ด่วนที่สุด

ที่ ดศ ๐๑๐๐.๔/๒๓๖๔๖

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษาฯ
อาคารรัฐประศาสนภักดี ถนนแจ้งวัฒนะ
เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐

๒๐ พฤศจิกายน ๒๕๖๖

เรื่อง การป้องกันและคุ้มครองข้อมูลส่วนบุคคล

เรียน เลขาธิการคณะรัฐมนตรี

อ้างถึง หนังสือสำนักเลขาธิการคณะรัฐมนตรี ด่วนที่สุด ที่ นร ๐๕๐๕/ว ๔๖๕ ลงวันที่ ๑๐ พฤศจิกายน ๒๕๖๖

ด้วยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ขอเสนอเรื่อง การป้องกันและคุ้มครองข้อมูลส่วนบุคคลมาเพื่อคณะรัฐมนตรีทราบ โดยเรื่องนี้เข้าข่ายที่จะให้นำเสนอคณะรัฐมนตรีได้ตามพระราชกฤษฎีกาว่าด้วยการเสนอเรื่องและการประชุมคณะรัฐมนตรี พ.ศ. ๒๕๔๘ มาตรา ๔ (๑๓)

ทั้งนี้ เรื่องดังกล่าวมีรายละเอียด ดังนี้

๑. <u>เหตุผลความจำเป็นที่ต้องเสนอคณะรัฐมนตรี</u>

ตามที่คราวประชุมคณะรัฐมนตรีเมื่อวันที่ ๗ พฤศจิกายน ๒๕๖๖ นายกรัฐมนตรีได้มีข้อสั่งการให้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเป็นหน่วยงานหลักร่วมกับหน่วยงานฝ่ายความมั่นคงที่เกี่ยวข้องพิจารณากำหนดแนวทางและกลไกในการป้องกันและคุ้มครองข้อมูลส่วนบุคคล การโจรกรรมข้อมูลและช่องทางในการโจรกรรม ให้เกิดความเหมาะสม เท่าทันเหตุการณ์ และครบถ้วนทุกมิติ และให้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมรายงานผลการดำเนินงานในภาพรวมให้คณะรัฐมนตรีทราบภายใน ๒ สัปดาห์ นั้น

๒. <u>ความเร่งด่วนของเรื่อง</u>

เพื่อรายงานคณะรัฐมนตรีทราบภายใน ๒ สัปดาห์ ตามมติคณะรัฐมนตรีเมื่อวันที่ ๗ พฤศจิกายน ๒๕๖๖

๓. <u>สาระสำคัญและข้อเท็จจริง</u>

เมื่อวันที่ ๙ พฤศจิกายน ๒๕๖๖ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้ดำเนินการจัดประชุมเพื่อกำหนดแนวทางการบูรณาการป้องกันและแก้ไขปัญหาอาชญากรรมทางไซเบอร์จากกรณีข้อมูลส่วนบุคคลรั่วไหลและมีการซื้อ - ขายในเว็บไซต์หรือแพลต์ฟอร์มต่างๆ โดยมีนายประเสริฐ จันทรรวงทอง รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นประธาน ศาสตราจารย์พิเศษวิศิษฏ์ วิศิษฏ์สรอรรถ ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม พร้อมด้วย พลตำรวจโท วรวัฒน์ วัฒน์นครบัญชา ผู้บัญชาการกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี นายศิวรักษ์ ศิวโมกษธรรม เลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล นายสมศักดิ์ เจริญไพฑูรย์ รองอธิบดีกรมการปกครอง ผู้แทนจากกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี และสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เข้าร่วมหารือกำหนดมาตรการในการแก้ไขปัญหาการซื้อ – ขายข้อมูลส่วนบุคคลทางออนไลน์ สรุปสาระสำคัญได้ดังนี้

/<u>สาเหตุและช่องทาง</u>...

