Tax Magazine: **ฉบับพฤษภาคม** 2565 / Section: Cover Story / Column: Cover Story
ผู้เขียน: ปริญญา หอมเอนก[1]

PDPA Final Call

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล องค์กรพร้อมหรือยัง?

PDPA หรือ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่มีการพูดถึงและเป็นประเด็นร้อนต่อเนื่องมาหลายปี กำลังจะมีการบังคับใช้ในวันที่ 1 มิถุนายน 2565 นี้แล้ว

เชื่อว่าองค์กรทั้งหลายคงได้ดำเนินการตาม พ.ร.บ. ฉบับนี้กันแล้ว แต่สำหรับเตรียมตัวโค้งสุดท้ายกับเวลาที่เหลืออยู่ เราอยากมาย้ำเรื่องสำคัญในการดูแลจัดการข้อมูลส่วนบุคคลด้วยความเข้าใจที่ถูกต้อง

เพื่อให้องค์กรพร้อมมากที่สุด สำหรับ PDPA ....Final Call

ประวัติความเป็นมาของ GDPR และ PDPA

ในอดีต อินเทอร์เน็ตและโซเชียลมีเดียยังไม่ได้รับความนิยมเท่าในปัจจุบัน เรื่องของข้อมูลส่วนบุคคลในเวลานั้นจึงยังไม่ค่อยมีใครพูดถึงและให้ความสำคัญเท่าใดนัก แต่ในหลายปีที่ผ่านมาจากความนิยมของโซเชียลมีเดีย การเติบโตของอินเทอร์เน็ต และการนำเทคโนโลยี Big Data และ AI มาใช้ในการวิเคราะห์ข้อมูลพฤติกรรมส่วนตัวของลูกค้าเพื่อประโยชน์ทางธุรกิจโดยที่ตัวลูกค้าเองส่วนใหญ่จะไม่ทราบถึงการวิเคราะห์ดังกล่าว ที่ทำให้เกิดความเสี่ยง มีผลกระทบทั้งทางตรงและทางอ้อมต่อตัวบุคคลที่ถูกนำข้อมูลส่วนตัวไปใช้โดยไม่ได้รับอนุญาต

จากนั้นจึงมีการพูดถึงเรื่องข้อมูลส่วนบุคคลและความเป็นส่วนตัวของข้อมูล โดยเริ่มจากหน่วยงาน OECD ได้พัฒนา OECD Guideline on the Protection of Privacy and Transborder Flow of Personal Data ในช่วงปี พ.ศ. 2513 - 2523 ปัจจุบันได้ถูกปรับปรุงพัฒนาเป็น Version ล่าสุดในปี พ.ศ. 2556 เห็นได้ว่า การให้ความสำคัญเรื่องข้อมูลส่วนบุคคลมีมานานกว่า 30 ปีแล้ว แต่เพิ่งจะมานิยมหลังจากสหภาพยุโรป หรือ EU ได้ออกระเบียบในกฎหมายสหภาพยุโรปว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ขึ้นในปี พ.ศ. 2559 และมีผลบังคับใช้ในปี พ.ศ. 2561 ที่เรารู้จักกันในนาม General Data Protection Regulation (GDPR) EU 2016/679 ใช้แทนคำสั่งคุ้มครองข้อมูล Data Protection Directive 95/46/EC นับจากที่ GDPR เริ่มบังคับใช้ได้เพียง 1 ปี พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลของไทย หรือที่เรารู้กันในชื่อย่อ “PDPA” ก็ถูกประกาศในราชกิจจานุเบกษาในปี พ.ศ. 2562

ปัจจุบันนับเป็นเวลากว่า 3 ปีที่ PDPA จะถูกนำมาบังคับใช้อย่างจริงจังในประเทศไทย ควบคู่กับการทำงานของหน่วยงาน Regulator ใหม่ล่าสุด “สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล” หรือ “สคส.” จะเห็นได้ว่าประเทศไทยมีการเตรียมการและมีความพร้อมในระดับหนึ่งที่ประชาชนได้รับรู้และเตรียมตัวกันมาหลายปี นับจากกฎหมายได้ถูกประกาศให้สาธารณชนได้รับทราบ

ทำไมเราต้องให้ความสำคัญกับเรื่องข้อมูลส่วนบุคคลและความเป็นส่วนตัวของข้อมูล

ในปัจจุบันเราได้ยินข่าว “ข้อมูลรั่วไหล” หรือข้อมูลส่วนบุคคลหลุดออกไปสู่สาธารณะหรือไปอยู่ในมือของมิจฉาชีพ ทำให้เกิดความเดือดร้อนต่อเจ้าของข้อมูลส่วนบุคคลไม่เว้นแต่ละวัน โดยมีอัตราการเกิดความเสียหายอย่างต่อเนื่อง สาเหตุที่ทำให้เราต้องให้ความสำคัญกับข้อมูลส่วนบุคคล ก็คือ เมื่อข้อมูลส่วนบุคคลอยู่กับตัวเราโดยที่เราสามารถ

