ธรรมนิติ
DHARMNITI

PDPA Insight
and Solutions for Business
การปรับตัวครั้งใหญ่ของผู้ประกอบการ

ดร.ปริญญา หอมเอนก

ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศและระบบเทคโนโลยีสารสนเทศ

- TAX IN FOCUS -

เอกสารภาษีอากร

- TAX IN FOCUS -

PDPA Insight

and Solutions for Business

การปรับตัวครั้งใหญ่ของผู้ประกอบการ

ดร.ปริญญา หอมเอนก

ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศและระบบเทคโนโลยีสารสนเทศ

- TAX IN FOCUS -

PDPA Insight and Solutions for Business
การปรับตัวครั้งใหญ่ของผู้ประกอบการ

ผู้เขียน	:	สำนักพิมพ์ ธรรมนิติ
พิมพ์ครั้งแรก	:	กันยายน 2565
ISBN (e-Book)	:	978-616-302-250-9
เจ้าของ	:	บริษัท ธรรมนิติ เพรส จำกัด
ที่ปรึกษา	:	ดารารัตน์ พืชมงคล
กองบรรณาธิการ	:	ศศิพินทุ์ อุษณีย์มาศ
ออกแบบ-จัดรูปเล่ม	:	คชาภา พูลสวัสดิ์

ข้อมูลทางบรรณานุกรมของหอสมุดแห่งชาติ

PDPA Insight and Solutions for Business การปรับตัวครั้งใหญ่ของผู้ประกอบการ.--
กรุงเทพฯ : ธรรมนิติ เพรส, 2565.
22 หน้า.
1. การป้องกันข้อมูล. 2. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562.
I. ชื่อเรื่อง.

342.0858
ISBN (e-Book) : 978-616-302-250-9

จัดจำหน่ายโดย

บริษัท ธรรมนิติ เพรส จำกัด เลขที่ 178 อาคารธรรมนิติ ชั้น 4
ซอยเพิ่มทรัพย์ (ประชาชื่น 20) ถนนประชาชื่น แขวงบางซื่อ เขตบางซื่อ กรุงเทพฯ 10800
โทรศัพท์ (02) 555-0713 โทรสาร (02) 555-0728

- คำนำ -

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act : PDPA) หรือชื่อที่เรียกกันคุ้นหูว่า PDPA เป็นกฎหมายที่ออกมาเพื่อป้องกันการละเมิดข้อมูลส่วนบุคคล (ซึ่งเป็นข้อมูลที่สามารถระบุถึงตัวเจ้าของข้อมูลนั้นได้ เช่น ชื่อ ที่อยู่ เบอร์โทรศัพท์ รูปถ่าย ลายนิ้วมือ ประวัติสุขภาพ ฯลฯ) รวมถึงการจัดเก็บข้อมูลและนำไปใช้โดยไม่ได้แจ้งให้ทราบ และไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล โดยกฎหมายนี้ได้เริ่มบังคับใช้อย่างเต็มรูปแบบแล้วเมื่อวันที่ 1 มิถุนายน 2565 ที่ผ่านมา

แน่นอนว่า PDPA คุ้มครองและให้สิทธิกับเจ้าของข้อมูลในการรับทราบ ยินยอม เข้าถึง เพิกถอนการเก็บและนำข้อมูลส่วนบุคคลไปใช้ รวมถึงลบทำลายข้อมูลส่วนตัวนั้นได้ ส่งผลให้ผู้บริหาร ผู้ประกอบการของบริษัทและองค์กรต่าง ๆ ต้องมีการปรับตัวครั้งใหญ่ ในการเก็บข้อมูลส่วนบุคคล ทั้งกับลูกค้าภายนอกและพนักงานภายในองค์กร เพื่อปฏิบัติให้ถูกต้องตาม พ.ร.บ. ฉบับนี้

