ปัญหากฎหมายคุ้มครองข้อมูลส่วนบุคคลของผู้ประกอบธุรกิจ SME[1]

เนติกร ตริตรอง[2]

กฎหมายคุ้มครองข้อมูลส่วนบุคคลนั้น มีวัตถุประสงค์เพื่อการคุ้มครองสิทธิเกี่ยวกับข้อมูลส่วนบุคคลของประชาชนในฐานะเจ้าของข้อมูลส่วนบุคคลโดยกำหนดหน้าที่และความรับผิดชอบให้บริษัท และ/หรือ องค์กรต่างๆ โดยไม่จำกัดขนาดของธุรกิจ (Business size) ที่ได้ดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของประชาชนที่ได้รับมามีหน้าที่และความรับผิดชอบปฏิบัติให้สอดคล้องกับกฎหมาย ซึ่งกฎหมายคุ้มครองข้อมูลส่วนบุคคลนั้นจะมีลักษณะที่แตกต่างจากกฎหมายฉบับอื่น กล่าวคือ ไม่ได้มุ่งเน้นเพียงสภาพบังคับให้กระทำหรือไม่กระทำเท่านั้น แต่ยังเสริมสร้างความตระหนักรู้ และการทบทวนกระบวนการทำงานเพื่อให้การกระทำใดๆก็ตามที่เกี่ยวข้องกับข้อมูลส่วนบุคคลเป็นไปอย่างเหมาะสม โดยตระหนักถึงมาตรการด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ความเป็นธรรมในการใช้ข้อมูล และความโปร่งใสต่อเจ้าของข้อมูลส่วนบุคคล ให้สอดคล้องกับวัตถุประสงค์ของกฎหมายคุ้มครองสิทธิความเป็นอยู่ส่วนตัวภายใต้หลักการของรัฐธรรมนูญแห่งราชอาณาจักรไทย

ด้วยเหตุนี้การที่รัฐบาลได้ออกประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพื่อกำหนดหลักเกณฑ์ เงื่อนไข กลไก และมาตรการในการคุ้มครองข้อมูลส่วนบุคคลแก่ บริษัท หรือองค์กรโดยไม่จำกัดขนาดของธุรกิจ (Business Size) ที่มีหน้าที่ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลจะต้องปฏิบัติให้สอดคล้องกับหลักเกณฑ์ที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนดนั้น อาจนำมาซึ่งปัญหาต่อผู้ประกอบธุรกิจ SME ในการปฏิบัติตามหลักเกณฑ์ที่หน่วยงานรัฐกำหนดได้มากน้อยหรือไม่เพียงใด

จากการศึกษากฎหมายเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย ซึ่งตราขึ้นมาโดยอาศัยอำนาจตามมาตรา 26 ประกอบมาตรา 32 มาตรา 33 และมาตรา 37 ของรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 ว่าด้วยเรื่องการจำกัดสิทธิและเสรีภาพของบุคคลนั้น จะก่อให้เกิดปัญหาต่อผู้ประกอบธุรกิจ SME ได้ จึงสามารถวิเคราะห์ถึงปัญหาต่างๆ ดังกล่าวต่อไปนี้

ประเด็นประการแรกปัญหาเกี่ยวกับการจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา 41 (2) และ (3) ของผู้ประกอบธุรกิจ SME เนื่องจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดหน้าที่

---

[1] บทความนี้เรียบเรียงจากการค้นคว้าอิสระ เรื่อง ปัญหากฎหมายคุ้มครองข้อมูลส่วนบุคคลของผู้ประกอบธุรกิจ SMEโดยมีอาจารย์ที่ปรึกษา คือ รองศาสตราจารย์สุเมธ จานประดับ และคณะกรรมการสอบ คือ รองศาสตราจารย์จุฑามาศ นิศารัตน์ และรองศาสตราจารย์ ดร. ปภาศรี บัวสวรรค์

[2] นักศึกษาปริญญาโท หลักสูตรนิติศาสตรมหาบัณฑิต (ส่วนภูมิภาค) คณะนิติศาสตร์ มหาวิทยาลัยรามคำแหง

ให้ผู้ประกอบธุรกิจ SME ที่ได้ทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลจะต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา 41 (2) (3) นั้น ยังไม่มีความชัดเจนในการตีความหมายของคำว่า “ข้อมูลจำนวนมาก” และการขยายความคำว่า “กิจกรรมหลัก” จึงก่อให้เกิดปัญหาในการตีความ เนื่องจากปัจจุบันยังไม่มีการตราประกาศกระทรวงออกมารองรับ และทำให้ผู้ประกอบธุรกิจ SME เกิดความสับสนว่ากิจกรรมหลักและจำนวนข้อมูลที่ตนได้จัดเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้น จะต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือไม่อย่างไร

