

กระทู้ถามที่ ๔๑๑ ร.

สภาผู้แทนราษฎร

๒๐ มีนาคม ๒๕๖๗

เรื่อง การบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลในหน่วยงาน และองค์กรต่าง ๆ

กราบเรียน ประธานสภาผู้แทนราษฎร

ข้าพเจ้าขอตั้งกระทู้ถาม ถาพนายกรัฐมนตรี ดังต่อไปนี้

จากปัญหาข้อมูลส่วนบุคคลของประชาชนมีการรั่วไหลไปสู่มีจฉาชีพ ซึ่งอาจเกิดจากการที่หน่วยงานนั้น ๆ ไม่ได้วางมาตรการกำกับดูแลเท่าที่ควร หรือขาดงบประมาณในการดำเนินการหรือเกิดการทุจริตในหน้าที่ของบุคลากร หรือผู้รับจ้าง จนทำให้มีจฉาชีพนำข้อมูลดังกล่าวไปหลอกลวงประชาชนด้วยกลวิธีต่าง ๆ ก่อให้เกิดความเดือดร้อน และความเสียหายในวงกว้าง จนไม่สามารถควบคุมได้อย่างทันท่วงที อีกทั้งหน่วยงานต่าง ๆ ที่มีหน้าที่จัดเก็บ ประมวลผล และเผยแพร่ข้อมูลส่วนบุคคลโดยส่วนใหญ่แล้วมีความเข้าใจคลาดเคลื่อนว่าหน่วยงานจำเป็นต้องจัดเก็บข้อมูลส่วนบุคคลของผู้อื่นไว้เพื่อทำตามหน้าที่และภารกิจของหน่วยงาน จึงไม่ต้องมีการดำเนินการใด ๆ เพื่อให้สอดคล้องกับพระราชบัญญัติแต่ในความเป็นจริงแล้วหน่วยงานนั้นจำเป็นต้องมีการจัดตั้งคณะทำงานเพื่อวางกระบวนการและแนวทางปฏิบัติให้ครบถ้วน เป็นไปตามพระราชบัญญัติ นอกจากนี้ เมื่อวันที่ ๑๔ กันยายน พ.ศ. ๒๕๖๖ มีประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง “การจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา ๔๑ (๒)” และมีผลบังคับใช้ตั้งแต่ช่วงกลางเดือน ธันวาคม พ.ศ. ๒๕๖๖ ที่ผ่านมา จึงขอเรียนถามว่า

๑. สถานการณ์ดำเนินงานของหน่วยงานต่าง ๆ ที่อยู่ภายใต้การกำกับดูแลของรัฐที่ต้องปฏิบัติตามพระราชบัญญัติ มีความคืบหน้าเป็นอย่างไร ขอทราบรายละเอียด

๒. รัฐบาลมีการวางแผนด้านงบประมาณ ในระยะ ๓ ปีข้างหน้า สำหรับหน่วยงานที่ยังไม่ได้ดำเนินการตามพระราชบัญญัติ ไว้อย่างไร ขอทราบรายละเอียด

๓. รัฐบาลมีแผนที่จะสนับสนุน ส่งเสริม ให้เกิดกระบวนการตรวจสอบ (audit) และรับรองมาตรฐานด้านการคุ้มครองข้อมูลส่วนบุคคล (เช่น ISO 27701) สำหรับหน่วยงานที่ต้องปฏิบัติตามพระราชบัญญัติหรือไม่ ขอทราบรายละเอียด

ขอให้ตอบในราชกิจจานุเบกษา

ขอแสดงความนับถืออย่างยิ่ง

สฤษฎ์พงษ์ เกียวข้อง

สมาชิกสภาผู้แทนราษฎร พรรคภูมิใจไทย

จังหวัดกระบี่

คำตอบกระทู้ถามที่ ๔๑๑ ร.

ของ นายสฤกษ์พงษ์ เกี่ยวข้อง สมาชิกสภาผู้แทนราษฎร พรรคภูมิใจไทย จังหวัดกระบี่ เรื่อง การบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลในหน่วยงาน และองค์กรต่าง ๆ

ข้าพเจ้า นายเศรษฐา ทวีสิน นายกรัฐมนตรี ขอตอบกระทู้ถาม เรื่อง การบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลในหน่วยงาน และองค์กรต่าง ๆ ของท่านสมาชิกผู้มีความเกี่ยวข้องตามที่ได้รับรายงานจากกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ดังนี้

