองข้อมูลส่วนบุคคลของ กทท. หรือประกาศความเป็นส่วนตัว (Privacy Notice) (ถ้ามีการจัดทำ) หรือ ตามที่ขอความยินยอมไว้

๓.๒ การดำเนินการลบทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ตามแต่กรณี

๓.๒.๑ <u>กรณี กทท. ไม่มีความจำเป็นต้องใช้งานข้อมูลส่วนบุคคลดังกล่าว หรือข้อมูลส่วนบุคคลดังกล่าวไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น</u>

๓.๒.๑.๑ ให้หน่วยงานที่รับผิดชอบข้อมูลส่วนบุคคลดังกล่าวเร่งดำเนินการลบทำลายหรือทำให้เป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้

๓.๒.๒ <u>กรณีเจ้าของข้อมูลส่วนบุคคลขอใช้สิทธิให้ลบทำลายข้อมูล (หรือขอถอนความยินยอม) ในกรณีใช้ฐานความยินยอมในการเก็บรวบรวมข้อมูลส่วนบุคคล</u>

๓.๒.๒.๑ พิจารณาว่า (วิเคราะห์ความเป็นไปได้ที่ข้อมูลส่วนบุคคลดังกล่าว) กทท. ยังมีความจำเป็นต้องเก็บรวบรวม ใช้งานข้อมูลส่วนบุคคลดังกล่าวหรือไม่

๓.๒.๒.๒ หากเป็นข้อมูลส่วนบุคคลที่ กทท. ไม่มีความจำเป็นต้องเก็บรวบรวม ใช้งานแล้ว ต้องดำเนินการลบทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้

๓.๒.๓ <u>กรณีมีเหตุผลความจำเป็นที่เหนือกว่าสิทธิของเจ้าของข้อมูล ในการขอให้ลบทำลายข้อมูล (หรือขอถอนความยินยอม)</u>

๓.๒.๓.๑ วิเคราะห์เหตุผลความจำเป็นของ กทท. ในการเก็บข้อมูลไว้ต่อไป

/การลบทำลาย...

การลบทำลายข้อมูล หรือ การทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ อาจยกเว้นไม่กระทำก็ได้ใน กรณีผู้ควบคุมข้อมูลส่วนบุคคลมีเหตุผลความจำเป็นที่เหนือกว่าสิทธิของเจ้าของข้อมูล เช่น

(ก) เพื่อวัตถุประสงค์การจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ การศึกษาวิจัยหรือสถิติ

(ข) เพื่อการสร้างประโยชน์สาธารณะตามหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลรายนั้น

(ค) เพื่อประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์

(ง) การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์

๓.๒.๓.๒ พิจารณานำมาตรการดูแลข้อมูลที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิเสรีภาพและประโยชน์ของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ

๓.๓ การแจ้งผลการดำเนินการให้เจ้าของข้อมูลรับทราบ ให้ดำเนินการแจ้งผลการดำเนินการของ กทท. ให้เจ้าของข้อมูลรับทราบ

๓.๔ บันทึกผลการดำเนินการลงรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Data Processing Activity : ROPA)

๔. การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล ตามมาตรา ๓๗ (๔)

วัตถุประสงค์ เพื่อแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่ DPO ของ กทท. โดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

ขั้นตอนการดำเนินงาน

๔.๑ กำหนดตัวพนักงานผู้รับผิดชอบกิจกรรมและวิธีการแจ้งเหตุละเมิดให้แก่ DPO ของ กทท. ให้ชัดเจน กรณีเป็นเหตุละเมิดที่มีความรุนแรงและเร่งด่วน

๔.๒ กำหนดวิธีปฏิบัติให้ DPO ของ กทท. ต้องดำเนินการแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบถึงเหตุละเมิดข้อมูลส่วนบุคคลได้ภายใน ๗๒ ชั่วโมง (นับแต่ทราบเหตุ)

๔.๓ การแจ้งเหตุละเมิดอาจได้รับยกเว้นไม่ต้องดำเนินการก็ได้ หากไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