ปัญหาประการที่สองปัญหาเกี่ยวกับการปฏิบัติตามมาตรฐานการรักษาความมั่นคงปลอดภัยของการโจมตีทางไซเบอร์ ตามมาตรา 37 (1) เนื่องจากกำหนดให้ผู้ประกอบธุรกิจ SME ที่ได้เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล จะต้องจัดให้มีมาตรฐานการรักษาความมั่นคงปลอดภัยเกี่ยวกับข้อมูลส่วนบุคคล ตามมาตรา 37 (1) ประกอบประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่องมาตราการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. 2565 โดยยึดหลักการรักษาไว้ซึ่งความมั่นคงปลอดภัยเกี่ยวกับการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) รวมถึงการเข้าถึงควบคุมการใช้งานข้อมูลส่วนบุคคล โดยแบ่งออกเป็น 3 กลุ่ม คือ มาตรการป้องกันด้านการบริหารจัดการ (Administrative safeguard) มาตรการป้องกันด้านเทคนิค (Technical safeguard) และมาตรการป้องกันทางกายภาพ (Physical safeguard) เป็นการกำหนดหลักเกณฑ์และแนวทางในการจัดการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่ค่อนข้างสูง ซึ่งจะทำให้ผู้ประกอบธุรกิจ SME ที่ได้ดำเนินการจัดเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเกิดอุปสรรคในการปฏิบัติตามกฎหมายจะต้องมีมาตราการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลในระดับเดียวกันกับผู้ประกอบธุรกิจขนาดใหญ่ ซึ่งอาจก่อให้เกิดความไม่เท่าเทียมการแข่งขันทางการค้าหรือไม่อย่างไร

ปัญหาประการที่สามปัญหาเกี่ยวกับบทลงโทษทางปกครองของกฎหมายคุ้มครองข้อมูลส่วนบุคคล ตามมาตรา 82 ถึง 89 เนื่องจากบทลงโทษทางปกครองตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้นใช้วิธีการปรับตามจำนวนที่กฎหมายกำหนด (Ordinary Fine) โดยการกำหนดช่วงของค่าปรับไว้ ซึ่งมีอัตราโทษปรับสูงสุดถึง 5 ล้านบาท ดังนั้น รัฐบาลจะต้องเปลี่ยนแนวคิดบทลงโทษเป็นวิธีการอื่นได้หรือไม่ เพื่อเป็นการขับเคลื่อนในภาคธุรกิจ SME ด้วยได้

จากการศึกษาค้นคว้าเกี่ยวกับกฎหมายรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 ประมวลกฎหมายอาญา ประมวลกฎหมายแพ่งและพาณิชย์ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ประกาศกระทรวงดิจิทัลเพื่อเศรฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อบังคับการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (General Data Protection Regulation) แนวทาง

ปฏิบัติการจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Guidelines on Data Protection Officers) 16/EN WP243 ผู้ศึกษาพบว่ามีข้อเสนอแนะดังนี้ คือ

1. ปัญหาเกี่ยวกับการจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา 41 (2) และ (3) ผู้ศึกษาพบว่าข้อเสนอแนะ คือ ควรมีการแก้ไขพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยนำข้อบังคับการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (General Data Protection Regulation) ว่าด้วยเรื่อง แนวทางปฏิบัติการจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Guidelines on Data Protection Officers) 16/EN EP243 มาปรับใช้ เพิ่มเติมคำนิยามว่า “ข้อมูลจำนวนมาก” ไว้ใน มาตรา 6 ดังนี้

มาตรา 6 ในพระราชบัญญัตินี้

“ข้อมูลจำนวนมาก” หมายความว่า ข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลได้ดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเกินกว่าหกพันรายขึ้นไป

“กิจกรรมหลัก” หมายความว่า การดำเนินการเพื่อให้บรรลุวัตถุประสงค์ขององค์กรนั้น เช่น การประมวลผลข้อมูลด้านสุขภาพเป็นกิจกรรมหลักของโรงพยาบาลให้บรรลุวัตถุประสงค์ของโรงพยาบาล ไม่รวมถึงกิจกรรมที่เป็นการสนับสนุน เช่น การจ่ายเงินลูกจ้าง การรับสมัครงาน เป็นต้น แม้จะเป็นกิจกรรมที่จำเป็นแต่มิใช่กิจกรรมหลักขององค์กร

มาตรา 41 (3) กิจกรรมหลักของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26 เป็นข้อมูลจำนวนมาก