คำตอบข้อที่ ๑

จากการรายงานของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ทราบว่า ในห้วงเวลาที่ผ่านมานับตั้งแต่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มีผลบังคับใช้เมื่อวันที่ ๑ มิถุนายน พ.ศ. ๒๕๖๕ คณะกรรมการตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ได้แก่ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล คณะกรรมการผู้เชี่ยวชาญ และสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ได้กำหนดหลักเกณฑ์ กลไก รวมถึงมาตรการกำกับดูแลเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลครอบคลุมทั้งหน่วยงานภาครัฐและภาคเอกชนอย่างต่อเนื่อง เช่น การออกประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตามมาตรา ๓๗ (๑) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคลที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลงแก้ไขหรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยไม่ชอบ การออกประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตามมาตรา ๓๗ (๔) กำหนดหลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล การออกประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่เป็นหน่วยงานของรัฐ และหน่วยงานหรือองค์กรที่มีข้อมูลส่วนบุคคลจำนวนมาก และจำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอตามมาตรา ๔๑ (๑) และ (๒) มีหน้าที่ต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เพื่อทำหน้าที่ในการให้คำแนะนำแก่บุคลากรหรือผู้รับจ้างของหน่วยงานหรือองค์กรดังกล่าวเกี่ยวกับการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ รวมถึงมีหน้าที่ในการประสานงานและให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลในกรณีที่มีปัญหาเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล โดยสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้ดำเนินการ ดังนี้

๑. รวบรวมข้อมูลเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) จำนวน ๒,๒๑๖ หน่วยงาน (ข้อมูล ณ วันที่ ๑๗ เมษายน ๒๕๖๗) (โดยมีการกำหนดเป้าหมายปี พ.ศ. ๒๕๖๗ - ๒๕๖๘ จำนวน ๒,๐๐๐ หน่วย) แบ่งออกเป็น ดังนี้

๑.๑ ภาครัฐ จำนวน ๑๒๔ หน่วยงาน ได้แก่

๑) ภาครัฐที่ไม่เข้าข่าย มาตรา ๔๑ (๑) จำนวน ๓๙ หน่วยงาน

๒) ภาครัฐตามมาตรา ๔๑ (๑) จำนวน ๘๕ หน่วยงาน

๑.๒ ภาคเอกชน จำนวน ๒,๐๙๒ หน่วยงาน ได้แก่

๑) ภาคเอกชนแต่งตั้งโดยสมัครใจ จำนวน ๑,๐๔๖ หน่วยงาน

๒) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา ๔๑ (๒) จำนวน ๗๔๙ หน่วยงาน

๓) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา ๔๑ (๓) จำนวน ๘๘ หน่วยงาน

๔) มาตรา ๔๑ (๒) และมาตรา ๔๑ (๓) จำนวน ๒๐๙ หน่วยงาน

๒. การดำเนินการป้องกันเชิงรุกโดยศูนย์เฝ้าระวัง การละเมิดข้อมูลส่วนบุคคล PDPC Eagle Eye
ดังนี้

๒.๑ ตรวจแล้ว จำนวน ๒๕,๐๖๓ หน่วยงาน

๒.๒ ตรวจพบข้อมูลร้ายไหล จำนวน ๕,๙๖๓ หน่วย (คิดเป็น ๒๓.๗๙% ของที่ตรวจแล้ว)

๒.๓ แก้ไขแล้ว จำนวน ๕,๘๙๒ หน่วย (คิดเป็น ๙๙.๙% ของที่ตรวจพบ)

โดยมีเป้าหมายการดำเนินงาน คือแผนการดำเนินงานระยะปานกลาง (ปี พ.ศ. ๒๕๖๘) จำนวน ๑๐๐,๐๐๐ หน่วย และแผนการดำเนินงานระยะยาว จำนวน ๓๐๐,๐๐๐ หน่วย

๓. ตรวจแนะนำกำกับดูแลให้หน่วยงานทั้งภาครัฐและเอกชน ปฏิบัติตามมาตรการที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนด ดังนี้

๓.๑ ตรวจหน่วยงานรัฐแล้ว จำนวน ๘๕ หน่วยงาน

๓.๒ ตรวจหน่วยงานรัฐ ร่วมกับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ตามที่สำนักงานคณะกรรมการพัฒนาระบบราชการ (สำนักงาน ก.พ.ร. กำหนด) โดยมีเป้าหมายการดำเนินงาน คือ แผนการดำเนินงานระยะปานกลาง (ปี พ.ศ. ๒๕๖๘) จำนวนเพิ่มขึ้นอีก ๒๕% สำหรับหน่วยงานที่มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) และแผนการดำเนินงานระยะยาว จำนวน ๑๐๐% สำหรับหน่วยงานที่มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

