PDPA คืออะไร ? – สรุป พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ที่ต้องรู้

PDPA คืออะไร ?

PDPA คือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ย่อมาจาก **Personal Data Protection Act B.E. 2562 (2019)** เป็นกฎหมายว่าด้วยการให้สิทธิ์กับเจ้าของข้อมูลส่วนบุคคล สร้างมาตรฐานการรักษาข้อมูลส่วนบุคคลให้ปลอดภัย และนำไปใช้ให้ถูกวัตถุประสงค์ตามคำยินยอมที่เจ้าของข้อมูลส่วนบุคคลอนุญาต โดยกฎหมาย PDPA Thailand ได้ประกาศไว้ในราชกิจจานุเบกษา เมื่อวันที่ 27 พฤษภาคม 2562 และปัจจุบันได้ถูกเลื่อนให้มีผลบังคับใช้ในวันที่ 1 มิถุนายน 2565

ทุกวันนี้ระบบดิจิทัลหรือระบบเครือข่ายออนไลน์กลายเป็นส่วนหนึ่งของชีวิตประจำวันของเราไปแล้ว มีแพลตฟอร์มมากมายให้เลือกใช้ และหลากหลายช่องทางในการติดต่อสื่อสารเพื่อวัตถุประสงค์ต่าง ๆ โดยแต่ละช่องทางที่เราใช้งานก็จะมีการเก็บข้อมูลส่วนบุคคลของเราก่อนเข้าใช้งานด้วย เช่น ชื่อ นามสกุล , Email , เบอร์โทรศัพท์, ที่อยู่ หรือข้อมูลส่วนตัวอื่น ๆ ตามแต่ที่เจ้าของช่องทางเรียกขอข้อมูล

ทั้งนี้ทั้งนั้น การที่เราจะให้ข้อมูลส่วนบุคคลใครไป ต้องมีการพิจารณาว่าให้ **ใคร** และให้ **เพราะอะไร?** อาทิเช่น หากเราจะสั่งซื้อของออนไลน์ เราก็ยินยอมที่จะให้ข้อมูลส่วนตัว ชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์ในการติดต่อ เพื่อใช้ข้อมูลเหล่านี้ในการส่งสินค้ามาให้เรา ซึ่งเป็นข้อมูลส่วนบุคคลที่สามารถเข้าใจได้และยินยอมที่จะให้ไปเพื่อส่งสินค้ามายังเรา หรือว่า ข้อมูลส่วนบุคคลที่ให้ต่อบริษัทเพื่อสมัครเข้าทำงาน

แต่เราจะรู้ได้อย่างไร? ว่าข้อมูลที่ให้ไปนั้นจะถูกใช้เพื่อวัตถุประสงค์นั้นจริง ๆ และไม่นำข้อมูลส่วนตัวของเราไปใช้เพื่อผลประโยชน์อื่นใด ที่นอกเหนือความยินยอมของเรา

กฎหมาย PDPA ที่บังคับใช้ในประเทศไทยนี้ จะมีบทบาทในการคุ้มครองและให้สิทธิที่เราควรมีต่อข้อมูลส่วนบุคคลของเราเองได้ รวมไปถึงการสร้างมาตรฐานของบุคคลหรือนิติบุคคลในการเก็บ รวบรวม หรือเพื่อการเปิดเผยข้อมูลส่วนบุคคลก็ตาม ซึ่งล้วนแล้วเกี่ยวข้องกับ พ.ร.บ. ฉบับนี้ที่จะต้องปฏิบัติตาม หากผู้ใดหรือองค์กรใดไม่ปฏิบัติตามย่อมมีบทลงโทษตามกฎหมายตามมา ซึ่งบทลงโทษนั้น มีทั้งโทษทางแพ่ง อาญา และทางปกครองด้วย

ดังนั้น PDPA ที่จะมีผลบังคับใช้ในวันที่ 1 มิถุนายน 2565 นี้ ก็นับว่าเป็นกฎหมายที่เราทุกคนควรทราบและตระหนักรู้ถึงสิทธิในข้อมูลส่วนบุคคลของเรา โดยเฉพาะอย่างยิ่งองค์กร บริษัท ห้างร้าน หรือแพลตฟอร์มต่าง ๆ ที่มีการเก็บข้อมูลส่วนบุคคล ไม่ว่าจะเป็นลูกค้า ผู้ใช้งาน หรือจะเป็นพนักงานที่ทำงานภายในองค์กรเองก็ตาม

องค์กรต่าง ๆ จึงได้รับผลกระทบพอสมควรกับการประกาศใช้ PDPA เพื่อเพิ่มมาตรฐานนโยบายการรักษาข้อมูลส่วนบุคคลให้ปลอดภัยและนำไปใช้ให้ถูกวัตถุประสงค์ตามคำยินยอนที่เจ้าของข้อมูลส่วนบุคคลได้ให้ไว้ และที่สำคัญต้องสอดคล้องต่อ PDPA ด้วย ทำให้กระบวนการทำ PDPA ไม่ใช่เรื่องที่ง่ายสักทีเดียว ที่เราจะทำได้ภายในระยะเวลาอันสั้น โดยเฉพาะองค์กรขนาดใหญ่ที่มีการเก็บรวบรวมข้อมูลส่วนบุคคลและมีการนำข้อมูลส่วนบุคคลไปใช้เป็นจำนวนมาก

อย่างไรก็ตาม บุคคลหรือองค์กรต่าง ๆ ก็ต้องดำเนินการกับข้อมูลส่วนบุคคลเพื่อให้สอดคล้องกับ PDPA ให้เรียบร้อย เพราะกฎหมายฉบับนี้ไม่ว่าอย่างไรอย่างไรก็จะมีผลกระทบต่อผู้ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลอย่างแน่นอน จึงควรเริ่มทำตั้งแต่เนิ่น ๆ ไว้ เพื่อป้องกันปัญหาที่จะอาจตามมาทางด้านกฎหมาย ซึ่งจะมีผลเสียหายต่อองค์กร หากวันใดวันหนึ่งเกิดมีข้อมูลรั่วไหล หรือเผลอนำข้อมูลส่วนบุคคลไปใช้อย่างไม่ถูกต้องแล้ว บุคคลหรือองค์กรที่ไม่ได้ดำเนินการตาม

PDPA ไว้ ย่อมเสียหายร้ายแรงกว่าผู้ที่ดำเนินการไว้แล้ว และผู้รับโทษตามกฎหมายก็อาจเป็นเจ้าของกิจการที่ต้องรับโทษแทนพนักงานเองก็เป็นได้ จึงนับว่าผู้นำองค์กรก็ควรตระหนักและให้ความใส่ใจต่อการทำ PDPA เป็นอย่างยิ่ง

PDPA กับ GDPR

PDPA (Personal Data Protection Act) ของประเทศไทย และ **GDPR (General Data Protection Regulation)** ซึ่งเป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป เป็นกฎหมายที่มีวัตถุประสงค์ในการคุ้มครองข้อมูลส่วนบุคคล ถึงแม้ว่า PDPA และ GDPR จะมีวัตถุประสงค์ที่คล้ายคลึงกันในการคุ้มครองข้อมูลส่วนบุคคล แต่ก็มีความแตกต่างในรายละเอียดและขอบเขตการบังคับใช้ที่สำคัญ องค์กรที่ดำเนินธุรกิจในประเทศไทยและมีการประมวลผลข้อมูลส่วนบุคคลของบุคคลในสหภาพยุโรปจำเป็นต้องปฏิบัติตามทั้งสองกฎหมายเพื่อให้สอดคล้องกับข้อกำหนดที่เกี่ยวข้อง

ข้อมูลส่วนบุคคล คืออะไร ?

ข้อมูลส่วนบุคคล (Personal Data) คือ ข้อมูลเกี่ยวกับบุคคลที่สามารถระบุตัวบุคคลนั้นได้ ทั้งทางตรงหรือทางอ้อม แต่จะไม่นับรวมข้อมูลของผู้ที่เสียชีวิตไปแล้ว

ซึ่งได้แก่ ชื่อ-นามสกุล หรือชื่อเล่น, รูปถ่าย, เลขประจำตัวประชาชน, เลขหนังสือเดินทาง, เลขบัตรประกันสังคม, เลขใบอนุญาตขับขี่, เลขประจำตัวผู้เสียภาษี, เลขบัญชีธนาคาร, เลขบัตรเครดิต (การเก็บเป็นภาพสำเนาบัตรประชาชนหรือสำเนาบัตรอื่นๆที่มีข้อมูลส่วนบุคคลที่กล่าวมาย่อมสามารถใช้ระบุตัวบุคคลได้โดยตัวมันเอง จึงถือเป็นข้อมูลส่วนบุคคล)
รวมถึง ที่อยู่, อีเมล์, เลขโทรศัพท์ / ข้อมูลอุปกรณ์หรือเครื่องมือ เช่น IP address, MAC address, Cookie ID / ข้อมูลระบุทรัพย์สินของบุคคล เช่น ทะเบียนรถยนต์, โฉนดที่ดิน / ข้อมูลที่สามารถเชื่อมโยงไปยังข้อมูลข้างต้นได้ เช่น วันเกิดและสถานที่เกิด, เชื้อชาติ,สัญชาติ, น้ำหนัก, ส่วนสูง, ข้อมูลตำแหน่งที่อยู่ (location), ข้อมูลการแพทย์, ข้อมูลการศึกษา, ข้อมูลทางการเงิน, ข้อมูลการจ้างงาน / ข้อมูลหมายเลขอ้างอิงที่เก็บไว้ในไมโครฟิล์ม แม้ไม่สามารถระบุไปถึงตัวบุคคลได้ แต่หากใช้ร่วมกับระบบดัชนีข้อมูลอีกระบบหนึ่งก็จะสามารถระบุไปถึงตัวบุคคลได้ / ข้อมูลการประเมินผลการทำงานหรือความเห็นของนายจ้างต่อการทำงานของลูกจ้าง / ข้อมูลบันทึกต่าง ๆ ที่ใช้ติดตามตรวจสอบกิจกรรมต่าง ๆ ของบุคคล เช่น log file / ข้อมูลที่สามารถใช้ในการค้นหาข้อมูลส่วนบุคคลอื่นในอินเทอร์เน็ต