TAX in Focus จึงนำสัมภาษณ์พิเศษ ดร.ปริญญา หอมเอนก ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์และระบบเทคโนโลยีสารสนเทศ มือวางอันดับต้น ๆ ของเมืองไทย ซึ่งมาร่วมพูดคุยกับวารสารเอกสารภาษีอากร ในประเด็นของ PDPA แบบเจาะลึก พร้อมคำแนะนำในการปรับตัว มานำเสนอในรูปแบบ Mini Guide Book เพื่อให้ผู้เกี่ยวข้องที่ได้อ่านปฏิบัติได้ถูกต้องตามกฎหมายด้วยความเข้าใจเพิ่มที่มากขึ้น

PDPA Insight
and Solutions for Business
การปรับตัวครั้งใหญ่ของผู้ประกอบการ

ในแวดวงไอทีโดยเฉพาะเรื่องของ Cybersecurity หากเอ่ยชื่อ ดร.ปริญญา หอมเอนก คงเป็นที่คุ้นเคยและรู้จักกันเป็นอย่างดี ด้วยความคร่ำหวอดอยู่ในวงการไอทีมากกว่า 20 ปี มีบทบาทที่หลากหลายทั้งเป็นอาจารย์พิเศษสอนนิสิตปริญญาตรี โท เอก ให้กับมหาวิทยาลัยชั้นนำ เป็นคอลัมนิสต์และนักเขียน เป็นวิทยากรและที่ปรึกษาด้านความมั่งคงปลอดภัยทางไซเบอร์ให้กับองค์กรของรัฐและเอกชน ปัจจุบันดำรงตำแหน่งกรรมการผู้ทรงคุณวุฒิในคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล กรรมการผู้ทรงคุณวุฒิด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ประธานกรรมการบริหาร บริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด และประธานเจ้าหน้าที่บริหาร บริษัท ไซเบอร์ตรอน จำกัด

ด้วยความรู้และประสบการณ์ด้านสารสนเทศทั้งในและต่างประเทศ จึงได้รับความไว้วางใจให้เป็นกรรมาธิการในคณะกรรมาธิการวิสามัญพิจารณาร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือ PDPA (Personal Data Protection Act)

กฎหมายพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีผลใช้บังคับทั้งฉบับแล้ว เมื่อวันที่ 1 มิถุนายน 2565 ที่ผ่านมา ซึ่งในระหว่างการขยายเวลาการใช้บังคับนั้น ผู้ควบคุมข้อมูลส่วนบุคคลยังคงต้องปฏิบัติตามมาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล โดยต้องจัดให้มีมาตรการเรื่องการเข้าถึงและการควบคุมการใช้งานข้อมูลส่วนบุคคล และแจ้งมาตรการดังกล่าวพร้อมสร้างความตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล นอกจากนี้ กระทรวงดิจิทัลฯ ก็ได้มีแผนงานเตรียมความพร้อมและสร้างความเข้าใจเรื่องการคุ้มครองข้อมูลส่วนบุคคลให้ผู้ประกอบการทุกประเภทกิจการและทุกขนาด โดยเฉพาะกลุ่ม SMEs

ถือเป็นโอกาสพิเศษที่วารสารเอกสารภาษีอากร ได้รับเกียรติจาก **ดร.ปริญญา หอมเอนก** ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์และระบบเทคโนโลยีสารสนเทศ มือวางอันดับต้น ๆ ของเมืองไทย มาร่วมพูดคุยถึง PDPA กันแบบเจาะลึก พร้อมคำแนะนำสำหรับผู้ประกอบการถึงการเตรียมพร้อมปรับตัวกับ พ.ร.บ. ฉบับนี้ รวมถึงปฏิบัติได้ถูกต้องตามกฎหมาย ไม่ต้องเสี่ยงกับโทษปรับที่สูงสุดถึง 5 ล้านบาท !

