โดย ผู้ช่วยศาสตราจารย์ ดร.จุฑาทิพ อัสสะบำรุงรัตน์
ภายใต้คณะทำงานศูนย์ติดตามความก้าวหน้า
และพัฒนาคู่มือ ISQM และกิจการพิเศษ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กับผู้ประกอบวิชาชีพตรวจสอบภายใน

ประเทศไทยได้มีกฎหมายที่ให้สิทธิ์กับประชาชนทุกคนสำหรับข้อมูลส่วนบุคคลของตนเอง มีสิทธิ์ในการอนุญาตหรือไม่อนุญาตให้นำข้อมูลส่วนบุคคลไปใช้ในวัตถุประสงค์ต่าง ๆ กฎหมายนี้ ได้แก่ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ซึ่งประกาศไว้ในราชกิจจานุเบกษาเมื่อวันที่ 27 พฤษภาคม พ.ศ. 2562 และมีผลบังคับใช้ในวันที่ 1 มิถุนายน พ.ศ. 2565 ที่ผ่านมากฎหมายนี้เป็นการสร้างมาตรฐานการรักษาข้อมูลส่วนบุคคลให้มีความปลอดภัย ดังนั้น องค์กรและหน่วยงานต่าง ๆ ที่มีข้อมูลส่วนบุคคลต้องมีมาตรฐานในการรักษาข้อมูลส่วนบุคคลดังกล่าวให้มีความปลอดภัยและนำไปใช้ตามวัตถุประสงค์ที่เจ้าของข้อมูลยินยอมเท่านั้น และต้องปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นี้ หากมีการละเมิดไม่ปฏิบัติตามกฎหมายนี้ องค์กรจะถูกลงโทษ

ตามกฎหมายทั้งโทษทางแพ่ง คือ ต้องจ่ายค่าสินไหมทดแทนความเสียหายให้แก่เจ้าของข้อมูล โทษทางอาญาซึ่งมีทั้งโทษจำคุกและโทษปรับ และโทษทางปกครอง คือ โทษปรับที่แยกจากโทษทางแพ่งและโทษทางอาญา อีกทั้งองค์กรสูญเสียชื่อเสียง และความเชื่อมั่นต่อองค์กรหรือหน่วยงาน ดังนั้น หน่วยงานตรวจสอบภายในจึงมีบทบาทอย่างมากในการลดความเสี่ยงให้กับองค์กร สร้างความเชื่อมั่นให้กับองค์กรว่ามีการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Compliance assurance)

จากการประชุม IIA International Conference 2022 ที่เมืองชิคาโก ประเทศสหรัฐอเมริกาในระหว่างวันที่ 17-20 กรกฎาคม พ.ศ. 2565 ที่ผ่านมา มีข้อเสนอแนะให้กับผู้ตรวจสอบภายในและหน่วยงานตรวจสอบภายใน ดังนี้

01 » ต้องเข้าใจกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล ได้แก่ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และหากองค์กรมีธุรกรรมกับต่างประเทศ องค์กรต้องศึกษากฎหมายของต่างประเทศด้วย เช่น GDPR CCPA เป็นต้น

ศึกษาและวิเคราะห์ถึงห่วงโซ่ของข้อมูลส่วนบุคคล (Personal Data Supply Chain)

2.1. ข้อมูลส่วนบุคคลนั้นเริ่มจากจุดไหน จากกระบวนการหรือขั้นตอนใด เริ่มที่ภายในองค์กรหรือได้รับจากหน่วยงานภายนอก

2.2. เส้นทางของข้อมูลส่วนบุคคล หลังจากที่องค์กรได้ข้อมูลส่วนบุคคลทั้งที่ได้มาจากเจ้าของข้อมูลเองหรือจากหน่วยงานอื่น ข้อมูลส่วนบุคคลดังกล่าวมีการส่งต่อไปให้ใคร แผนกใด หน่วยงานใด หรือองค์กรใดบ้าง และผู้ที่ได้รับข้อมูลส่วนบุคคลไปในห่วงโซ่นั้นนำไปใช้ตรงตามวัตถุประสงค์ที่เจ้าของข้อมูลส่วนบุคคลอนุญาตหรือไม่

2.3. การควบคุมภายในที่เกี่ยวข้องกับข้อมูลส่วนบุคคลในแต่ละจุดของห่วงโซ่เพียงพอหรือไม่ ที่จะให้มั่นใจว่าข้อมูลส่วนบุคคลนั้นไม่ถูกเผยแพร่หรือถูกขโมยออกไป