นอกจากนี้ ยังมีข้อมูลส่วนบุคคลอีกประเภท ที่ PDPA หรือ พ.ร.บ. ฉบับนี้ให้ความสำคัญและมีบทลงโทษที่รุนแรงด้วย กรณีเกิดการรั่วไหลสู่สาธารณะ คือ **ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Personal Data)** เช่น ข้อมูล เชื้อชาติ, เผ่าพันธุ์, ความคิดเห็นทางการเมือง, ความเชื่อในลัทธิ ศาสนาหรือปรัชญา, พฤติกรรมทางเพศ, ประวัติอาชญากรรม, ข้อมูลสุขภาพ ความพิการ หรือข้อมูลสุขภาพจิต, ข้อมูลสหภาพแรงงาน, ข้อมูลพันธุกรรม, ข้อมูลชีวภาพ, ข้อมูลทางชีวมิติ (Biometric) เช่น รูปภาพใบหน้า, ลายนิ้วมือ, ฟิล์มเอกซเรย์, ข้อมูลสแกนม่านตา, ข้อมูลอัตลักษณ์เสียง, ข้อมูลพันธุกรรม เป็นต้น และข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด

เหตุที่ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Personal Data) เป็นข้อมูลที่มีบทลงโทษที่รุนแรงกว่าข้อมูลส่วนบุคคลทั่วไป (Personal Data) นั่นเป็นเพราะ หากข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนมีการรั่วไหลไปสู่สาธารณะแล้ว จะเกิดผลเสียที่ร้ายแรงกับผู้เป็นเจ้าของข้อมูลส่วนบุคคล (Data Subject) ได้มากกว่าข้อมูลส่วนบุคคลอื่นๆ มีผลต่อสิทธิเสรีภาพของบุคคล เช่น สิทธิเสรีภาพในความคิด ความเชื่อทางศาสนา การแสดงออก การชุมนุม สิทธิในชีวิตร่างกาย การอยู่อาศัย การไม่ถูกเลือกปฏิบัติ ซึ่งอาจจะก่อให้เกิดการแทรกแซงซึ่งสิทธิเสรีภาพและการเลือกปฏิบัติต่อการใช้สิทธิเสรีภาพของบุคคลได้มากกว่าข้อมูลส่วนบุคคลทั่วไป ยกตัวอย่างเช่น ข้อมูลพฤติกรรมทางเพศ เชื่อชาติ ศาสนา ประวัติอาชญากรรม ถ้ารั่วไหลไปแล้ว ข้อมูลเหล่านี้จะนำมาสู่ความเป็นอคติและจะมีผลกระทบต่อชีวิตส่วนบุคคลได้มากกว่าข้อมูลทั่วไปเป็นอย่างมาก

ใครบ้างที่มีส่วนเกี่ยวข้องกับข้อมูลส่วนบุคคล ?

เราสามารถแบ่งผู้ที่มีส่วนเกี่ยวข้องกับข้อมูลส่วนบุคคล ในกฎหมาย PDPA ได้ 3 ประเภท ประกอบด้วย

1. เจ้าของข้อมูลส่วนบุคคล หรือ Data Subject คือ บุคคลที่ข้อมูลสามารถระบุไปถึงได้

2. ผู้ควบคุมข้อมูลส่วนบุคคล หรือ Data Controller คือ บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

3. ผู้ประมวลผลข้อมูลส่วนบุคคล หรือ Data Processor คือ บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

แล้ว PDPA ให้เจ้าของข้อมูลส่วนบุคคล (Data Subject) ได้รับสิทธิอะไรบ้าง ?

เพื่อให้ง่ายต่อความเข้าใจในสิทธิของเจ้าของข้อมูล (Data Subject) เรามาทำความรู้จักกับคำว่า **ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)** เพิ่มเติมอีกสักหน่อย

ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) คืออะไร ? ผู้ควบคุมข้อมูลส่วนบุคคล หรือ Data Controller หมายถึงบุคคลหรือนิติบุคคล ที่มีส่วนในการเก็บ รวบรวมใช้ หรือเปิดเผยข้อมูลส่วนบุคคล และหากดูที่ความหมายอย่างละเอียดแล้ว นั่นหมายความว่าเพียงแค่เรามีการเก็บข้อมูลส่วนบุคคลของผู้อื่นไว้ ก็ถือว่าเราเป็นผู้ควบคุมข้อมูลส่วนบุคคล ที่จะต้องปฏิบัติตามกฎหมาย PDPA ไปด้วยเหมือนกัน

ใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 จะให้ **สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Right)** สรุปได้ดังต่อไปนี้

- สิทธิได้รับการแจ้งให้ทราบ

เจ้าของข้อมูลมีสิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคล หรือขอให้เปิดเผยถึงการได้มาของข้อมูลส่วนบุคคลดังกล่าวที่ตนไม่ได้ให้ความยินยอมได้ โดยสิทธินี้จะต้องไม่ขัดต่อกฎหมายหรือคำสั่งศาล หรือส่งผลกระทบที่อาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น ถ้าไม่ขัดหรือส่งผลกระทบดังกล่าว เจ้าของข้อมูลส่วนบุคคลจะได้รับสิทธิภายใน 30 วันนับจากวันที่ ผู้ควบคุมข้อมูลส่วนบุคคล ได้รับคำขอ การเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ ก่อนหรือในขณะที่เก็บรวบรวมข้อมูล (ยกเว้นเจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดนั้นอยู่แล้ว เช่น ไปธนาคารเพื่อจะไปเปิดบัญชี หรือว่าการสมัครใช้ผลิตภัณฑ์หรือบริการต่าง ๆ) โดยมีรายละเอียดการแจ้งให้ทราบ เช่น เก็บข้อมูลส่วนบุคคลอะไรบ้าง, วัตถุประสงค์การเก็บข้อมูล, การนำไปใช้หรือส่งต่อไปมีให้ใครบ้าง, วิธีเก็บข้อมูลอย่างไร, เก็บข้อมูลนานแค่ไหน, วิธีขอการเปลี่ยนแปลง แก้ไข เพิกถอนข้อมูลส่วนบุคคลที่ให้ไปสามารถทำได้อย่างไรบ้าง

- สิทธิขอเข้าถึงข้อมูลส่วนบุคคล

เจ้าของข้อมูลมีสิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคล หรือขอให้เปิดเผยถึงการได้มาของข้อมูลส่วนบุคคลดังกล่าวที่ตนไม่ได้ให้ความยินยอมได้ โดยสิทธินี้จะต้องไม่ขัดต่อกฎหมายหรือคำสั่งศาล หรือส่งผลกระทบที่อาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น ถ้าไม่ขัดหรือส่งผลกระทบดังกล่าว เจ้าของข้อมูลส่วนบุคคลจะได้รับสิทธิภายใน 30 วันนับจากวันที่ ผู้ควบคุมข้อมูลส่วนบุคคล ได้รับคำขอ

- สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคลมีสิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับตนเมื่อใดก็ได้ แต่ต้องไม่ขัดด้วยกฎหมายที่สำคัญยิ่งกว่า หรือขัดต่อสิทธิการเรียกร้องตามกฎหมาย หรือข้อมูลส่วนบุคคลนั้นเป็นไปเพื่อการวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ สถิติ

- สิทธิขอให้ลบหรือทำลาย

กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลได้ทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่เปิดเผยต่อสาธารณะ และผู้ควบคุมข้อมูลส่วนบุคคลถูกขอให้ลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลเจ้าของได้ โดยผู้ควบคุมข้อมูลส่วนบุคคลจะต้องผู้รับผิดชอบดำเนินการทั้งในทางเทคโนโลยีและค่าใช้จ่ายเอง

- สิทธิในการเพิกถอนความยินยอม

ถ้าเจ้าของข้อมูลเคยให้ความยินยอมในการใช้ข้อมูลไปแล้ว ต่อมาภายหลังต้องการยกเลิกความยินยอมนั้น ก็สามารถทำเมื่อใดก็ได้ และการยกเลิกความยินยอมนั้นจะต้องทำได้ง่ายเหมือนกับตอนแรกที่เจ้าของข้อมูลให้ความยินยอมด้วย โดยการยกเลิกจะต้องไม่ขัดต่อข้อจำกัดสิทธิในการถอนความยินยอมทางกฎหมาย หรือสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคลที่ได้ให้ความยินยอมไปก่อนหน้านี้

- สิทธิขอให้ระงับการใช้ข้อมูล

เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลระงับการใช้ข้อมูลส่วนบุคคล ไม่ว่าจะในกรณีที่เกิดการเปลี่ยนใจไม่ต้องการให้ข้อมูลแล้ว หรือเปลี่ยนใจระงับการทำลายข้อมูลเมื่อครบกำหนดที่ต้องทำลาย เพราะมีความจำเป็นต้องนำข้อมูลไปใช้ในทางกฎหมาย หรือการเรียกร้องสิทธิ ก็สามารถทำได้

- สิทธิในการขอให้แก้ไขข้อมูลส่วนบุคคล

เจ้าของข้อมูลมีสิทธิที่จะขอแก้ไขข้อมูลส่วนบุคคลของตนเองให้มีความถูกต้อง เป็นปัจจุบัน และไม่ก่อให้เกิดความเข้าใจผิดได้ โดยการแก้ไขนั้นจะต้องเป็นไปด้วยความสุจริต และไม่ขัดต่อหลักกฎหมาย

- สิทธิในการขอให้โอนข้อมูลส่วนบุคคล

ในกรณีที่เจ้าของข้อมูลต้องการนำข้อมูลที่เคยให้ไว้กับผู้ควบคุมข้อมูลรายหนึ่ง ไปใช้กับผู้ควบคุมข้อมูลอีกราย เช่น ผู้ควบคุมข้อมูลส่วนบุคคลรายแรกได้จัดทำข้อมูลส่วนบุคคลของเราไปในอยู่ในรูปแบบต่าง ๆ ที่เข้าถึงได้ด้วยวิธีการอัตโนมัติ เจ้าของข้อมูลสามารถขอให้ผู้ควบคุมข้อมูลส่วนบุคคลที่จัดทำข้อมูลนั้น ทำการส่งหรือโอนข้อมูลดังกล่าวให้

ได้ หรือจะขอให้ส่งไปยังผู้ควบคุมข้อมูลส่วนบุคคลรายอื่นโดยตรงก็สามารถทำได้ หากไม่ติดขัดทางวิธีการและเทคนิค โดยการใช้สิทธินั้นต้องไม่ขัดต่อกฎหมาย สัญญา หรือละเมิดสิทธิเสรีภาพของบุคคลอื่น

ผู้ควบคุมข้อมูลส่วนบุคคล จะสามารถรวบรวม ใช้ หรือเปิดเผย ข้อมูลส่วนบุคคล ก็ต่อเมื่อ ?