---

[1] ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศและระบบเทคโนโลยีสารสนเทศ ACIS Professional Center/Cybertron

ควบคุมได้ ปัญหาจะยังไม่เกิดจนกว่าข้อมูลส่วนบุคคลของเราจะถูกนำไปใช้หรือถูกเข้าถึงโดยมิชอบโดยบุคคลอื่น ทั้งที่เรารู้ตัวจากการแจ้งให้ทราบหรือโดยที่เราไม่รู้ตัวเลยก็มีให้เห็นอยู่เป็นประจำ จนเกิดคำถามที่ว่า “เขารู้ข้อมูลส่วนตัวของเราได้อย่างไร ?” ไม่ว่าจะเป็นชื่อ ที่อยู่ เบอร์โทรศัพท์ อีเมล เลขประจำตัวบัตรประชาชน หรือเลขบัญชีธนาคาร โดยข้อมูลส่วนบุคคลของเรา ถือเป็นสินทรัพย์สารสนเทศ หรือ “Information Asset” ที่สามารถนำไปทำประโยชน์ได้โดยมีผู้ได้ประโยชน์จากการประมวลผลข้อมูลส่วนบุคคลของเรา และผู้เสียประโยชน์ก็คือตัวเรานั่นเอง

ดังนั้น พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล จึงเน้นไปที่ข้อมูลส่วนบุคคล ไม่ได้เน้นไปที่ข้อมูลขององค์กร เมื่อมีการรั่วไหลของข้อมูลส่วนบุคคลและทำให้สามารถระบุตัวตนของบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ให้ถือว่าเกิดการละเมิดข้อมูลส่วนบุคคลขึ้นแล้ว ทำให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องมีหน้าที่รับผิดชอบในเหตุการณ์รั่วไหลของข้อมูลดังกล่าวตามกฎหมาย

จึงสรุปได้ว่า เรื่องความเป็นส่วนตัวของข้อมูลในยุคนี้ **ร่องรอยทางดิจิทัล** หรือ “Digital Footprint“ มีความสำคัญอย่างมาก สามารถสร้างความเดือดร้อนความเสียหายต่อบุคคลที่ข้อมูลส่วนบุคคลหลุดออกไปโดยไม่ได้ตั้งใจและไม่เต็มใจ เมื่อมีความเสียหายเกิดขึ้นโดยเฉพาะด้านชื่อเสียงทั้งบุคคลและองค์กรแล้ว ก็ยากที่จะกลับมาเหมือนตอนที่ข้อมูลยังไม่หลุดรั่วออกไป ว่ากันว่าในยุคไซเบอร์ “ Reputational Risk” หรือความเสี่ยงด้านชื่อเสียงและภาพลักษณ์ ถือเป็นความเสี่ยงที่เกิดความเสียหายสูงสุดต่อเจ้าของข้อมูลส่วนบุคคล เพราะในโลกไซเบอร์มีข้อมูล “Digital Footprint” ถูกเก็บไว้อยู่ในระบบ Cloud เป็นจำนวนมาก เก็บไว้ย้อนหลังเป็นเวลาหลายปี ทำให้มีความเสี่ยงต่อเจ้าของข้อมูลทั้งทางตรงและทางอ้อมอยู่ตลอดเวลาที่ยังมีการเข้าถึง “Digital Footprint” ได้

เรื่องการป้องกันข้อมูล หรือ “Data Protection” **จึงกลายเป็นเรื่องสำคัญที่หลีกเลี่ยงไม่ได้ โดยต้องเริ่มจากเรื่องความมั่นคงปลอดภัยของข้อมูล หรือ** “Data Security” **เสียก่อนที่จะมาพูดกันต่อในเรื่องของความเป็นส่วนตัวของข้อมูล หรือ** “Data Privacy” **ดังคำกล่าวที่ว่า** “You Can Get Security Without Privacy But You Can’t Get Privacy Without Security”