ภาคผนวก

ตัวอย่างการประเมินความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

๑) ตัวอย่างกรณีความเสี่ยงต่ำ: ข้อมูลส่วนบุคคลถูกเข้ารหัส (ไม่สามารถเปิดอ่านได้หากไม่ทราบรหัสผ่าน) ถูกซอฟต์แวร์เรียกค่าไถ่ (Ransomware) เข้ารหัสจนไม่สามารถใช้งานได้ และไม่ได้ถูกโจรกรรมข้อมูลออกไป อย่างไรก็ตามผู้ควบคุมข้อมูลส่วนบุคคลมีระบบสำรองรองรับการบริการได้อย่างต่อเนื่อง กรณีนี้ถือได้ว่ามีความเสี่ยงต่ำที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการเพียงบันทึกเหตุการณ์ไว้ (เป็นการภายใน) ก็เพียงพอ ไม่จำเป็นต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ และ ไม่จำเป็นต้องแจ้งเจ้าของข้อมูลส่วนบุคคลทราบ

๒) ตัวอย่างกรณีความเสี่ยงสูง: เว็บไซต์รับสมัครงานออนไลน์ถูกละเมิด โดยผู้โจมตีทำการฝังมัลแวร์เพื่อเข้าถึงข้อมูลใบสมัครงานออนไลน์ (ตรวจพบ ๑ เดือนหลังมัลแวร์ถูกติดตั้ง) เนื้อหาข้อมูลเป็นข้อมูลทั่วไปเพื่อการสมัครงาน อย่างไรก็ตาม ถือว่ามีความเสี่ยงสูงที่เหตุการณ์ดังกล่าวจะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล เช่นนี้ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการบันทึก (เป็นการภายใน) ว่าเคยมีเหตุโจรกรรม พร้อมทั้งแจ้งเหตุดังกล่าว (ภายใน ๗๒ ชั่วโมง) ไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ และยังต้องแจ้งเจ้าของข้อมูลส่วนบุคคลทราบด้วย

๓) ตัวอย่างกรณีความเสี่ยงต่ำ: เจ้าหน้าที่ของหน่วยงานส่งอีเมลไปยังผู้รับผิดพลาด ซึ่งแนบไฟล์รายชื่อผู้เข้ารับการอบรมหลักสูตรภาษาอังกฤษ ซึ่งประกอบไปด้วย ชื่อ-นามสกุล ที่อยู่อีเมล และข้อจำกัดด้านอาหาร ซึ่งมีเพียง ๒ คน ใน ๑๕ คนที่ระบุว่า แพ้น้ำตาลแลคโตสในนม (ถือเป็นข้อมูลสุขภาพ) กรณีนี้อีเมลถูกส่งไปยังผู้เข้ารับการอบรมในรุ่นก่อนหน้าแทนที่จะเป็นเจ้าหน้าที่ของโรงแรมที่จัดอาหาร ซึ่งถือเป็นการทำให้ข้อมูลส่วนบุคคลรั่วไหล อย่างไรก็ตามแม้ข้อมูลสุขภาพ จะถูกเผยแพร่ไปยังผู้ไม่เกี่ยวข้อง แต่ก็ไม่สามารถระบุความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลได้แน่ชัด เช่นนี้ ถือว่าเป็นกรณีที่มีความเสี่ยงต่ำ ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการเพียงบันทึกเหตุการณ์ไว้ (เป็นการภายใน) ก็เพียงพอ ไม่จำเป็นต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ และ ไม่จำเป็นต้องแจ้งเจ้าของข้อมูลส่วนบุคคลทราบ

หมายเหตุ กรณีตัวอย่างและวิธีปฏิบัติข้างต้นอ้างอิงจาก Guidelines 01/2021 on Examples regarding Data Breach Notification สามารถศึกษาวิธีการปฏิบัติเพิ่มเติมได้จาก https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2021/guidelines-012021-examples-regarding-data-breach_en