บุคคลธรรมดา หรือนิติบุคคล (บริษัท ห้างร้าน มูลนิธิ สมาคม หน่วยงาน องค์กร ร้านค้า หรืออื่นใดก็ตาม) หากมีการเก็บรวบรวมข้อมูลส่วนบุคคลไว้ หรือมีการนำข้อมูลส่วนบุคคลไปใช้ หรือนำไปเปิดเผยไม่ว่าจะวัตถุประสงค์ใดก็ตาม จำเป็นต้องได้รับ คำยินยอม (Consent) จากเจ้าของข้อมูลด้วย เว้นแต่จะเป็นไปตามข้อยกเว้นที่ พ.ร.บ.กำหนดไว้ โดยมีข้อยกเว้นดังต่อไปนี้

ข้อยกเว้นสำหรับข้อมูลส่วนบุคคลทั่วไป (Personal Data)

– จัดทำเอกสารประวัติศาสตร์ หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ ที่เกี่ยวข้องกับ การศึกษาวิจัยหรือการจัดทำสถิติ

– เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

– จำเป็นเพื่อปฏิบัติตามสัญญากับเจ้าของข้อมูล เช่น การซื้อขายของออนไลน์ ต้องใช้ชื่อ ที่อยู่ เบอร์โทรศัพท์

อีเมล

– จำเป็นเพื่อประโยชน์สาธารณะ และการปฏิบัติหน้าที่ในการใช้อำนาจรัฐ

– จำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือของบุคคลอื่น

– เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล เช่น ส่งข้อมูลพนักงานให้กรมสรรพากรเรื่องภาษี เป็นต้น

ข้อยกเว้นสำหรับข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Personal Data)

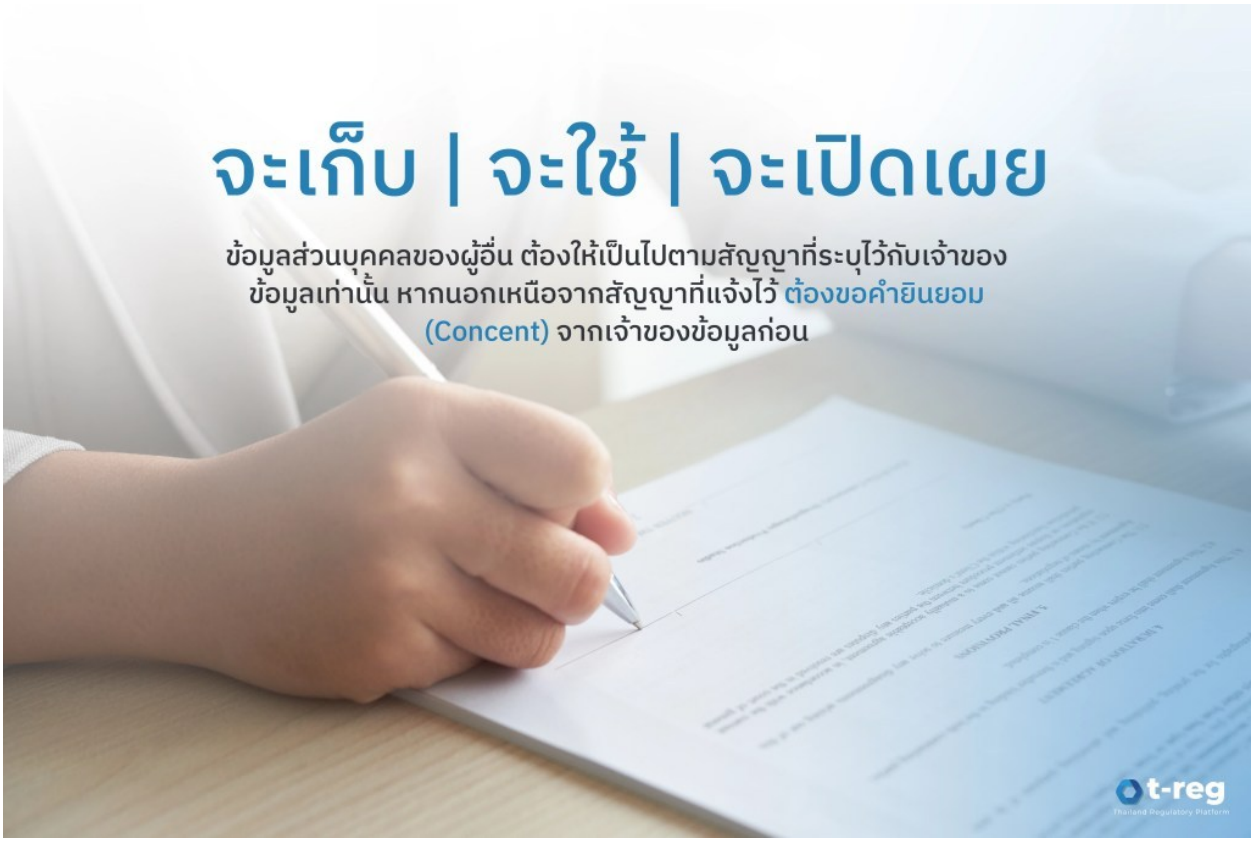
– เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

– การดำเนินกิจกรรมที่ชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของ มูลนิธิ สมาคม องค์กรไม่แสวงหากำไร เช่น เรื่องศาสนาหรือความคิดเห็นทางการเมือง ซึ่งจำเป็นต้องเปิดเผยให้ทราบก่อนเข้าองค์กรนั้น ๆ เป็นต้น

– เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล เช่น บุคคลสาธารณะที่มีข้อมูลที่เปิดเผยต่อสาธารณะอยู่แล้วในความยินยอมของเจ้าของข้อมูล

– เป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย เช่น เก็บลายนิ้วมือของผู้ที่บุกรุกเพื่อนำไปใช้ในชั้นศาล เป็นต้น

– เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์ เกี่ยวกับ เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ เช่น การเก็บข้อมูลสุขภาพของพนักงานซึ่งเป็นข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Personal Data) องค์กรมักใช้ข้อนี้ในการอ้างสิทธิที่จำเป็นต้องเก็บข้อมูลนี้ไว้ เป็นต้น / ประโยชน์ด้านสาธารณะสุข, การคุ้มครองแรงงาน, การประกันสังคม, หลักประกันสุขภาพแห่งชาติ / การศึกษาวิจัยทางวิทยาศาสตร์, ประวัติศาสตร์, สถิติ, หรือประโยชน์สาธารณะอื่น / ประโยชน์สาธารณะที่สำคัญ



คำถามที่มักพบบ่อย : ข้อมูลเก่าที่เคยเก็บไว้ก่อนที่ พ.ร.บ. นี้จะบังคับใช้ ต้องทำอย่างไร ?

ข้อมูลส่วนบุคคลที่ได้เก็บรวบรวมไว้ ก่อนหน้าที่ PDPA จะบังคับใช้ใน **วันที่ 1 มิถุนายน 2565** ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องทำอย่างไรบ้าง ตามมาตรา 95 ใน พ.ร.บ.ได้ระบุไว้ว่า

“ ให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรวมรวมและใช้ข้อมูลส่วนบุคคลนั้นต่อไปได้ตามวัตถุประสงค์เดิม ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคลต้องกำหนดวิธีการยกเลิกความยินยอม และเผยแพร่ประชาสัมพันธ์ให้เจ้าของข้อมูลส่วนบุคคลที่ไม่ประสงค์ให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวมรวม และใช้ข้อมูลส่วนบุคคลดังกล่าวสามารถแจ้งยกเลิกความยินยอมได้โดยง่าย ”

การส่ง หรือ โอนข้อมูลส่วนบุคคลไปยังต่างประเทศก็สำคัญ

ผู้ควบคุมข้อมูลส่วนบุคคล จะส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ ต้องตรวจสอบว่าประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลนั้น มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอหรือไม่ ยกเว้นว่าจะเป็นไปเพื่อเป็นไปตามกฎหมาย, ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล, จำเป็นเพื่อปฏิบัติตาม

สัญญา, ป้องกันอันตรายที่จะเกิดต่อเจ้าของข้อมูลที่ไม่สามารถให้ยินยอมในขณะนั้นได้ หรือเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะที่สำคัญ

เมื่อ PDPA บังคับใช้แล้วแต่ไม่ได้ปฏิบัติตาม จะมีบทลงโทษอะไรบ้าง ?

ถ้าไม่ปฏิบัติตาม PDPA บทลงโทษของผู้ที่ไม่ปฏิบัติตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (PDPA) มีถึง 3 ประเภท ได้แก่

- **โทษทางแพ่ง**

กำหนดให้ชดใช้ค่าสินไหมทดแทนที่เกิดขึ้นจริงให้กับเจ้าของข้อมูลส่วนบุคคลที่ได้รับความเสียหายจากการละเมิด และอาจจะต้องจ่ายบวกเพิ่มอีกเป็นค่าค่าสินไหมทดแทนเพื่อการลงโทษเพิ่มเติมสูงสุดได้อีก 2 เท่าของค่าเสียหายจริง ยกตัวอย่างเช่น หากศาลตัดสินว่าให้ผู้ควบคุมข้อมูลส่วนบุคคล ต้องชดใช้ค่าสินไหมทดแทนแก่เจ้าของข้อมูลส่วนบุคคล เป็นจำนวน 1 แสนบาท ศาลอาจมีคำสั่งกำหนดค่าสินไหมเพื่อการลงโทษเพิ่มอีก 2 เท่าของค่าเสียหายจริง เท่ากับว่าจะต้องจ่ายเป็นค่าปรับทั้งหมด เป็นจำนวนเงิน 3 แสนบาท

- **โทษทางอาญา**

มีทั้งโทษจำคุกและโทษปรับ โดยมีโทษจำคุกสูงสุดไม่เกิน 1 ปี หรือ ปรับไม่เกิน 1 ล้านบาท หรือทั้งจำทั้งปรับ โดยโทษสูงสุดดังกล่าวจะเกิดจากการไม่ปฏิบัติตาม PDPA ในส่วนการใช้ เปิดเผย หรือส่งโอนข้อมูลไปยังต่างประเทศ ประเภทข้อมูลที่มีความละเอียดอ่อน (Sensitive Personal Data) ส่วนกรณีหากผู้กระทำความผิด คือ บริษัท (นิติบุคคล) ก็อาจจะสงสัยว่าใครจะเป็นผู้ถูกจำคุก เพราะบริษัทติดคุกไม่ได้ ในส่วนตรงนี้ก็อาจจะตกมาที่ ผู้บริหาร, กรรมการ หรือบุคคลซึ่งรับผิดชอบในการดำเนินงานของบริษัทนั้น ๆ ที่จะต้องได้รับการลงโทษจำคุกแทน