๔. สร้างเครือข่ายเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเพื่อให้เกิดการคุ้มครองที่เข้มแข็งและทั่วถึง ปัจจุบันมีเครือข่ายเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ดังนี้

๔.๑ ภาครัฐ จำนวน ๑๒๔ หน่วยงาน

๔.๒ ภาคเอกชน จำนวน ๒,๑๔๗ หน่วยงาน

โดยมีเป้าหมายการดำเนินงาน คือกำกับดูแลให้หน่วยงานรัฐและเอกชนจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ตามที่กฎหมายกำหนด

ภายหลังจากที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มีผลบังคับใช้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้สร้างความตระหนักรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลโดยจัดอบรมสัมมนาทางวิชาการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลแก่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลสำหรับเจ้าหน้าที่ของรัฐและผู้ที่สนใจอย่างสม่ำเสมอ ตลอดจนได้มีการเผยแพร่สรุปเรื่องราวหรือที่เกี่ยวข้องกับการปฏิบัติงานตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ เพื่อให้หน่วยงานของรัฐ

และเอกชนปฏิบัติงานได้อย่างถูกต้อง ครบถ้วน และสอดคล้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และยังมีมาตรการเชิงรุกโดยได้จัดให้เจ้าหน้าที่ของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเข้าตรวจ แนะนำการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ แก่หน่วยงานที่มีข้อมูลส่วนบุคคลจำนวนมาก ตามแบบตรวจแนะนำการกำกับการคุ้มครองข้อมูลส่วนบุคคล

จากการดำเนินการดังกล่าวข้างต้นมาอย่างต่อเนื่องเป็นเหตุให้ปัจจุบันหน่วยงานของรัฐหลายแห่ง ได้พัฒนาแนวทางการปฏิบัติงานสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มากยิ่งขึ้น เห็นได้จากการเผยแพร่ข้อมูลบนเว็บไซต์ของหน่วยงานรัฐจะมีการลบหรือการตัดทอนข้อมูลส่วนบุคคลออกเพื่อไม่ให้เป็นการรุกรานซึ่งสิทธิส่วนบุคคลโดยไม่สมควรหรือการพรากข้อมูลบางส่วน ของตัวเลขประจำตัวผู้เสียภาษีอากรหรือเลขประจำตัวประชาชนในกรณีที่มีกฎหมายกำหนดให้หน่วยงานของรัฐมีหน้าที่ต้องเปิดเผยข้อมูลดังกล่าวต่อประชาชน ซึ่งการดำเนินการดังกล่าวเป็นไปตามหลัก ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพียงพอที่จำเป็นเพื่อลดความเสี่ยงมิให้มีการนำข้อมูลส่วนบุคคลไปใช้ โดยไม่เหมาะสมหรืออาจเป็นผลร้ายต่อเจ้าของข้อมูลส่วนบุคคล

คำตอบข้อที่ ๒

จากการรายงานของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ทราบว่า สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล มีการวางแผนด้านงบประมาณในระยะ ๓ ปี ข้างหน้า สำหรับหน่วยงานที่ยังไม่ดำเนินการตามพระราชบัญญัติ โดยมีการจัดทำแผนค่าของงบประมาณรายจ่ายประจำปี โครงการต่อเนื่อง พ.ศ. ๒๕๖๗ - ๒๕๗๐ เพื่อการสร้างความรู้ความเข้าใจ สนับสนุน ส่งเสริม และให้คำปรึกษาหารือ และรับเรื่องร้องเรียนเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของประเทศ รวมทั้งขยายการให้บริการแพลตฟอร์มภาครัฐเพื่อรองรับการปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล เพื่อลดภาระด้านงบประมาณในภาพรวมของภาครัฐรวมทั้งสร้างความเชื่อมั่นให้กับประชาชนในการใช้เทคโนโลยีดิจิทัล และสนับสนุนการพัฒนาเศรษฐกิจดิจิทัล ตามนโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม และให้สอดคล้องตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ จำนวน ๕ โครงการ ซึ่งมีการวางแผนของงบประมาณต่อเนื่องตั้งแต่ปี พ.ศ. ๒๕๖๗ - ๒๕๗๐ โดยในปีงบประมาณ พ.ศ. ๒๕๖๘ ภายหลังจากที่คณะรัฐมนตรีได้พิจารณาค่าของงบประมาณแล้ว ได้รับวงเงินสำหรับดำเนินโครงการ ดังนี้