สาเหตุและช่องทางการเกิดข้อมูลรั่วไหล

๑) หน่วยงานภาครัฐขาดระบบเฝ้าระวังและตรวจสอบ และความเอาใจใส่และละเลยกระบวนการรักษาความมั่นคงปลอดภัยของข้อมูลทำให้เกิดการเผยแพร่ข้อมูลส่วนบุคคลหรือข้อมูลส่วนบุคคลรั่วไหล (Personal Data Breach) ปรากฏหรือเปิดเผยต่อสาธารณะโดยไม่จำเป็น และไม่ได้รับอนุญาตจากเจ้าของข้อมูล

๒) เจ้าหน้าที่ภาครัฐและหน่วยงานไม่ได้จัดให้มีระบบการรักษาความมั่นคงปลอดภัยของข้อมูลที่ดีพอทั้งจากการนำข้อมูลไปเก็บอยู่ใน Data Center ของบริษัทเอกชน หรือไม่จัดให้มีการรักษาความปลอดภัยเพียงพอให้แก่ระบบคอมพิวเตอร์ต่างๆ (Computer Server) ขาดการตรวจสอบเฝ้าระวังที่ดีพอทำให้มีช่องโหว่ในระบบ เป็นความเสี่ยงที่ทำให้เกิดการรั่วไหลของข้อมูลส่วนบุคคล การโจมตีหรือบุกรุกจาก Hacker ทำให้สามารถเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตและนำข้อมูลออกไปเผยแพร่ ซึ่งพบได้บ่อยจากหน่วยงานที่ไม่มีหรือขาดระบบรักษาความปลอดภัยเพียงพอ ขาดการตรวจจับ เฝ้าระวังการบุกรุกเข้าถึงระบบจากภายนอก การตั้งค่าระบบที่ผิดพลาด เป็นต้น

๓) เจ้าหน้าที่ภาครัฐและหน่วยงานขาดการการสร้างความตระหนักรู้ด้านการคุ้มครองข้อมูลส่วนบุคคล การสื่อสารให้บุคลากร พนักงาน หรือลูกจ้างในองค์กรเห็นถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล ความเสี่ยงที่อาจเกิดจากการใช้ข้อมูลส่วนบุคคลในการทำงานโดยขาดความระมัดระวังส่งผลให้เกิดโทษต่อหน่วยงานและส่วนตัวอย่างไร การสร้างเสริมความตระหนักรู้ให้แก่บุคลากร พนักงานหรือลูกจ้าง เป็นการป้องกันความผิดพลาดที่เกิดจากบุคคล (human error) ในการนำข้อมูลส่วนบุคคลไปใช้ในการทำงานขององค์กร

๔. ประโยชน์และผลกระทบ

-

๕. ค่าใช้จ่ายและแหล่งที่มา หรือการสูญเสียรายได้

-

๖. ความเห็นหรือความเห็นชอบ/อนุมัติของหน่วยงานที่เกี่ยวข้อง

-

๗. ข้อกฎหมายและมติคณะรัฐมนตรีที่เกี่ยวข้อง

-

๘. ข้อเสนอของหน่วยงานของรัฐ/คณะกรรมการเจ้าของเรื่อง

ที่ประชุมเห็นชอบแนวทางร่วมกันกำหนดมาตรการป้องกันและคุ้มครองข้อมูลส่วนบุคคลโดยมีข้อเสนอแนะและแนวทางการแก้ไข ดังนี้

ระยะเร่งด่วน ๓๐ วัน

๑) ให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตรวจสอบข้อมูลที่เปิดเผยต่อสาธารณะจัดตั้งศูนย์เฝ้าระวังการละเมิดข้อมูลส่วนบุคคล (PDPC Eagle Eye) และเร่งตรวจสอบค้นหาเฝ้าระวัง การรั่วไหลของข้อมูลส่วนส่วนบุคคลว่าเกิดขึ้นจากหน่วยงานใด หรือช่องทางใด และเมื่อพบข้อบกพร่องของการรักษาความมั่นคงปลอดภัยของข้อมูลของหน่วยงานต่าง ๆ เร่งประสานแจ้งเตือนการรั่วไหลของ

/ข้อมูลส่วนบุคคล...