- **โทษทางปกครอง**

โทษปรับ มี ตั้งแต่ 1 ล้านบาทจนถึงสูงสุดไม่เกิน 5 ล้านบาท ซึ่งโทษปรับสูงสุด 5 ล้านบาท จะเป็นกรณีของการไม่ปฏิบัติตาม PDPA ในส่วนการใช้ข้อมูล หรือเปิดเผยข้อมูล หรือส่งโอนข้อมูลไปยังต่างประเทศของประเภทข้อมูลที่มีความละเอียดอ่อน (Sensitive Personal Data) ซึ่งโทษทางปกครองนี้จะแยกต่างหากกับการชดใช้ค่าเสียหายที่เกิดจากโทษทางแพ่งและโทษทางอาญาด้วย

เมื่อ**วันที่ 14 กันยายน พ.ศ. 2566** ที่ผ่านมา ทางคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (PDPC) ได้เผยแพร่ประกาศฉบับใหม่ที่มี เนื้อหาเพิ่มเติมมาตราที่ 41(2) ซึ่งมีกำหนดว่า กิจการใดบ้างต้องจัดให้มี “เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล” โดยมีผลบังคับใช้ในวันที่ 13 ธันวาคม พ.ศ. 2566

DPO (Data Protection Officer) หรือ “เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล” คือ เจ้าหน้าที่ที่ทำหน้าที่หลักเป็นเหมือนตัวแทนของเจ้าของข้อมูลในการตรวจสอบว่าองค์กรมีการนำข้อมูลส่วนบุคคลทั้งภายใน (ข้อมูลพนักงาน) และภายนอก (ข้อมูลลูกค้า) ไปใช้อย่างถูกต้องตามกฎหมายหรือไม่ นอกจากนั้น DPO ยังเป็นผู้ที่คอยประสานงานระหว่างองค์กร เจ้าของข้อมูล (Data Subject) และสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (PDPC) ในกรณีที่เกิดเหตุละเมิดอีกด้วย

ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่ต้องจัดให้มี DPO คือกิจการที่ **มีการดำเนินกิจกรรมหลัก** ที่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ซึ่งจำเป็นต้อง**ตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ** โดยเหตุที่มีข้อมูลส่วนบุคคล**เป็นจำนวนมาก**

หากสนใจรายละเอียดเกี่ยวกับ DPO เพิ่มเติม สามารถอ่านต่อได้ ที่นี่

สรุปใจความสำคัญของ PDPA

จะเห็นได้ว่า PDPA หรือ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล มีหัวใจสำคัญก็เพื่อต้องการรักษาสิทธิที่พึงมีแก่เจ้าของข้อมูล ว่าข้อมูลส่วนตัวของเราจะปลอดภัย และถูกนำไปใช้อย่างถูกต้องเหมาะสมตามความต้องการและยินยอมของเจ้าของข้อมูลอย่างแท้จริง อย่างไรก็ตาม ผู้เป็นเจ้าของข้อมูลก็ควรพิจารณาอย่างรอบคอบเช่นกันว่าการให้ข้อมูลส่วนบุคคลในแต่ละครั้ง ***เป็นไปเพื่อวัตถุประสงค์อะไร? ข้อมูลที่ให้ไปมีเพียงพอกับวัตถุประสงค์นั้นแล้วหรือยัง?*** หากมองว่ามีการให้ข้อมูลส่วนบุคคลนั้นไม่เกี่ยวข้องกับวัตถุประสงค์ของการขอข้อมูล เราก็สามารถปฏิเสธการให้ข้อมูลนั้นได้ เพื่อเป็นการป้องกันการนำข้อมูลไปใช้ในทางที่ผิดหรือหาผลประโยชน์จากข้อมูลส่วนบุคคลของตน

สำหรับในส่วนผู้เก็บข้อมูลนั้น นับว่าได้รับผลกระทบโดยตรงเป็นอย่างมากกับ PDPA ที่จะต้องปฏิบัติตาม ผู้ควบคุมข้อมูลส่วนบุคคลจึงต้องมีการกำหนดนโยบายความปลอดภัยของข้อมูลส่วนบุคคลภายในองค์กรและให้ความรู้แก่บุคลากรในองค์กร, รู้ขอบเขตการเก็บรวบรวม ใช้ เผยแพร่ข้อมูลส่วนบุคคล, มีระบบการจัดเก็บข้อมูลส่วนบุคคลที่ปลอดภัย จำกัดการเข้าถึงข้อมูลส่วนบุคคล รวมไปถึงการบันทึกกิจกรรมการใช้ข้อมูลส่วนบุคคล สิ่งเหล่านี้ล้วนจำเป็นอย่างยิ่งที่ผู้ควบคุมข้อมูลจะต้องปฏิบัติตามเพื่อให้สอดคล้องกับ PDPA ต่อไป มาถึงตรงนี้ผู้อ่านก็พอจะทราบแล้วว่า PDPA คืออะไร ? และเกี่ยวข้องกับเราอย่างไร

สรุปแล้ว PDPA คืออะไร และเกี่ยวข้องกับเราอย่างไร?

สรุป PDPA ฉบับเข้าใจง่าย คือ PDPA เกี่ยวข้องกับเราทุกคน เพราะทุกคนมีข้อมูลส่วนตัว ทุกคนควรรู้สิทธิที่เรามีต่อข้อมูลส่วนตัวของเราว่าเราทำอะไรได้บ้าง หากไม่รู้สิทธิที่มีอาจถูกเอาเปรียบ ทำให้เกิดความเสียหายภายหลังได้ รวมถึงค่าสินไหมที่ควรได้รับก็ไม่ได้

และทุกองค์กร มีการเก็บข้อมูลส่วนตัว ดังนั้นแล้วบุคคลากรในองค์กรต้องทราบขอบเขตใน การนำข้อมูลส่วนบุคคลไปใช้ไปเปิดเผยรวม ถึงการจัดเก็บข้อมูลส่วนตัวให้ปลอดภัย หากเกิดความเสียหายอันเกิดจากการเก็บรวบรวม การใช้ การเปิดเผยข้อมูลส่วนบุคคลโดยไม่เป็นไปตาม PDPA แล้ว ก็จะได้รับบทลงโทษ

ที่มา PDPA คืออะไร ? - สรุป พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ที่ต้องรู้

กรณีไหนบ้าง สามารถใช้ ‘ข้อมูลส่วนบุคคล’ ได้โดยไม่ต้องขอความยินยอม

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือกฎหมาย PDPA กฎหมายที่ออกมาคุ้มครองสิทธิเกี่ยวกับข้อมูลส่วนบุคคล ที่มีผลบังคับใช้ในประเทศไทยเมื่อ 1 มิถุนายน 65 ที่ผ่านมา โดยมีบทบาทสำคัญในการคุ้มครองและให้สิทธิที่เรามีต่อข้อมูลส่วนบุคคล และสร้างมาตรฐานในการเก็บรักษา รับรวม ใช้ข้อมูล ขององค์กร เหตุด้วยปัจจุบันมีการล่วงละเมิดสิทธิข้อมูลส่วนบุคคลเพิ่มมากขึ้นจนสร้างความเดือดร้อนให้กับหลายบุคคล ซึ่งล้วนเกี่ยวข้องกับ พ.ร.บ.ฉบับนี้ทั้งสิ้น โดยหากผู้ใดไม่ปฏิบัติตามย่อมมีบทลงโทษตามกฎหมาย โดยหลักเกณฑ์สำคัญของกฎหมาย PDPA คือ ไม่ว่าจะเป็นการเก็บรวบรวม ใช้ หรือเผยแพร่ข้อมูลส่วนบุคคล ต้อง “ขอความยินยอม” จาก “เจ้าของข้อมูลส่วนบุคคล” ให้ถูกต้องก่อน

การขอความยินยอม (Consent) ตามกฎหมาย PDPA ถือว่าเป็นขั้นตอนที่สำคัญมากที่สุด เพราะถ้าไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลที่ถือเป็นผู้ดูแล ก็จะไม่สามารถข้อมูลนั้นมาใช้ได้ โดยเมื่อมีการได้รับความยินยอมจากเจ้าของข้อมูลแล้ว องค์กรก็จะต้องใช้ข้อมูลตามวัตถุประสงค์ที่ได้แจ้งไว้ และจะต้องดูแลรักษาข้อมูลนั้นให้ปลอดภัย ป้องกันการที่ผู้อื่นละเมิดสิทธิความเป็นส่วนตัวของเจ้าของข้อมูล ซึ่งหากข้อมูลรั่วไหลออกไปก็อาจนำมาซึ่งความเดือดร้อนหรือสร้างความเสียหาย และผู้ควบคุมข้อมูลส่วนบุคคลก็อาจมีความผิดตามกฎหมาย ทั้งทางแพ่ง อาญา และปกครองได้

PDPA มีผลบังคับใช้ หากไม่สามารถปฏิบัติตามได้ถูกต้องจะมีบทลงโทษทางกฎหมายดังนี้

โทษทางอาญา -> จะมีทั้งโทษจำคุกและโทษปรับ โดยมีโทษจำคุกสูงสุดไม่เกิน 1 ปี หรือปรับไม่เกิน 1 ล้านบาท หรือทั้งจำทั้งปรับ

โทษทางแพ่ง -> จะมีการกำหนดให้ใช้สินไหมทดแทนที่เกิดขึ้นจริงกับเจ้าของข้อมูลส่วนบุคคล (ที่ได้รับความเสียหายจากการถูกละเมิด)

โทษทางปกครอง -> จะมีโทษปรับ โดยมีตั้งแต่ 1 ล้านบาท – 5 ล้านบาท

อย่างไรก็ตาม กฎหมายนี้ยังมีข้อยกเว้นในบางกรณี ว่าสามารถใช้ข้อมูลส่วนบุคคลได้โดยไม่ต้องรอขอความยินยอมดังต่อไปนี้

เก็บรวบรวม ใช้ เผยแพร่ข้อมูลส่วนบุคคลแบบใด สามารถใช้ได้โดยไม่ต้องรอขอความยินยอม

1. การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของบุคคล ที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์ส่วนตน หรือเพื่อกิจกรรมในครอบครัวของบุคคลนั้นเท่านั้น
2. การดำเนินการของหน่วยงานรัฐที่มีหน้าที่ รักษาความมั่นคงของรัฐ, การรักษาความปลอดภัยของประชาชน
3. บุคคลหรือนิติบุคคลซึ่งใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวมข้อมูลไว้เฉพาะเพื่อกิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรม ตามจริยธรรมวิชาชีพ
4. กรณีป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูล หรือเพื่อประโยชน์สาธารณะ
5. สภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมการที่แต่งตั้งโดยสภาดังกล่าว ซึ่งเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ในการพิจารณาตามหน้าที่และอำนาจของสภาผู้แทนราษฎร วุฒิสภา รัฐสภา หรือคณะกรรมาธิการ แล้วแต่กรณี
6. เป็นการพิจารณาพิพากษาของศาล และการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี หรือดำเนินงานตามกระบวนการยุติธรรมทางอาญา
7. การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