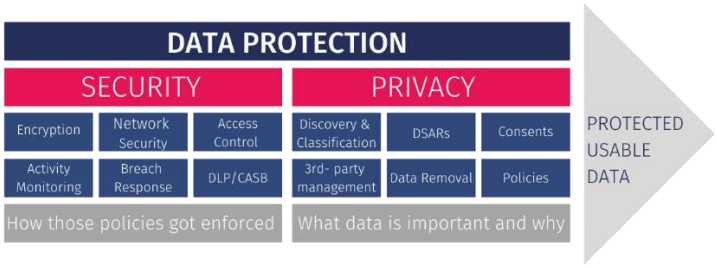
PDPA **กฎหมายใกล้ตัว เกี่ยวข้องกับเราอย่างไร ?**

PDPA ย่อมาจาก Personal Data Protection Act หรือ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีวัตถุประสงค์บัญญัติขึ้นเพื่อให้การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพ และเพื่อให้มีมาตรการเยียวยาเจ้าของข้อมูลส่วนบุคคลจากการถูกละเมิดสิทธิในข้อมูลส่วนบุคคลมีประสิทธิภาพ กฎหมายได้กำหนดสิทธิของเจ้าของข้อมูลส่วนบุคคล เน้นไปที่การรักษาข้อมูลส่วนบุคคลให้ปลอดภัย เป็นหน้าที่ของผู้คุ้มครองข้อมูลส่วนบุคคล โดยข้อมูลส่วนบุคคลต้องถูกนำไปใช้ให้ตรงกับวัตถุประสงค์ตามคำยินยอมที่เจ้าของข้อมูลส่วนบุคคลอนุญาต โดยกฎหมายได้ประกาศไว้ในราชกิจจานุเบกษาเมื่อวันที่ 27 พฤษภาคม 2562 และกำลังจะมีผลบังคับใช้ในวันที่ 1 มิถุนายน 2565 โดยในตัวบทกฎหมายหลายมาตราสามารถบังคับใช้ได้โดยไม่จำเป็นต้องรอให้กฎหมายลำดับรองภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ประกาศใช้ทั้งหมด

ความเข้าใจผิดเกี่ยวกับ GDPR/PDPA **และ** Data Protection/Data Security/Data Privacy

ตัวอักษรย่อ “DP” ใน “GDPR” และ “PDPA” ย่อมาจากคำว่า “Data Protection” ไม่ใช่ “Data Privacy” และใน GDPR ทุกมาตราไม่มีการกล่าวถึง “Data Privacy” เลย มีแต่การกล่าวถึง “Data Protection” ในหลายมาตราของ GDPR โดย Data Protection หมายถึง “การป้องกันข้อมูล” ซึ่งอาศัยหลักการพื้นฐานด้านความมั่นคงปลอดภัย “CIA Triad” ได้แก่ Confidentiality, Integrity และ Availability หากเรื่องความมั่นคงปลอดภัยของข้อมูลยังปฏิบัติไม่ได้ คงไม่ต้องพูดถึงเรื่อง

“Data Privacy” หรือความเป็นส่วนตัวของข้อมูล เพราะในความหมายของ “Data Privacy” จะมีความหมายที่กว้างกว่า “Data Protection” แต่ต้องปฏิบัติเรื่อง “Data Protection” ให้ได้ก่อนเป็นพื้นฐาน แล้วค่อยมาลงรายละเอียดต่อเรื่อง “Data Privacy” ที่เป็นเรื่องที่ต้องทำเพิ่มเติม จึงไม่น่าแปลกใจที่องค์กรต้องปฏิบัติตาม ISO/IEC 27001:2013 ก่อน ถึงจะทำ ISO/IEC 27701:2019 ได้



รูปที่ 1: About Data Protection, Data Security and Data Privacy

Credit : Data Privacy Manager https://dataprivacymanager.net/

การป้องกันข้อมูลหรือ“Data Protection”ที่ถูกกำหนดไว้ทั้งในกฎหมาย PDPA และ GDPR เป็นการผสมผสานกันของ 2 เรื่องสำคัญ ได้แก่ “Data Security” และ “Data Privacy” หมายถึง ต้องทำทั้ง “Security” และ “Privacy” (ดูรูปที่ 1) โดย “Data Security” หรือการรักษาความมั่นคงปลอดภัยข้อมูลจะมุ่งเน้นไปที่ CIA Triad ดังที่กล่าวมาแล้ว เน้นไปที่การป้องกันผู้ที่ไม่เกี่ยวข้องเข้าถึงข้อมูลได้โดยมิชอบ เริ่มตั้งแต่การมีระบบ Access Control และ Network Security ที่ได้มาตรฐาน การทำ Two Factors Authentication (2FA) เป็นส่วนหนึ่งของ Data Security การเข้ารหัสรหัสข้อมูลหรือ Data Encryption รวมไปถึงการเตรียมการเรื่อง Data Breach Response การเฝ้าระวังข้อมูลรั่วไหลโดยมีศูนย์ Security Operation Center (SOC) และทีมงาน Incident Response (IR) เป็นต้น