02»

03» ทำการประเมินความเสี่ยงในการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Assess Compliance Risk) โดยประเมินทั้งโอกาสที่องค์กรไม่ได้ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือปฏิบัติตามแต่ยังไม่ครบถ้วนตามที่กฎหมายกำหนด และประเมินผลกระทบที่จะเกิดขึ้นทั้งที่เป็นจำนวนเงินและไม่เป็นจำนวนเงิน ซึ่งผู้ตรวจสอบภายในมีความจำเป็นอย่างยิ่งที่ต้องเข้าใจห่วงโซ่ของข้อมูลส่วนบุคคล ความเสี่ยงและการควบคุมภายในที่เกี่ยวข้อง ตัวอย่างเช่น บางองค์กรมีการอนุญาตให้พนักงานสามารถใช้อุปกรณ์ส่วนตัว ได้แก่ โทรศัพท์ โน๊ตบุ๊ค ในการทำงานที่องค์กร เพื่อเพิ่มความคล่องตัวในการทำงาน ซึ่งอุปกรณ์ส่วนตัวเหล่านั้นมีการเชื่อมต่อกับระบบภายในขององค์กร เช่น โรงพยาบาลที่มีความจำเป็นต้องอนุญาตให้แพทย์ใช้โทรศัพท์มือถือส่วนตัวในการดูข้อมูลของคนไข้เพื่อใช้ในการรักษาพยาบาล กรณีเช่นนี้โรงพยาบาลมีความเสี่ยงเกิดขึ้นจากมิจฉาชีพเจาะเข้าระบบโรงพยาบาลผ่านโทรศัพท์ของแพทย์ เป็นต้น นอกจากนี้ผู้ตรวจสอบภายในควรประเมินระดับความเข้าใจในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ของพนักงานในองค์กรด้วย

สอบทานการควบคุมภายในที่เกี่ยวข้องกับการรักษาและป้องกันข้อมูลส่วนบุคคลในแต่ละจุดว่ามีความเพียงพอและมีประสิทธิภาพ ประสิทธิผลในการช่วยลดความเสี่ยงของการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งการสอบทานนี้ควรที่จะทำอย่างต่อเนื่อง (Ongoing review) จากกรณีของโรงพยาบาล ผู้ตรวจสอบภายในต้องสอบทานตั้งแต่นโยบายของโรงพยาบาลว่ามีการกำหนดสิทธิ์ของแพทย์ในการเข้าถึงข้อมูลใดบ้าง การตั้งค่าการเข้าถึงข้อมูลของทุกอุปกรณ์ทั้งในภาพรวมและแยกรายอุปกรณ์เป็นอย่างไร และจุดที่เชื่อมต่อระหว่างอุปกรณ์ส่วนตัวของแพทย์กับฐานข้อมูลของโรงพยาบาลมีการควบคุมภายในที่เพียงพอหรือไม่ อย่างไร

04»

05» หากมีการเปลี่ยนแปลงของกระบวนการทางธุรกิจ (Change in business process) ผู้ตรวจสอบภายในควรทำความเข้าใจการเปลี่ยนแปลง ทำการประเมินความเสี่ยงและการควบคุมภายในที่เกี่ยวข้อง ซึ่งการเปลี่ยนแปลงเกิดขึ้นตลอดเวลาในปัจจุบัน ผู้ตรวจสอบภายในจึงต้องเรียนรู้ และปรับขอบเขตและแนวทางการตรวจสอบให้สอดคล้องกับการเปลี่ยนแปลงของกระบวนการทางธุรกิจที่เกิดขึ้นตลอดเวลา

ข้อมูลในปัจจุบันมีมูลค่าที่ประเมินไม่ได้ สามารถส่งผลทั้งทางบวกและทางลบต่อทุกคน ต่อองค์กร ต่อสังคม ดังนั้น นอกเหนือจากการที่ผู้ตรวจสอบภายในจะประเมินการปฏิบัติตามกฎหมายแล้ว จะเป็นการดีกว่าไหมหากผู้ตรวจสอบภายในคิดในมุมมองที่ว่าข้อมูลส่วนตัวของท่านถูกบริหารจัดการอย่างไร

เอกสารอ้างอิง

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

The Personal Data Supply Chain: What It Means to You and Your Company Now Audit Wise, presented by Frank Vukovits, CIA, CISA Fastpath Solutions in 2022 IIA International Conference