อย่างไรก็ตาม ถึงแม้จะมีข้อยกเว้นในบางกรณีข้างต้น แต่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล จะต้องมีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานตามหลัก PDPA ด้วย

ที่มา กรณีไหนบ้าง สามารถใช้ ‘ข้อมูลส่วนบุคคล’ ได้โดยไม่ต้องขอความยินยอม –

บทลงโทษหากไม่ปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA)

PDPA คืออะไร

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือกฎหมาย PDPA (Personal Data Protection Act) เป็นกฎหมายที่คุ้มครองข้อมูลส่วนบุคคลที่สามารถระบุถึงตัวเจ้าของข้อมูลนั้นได้ เช่น ชื่อ ที่อยู่ เบอร์โทรศัพท์ บัญชีธนาคาร อีเมล ไอดีไลน์ บัญชีผู้ใช้ของเว็บไซต์ ลายนิ้วมือ ประวัติสุขภาพ เป็นต้น ซึ่งธุรกิจควรมีการเตรียมความพร้อมในการจัดวางโครงสร้างหรือระบบรองรับการใช้และจัดเก็บข้อมูลส่วนบุคคล รวมถึงการจัดทำเอกสารทางกฎหมายให้เป็นไปตามมาตรฐานไว้แต่เนิ่นๆ เนื่องจากกฎหมาย PDPA กำลังจะมีการบังคับใช้เต็มรูปแบบในเดือนมิถุนายน 2565 นี้

ข้อมูลส่วนบุคคลมีอะไรบ้าง

การจัดการข้อมูลส่วนบุคคลของธุรกิจโดยเฉพาะอย่างยิ่งการใช้หรือเก็บข้อมูลส่วนบุคคลที่กฎหมาย PDPA กำหนดว่าจะต้องขอความยินยอม (Consent) และแจ้งวัตถุประสงค์ให้เจ้าของข้อมูลส่วนบุคคลรู้ถือว่ามีความสำคัญมาก เนื่องจากข้อมูลส่วนบุคคลแบ่งออกเป็น 2 ประเภท คือ ข้อมูลส่วนบุคคลทั่วไป และข้อมูลส่วนบุคคลที่อ่อนไหว ซึ่งกฎหมายกำหนดความเข้มงวดในการเก็บข้อมูลส่วนบุคคลทั้ง 2 ประเภทต่างกัน สำหรับข้อมูลส่วนบุคคลที่อ่อนไหวเป็นข้อมูลที่มีความเสี่ยงต่อการถูกละเมิดมากกว่าข้อมูลส่วนบุคคลทั่วไป ดังนั้น ธุรกิจจึงควรเก็บข้อมูลเท่าที่จำเป็นและเก็บตามวัตถุประสงค์ที่ได้แจ้งไว้กับเจ้าของข้อมูลเท่านั้น โดยข้อมูลส่วนบุคคลประเภทต่างๆ มีรายละเอียด ดังนี้

ข้อมูลส่วนบุคคลทั่วไป (Personal Data)

เป็นข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม ทั้งข้อมูลในรูปแบบออนไลน์หรือออฟไลน์ เช่น ชื่อ ที่อยู่ เบอร์โทรศัพท์ อีเมล เลขบัตรประชาชน เลขที่บัญชีธนาคาร

ข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Personal Data)

เป็นข้อมูลที่ระบุตัวบุคคลได้เฉพาะเจาะจงมากขึ้น เช่น เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ศาสนา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ (face ID, ลายนิ้วมือ) หรือข้อมูลอื่นในทำนองเดียวกัน ซึ่งข้อมูลเหล่านี้มีความละเอียดอ่อนสูง ถ้าถูกนำไปใช้โดยไม่ได้รับอนุญาตอาจเป็นอันตรายต่อเจ้าของข้อมูลหรือได้รับการปฏิบัติอย่างไม่เป็นธรรมได้ ดังนั้น กฎหมาย PDPA จึงต้องให้ความคุ้มครองอย่างเข้มงวดมากกว่าข้อมูลส่วนบุคคลทั่วไป

สิทธิของเจ้าของข้อมูลส่วนบุคคล

กฎหมาย PDPA กำหนดหน้าที่ให้ธุรกิจในฐานะผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ขอความยินยอม (Consent) ต่อเจ้าของข้อมูลส่วนบุคคล เพื่อเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล ดังนั้น จึงเป็นสิทธิของเจ้าของข้อมูลส่วนบุคคลที่จะให้ความยินยอมให้ใช้ข้อมูลเหล่านั้นหรือไม่ก็ได้ ในกรณีที่ให้ความยินยอมแล้ว เจ้าของข้อมูลก็ยังคงมีสิทธิในข้อมูลของตัวเองตามกฎหมาย และสามารถใช้สิทธินั้นได้โดยแบ่งออกได้ ดังนี้

1. สิทธิได้รับการแจ้งให้ทราบ

ผู้ควบคุมข้อมูลส่วนบุคลล จะต้องแจ้งรายละเอียดและวัตถุประสงค์ในการรวบรวมข้อมูล การใช้ หรือเผยแพร่ให้เจ้าของข้อมูลทราบก่อนหรือขณะเก็บรวบรวมข้อมูล โดยเจ้าของข้อมูลมีสิทธิที่จะทราบว่าจะจัดเก็บข้อมูลอะไรบ้าง รวมถึงระยะเวลาการจัดเก็บ สถานที่ และวิธีการติดต่อกับผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งเรามักจะเห็นการแจ้งข้อมูลเหล่านี้ตามข้อกำหนดและเงื่อนไขก่อนที่ผู้ใช้งานเว็บไซต์จะสมัครสมาชิก หรืออาจเป็นการขอความยินยอมผ่านแบบฟอร์มก็ได้

2. สิทธิในการแก้ไขข้อมูล

เจ้าของข้อมูลมีสิทธิที่จะขอแก้ไขข้อมูลส่วนบุคคลของตนเองให้ถูกต้อง เป็นปัจจุบัน และไม่ก่อให้เกิดความเข้าใจผิดได้ โดยตามเว็บไซต์ส่วนใหญ่ เราจะสามารถเข้าไปแก้ไขข้อมูลส่วนตัว เช่น ที่อยู่ เบอร์โทรศัพท์ รหัสผ่าน ในหน้าบัญชีสมาชิกเองได้

3. สิทธิในการเพิกถอนความยินยอม

กรณีเจ้าของข้อมูลเคยให้ความยินยอมในการใช้ข้อมูลไป ต่อมาเกิดเปลี่ยนใจหรือไม่ได้ใช้บริการกับธุรกิจนั้นแล้ว ก็สามารถยกเลิกความยินยอมนั้นเมื่อไหร่ก็ได้ เช่น เราสามารถขอยกเลิกติดตามข่าวสารทางอีเมลของเว็บไซต์ได้ โดยกดที่ปุ่ม unsubscribe ที่แนบมาในอีเมล โดยการยกเลิกนี้ไม่ควรเป็นวิธีที่ยุ่งยากซับซ้อน ไม่กำหนดเงื่อนไข หรือต้องให้เจ้าของข้อมูลส่วนบุคคลเสียค่าใช้จ่าย

4. สิทธิในการขอระงับการใช้ข้อมูล

ในกรณีที่เจ้าของข้อมูลส่วนบุคคลเปลี่ยนใจไม่ต้องการให้ข้อมูลแล้ว หรือไม่ต้องการให้ทำลายข้อมูลเมื่อครบกำหนดที่ต้องทำลาย เพราะมีความจำเป็นต้องนำข้อมูลไปใช้ในทางกฎหมาย หรือการเรียกร้องสิทธิ ก็สามารถทำได้

5. สิทธิในการเข้าถึง ขอสำเนา หรือให้เปิดเผยถึงการได้มาของข้อมูลส่วนบุคคล

ถ้าเจ้าของข้อมูลส่วนบุคคลไม่แน่ใจว่าได้เคยให้ความยินยอมกับภาคธุรกิจไปหรือไม่ ก็สามารถใช้สิทธิการเข้าถึงข้อมูลนั้นได้โดยต้องไม่ขัดต่อกฎหมายหรือคำสั่งศาล และการใช้สิทธินั้นต้องไม่ละเมิดสิทธิหรือเสรีภาพของบุคคลอื่น

ตัวอย่างเช่นผู้ใช้งานเว็บไซต์อาจเข้าไปดูข้อมูลตนเองในบัญชีสมาชิกของตนเองได้ หรือร้องขอกับผู้ดูแลระบบเพื่อขอดูข้อมูลของตนเองได้

6. สิทธิในการขอรับและให้โอนย้ายข้อมูลส่วนบุคคล

ในกรณีที่เจ้าของข้อมูลส่วนบุคคลต้องการให้ธุรกิจที่มีข้อมูลส่วนบุคคลของตนโอนข้อมูลนั้นให้กับอีกธุรกิจอีกราย ซึ่งข้อมูลที่โอนไปนั้น เจ้าของข้อมูลส่วนบุคคลก็ยังขอรับสำเนาข้อมูลนั้นจากธุรกิจที่เป็นผู้จัดทำข้อมูลได้อีกด้วย แต่การใช้วิธีการดังกล่าวต้องไม่ขัดต่อกฎหมาย สัญญา หรือละเมิดสิทธิเสรีภาพของบุคคลอื่น เช่น การย้ายพนักงานจากบริษัทหนึ่งไปยังอีกบริษัทหนึ่ง ตัวพนักงานก็สามารถใช้สิทธิให้บริษัทแรกโอนย้ายข้อมูลส่วนบุคคลไปยังบริษัทที่กำลังจะย้ายไปได้ รวมถึงขอรับสำเนาข้อมูลของตนเองได้

7. สิทธิในการขอคัดค้านการเก็บรวบรวมใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคลสามารถคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้ โดยร้องขอต่อผู้ควบคุมข้อมูลเมื่อไรก็ได้ โดยร้องขอผ่านแบบฟอร์มที่ผู้ให้บริการจัดไว้ หรือติดต่อกับผู้ดูแลระบบ

8. สิทธิในการขอให้ลบ หรือทำลายข้อมูลส่วนบุคคล

ธุรกิจจะต้องเป็นผู้รับผิดชอบค่าใช้จ่าย ถ้าเจ้าของข้อมูลขอให้ธุรกิจลบหรือทำลายข้อมูลส่วนบุคคล หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวตนได้ ในกรณีที่ข้อมูลส่วนบุคคลหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ หรือธุรกิจนำข้อมูลไปเผยแพร่ในที่สาธารณะ หรือเจ้าของข้อมูลเห็นว่าข้อมูลของตนนั้นสามารถเข้าถึงได้ง่ายเกินไป