สำหรับ “Data Privacy” จะเน้นไปที่กระบวนการในการรักษาความเป็นส่วนตัวของข้อมูล การขอความยินยอมในการนำข้อมูลส่วนบุคคลไปใช้ได้เฉพาะผู้ที่ได้รับอนุญาต การปฏิบัติตามกฎหมายการบริหารจัดการบุคคลที่ 3 ที่มีความเกี่ยวข้องกับข้อมูลส่วนบุคคล

รูปที่ 2 : Data Privacy <> Data Security

Credit : Data Privacy Manager https://dataprivacymanager.net/

ตัวอย่างที่ชัดเจนของความแตกต่างระหว่าง “Data Security” และ “Data Privacy” ได้แก่ การใช้งานฟรีอีเมล โดยชื่อผู้ใช้และรหัสผ่าน อาจรวมถึงการใช้ 2FA เป็นเรื่องของ “Data Security” แต่การที่ผู้ให้บริการฟรีอีเมล เช่น Hotmail (Microsoft) หรือ Gmail (Google) จะนำข้อมูลของเราไปใช้ในการทำธุรกิจของเขา เป็นเรื่องของ “Data Privacy” ที่เขาต้อง

ตกลงกับเราซึ่งเป็นผู้ใช้บริการเสียก่อนว่าเราจะยินยอมให้เขานำข้อมูลของเราไปใช้หรือไม่ อีกทั้ง เขายังต้องจัดเก็บข้อมูลของเราให้มีความมั่นคงปลอดภัยซึ่งเป็นส่วนหนึ่งของ “Data Security” อีกด้วย

ข้อมูลส่วนบุคคลรั่วไหลจากช่องทางไหนได้บ้าง ?

ในปัจจุบันปัญหาข้อมูลส่วนบุคคลรั่วไหลกลายเป็นปัญหาระดับโลกที่แก้ไม่ตกและเกิดขึ้นอย่างมีนัยยะ สำคัญต่อเนื่อง มีแนวโน้มที่จะเพิ่มขึ้นทุกวัน ไม่ว่าจะเกิดจากแฮกเกอร์ มิจฉาชีพ หรือพนักงานในองค์กรเอง แม้กระทั่งเกิดจากการที่ผู้ให้บริการ Cloud/Social Media ทำข้อมูลรั่วไหลเสียเองก็มีความเป็นไปได้ทั้งสิ้น ปัญหาข้อมูลส่วนบุคคลรั่วไหลเป็นปัญหาที่เราต้องเปลี่ยน Mindset จาก “IF” เป็น “WHEN” เนื่องจากข้อมูลส่วนบุคคลอาจรั่วไหลได้ผ่านทางช่องทางที่หลากหลายไม่ว่าจะเป็นอิเล็กทรอนิกส์เมล โปรแกรม Chat ยอดนิยมต่าง ๆ ไม่ว่าจะเป็น LINE, WhatsApp, Facebook Messenger การรั่วไหลผ่านทางเว็บไซต์ และ Cloud Drive ต่าง ๆ ไม่ว่าจะเป็น OneDrive, Google Drive, Dropbox แม้กระทั่งการรั่วไหลจากเครื่อง PC, Notebook, Smartphone ไปจนถึงการรั่วไหลด้านกายภาพจากการถูกขโมยหรือสูญหาย

ดังนั้นการเตรียมความพร้อมในเรื่องปัญหาข้อมูลส่วนบุคคลรั่วไหลทั้งส่วนตัวและองค์กรจึงมีความสำคัญอย่างยิ่ง เนื่องจากความเสี่ยงและอุบัติการณ์ที่ข้อมูลส่วนบุคคลรั่วไหลสามารถเกิดขึ้นได้กับทุกคน ทุกองค์กร ทุกที่ และทุกเวลา ไม่ได้ขึ้นกับขนาดของธุรกิจแต่อย่างใด

เมื่อข้อมูลส่วนบุคคลรั่วไหลเราควรทำอย่างไร?