๑. โครงการพัฒนาบุคลากรด้านการคุ้มครองข้อมูลส่วนบุคคลของประเทศ จำนวน ๕.๗๓๕๒ ล้านบาท
๒. โครงการเพิ่มประสิทธิภาพและขยายการให้บริการแพลตฟอร์มภาครัฐเพื่อรองรับการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (GPPC : Government Platform for PDPA Compliance) จำนวน ๗๙.๙๓๘๘ ล้านบาท
๓. โครงการศูนย์บริการประชาชน PDPC Center จำนวน ๔๐.๓๘๘๔ ล้านบาท
๔. โครงการคุ้มครองข้อมูลส่วนบุคคลเชิงรุก (PDPC Eagle Eye) จำนวน ๕๒.๑๕๓๒ ล้านบาท
๕. โครงการพัฒนากฎหมายด้านการคุ้มครองข้อมูลส่วนบุคคลของประเทศ จำนวน ๘.๖๔๗๒ ล้านบาท

คำตอบข้อที่ ๓

จากการรายงานของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ทราบว่า สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล มีแผนการดำเนินงานในการสนับสนุน ส่งเสริม ให้เกิดกระบวนการตรวจสอบ และรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล โดยสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล กำหนดหลักเกณฑ์การตรวจสอบ (audit) และรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล (ไม่ได้นำ ISO 27701 มาใช้) ทั้งนี้ เพื่อให้สอดคล้องกับหน้าที่และอำนาจของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลในการวิเคราะห์รับรองความสอดคล้องและความถูกต้องตามมาตรฐานมาตรฐาน หรือกลไกการกำกับดูแลที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งตรวจสอบ และรับรองนโยบายในการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มาตรา ๔๔ (๓) ดังนี้

๑. ในปีงบประมาณ พ.ศ. ๒๕๖๗ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ได้ดำเนินการเกี่ยวกับการจัดทำข้อปฏิบัติและการรับรองความสอดคล้องภายใต้โครงการศูนย์บริการ (PDPA Center) โดยมีวัตถุประสงค์ ๓ ประการ ดังนี้

๑.๑ จัดทำแนวปฏิบัติและหลักเกณฑ์ประเมินความสอดคล้องด้านการคุ้มครองข้อมูลส่วนบุคคลที่ครอบคลุมผู้ควบคุมข้อมูลส่วนบุคคล และผู้เกี่ยวข้องทั้ง ๑๐ ด้าน ได้แก่

- ๑) ด้านการกำกับดูแลการคุ้มครอง ข้อมูลส่วนบุคคล
- ๒) ด้านนโยบายองค์กร
- ๓) ด้านส่งเสริมการตระหนักรู้ในการคุ้มครองข้อมูลส่วนบุคคล
- ๔) ด้านการตอบสนองต่อสิทธิของเจ้าของข้อมูลส่วนบุคคล
- ๕) ด้านความโปร่งใส
- ๖) ด้านการบันทึกรายการ ประมวลผลและฐานทางกฎหมาย
- ๗) ด้านข้อตกลงและการแบ่งปันข้อมูลส่วนบุคคล
- ๘) ด้านการประเมินผลกระทบเพื่อการจัดการความเสี่ยง
- ๙) ด้านการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล
- ๑๐) ด้านการตอบสนอง ต่อเหตุการณ์ละเมิดข้อมูลส่วนบุคคลและเฝ้าติดตาม

๑.๒ เครื่องหมายการรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล

๑.๓ คู่มือกระบวนการยื่นรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล

๒. ในปีงบประมาณ พ.ศ. ๒๕๖๘ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล มีแผนดำเนินโครงการเพื่อสนับสนุนและส่งเสริมให้เกิดกระบวนการตรวจสอบ และรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลอย่างต่อเนื่อง โดยจัดทำระบบสำหรับตรวจรับรองความสอดคล้องตามมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล และเปิดให้หน่วยงาน ทั้งภาครัฐและเอกชนที่ต้องปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ยื่นคำขอเข้าสู่กระบวนการ ตรวจสอบ เพื่อขอรับรอง

ความสอดคล้องตามมาตรฐานคุ้มครองข้อมูลส่วนบุคคล และมีการจัดทำระบบสำหรับการเสริมสร้างและพัฒนาเครือข่าย (DPO Network) เพื่อการกำกับดูแล และติดตามประเมินผลการกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคลของประเทศ ภายใต้โครงการคุ้มครองข้อมูลส่วนบุคคลเชิงรุก (PDPC Eagle Eye) ต่อไป