ทั้งนี้ ก็เพื่อเป็นการกำหนดขอบเขตความชัดเจนของจำนวนข้อมูลส่วนบุคคลจำนวนมาก และกิจกรรมหลัก ให้สะดวกต่อการพิจารณาและทำให้ผู้ประกอบธุรกิจ SME ที่ไม่ได้มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลซึ่งไม่เกินกว่าหกพันรายขึ้นไป และ/หรือไม่ได้มีกิจกรรมหลักในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลที่มีความอ่อนไหว ไม่ต้องรับภาระต้นทุนค่าใช้จ่ายในการว่าจ้างเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเพื่อดำเนินการให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล หรือเสี่ยงที่จะต้องระวางโทษทางปกครองตามมาตรา 82 ของกฎหมายคุ้มครองข้อมูลส่วนบุคคล อันเนื่องมาจากการไม่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

2.ปัญหาเกี่ยวกับการปฏิบัติตามมาตรฐานการรักษาความมั่นคงปลอดภัยของการโจมตีทางไซเบอร์ ตามมาตรา 37 (1) ผู้ศึกษาพบว่าข้อเสนอแนะ คือ ควรมีการแก้ไข ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. 2565 โดยนำแนวปฏิบัติการบริหารความเสี่ยงของผู้ประกอบธุรกิจขนาดกลางและขนาดย่อย (SMEs) ของสำนักงานสหภาพยุโรปเพื่อความมั่นคงทางไซเบอร์ (ENISA) ซึ่งกำหนดแนวทางปฏิบัติของผู้ประกอบธุรกิจ SME มาประยุกต์ใช้ในการประเมินความเสี่ยงความมั่นคงปลอดภัยของผู้ประกอบธุรกิจ SME ไว้เป็นการเฉพาะ 4 ระยะเท่านั้น โดยเพิ่มเติมเข้ามาในข้อ 9.

ของประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. 2565 ดังนี้

ข้อ 9. ผู้ประกอบธุรกิจ SME ที่ได้ดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในฐานะผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ซึ่งควรครอบคลุมถึงมาตรการป้องกันด้านการบริหารจัดการ (administrative safeguard) มาตราป้องกันด้านเทคนิค (Technical safeguard) และมาตรการป้องกันทางกายภาพ (Physical safeguard) ในเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล (access control) โดยอย่างน้อยต้องประกอบด้วยการดำเนินการ ดังนี้

(1) การประเมินความเสี่ยง (Risk Assessment) โดยคำนึงถึงสถานะความเสี่ยงที่สำคัญที่อาจจะก่อให้เกิดขึ้นกับทรัพย์สินสารสนเทศ และระวังภัยคุกคามและเหตุการณ์ที่จะละเมิดข้อมูลส่วนบุคคล ทั้งนี้ เท่าที่จำเป็นเหมาะสม และเป็นไปได้ตามระดับความเสี่ยง

(2) การจัดการความเสี่ยง (Risk Treatment) การฟื้นฟูความเสียหายที่อาจจะเกิดขึ้นจากภัยคุกคามและเหตุการละเมิดคุ้มครองข้อมูลส่วนบุคคล โดยคำนึงถึงการบรรเทาความเสี่ยง (Mitigation) การถ่ายโอนความเสี่ยง (Transfer) การหลีกเลี่ยงความเสี่ยง (Retention) ให้เป็นไปตามระดับความเสี่ยง

(3) การพิจารณายอมรับความเสี่ยง (Risk Acceptance) โดยการบริหารจัดหารการเข้าถึงของผู้ใช้งาน (User access management) เพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาตแล้ว ตลอดจนการกำหนดเกี่ยวกับการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคล

(4) การสื่อสารรายละเอียดเกี่ยวกับความเสี่ยง (Risk Communication) จะต้องมีการจัดวิธีการสื่อสารให้กับผู้ที่เกี่ยวข้องทราบเกี่ยวกับความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัย (Privacy and Security awareness) และการแจ้งนโยบาย แนวปฏิบัติ และมาตรการด้านการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคลอย่างเหมาะสม ให้บุคลากร พนักงาน ลูกจ้าง หรือบุคคลที่เป็นผู้ใช้งาน (User) หรือเกี่ยวข้องกับการเข้าถึง เก็บรวบรวม ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคล ทราบและปฏิบัติ

ประกอบกับให้หน่วยงานภาครัฐที่เชี่ยวชาญทางด้านไซเบอร์ อาทิเช่น สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เป็นผู้ดำเนินการตรวจสอบมาตราฐานการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และออกเอกสารรับรองถึงมาตราฐานความปลอดภัยทางด้านไซเบอร์ (Certificate Framework) ให้ เพื่อเป็นหลักฐานว่าได้ปฏิบัติตามมาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลสอดคล้องกับกฎหมายแล้ว

ทั้งนี้ ก็เพื่อเป็นการลดภาระต้นทุนค่าใช้จ่ายแก่ผู้ประกอบธุรกิจ SME ในการปฏิบัติตามมาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลในระดับที่ไม่ต้องเทียบเท่ากับผู้ประกอบธุรกิจขนาดใหญ่ และ