9. สิทธิในการร้องเรียน

เจ้าของข้อมูลมีสิทธิร้องเรียนต่อพนักงานเจ้าหน้าที่และคณะกรรมการตาม PDPA ได้ ถ้าผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล ฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมาย รวมถึงมีสิทธิในการเรียกค่าสินไหมทดแทนทางศาลด้วย

บทลงโทษหากไม่ปฏิบัติตาม PDPA

ในกรณีที่เจ้าของข้อมูลส่วนบุคคลได้ร้องขอตามสิทธิ PDPA แล้ว แต่ธุรกิจเพิกเฉย ไม่ปฏิบัติตามหน้าที่ที่ต้องพิจารณาคำร้องและดำเนินการตามคำร้องเพื่อให้เป็นไปตามสิทธิของเจ้าของข้อมูล หรือถ้าธุรกิจไม่ปฏิบัติตาม PDPA จนเกิดเหตุการณ์ที่ข้อมูลส่วนบุคคลถูกละเมิดก็อาจเกิดผลกระทบต่อธุรกิจได้ บทลงโทษ PDPA จึงกำหนดโทษไว้ 3 ส่วนด้วยกัน คือ โทษทางแพ่ง โทษทางอาญา และโทษทางปกครอง

โทษทางแพ่ง

ธุรกิจที่ทำให้เจ้าของข้อมูลส่วนบุคคลเสียหายจะต้องใช้ค่าสินไหมทดแทน ไม่ว่าจะจงใจให้เกิดเหตุการณ์นั้นขึ้นหรือไม่ตั้งใจก็ตาม ยกเว้นว่าจะพิสูจน์ได้ว่าเกิดจากเหตุสุดวิสัยหรือเกิดจากการกระทำหรือละเว้นการกระทำของเจ้าของข้อมูลส่วนบุคคลนั้นเอง หรือเป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติการตามหน้าที่และอำนาจตามกฎหมาย ดังนั้น ภาคธุรกิจจึงควรสร้าง Awareness ให้พนักงานในองค์กรรู้หน้าที่และความรับผิดชอบของตน ด้วยการเทรนนิ่งหรือให้ความรู้ PDPA จากบริการ PDPA Training & Seminars ของ PDPA Coreเพื่อลดความเสี่ยงจากการดำเนินงานเกี่ยวกับข้อมูลส่วนบุคคลผิดพลาดโดยไม่ตั้งใจ ซึ่งอาจนำไปสู่การละเมิดข้อมูลส่วนบุคคลและถือเป็นความผิดตามกฎหมาย PDPA ได้

สำหรับค่าสินไหมทดแทนจะรวมถึงค่าใช้จ่ายที่เจ้าของข้อมูลได้จ่ายไปตามความจำเป็น เพื่อป้องกันความเสียหายที่กำลังจะเกิดขึ้น หรือระงับความเสียหายที่เกิดขึ้นด้วย และศาลอาจกำหนดให้ผู้กระทำผิดจ่ายเพิ่มเติมจากจำนวนค่าสินไหมทดแทนที่แท้จริงได้ แต่ต้องไม่เกินกว่า 2 เท่าของค่าสินไหมทดแทนที่แท้จริง บทลงโทษ PDPA ในทางแพ่ง มีอายุความ 3 ปี นับแต่วันที่ผู้เสียหายรู้ถึงความเสียหาย และรู้ตัวผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ต้องรับผิด หรือ 10 ปีนับแต่วันที่มีการละเมิดข้อมูลส่วนบุคคล

โทษทางอาญา

บทลงโทษ PDPA ทางอาญานั้นสามารถยอมความได้ โดยความผิดเกิดจากการที่ธุรกิจในฐานะผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคลอ่อนไหวนอกเหนือไปจากวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลไว้ หรือโอนข้อมูลอ่อนไหวไปยังต่างประเทศโดยไม่ชอบด้วยกฎหมาย ซึ่งผลของความเสียหายต่อเจ้าของข้อมูลส่วนบุคคลก็จะแตกต่างกัน โดยมีรายละเอียดดังนี้

- การกระทำความผิดนั้นอาจทำให้เจ้าของข้อมูลส่วนบุคคลเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ
- ความกระทำความผิดนั้นเกิดจากการที่ธุรกิจแสวงหาประโยชน์สำหรับตนเองหรือผู้อื่นโดยทุจริต ต้องระวางโทษจำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 1,000,000 บาท หรือทั้งจำทั้งปรับ
- ความผิดฐานเปิดเผยข้อมูลส่วนบุคคล ผู้ใดล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตาม PDPA แล้วนำไปเปิดเผยแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ
- ในกรณีที่ผู้กระทำผิดเป็นนิติบุคคล บุคคลที่กระทำความผิดต้องรับผิดชอบในการดำเนินงานของนิติบุคคลนั้นๆ และรับโทษตามความผิดนั้นๆ อีกด้วย

อย่างไรก็ตาม ผู้ควบคุมข้อมูลส่วนบุคคลได้รับการยกเว้นความผิดในกรณีที่เป็นการเปิดเผยข้อมูลส่วนบุคคลตามหน้าที่ หรือเพื่อประโยชน์แก่การสอบสวน หรือการพิจารณาคดี หรือเปิดเผยแก่หน่วยงานของรัฐในประเทศหรือต่างประเทศที่มีอำนาจหน้าที่ หรือเปิดเผยที่ได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับการฟ้องร้องคดีต่างๆ ที่เปิดเผยต่อสาธารณะ

โทษทางปกครอง

บทลงโทษ PDPA ในทางปกครอง มีอัตราโทษปรับทางปกครองสูงสุดไม่เกิน 5,000,000 บาท หรือในกรณีที่คณะกรรมการผู้เชี่ยวชาญเห็นสมควรอาจจะสั่งให้แก้ไขหรือตักเตือนก่อนก็ได้ โดย PDPA กำหนดโทษของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล ตัวแทน และโทษทางปกครองอื่นๆ ดังนี้

โทษของผู้ควบคุมข้อมูลส่วนบุคคล

- ไม่ขอความยินยอมหรือไม่แจ้งผลกระทบจากการถอนความยินยอม
- ไม่แจ้งการเก็บข้อมูลส่วนบุคคล
- ไม่ให้เจ้าของข้อมูลส่วนบุคคลเข้าถึงข้อมูลตามสิทธิ
- ไม่ทำบันทึกรายการตามที่กฎหมายกำหนด
- ไม่มีเจ้าหน้าที่หรือไม่จัดให้มีเจ้าหน้าที่ดูแลข้อมูลส่วนบุคคลอย่างเพียงพอ
- เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากฐานทางกฎหมาย
- ใช้ข้อมูลส่วนบุคคลผิดไปจากวัตถุประสงค์ที่แจ้งเอาไว้
- เก็บข้อมูลส่วนบุคคลเกินกว่าที่จำเป็น
- เก็บข้อมูลส่วนบุคคลจากแหล่งอื่นที่ต้องห้ามตามกฎหมาย
- ทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
- ไม่ปฏิบัติตามหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล

โทษของผู้ประมวลผลข้อมูลส่วนบุคคล

- การไม่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือไม่มีการสนับสนุนการปฏิบัติหน้าที่อย่างเพียงพอ
- การไม่ปฏิบัติตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล การไม่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม
- การไม่จัดทำบันทึกรายการกิจกรรมการประมวลผล
- การโอนข้อมูลส่วนบุคคลทั่วไปและข้อมูลส่วนบุคคลที่อ่อนไหวไปต่างประเทศโดยไม่ชอบด้วยกฎหมาย

บทลงโทษ PDPA ทางปกครองอื่นๆ

- ตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล ไม่จัดให้มีบันทึกรายการประมวลผลข้อมูลส่วนบุคคล
- ไม่ปฏิบัติตามคำสั่งคณะกรรมการผู้เชี่ยวชาญ หรือไม่มาชี้แจงข้อเท็จจริง หรือไม่ส่งข้อมูลให้คณะกรรมการผู้เชี่ยวชาญ

สิ่งสำคัญที่ธุรกิจในฐานะผู้ควบคุมข้อมูลส่วนบุคคลจะต้องปฏิบัติ คือ การดำเนินการตามสิทธิของเจ้าของข้อมูลส่วนบุคคล โดยเฉพาะการขอความยินยอม (Consent) ตามกฎหมาย PDPA ถือว่าเป็นขั้นตอนที่สำคัญมากที่สุด เพราะถ้าไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลแล้ว ธุรกิจก็ไม่อาจนำข้อมูลนั้นมาใช้ได้ และเมื่อได้รับความยินยอมแล้วก็จะต้องใช้ข้อมูลตามวัตถุประสงค์ที่ได้แจ้งไว้ รวมทั้งดูแลรักษาข้อมูลนั้นให้ปลอดภัย ป้องกันผู้อื่นละเมิดสิทธิความเป็นส่วนตัวของเจ้าของข้อมูล

ที่มาบทลงโทษหากไม่ปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA) | PDPA Core

ข้อมูลส่วนบุคคล ข้อมูลอ่อนไหว คืออะไร มีกี่ประเภท มีอะไรบ้าง ?

ในกฎหมาย PDPA พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (กำหนดการเลื่อนบังคับใช้ ในวันที่ 1 มิถุนายน 2565) มีหลายต่อหลายท่านต่างมีคำถามเดียวกันเมื่อได้ยินชื่อพระราชบัญญัตินี้เป็นครั้งแรกว่า ข้อมูลส่วนบุคคลคืออะไร? แล้วข้อมูลส่วนบุคคลมีอะไรบ้าง? บทความนี้จะพาทุกท่านรับทราบถึงรายละเอียดดังกล่าว เพื่อสร้างความเข้าใจในขั้นพื้นฐานต่อกฎหมายพระราชบัญญัติฉบับนี้ให้มากยิ่งขึ้น

ข้อมูลส่วนบุคคลแบ่งออกเป็น 2 ประเภท ได้แก่

1.ข้อมูลส่วนบุคคล (Personal Data)

อาจจะได้ยินเรียกกันว่า ข้อมูลส่วนบุคคลทั่วไป / ข้อมูลส่วนบุคคลปกติ / ข้อมูลส่วนบุคคลพื้นฐาน

2.ข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Personal Data)

อาจจะได้ยินเรียกกันว่า ข้อมูลส่วนบุคคลที่ละเอียดอ่อน

ข้อมูลส่วนบุคคล Personal Data คืออะไร?