จากหลากหลายช่องทางที่ข้อมูลส่วนตัวสามารถรั่วไหลได้ การป้องกันไม่ให้ข้อมูลส่วนตัวของเรารั่วไหลแบบ 100% จึงเป็นไปได้ยากมาก ดังนั้นเราควรมีการเตรียมการไว้ล่วงหน้า เช่น ไม่เก็บข้อมูลสำคัญไว้ใน Cloud Drive หรือทำการเข้ารหัสข้อมูลและสำหรับสำรองข้อมูลไว้ก่อนที่จะเกิดเหตุการณ์ไม่พึงประสงค์ เมื่อข้อมูลรั่วไหลจะได้ไม่เกิดผลกระทบกับตัวเรามากนัก และเมื่อข้อมูลได้รั่วไหลไปแล้ว ก็ต้องกลับมาตั้งสติปฏิบัติตามขั้นตอนที่เราได้ทำการศึกษาและเตรียมการไว้ล่วงหน้าในการกู้ข้อมูลกับคืนมาใช้งานได้ตามปกติ

เมื่อข้อมูลส่วนบุคคลรั่วไหล องค์กรควรทำอย่างไร?

การเตรียมการเรื่อง “Breach Response” เป็นส่วนหนึ่งในหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล

- ต้องปฏิบัติตามกฎหมายเมื่อมีเหตุการณ์ไม่พึงประสงค์เกิดขึ้นกับข้อมูลที่มีความเสี่ยง
- ต้องรีบแจ้งให้กับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลให้ทราบภายใน 72 ชั่วโมง ตามมาตรา 37 (4) และข้อมูลที่มีความเสี่ยงสูงต้องแจ้งกับเจ้าของข้อมูลส่วนบุคคลโดยไม่ชักช้าอีกด้วย
- การแต่งตั้งโฆษกประจำองค์กรที่มีหน้าที่ชี้แจงกับนักข่าวก็เป็นเรื่องสำคัญในการทำ “Crisis Management” เพื่อไม่ให้เกิดผลกระทบต่อชื่อเสียงและภาพลักษณ์ขององค์กร
- การเตรียมการก่อนการเกิดเหตุการณ์ไม่พึงประสงค์กับข้อมูลส่วนบุคคล ก็เป็นเรื่องสำคัญไม่ว่าจะเป็นการทำ “Data Pseudonymization” หรือ “Data Encryption” ก็เป็นเรื่องที่องค์กรควรจัดเตรียมการให้พร้อมต่อการถูกโจมตีโดยผู้ไม่หวังดีที่อาจเกิดขึ้นได้ทุกเวลา

การทำความเข้าใจกับคำศัพท์พื้นฐานที่เกี่ยวข้องกับ PDPA

- **ความแตกต่างของ Data Controller และ Data Processor**

ผู้ควบคุมข้อมูลส่วนบุคคล หรือ Data Controller เป็นผู้มีหน้าที่รับผิดชอบสูงสุดในการปฏิบัติตาม PDPA เนื่องจากผู้ควบคุมข้อมูลส่วนบุคคล มีอำนาจในการตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล นับเป็นผู้รับผิดชอบหลักเวลาเกิดคดีความเกี่ยวกับ PDPA ซึ่งอาจเป็นบุคคลหรือนิติบุคคลก็ได้ **แต่จะไม่ใช่การกำหนดให้พนักงานในองค์กรคนใดคนหนึ่งหรือเจ้าหน้าที่ของบริษัทมาเป็นผู้ควบคุมข้อมูลส่วนบุคคล** ซึ่งไม่ถูกต้องตามหลักการ รวมไปถึงผู้ประมวลผลข้อมูลส่วนบุคคลหรือ Data Processor นับเป็นผู้ที่รับผิดชอบรองลงมาจากผู้ควบคุมข้อมูลส่วนบุคคล โดยทำหน้าที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคลจึงจัดได้ว่าเป็นผู้รับผิดชอบรองมาจากผู้ควบคุมข้อมูลส่วนบุคคล

ดังนั้นการตรวจสอบสัญญาทางกฎหมายระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลจึงมีความสำคัญมาก จำเป็นต้องมีการทบทวนให้ถูกต้องชัดเจนให้เข้าใจตรงกันทั้ง 2 ฝ่าย

- **ความแตกต่างของ Privacy Policy และ Privacy Notice**

Privacy Policy คือ นโยบายการคุ้มครองข้อมูลส่วนบุคคลที่องค์กรควรกำหนดให้มี แต่กฎหมายไม่ได้กำหนดให้จัดทำขึ้นแต่ควรทำ เพื่อเป็นประโยชน์ในการบริหารจัดการข้อมูลขององค์กรเอง เป็นเอกสารที่สื่อสารถึงบุคลากรในองค์กรโดยมีขอบเขตเป็นนโยบายและแนวปฏิบัติขององค์กรในการคุ้มครองข้อมูลส่วนบุคคล กำหนดทิศทางในการเก็บรวบรวมไว้หรือเปิดเผยข้อมูลรายบุคคลเพื่อให้สอดคล้องกับหลักการและเงื่อนไขตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