เรื่องที่ผู้บริหารหรือผู้ที่เกี่ยวข้องยังเข้าใจผิด เกี่ยวกับ PDPA อยู่คือเรื่องใด

จากการที่ได้ไปบรรยายเรื่องการเตรียมความพร้อมกับ PDPA สิ่งที่หน่วยงานต่าง ๆ ยังเข้าใจผิดกันอยู่คือ

เรื่องเข้าใจผิดแรก : PDPA ทำเฉพาะเรื่อง Privacy เพียงอย่างเดียวเท่านั้น

หลายองค์กรเมื่อดำเนินการในเรื่องความเป็นส่วนตัวไปแล้ว ก็เข้าใจว่าได้ปฏิบัติตามข้อกำหนดในเรื่องของความเป็นส่วนตัว หรือ Privacy Compliance ครบถ้วนเรียบร้อย จึงอาจจะละเลยการทำให้ข้อมูลมีความมั่นคงปลอดภัยจากภัยคุกคามทางไซเบอร์ (Cybersecurity) เช่น ถูกแฮ็กหรือข้อมูลรั่วไหล ซึ่งเป็นเรื่องพื้นฐานสำคัญมากที่ควรจะดำเนินการก่อน ดังเช่นคำกล่าวที่ว่า “You can get security without privacy but you can’t get privacy without security” อยากให้ทุกคนเข้าใจหลักคิดเบื้องต้นตรงนี้ก่อน ก็คือ ต้องทำ Data Privacy กับ Data Security ควบคู่ไปด้วยกัน ถ้าเข้าใจแล้วการปฏิบัติตาม PDPA ก็จะสำเร็จได้

ดังนั้นองค์กรต้องดูแลความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลซึ่งเป็นเรื่องพื้นฐานเสียก่อน จึงจะสร้างความเป็นส่วนตัวของเจ้าของข้อมูลได้สำเร็จ

ประเด็นนี้ถือเป็นเรื่องที่คนส่วนใหญ่เข้าใจผิดกัน บริษัท/ผู้ประกอบการต่าง ๆ มุ่งแต่จะไปทำเรื่องของการเตรียมเอกสารนโยบายความเป็นส่วนตัว การขอความยินยอมหรือ Consent จากเจ้าของข้อมูลส่วนบุคคล ปรับปรุงเว็บไซต์เรื่องนโยบายคุกกี้ เมื่อทำเสร็จเรียบร้อยก็เข้าใจว่าปฏิบัติตามกฎหมายแล้ว แต่จริง ๆ แล้วเป็นแค่เพียงขั้นตอนของการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล (Data Subject) เนื่องจากกฎหมายกำหนดให้เจ้าของข้อมูลส่วนบุคคลต้องยินยอมเสียก่อน องค์กรต้องมีฐานในการประมวลผลข้อมูลส่วนบุคคล ซึ่งหนึ่งในฐานการประมวลผลคือฐานความยินยอม (ในการพิจารณาฐานความยินยอม องค์กรต้องศึกษารายละเอียดเพิ่มเติม เนื่องจากมักมีความเข้าใจผิดว่า PDPA กำหนดให้องค์กรต้องขอความยินยอมในการประมวลผลข้อมูลส่วนบุคคลเท่านั้น) แต่ขั้นตอนต่อมาคือเมื่อบริษัท/ผู้ประกอบการได้ข้อมูลมาเก็บรวบรวมแล้ว หากดูแลรักษาไม่ดี ข้อมูลเกิดรั่วไหลก็มีโทษทางกฎหมายเช่นเดียวกัน ซึ่งจะกระทบกับมาตรฐานการรักษาข้อมูลให้มั่นคง

ปลอดภัยตามหลัก CIA คือ Confidentiality, Integrity และ Availability ซึ่ง CIA นั้นหมายถึง