สร้างความเท่าเทียมต่อการแข่งขันทางการค้า เนื่องจากการปฏิบัติตามประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. 2565 โดยไม่จำกัดขนาดประเภทของธุรกิจนั้น ผู้ประกอบธุรกิจ SME จะต้องจัดให้มีมาตรการในการคุ้มครองความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่เข้มงวดและมีค่าใช้จ่ายที่ค่อนข้างสูง

3. ปัญหาเกี่ยวกับบทลงโทษทางปกครองของกฎหมายคุ้มครองข้อมูลส่วนบุคคล ตามมาตรา 82 ถึง 89 ผู้ศึกษาพบว่าข้อเสนอแนะ คือ ควรมีการแก้ไข มาตรา 82 ถึง 89 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล โดยวิธีการกำหนดโทษปรับทางปกครองจากจำนวนร้อยละของรายได้ทั่วโลกในปีงบประมาณที่ผ่านมา ตามข้อบังคับการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (General Data Protection Regulation) มาประยุกต์ใช้โดยปรับตามรายได้ให้มีความสัมพันธ์กับสัดส่วนของภาวะทางเศรษฐกิจและการเงิน (Proportionment according to Economy or Financial Circumstances) เช่น

มาตรา 82 ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดไม่ปฏิบัติตามมาตรา 23 มาตรา 30 วรรคสี่ มาตรา 39 วรรคหนึ่ง มาตรา 41 วรรคหนึ่ง หรือมาตรา 42 วรรคสองหรือวรรคสาม หรือไม่ขอความยินยอมตามแบบหรือข้อความที่คณะกรรมการประกาศกำหนดตามมาตรา 19 วรรคสาม หรือ ไม่แจ้งผลกระทบจากการถอนความยินยอมตามมาตรา 19 วรรคหก หรือไม่ปฏิบัติตามมาตรา 23 ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา 25 วรรคสอง ต้องระวางโทษปรับทางปกครองร้อยละ 2 ของรายได้ทั่วโลกในปีงบประมาณที่ผ่านมา

มาตรา 83 ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามมาตรา 21 มาตรา 22 มาตรา 24 มาตรา 25 วรรคหนึ่ง มาตรา 27 วรรคหนึ่งหรือวรรคสอง มาตรา 28 มาตรา 32 วรรคสอง หรือมาตรา 37 หรือขอความยินยอมโดยการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคล เข้าใจผิดในวัตถุประสงค์ หรือไม่ปฏิบัติตามมาตรา 21 ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา 25 วรรคสอง หรือส่งหรือโอนข้อมูลส่วนบุคคลโดยไม่เป็นไปตามมาตรา 29 วรรคหนึ่งหรือวรรคสาม ต้องระวางโทษปรับทางปกครองร้อยละ 4 ของรายได้ทั่วโลกในปีงบประมาณที่ผ่านมา

มาตรา 84 ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา 26 วรรคหนึ่งหรือวรรคสาม หรือฝ่าฝืนมาตรา 27 วรรคหนึ่งหรือวรรคสอง หรือมาตรา 28 อันเกี่ยวกับข้อมูลส่วนบุคคล ตามมาตรา 26 หรือส่งหรือโอนข้อมูลส่วนบุคคลตามมาตรา 26 โดยไม่เป็นไปตามมาตรา 29 วรรคหนึ่งหรือวรรคสาม ต้องระวางโทษปรับทางปกครองร้อยละ 4 ของรายได้ทั่วโลกในปีงบประมาณที่ผ่านมา

ทั้งนี้ ก็เพื่อทำให้เกิดความเท่าเทียมในการแข่งขันทางการค้า และลดภาระของผู้ประกอบธุรกิจ SME ซึ่งถือว่าเป็นธุรกิจที่สำคัญในการสร้างความหลากหลายให้กับระบบเศรษฐกิจประเทศไทย ไม่ว่าจะเป็นการทำให้เกิดธุรกิจประเภทต่างๆที่หลากหลาย การจ้างงาน หรือการกระจายความเจริญทางเศรษฐกิจในประเทศ และสร้าง

ความเข้มแข็งให้กับบทลงโทษทางปกครองเนื่องจากจะทำให้ทั้งผู้ประกอบธุรกิจขนาดใหญ่และผู้ประกอบธุรกิจ SME เกรงกลัวต่อการฝ่าฝืนโทษทางปกครองตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

เอกสารอ้างอิง

ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย. **Thailand Data Protection Guideline 3.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล.**, มหาวิทยาลัยจุฬาลงกรณ์, 2564.

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล. **คู่มือ PDPA สำหรับผู้ประกอบการ SMEs**., สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล, 2565.