สำหรับ “Privacy Notice” คือ ประกาศความเป็นส่วนตัวให้เจ้าของข้อมูลส่วนบุคคลให้รับทราบเกี่ยวกับวิธีในการเก็บรวบรวมไว้หรือเปิดเผยข้อมูลส่วนบุคคล โดยกฎหมายกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องแจ้งให้เจ้าของข้อมูลทราบถึงรายละเอียดจัดเก็บรวบรวมข้อมูลตามมาตรา 23 PDPA โดย Privacy Policy อาจครอบคลุม Privacy Notice ก็ได้โดยพิจารณาจากเนื้อหาภายใน หากครบถ้วนตามที่กฎหมายกำหนดก็จะถือว่ามีการแจ้งวัตถุประสงค์ตามมาตรา 23 PDPA แล้ว

ทำความเข้าใจในบทบาทหน้าที่ของ DPO

หลายคนอาจสงสัยว่าอาชีพใหม่ที่กำลังมาแรงในขณะนี้ ได้แก่ อาชีพ “เจ้าหน้าที่คุ้มครองข้อมูล” หรือ Data Protection Officer มีหน้าที่ตามมาตรา 42 พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล อย่างไร ?

หน้าที่หลักของ DPO มี 4 ข้อดังนี้

1. ให้คำแนะนำแก่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวกับการปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล
2. ประสานงานและให้ความร่วมมือกับสำนักงาน ในกรณีที่มีปัญหาเกี่ยวข้องกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลผลข้อมูลส่วนบุคคล
3. ตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล
4. รักษาความลับของข้อมูลส่วนบุคคลที่ล่วงรู้หรือได้มาจากการปฏิบัติหน้าที่ DPO

การปฏิบัติหน้าที่ DPO สามารถเป็นได้ทั้งพนักงานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล อีกทั้งยังสามารถ Outsource ให้บริษัทที่ให้บริการ DPO ภายนอกสามารถปฏิบัติหน้าที่ DPO ได้เช่นกัน โดยเป็นผู้รับจ้างให้บริการตามสัญญากับผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล

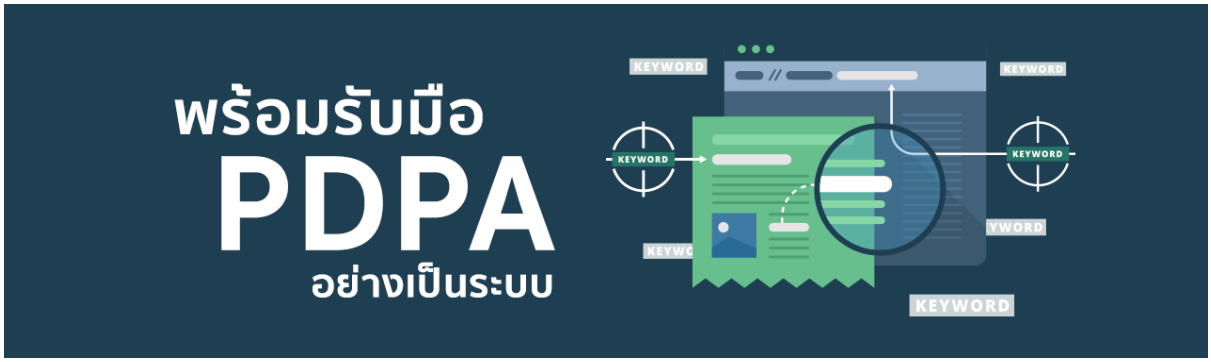
แนวทางจัดทำบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล ROPA (Records of Processing Activities)

เราได้ยินคำว่า“ROPA” กันบ่อยครั้งในช่วงหลายเดือนที่ผ่านมาว่าเป็นเรื่องที่องค์กรต้องปฏิบัติตาม PDPA มาตรา 39 โดย ROPA ย่อมาจาก Records of Processing Activities หมายถึง การบันทึกกิจกรรมการประมวลผลขององค์กรที่เกี่ยวข้องกับข้อมูลส่วนบุคคล โดยจะต้องอยู่ในรูปแบบข้อความที่เป็นลายลักษณ์อักษรหรืออิเล็กทรอนิกส์

ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดทำและเก็บรักษาบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล ประกอบด้วยประเภทกิจกรรมโดยมีรายละเอียดดังต่อไปนี้

1. ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม
2. วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท
3. ข้อมูลที่เกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล
4. ระยะเวลาในการเก็บรักษาและการลบข้อมูลส่วนบุคคล
5. สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล
6. การใช้หรือเปิดเผยข้อมูลที่ได้รับการยกเว้นไม่ต้องขอความยินยอม
7. การปฏิเสธคำขอหรือการคัดค้าน
8. อธิบายเกี่ยวกับมาตรการในการรักษาความมั่นคงปลอดภัยตามมาตรา 37 (1)