- การรักษาความลับ (Confidentiality) สิทธิในการเข้าถึงข้อมูลเฉพาะผู้ได้รับอนุญาต
- ความถูกต้องครบถ้วน (Integrity) ข้อมูลที่จัดเก็บ ส่งต่อ และนำไปใช้ ต้องเป็นข้อมูลที่ถูกต้อง และไม่ถูกแก้ไขโดยผู้ไม่มีสิทธิ
- ความพร้อมใช้งาน (Availability) ผู้มีสิทธิต้องเข้าถึงข้อมูลเพื่อใช้งานได้เมื่อจำเป็น

เรื่องเข้าใจผิดที่ 2 : PDPA เป็นภาระ

หลายคนคิดว่าการดำเนินการตาม พ.ร.บ. PDPA ฉบับนี้ทำให้มีค่าใช้จ่ายที่ไม่เกิดประโยชน์กับองค์กร จริง ๆ แล้วสิ่งที่ทำนั้นเมื่อเป็นประโยชน์กับลูกค้าก็จะกลับมาเป็นประโยชน์กับองค์กรด้วยเช่นกัน PDPA ถือเป็นการลงทุน เพราะข้อมูลลูกค้าเป็นทรัพย์สิน จึงต้องมีการป้องกัน

ฉะนั้น การที่เราป้องกันไม่ให้ข้อมูลรั่วไหลหลังจากมีการจัดเก็บข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคล ไม่ว่าจะเป็นข้อมูลลูกค้าและข้อมูลพนักงานจึงเป็นเรื่องสำคัญ ข้อมูลส่วนบุคคลต้องมีการดูแลและถือเป็นทรัพย์สินของบริษัท/ผู้ประกอบการ หากข้อมูลส่วนบุคคลรั่วไหลออกไปไม่ว่าทางตรงหรือทางอ้อมก็ถือว่ามีความผิดตามกฎหมาย แล้วหากไม่มีฐานในการประมวลผลให้ทำได้ตามกฎหมาย (Lawful Basis) ความผิดก็ยิ่งรุนแรงขึ้น ฉะนั้น ผู้บริหารจึงต้องมองภาพใหญ่ว่า PDPA เป็นการลงทุนเพื่อความเติบโตอย่างยั่งยืน ไม่ใช่เป็นการใช้จ่ายเพื่อทำให้จบ ๆ ไป จะได้ไม่โดนปรับหรือมีความผิดเมื่อเจ้าหน้าที่ตามกฎหมายมาตรวจ

*ดังนั้น ให้ถือหลัก **"ใจเขาใจเรา"** เราอยากให้คนอื่นทำอย่างไรกับเรา ก็ควรทำแบบนั้นกับลูกค้าหรือพนักงานด้วยเช่นกัน การทำ PDPA ถือเป็นเสน่ห์ของบริษัท/ผู้ประกอบการ และแสดงถึงความมีธรรมาภิบาล ใส่ใจเรื่อง Corporate Governance (CG) และธรรมาภิบาลข้อมูล (Data Governance) แสดงให้เห็นว่าการบริหารจัดการของบริษัท/ผู้ประกอบการ มีประสิทธิภาพ โปร่งใส ตรวจสอบได้ และคำนึงถึงผู้มีส่วนได้เสียทุกฝ่าย ไม่ว่าบริษัท/ผู้ประกอบการนั้นจะจดทะเบียนหรือไม่ หากดูแลเรื่องนี้อย่างดี มีการสื่อสารให้ลูกค้าทราบถึงวัตถุประสงค์ของการนำข้อมูลไปใช้อย่างชัดเจน มีการประมวลผลข้อมูลส่วนบุคคลในแต่ละวัตถุประสงค์ที่สัมพันธ์กับกฎหมาย ไม่มีการใช้ข้อมูลส่วนบุคคลเกินกว่าวัตถุประสงค์ หากมีข้อมูลรั่วไหลก็แจ้งให้ทราบภายใน 72 ชั่วโมง จะเป็นการแสดงความบริสุทธิ์ใจกับลูกค้า และกลายเป็นประโยชน์ของบริษัทเมื่อลูกค้าเกิดความประทับใจ*