ข้อมูลส่วนบุคคลแก่หน่วยงานนั้น เพื่อระงับยับยั้งไม่ให้เกิดความเสี่ยงหรือความเสียหายที่อาจเกิดขึ้นโดยเร็ว จากการเฝ้าระวังตรวจสอบที่ผ่านมา (ข้อมูลตั้งแต่วันที่ ๙ - ๒๐ พฤศจิกายน ๒๕๖๖) มีผลจากการเร่งตรวจสอบ ดังนี้

- ดำเนินการตรวจสอบแล้ว จำนวน ๓,๑๑๙ หน่วยงาน (ภาครัฐ/ภาคเอกชน)
- ตรวจพบข้อมูลรั่วไหล/แจ้งเตือนหน่วยงาน จำนวน ๑,๑๕๘ เรื่อง
- หน่วยงานแก้ไขแล้ว จำนวน ๗๘๑ เรื่อง
- พบกรณีซื้อ – ขายข้อมูลส่วนบุคคล ๓ เรื่อง ซึ่งอยู่ระหว่างสืบสวนดำเนินคดีร่วมกับกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.)

ทั้งนี้ ภายใน ๓๐ วัน ศูนย์ PDPC Eagle Eye มีเป้าหมายตรวจสอบ ให้ครบ ๙,๐๐๐ หน่วยงาน

๒) ให้สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติดำเนินการตรวจสอบเฝ้าระวัง และวิเคราะห์ความเสี่ยงของพฤติกรรมหรือช่องโหว่ต่างๆ ที่อาจทำให้เกิดข้อมูลรั่วไหลของหน่วยงานต่างๆ โดยเฉพาะอย่างยิ่งหน่วยงานภาครัฐที่เป็นหน่วยงานในลักษณะหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) ทั้ง ๗ ด้าน ได้แก่ ด้านความมั่นคงภาครัฐ ด้านบริการภาครัฐที่สำคัญ ด้านการเงินการธนาคาร ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม ด้านการขนส่งและโลจิสติกส์ ด้านพลังงานและสาธารณูปโภค และด้านสาธารณสุข ซึ่งปัจจุบันมีหน่วยงาน CII จำนวน ๕๔ หน่วยงาน หากพบข้อบกพร่องของการรักษาความมั่นคงปลอดภัยของระบบหรือข้อมูลของหน่วยงานต่าง ๆ เร่งประสานแจ้งเตือนช่องโหว่หรือการรั่วไหลของข้อมูลส่วนบุคคลแก่หน่วยงานนั้น เพื่อระงับยับยั้งไม่ให้เกิดความเสี่ยงหรือความเสียหายที่อาจเกิดขึ้นโดยเร็ว จากการเฝ้าระวังตรวจสอบที่ผ่านมา สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติตรวจพบการโจมตีไซเบอร์เกี่ยวกับข้อมูลรั่วไหล (ข้อมูลตั้งแต่วันที่ ๙ - ๒๐ พฤศจิกายน ๒๕๖๖) ดังนี้

๑. การตรวจสอบช่องโหว่ จำนวน ๙๑ หน่วยงาน ซึ่ง สกมช. พบว่าทั้ง ๙๑ หน่วยงาน มีความเสี่ยง โดยมีความเสี่ยงระดับสูง จำนวน ๒๑ หน่วยงาน และ สกมช. ได้แจ้งแก้ไขทั้ง ๙๑ หน่วยงานแล้ว

๒. การตรวจพบการโจมตีทางไซเบอร์ เกี่ยวกับข้อมูลส่วนบุคคล จำนวน ๑๑ เหตุการณ์ โดยแบ่งเป็น