โดย ROPA ต้องทำให้สามารถเข้าถึงได้ง่าย และเมื่อมีการร้องขอ ผู้ควบคุมข้อมูลส่วนบุคคลต้องสามารถแสดงให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลสามารถตรวจสอบได้



Checklist โค้งสุดท้าย PDPA

5 ข้อควรปฏิบัติสำหรับพนักงาน/ประชาชน

1. เวลาอ่านและศึกษา พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล เพื่อให้เข้าใจในคำศัพท์และ Terminology ต่าง ๆ ที่เกี่ยวกับ PDPA
2. ฝึกอบรมหาความรู้ด้วยตนเองหรือเข้าฟังสัมมนาที่องค์กรจัดให้เพื่อทำความเข้าใจ PDPA มากขึ้น
3. รับรู้สิทธิของตนเองที่สามารถขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามกฎหมายได้ หลังจากวันที่กฎหมายมีผลบังคับใช้
4. ควรพิจารณาให้ถี่ถ้วนเวลาที่ต้องให้ความยินยอมกับ Mobile/Web Application หรือหน่วยงานที่เราจำเป็นต้องให้ข้อมูลส่วนบุคคลว่าเราควรยินยอมหรือไม่ยินยอมให้ข้อมูลส่วนบุคคล เพื่อไม่ให้เกิดผลกระทบในภายหลัง

5. สละเวลาตั้งค่าความมั่นคงปลอดภัยต่าง ๆ ใน Mobile/Web Application ที่เราใช้งานอยู่ ไม่ว่าจะเป็น Social Media, Free Email หรือ Mobile Banking และ Online Shopping ต่าง ๆ เพื่อป้องกันไม่ให้เกิดการรั่วไหลของข้อมูลส่วนบุคคล

11 ข้อควรปฏิบัติสำหรับองค์กร[2]

1. แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล DPO ให้เป็นไปตามมาตรา 41 PDPA
2. จัดทำประกาศความเป็นส่วนตัว (Privacy Notice) ให้เป็นไปตามมาตรา 23 PDPA
3. จัดทำบันทึกรายการกิจกรรมการประมวลผล (ROPA) ให้เป็นไปตามมาตรา 39 PDPA (ในกรณีที่เข้าข่ายต้องปฏิบัติตาม PDPA)
4. จัดทำแบบขอความยินยอมในกรณีที่มีความจำเป็นต้องใช้ (Consent Form) ให้เป็นไปตามมาตรา 19 PDPA
5. จัดทำข้อตกลงการประมวลผลในกรณีที่มีการจ้างผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement) ให้เป็นไปตามมาตรา 40 PDPA
6. ควรจัดตั้งคณะทำงาน PDPA ภายในองค์กร
7. การสำรวจข้อมูลภายในองค์กรและจัดทำผังวงจรชีวิตข้อมูลส่วนบุคคล (Data Inventory)
8. ควรจัดทำนโยบายและแนวทางปฏิบัติขององค์กรในเรื่องการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy and Code of Practices)
9. ในกรณีที่มีการแบ่งปันหรือแลกเปลี่ยนข้อมูลระหว่างองค์กร ควรจัดทำข้อตกลงการแลกเปลี่ยนข้อมูลส่วนบุคคล (Data Sharing Agreement)
10. ควรสร้างความตระหนักรู้และฝึกอบรมเรื่องการคุ้มครองข้อมูลส่วนบุคคลให้แก่พนักงานและผู้บริหารองค์กร (Capacity Building and Awareness Raising)
11. ควรกำกับดูแลและตรวจสอบอย่างสม่ำเสมอ (Audit and Compliance)