ข้อมูลส่วนบุคคล (Personal Data) คือ ข้อมูลใด ๆ ที่สามารถระบุตัวบุคคลนั้นได้ (ระบุไปถึงเจ้าของข้อมูล) ไม่ว่าจะเป็นทางตรงหรือทางอ้อมก็ตาม แต่จะไม่รวมไปถึงข้อมูลของผู้ที่เสียชีวิตแล้ว หรือ ข้อมูลของนิติบุคคล เช่น บริษัท มูลนิธิ สมาคม องค์กร

ตัวอย่าง ข้อมูลส่วนบุคคล (Personal Data) มีอะไรบ้าง

1. ชื่อ-นามสกุล หรือชื่อเล่น
2. เลขประจำตัวประชาชน, เลขหนังสือเดินทาง, เลขบัตรประกันสังคม, เลขใบอนุญาตขับขี่, เลขประจำตัวผู้เสียภาษี, เลขบัญชีธนาคาร, เลขบัตรเครดิต (การเก็บเป็นภาพสำเนาบัตรประชาชนหรือสำเนาบัตรอื่น ๆ ที่มีข้อมูลส่วนบุคคลที่กล่าวมาย่อมสามารถใช้ระบุตัวบุคคลได้โดยตัวมันเอง จึงถือเป็นข้อมูลส่วนบุคคล)
3. ที่อยู่, อีเมล์, เลขโทรศัพท์
4. ข้อมูลอุปกรณ์หรือเครื่องมือ เช่น IP address, MAC address, Cookie ID
5. ข้อมูลระบุทรัพย์สินของบุคคล เช่น ทะเบียนรถยนต์, โฉนดที่ดิน

6. ข้อมูลที่สามารถเชื่อมโยงไปยังข้อมูลข้างต้นได้ เช่น วันเกิดและสถานที่เกิด, เชื้อชาติ,สัญชาติ, น้ำหนัก, ส่วนสูง, ข้อมูลตำแหน่งที่อยู่ (location), ข้อมูลการแพทย์, ข้อมูลการศึกษา, ข้อมูลทางการเงิน, ข้อมูลการจ้างงาน
7. ข้อมูลหมายเลขอ้างอิงที่เก็บไว้ในไมโครฟิล์ม แม้ไม่สามารถระบุไปถึงตัวบุคคลได้ แต่หากใช้ร่วมกับระบบดัชนีข้อมูลอีกระบบหนึ่งก็จะสามารถระบุไปถึงตัวบุคคลได้ ดังนั้น
8. ข้อมูลการประเมินผลการทำงานหรือความเห็นของนายจ้างต่อการทำงานของลูกจ้าง
9. ข้อมูลบันทึกต่าง ๆ ที่ใช้ติดตามตรวจสอบกิจกรรมต่าง ๆ ของบุคคล เช่น log file
10. ข้อมูลที่สามารถใช้ในการค้นหาข้อมูลส่วนบุคคลอื่นในอินเทอร์เน็ต

ตัวอย่าง ข้อมูลที่ไม่เป็นข้อมูลส่วนบุคคล มีอะไรบ้าง

1. เลขทะเบียนบริษัท
2. ข้อมูลสำหรับการติดต่อทางธุรกิจที่ไม่ได้ระบุถึงตัวบุคคล เช่น หมายเลขโทรศัพท์ หรือแฟกซ์ที่ทำงาน, ที่อยู่สำนักงาน, อีเมล์ที่ใช้ในการทำงาน, อีเมล์ของบริษัท เช่น info@company.com เป็นต้น
3. ข้อมูลนิรนาม (Anonymous Data) หรือข้อมูลแฝง (Pseudonymous Data) หมายถึงข้อมูลหรือชุดข้อมูลที่ถูกทำให้ไม่สามารถระบุตัวบุคคลได้อีกโดยวิธีการทางเทคนิค
4. ข้อมูลผู้ตาย

ข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Personal Data) คืออะไร?

ข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Personal Data) คือ ข้อมูลส่วนบุคคลที่เป็นเรื่องส่วนตัวโดยแท้ของบุคคล แต่มีความละเอียดอ่อนและสุ่มเสี่ยงต่อการถูกใช้ในการเลือกปฏิบัติอย่างไม่เป็นธรรม จึงจำเป็นต้องดำเนินการด้วยความระมัดระวังเป็นพิเศษ

ตัวอย่าง ข้อมูลส่วนบุคคลที่ข้อมูลอ่อนไหว มีอะไรบ้าง

1. เชื้อชาติ
2. เผ่าพันธุ์

3. ความคิดเห็นทางการเมือง
4. ความเชื่อในลัทธิ ศาสนาหรือปรัชญา
5. พฤติกรรมทางเพศ
6. ประวัติอาชญากรรม
7. ข้อมูลสุขภาพ ความพิการ หรือข้อมูลสุขภาพจิต
8. ข้อมูลสหภาพแรงงาน
9. ข้อมูลพันธุกรรม
10. ข้อมูลชีวภาพ
11. ข้อมูลทางชีวมิติ (Biometric) เช่น รูปภาพใบหน้า, ลายนิ้วมือ, ฟิล์มเอกซเรย์, ข้อมูลสแกนม่านตา, ข้อมูลอัตลักษณ์เสียง, ข้อมูลพันธุกรรม
12. ข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด

โดย พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล มีสาระสำคัญอย่างหนึ่งที่ได้ระบุไว้ในมาตราที่ 19 ใจความว่า

ผู้ควบคุมข้อมูลส่วนบุคคลจะกระทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล ส่วนบุคคลไม่ได้หากเจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอมไว้ก่อนหรือในขณะนั้น เว้นแต่บทบัญญัติ แห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้

หากจะขยายความให้ง่ายต่อความเข้าใจมากยิ่งขึ้น จะกล่าวได้ว่า ไม่ว่าจะเป็นบุคคลธรรมดาทั่วไป หรือเป็นบริษัท ห้างร้าน มูลนิธิ สมาคม หน่วยงาน องค์กร ร้านค้า หรืออื่นใดก็ตาม หากมีการเก็บข้อมูลส่วนบุคคลไว้ หรือมีการนำข้อมูลส่วนบุคคลไปใช้ หรือนำไปเปิดเผยไม่ว่าจะวัตถุประสงค์ใดก็ตาม จำเป็นต้องได้รับคำยินยอม(Consent) จากเจ้าของข้อมูลด้วย เว้นแต่จะเป็นไปตามข้อยกเว้นใน พ.ร.บ.ที่ได้กำหนดไว้เท่านั้น ซึ่งได้ระบุรายละเอียดไว้ในมาตรา 24, 26, 27 โดยสรุปข้อยกเว้นไว้ดังต่อไปนี้

ข้อยกเว้นที่ไม่จำเป็นต้องขอคำยินยอม(Consent) สำหรับข้อมูลส่วนบุคคลทั่วไป(Personal Data)

- จัดทำเอกสารประวัติศาสตร์ หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ ที่เกี่ยวข้องกับ การศึกษาวิจัยหรือการจัดทำสถิติ
- เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล
- จำเป็นเพื่อปฏิบัติตามสัญญากับเจ้าของข้อมูล เช่น การซื้อขายของออนไลน์ ต้องใช้ชื่อ ที่อยู่ เบอร์โทรศัพท์ อีเมล
- จำเป็นเพื่อประโยชน์สาธารณะ และการปฏิบัติหน้าที่ในการใช้อำนาจรัฐ
- จำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือของบุคคลอื่น
- เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล เช่น ส่งข้อมูลพนักงานให้กรมสรรพากรเรื่องภาษี เป็นต้น

ข้อยกเว้นที่ไม่จำเป็นต้องขอคำยินยอม(Consent) สำหรับข้อมูลส่วนบุคคลที่อ่อนไหว(Sensitive Personal Data)

- เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล
- การดำเนินกิจกรรมที่ชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของ มูลนิธิ สมาคม องค์กรไม่แสวงหากำไร เช่น เรื่องศาสนาหรือความคิดเห็นทางการเมือง ซึ่งจำเป็นต้องเปิดเผยให้ทราบก่อนเข้าองค์กรนั้น ๆ เป็นต้น
- เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล เช่น บุคคลสาธารณะที่มีข้อมูลที่เปิดเผยต่อสาธารณะอยู่แล้วในความยินยอมของเจ้าของข้อมูล
- เป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย เช่น เก็บลายนิ้วมือของผู้ที่บุกรุกเพื่อนำไปใช้ในชั้นศาล เป็นต้น
- เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์ เกี่ยวกับ
  – เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ เช่น การเก็บข้อมูลสุขภาพของพนักงานซึ่งเป็นข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Personal Data) องค์กรมักใช้ข้อนี้ในการอ้างสิทธิที่จำเป็นต้องเก็บข้อมูล

นี้ไว้ เป็นต้น

– ประโยชน์ด้านสาธารณะสุข, การคุ้มครองแรงงาน, การประกันสังคม, หลักประกันสุขภาพแห่งชาติ

– การศึกษาวิจัยทางวิทยาศาสตร์, ประวัติศาสตร์, สถิติ, หรือประโยชน์สาธารณะอื่น

– ประโยชน์สาธารณะที่สำคัญ

หากท่านใดมีโอกาสได้อ่านเนื้อหา พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (PDPA) ฉบับเต็มแล้ว จะสังเกตได้ว่ากฎหมายฉบับนี้ได้ให้ความสำคัญต่อการจัดการและให้ความคุ้มครองกับ ข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Personal Data) เป็นพิเศษ มากกว่าข้อมูลส่วนบุคคลทั่วไป(Personal Data)อาจด้วยเหตุผลที่ว่าหากข้อมูลส่วนบุคคลที่อ่อนไหวมีการรั่วไหลต่อสาธารณชนไปแล้ว ย่อมจะส่งผลต่อสิทธิเสรีภาพของบุคคลได้มากกว่า เช่น สิทธิเสรีภาพในความคิด ความเชื่อทางศาสนา การแสดงออก การชุมนุม สิทธิในชีวิตร่างกาย การอยู่อาศัย การไม่ถูกเลือกปฏิบัติ ซึ่งอาจจะก่อให้เกิดการแทรกแซงซึ่งสิทธิเสรีภาพและการเลือกปฏิบัติต่อการใช้สิทธิเสรีภาพของบุคคลได้มากกว่าข้อมูลส่วนบุคคลทั่วไป ดังนั้นบทลงโทษต่อผู้ละเมิดอันเกี่ยวเนื่องกับข้อมูลส่วนบุคคลที่อ่อนไหวจึงมีบทลงโทษที่สูงกว่าตามไปด้วย