- กรณีข้อมูลรั่วไหล (Data Leak) ส่ง สคส. เพื่อดำเนินการตามกฎหมาย จำนวน ๘ เหตุการณ์
- กรณีข้อมูลถูกละเมิดหรือถูกโจมตี (Data Breach) ส่ง บช.สอท. สืบสวนดำเนินคดี จำนวน ๓ เหตุการณ์

๓) ให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ร่วมกับหน่วยงานที่เกี่ยวข้อง อาทิ สภาหอการค้าแห่งประเทศไทย สภาอุตสาหกรรมแห่งประเทศไทย สมาคมธนาคารไทย สมาคมประกันชีวิตไทย สมาคมโรงแรมไทย รวมถึงเครือข่ายภาคสื่อมวลชนสร้างความตระหนักรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล การป้องกันความเสี่ยงต่าง ๆ ที่อาจเกิดขึ้นหากไม่ปฏิบัติตามระเบียบขั้นตอนการรักษาความปลอดภัยของหน่วยงาน ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Awareness Training) เช่น การป้องกันการบุกรุกจากบุคคลภายนอก การตั้งค่าระบบอย่างปลอดภัย

/และการบังคับ...

และการบังคับใช้กฎหมายตามอำนาจหน้าที่อย่างเคร่งครัด ทั้งนี้ ในวันที่ ๑๖ พ.ย. ๖๖ ได้มีการจัดอบรม DPO (Data Protection Officer) สำหรับหน่วยงานรัฐ ที่มีข้อมูลส่วนบุคคลจำนวนมาก จำนวน ๘๕ หน่วยงาน เพื่อกำชับให้ดูแลข้อมูลส่วนบุคคลอย่างถูกต้องตามกฎหมาย และให้ความรู้ตลอดจนแนวปฏิบัติที่ถูกต้อง

๔) ให้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมและกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยีเร่งรัดมาตรการปิดกั้นกรณีการซื้อ – ขายข้อมูลส่วนบุคคลที่ผิดกฎหมาย และสืบสวนดำเนินคดี ตลอดจนจับกุมผู้กระทำความผิดโดยเร็ว

ระยะ ๖ เดือน

เพื่อป้องกันและลดปัญหาการรั่วไหลของข้อมูลส่วนบุคคลจากการที่หน่วยงานภาครัฐส่งข้อมูลแก่หน่วยงานภายนอก หรือขาดบุคลากรในการกำกับดูแลงานด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน เห็นควรส่งเสริมการใช้งานระบบคลาวด์กลางภาครัฐที่มีความน่าเชื่อถือ เป็นระบบที่มีความมั่นคงปลอดภัยตามหลักวิชาการสากล สามารถรองรับการใช้งานของบุคลากรของหน่วยงานต่าง ๆ ได้อย่างปลอดภัยไม่เกิดการโจรกรรมหรือการรั่วไหลของข้อมูล

ระยะ ๑๒ เดือน

ประเมินและปรับปรุง พัฒนากฎหมายที่เกี่ยวข้องให้สามารถบังคับใช้กฎหมายให้ทันสมัยต่อบริบทของสังคมและพฤติการณ์ที่เปลี่ยนไป เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. ๒๕๖๒ เป็นต้น เพื่อเพิ่มประสิทธิภาพการบังคับใช้กฎหมายของเจ้าหน้าที่ในการตรวจสอบและป้องกันอาชญากรรมทางไซเบอร์ที่ดียิ่งขึ้น

จึงเรียนมาเพื่อโปรดพิจารณานำเสนอคณะรัฐมนตรีต่อไป

ขอแสดงความนับถือ

(นายประเสริฐ จันทรรวงทอง)
รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
กองป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีสารสนเทศ
โทร. ๐ ๒๑๔๑ ๖๙๖๗
โทรสาร ๐ ๒๑๔๓ ๘๐๓๔
ไปรษณีย์อิเล็กทรอนิกส์ : saraban@mdes.go.th