สิ่งที่องค์กรไม่ควรทำในการปฏิบัติตาม PDPA

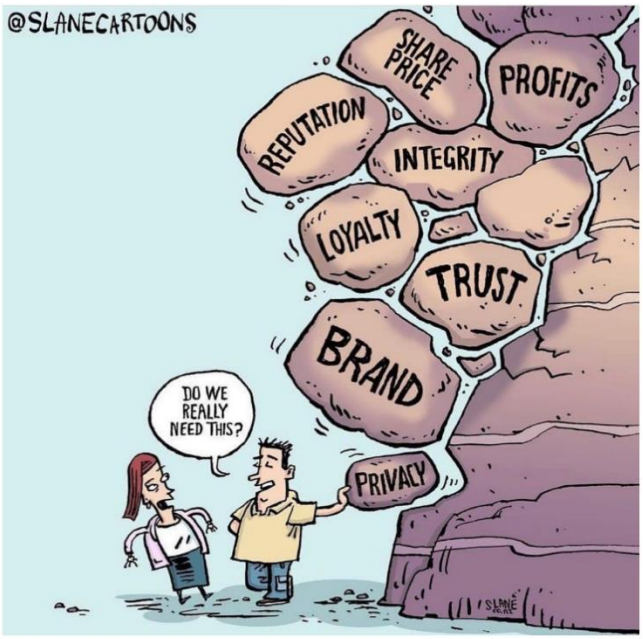
การจัดซื้อจัดจ้างเครื่องมือหรือ Software สำเร็จรูปมาใช้งานในองค์กรเพื่อให้ผ่านเส้นตายการบังคับใช้ PDPA เป็นสิ่งที่ผู้บริหารองค์กรหลายท่านเข้าใจผิดว่า เมื่อซื้อหรือเช่าใช้ Software มาแล้วจะทำให้ผ่าน PDPA ซึ่งความเป็นจริงการลงทุนซื้อระบบโดยยังไม่ได้ทำความเข้าใจอย่างถ่องแท้กับตัวบทกฎหมายและยังไม่มีกระบวนการปฏิบัติที่ดีรองรับ ไม่สามารถทำให้เกิดความสำเร็จตามที่ตั้งใจไว้ได้ เพราะลำพัง Tool หรือ Software ไม่สามารถทำให้องค์กรผ่าน PDPAได้ จำเป็นต้องปฏิบัติตาม 11 ข้อดังที่ได้กล่าวไว้ในตอนต้นเสียก่อน แล้วค่อยพิจารณาจัดซื้อหรือเช่าใช้ Software เพื่อทำ Data Inventory และ ROPA รวมถึงเรื่องการประมวลผล DSRs (Data Subject Requests) ไปจนถึงการบริหารจัดการ Cookies ในเว็บไซต์ขององค์กรแบบอัตโนมัติ ซึ่งเป็นเพียงส่วนหนึ่งในการปฏิบัติตาม PDPA

ข้อคิดเกี่ยวกับการปฏิบัติตาม PDPA ประโยชน์แฝงที่องค์กรอาจมองไม่เห็น

---

[2] อ้างอิง : ประกาศจาก Facebook สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ทำไมองค์กรถึงต้องให้ความสำคัญกับ Cybersecurity และ Data Privacy



Credit ภาพการ์ตูน By Chris Slane, @slanecartoon

ปัจจุบันและอนาคตความเสี่ยงทางด้านภาพลักษณ์และชื่อเสียง (Reputational Risk) จัดเป็นความเสี่ยงที่สูงสุดของบุคคลและองค์กร เมื่อเสียชื่อเสียงไปแล้วต้องใช้เวลานานกว่าที่จะสามารถกู้กลับคืนมาได้ เพราะเรื่องราวที่เราไม่พึงประสงค์จะให้เกิดขึ้น อาจจะอยู่ในข่าวหรือความทรงจำเป็น Digital footprints ไปอีกนานเท่านาน

ดังนั้นการให้ความสำคัญเรื่องการปฏิบัติตาม PDPA จึงเป็นเรื่องสำคัญที่ก่อให้เกิดประโยชน์อย่างมากต่อองค์กรในระยะยาว เพราะเรื่องความไว้เนื้อเชื่อใจ (Trust) ของลูกค้าและพนักงานเป็นเรื่องสำคัญขององค์กรในศตวรรษที่ 21 การใช้งบประมาณทั้งด้านปรึกษา ค่าฝึกอบรม ค่าซอฟต์แวร์ต่าง ๆ รวมถึงค่าใช้จ่ายในการทำ DPO Outsourcing อาจจะมองเป็นค่าใช้จ่ายขององค์กร แต่จริง ๆ แล้วเป็นการลงทุนที่จะปกป้องข้อมูลส่วนบุคคลของลูกค้าและพนักงานตลอดจนการรักษาชื่อเสียงและภาพลักษณ์ขององค์กรไว้ว่าจะเป็นการรักษา Brand Loyalty และ Trust ไปจนถึงราคาหุ้นหรือผลกำไรของบริษัท ส่งผลให้เกิดประโยชน์ต่อองค์กรในระยะยาว

จึงเห็นควรให้เจ้าของกิจการหรือผู้บริหารระดับสูงขององค์กรควรให้การสนับสนุนการปฏิบัติตาม PDPA ทั้งนี้เพื่อความยั่งยืน (Sustainability) ขององค์กรในระยะยาวต่อไป

++++++++++++++++++++++++++++++++++