บทลงโทษใน พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (PDPA) ได้แก่

- **โทษทางแพ่ง** โทษทางแพ่งกำหนดให้ชดใช้ค่าสินไหมทดแทนที่เกิดขึ้นจริงให้กับเจ้าของข้อมูลส่วนบุคคลที่ได้รับความเสียหายจากการละเมิด และอาจจะต้องจ่ายบวกเพิ่มอีกเป็นค่าสินไหมทดแทนเพื่อการลงโทษเพิ่มเติมสูงสุดได้อีก 2 เท่าของค่าเสียหายจริง ตัวอย่าง หากศาลตัดสินว่าให้ผู้ควบคุมข้อมูลส่วนบุคคล ต้อง

ชดใช้ค่าสินไหมทดแทนแก่เจ้าของข้อมูลส่วนบุคคล เป็นจำนวน 1 แสนบาท ศาลอาจมีคำสั่งกำหนดค่าสินไหมเพื่อการลงโทษเพิ่มอีก 2 เท่าของค่าเสียหายจริง เท่ากับว่าจะต้องจ่ายเป็นค่าปรับทั้งหมด เป็นจำนวนเงิน 3 แสนบาท

- **โทษทางอาญา** โทษทางอาญาจะมีทั้งโทษจำคุกและโทษปรับ โดยมี โทษจำคุกสูงสุดไม่เกิน 1 ปี หรือ ปรับไม่เกิน 1 ล้านบาท หรือทั้งจำทั้งปรับ โดยโทษสูงสุดดังกล่าวจะเกิดจากการไม่ปฏิบัติตาม PDPA ในส่วนการใช้ข้อมูล หรือเปิดเผยข้อมูล หรือส่งโอนข้อมูลไปยังต่างประเทศ ประเภทข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Personal Data) ส่วนกรณีหากผู้กระทำความผิด คือ บริษัท(นิติบุคคล) ก็อาจจะสงสัยว่าใครจะเป็นผู้ถูกจำคุก เพราะบริษัทติดคุกไม่ได้ ในส่วนตรงนี้ก็อาจจะตกมาที่ ผู้บริหาร, กรรมการ หรือบุคคลซึ่งรับผิดชอบในการดำเนินงานของบริษัทนั้น ๆ ที่จะต้องได้รับการลงโทษจำคุกแทน
- **โทษทางปกครอง** โทษปรับ มีตั้งแต่ 1 ล้านบาทจนถึงสูงสุดไม่เกิน 5 ล้านบาท ซึ่งโทษปรับสูงสุด 5 ล้านบาท จะเป็นกรณีของการไม่ปฏิบัติตาม PDPA ในส่วนการใช้ข้อมูล หรือเปิดเผยข้อมูล หรือส่งโอนข้อมูลไปยังต่างประเทศของประเภทข้อมูลส่วนบุคคลที่อ่อนไหว(Sensitive Personal Data) ซึ่งโทษทางปกครองนี้จะแยกต่างหากกับการชดใช้ค่าเสียหายที่เกิดจากโทษทางแพ่งและโทษทางอาญาด้วย

สรุป

ในกฎหมาย พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (PDPA) สามารถแบ่งข้อมูลส่วนบุคคลเป็น 2 ประเภท ได้แก่ **1. ข้อมูลส่วนบุคคลทั่วไป(Personal Data)** คือ ข้อมูลที่สามารถระบุไปถึงตัวบุคคลได้ไม่ว่าทางตรงหรือทางอ้อม และ **2.ข้อมูลส่วนบุคคลที่ละเอียดอ่อน(Sensitive Personal Data)** คือ ข้อมูลที่ต้องให้ความระมัดระวังเป็นพิเศษต่อการเก็บรวบรวม ใช้ หรือประมวลผล โดยกฎหมายฉบับนี้ได้ให้ความสำคัญต่อการจัดการและคุ้มครองต่อข้อมูลที่อ่อนไหวที่มากกว่าข้อมูลส่วนบุคคลทั่วไป ซึ่งโทษในกฎหมายฉบับนี้มีทั้ง **โทษทางแพ่ง โทษทางอาญา และโทษทางปกครอง**

ที่มา ข้อมูลส่วนบุคคล ข้อมูลอ่อนไหว มีอะไรบ้าง - OpenPDPA

ประกาศ เรื่อง นโยบายคุ้มครองข้อมูลส่วนบุคคล...หน่วยงาน หรือ บริษัท... ขอประกาศเจตนารมณ์ในการมุ่งมั่นปฏิบัติตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และหลักเกณฑ์หรือข้อกำหนดตามที่คณะกรรมการคุ้มครองข้อมูลส่วน บุคคลได้กำหนดมาตรการ ข้อปฏิบัติ ประกาศ หรือระเบียบปฏิบัติตามหน้าที่และอำนาจที่กฎหมายกำหนดทั้งในปัจจุบันและ อนาคต ให้ครอบคลุมผู้ที่เกี่ยวข้อง

จึงได้จัดทำนโยบายคุ้มครองข้อมูลส่วน (Personal Data Protection Policy) ฉบับนี้ขึ้นและถือเป็นส่วนหนึ่งในการแจ้งสิทธิความเป็นส่วนตัว (Privacy Notice) ให้เจ้าของข้อมูลส่วนบุคคลทราบด้วย

ข้อมูลส่วนบุคคล

1.1 ลักษณะของข้อมูลส่วนบุคคล

ในเอกสารฉบับนี้

ข้อมูลส่วนบุคคล หมายถึง ข้อมูลใด ๆ ที่เกี่ยวกับบุคคลธรรมดาที่ทำให้สามารถระบุถึงตัวบุคคลธรรมดานั้นได้ไม่ว่าทางตรงหรือทางอ้อม โดยไม่รวมถึงข้อมูลส่วนบุคคลของผู้ถึงแก่กรรม

ข้อมูลส่วนบุคคลที่มีความอ่อนไหว หมายถึง ข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ (เช่น การสแกนลายนิ้วมือ การสแกนใบหน้า เป็นต้น) หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

1.2 ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม

หน่วยงาน หรือ บริษัท อาจมีการเก็บรวบรวมข้อมูลส่วนบุคคลของท่าน ดังต่อไปนี้

ข้อมูลส่วนบุคคลทั่วไป:

- (ก) ข้อมูลส่วนตัว ได้แก่ ชื่อและนามสกุล
- (ข) ข้อมูลติดต่อ ได้แก่ ที่อยู่ หมายเลขโทรศัพท์
- (ค) ข้อมูลเกี่ยวกับการใช้งานระบบอิเล็กทรอนิกส์ ได้แก่ email และคุกกี้ (Cookies)
- (จ) ข้อมูลที่ท่านได้ให้ไว้เมื่อท่านติดต่อ หรือร่วมกิจกรรมใด ๆ กับหน่วยงาน หรือ บริษัท เป็นต้น

2. การเคารพสิทธิในความเป็นส่วนบุคคล

หน่วยงาน หรือ บริษัท เคารพสิทธิในข้อมูลส่วนบุคคลของเจ้าของข้อมูล และตระหนักดีว่าเจ้าของข้อมูล ย่อมมีความประสงค์ที่จะได้รับความมั่นคงปลอดภัยเกี่ยวกับข้อมูลของตน ข้อมูลส่วนบุคคลที่หน่วยงาน หรือ บริษัท ได้รับมา จะถูกนำไปใช้ตามวัตถุประสงค์ที่เกี่ยวข้องเท่านั้น โดยหน่วยงาน หรือ บริษัท มีมาตรการเข้มงวดในการรักษาความมั่นคงปลอดภัย ตลอดจนการป้องกันมิให้มีการนำข้อมูลส่วนบุคคลไปใช้โดยมิชอบด้วยกฎหมาย

3. การเก็บรวบรวมข้อมูลส่วนบุคคล

ในการเก็บรวบรวมข้อมูลส่วนบุคคลจากเจ้าของข้อมูลโดยตรง และการนำข้อมูลส่วนบุคคลไปใช้ รวมถึงการเปิดเผยข้อมูลส่วนบุคคล หน่วยงาน หรือ บริษัท จะขอความยินยอมจากเจ้าของข้อมูลก่อนหรือขณะทำการเก็บรวบรวม หากกฎหมายกำหนดให้ต้องขอความยินยอม และจะดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลเท่าที่จำเป็นตามวัตถุประสงค์ที่หน่วยงาน หรือ บริษัท ระบุไว้โดยแจ้งชัด

ทั้งนี้ หน่วยงาน หรือ บริษัท อาจรวบรวมข้อมูลส่วนบุคคลที่ได้รับมาจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง เช่น จากสื่อสาธารณะต่าง ๆ เฉพาะในกรณีที่มีความจำเป็นด้วยวิธีการตามที่กฎหมายกำหนด

4. วัตถุประสงค์ในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล

หน่วยงาน หรือ บริษัท เก็บรวบรวม ใช้ และเปิดเผย ข้อมูลส่วนบุคคลของท่านตามวัตถุประสงค์ดังต่อไปนี้

- เพื่อประโยชน์ในการให้หรือรับบริการในรูปแบบต่าง ๆ
- การค้นคว้า หรือการวิจัย
- เพื่อประโยชน์ในการจัดทำฐานข้อมูลสำหรับการวิเคราะห์และนำเสนอบริการ
- เพื่อประโยชน์ในการปรับปรุงคุณภาพในการดำเนินงาน การให้บริการ และการดำเนินการที่เกี่ยวข้องกับหน่วยงาน หรือ บริษัท
- เพื่อการวิเคราะห์และติดตามการใช้บริการทางเว็บไซต์ และวัตถุประสงค์ในการตรวจสอบย้อนหลังในกรณีที่เกิดปัญหาการใช้งาน
- เพื่อการเข้าร่วมกิจกรรมต่างๆ ของหน่วยงาน หรือ บริษัท
- เพื่อปฏิบัติตามกฎหมายหรือกฎระเบียบที่ใช้บังคับกับหน่วยงาน หรือ บริษัท ทั้งในปัจจุบันและ ในอนาคต

ทั้งนี้หากภายหลังมีการเปลี่ยนแปลงวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคล หน่วยงาน หรือ บริษัท จะแจ้งให้ท่านทราบ และดำเนินการอื่นใดตามที่กฎหมายกำหนด รวมถึงจัดให้มีบันทึกการแก้ไขเพิ่มเติมไว้เป็นหลักฐาน

5. ระยะเวลาในการจัดเก็บข้อมูลส่วนบุคคล

หน่วยงาน หรือ บริษัท จะเก็บรักษาข้อมูลส่วนบุคคลของท่านเป็นระยะเวลาเท่าที่จำเป็นเพื่อวัตถุประสงค์ในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลซึ่งได้ระบุไว้ในคำประกาศฉบับนี้ ตามหลักเกณฑ์ที่ใช้กำหนดระยะเวลาเก็บได้แก่ ระยะเวลาที่หน่วยงาน หรือ บริษัท ยังมีความสัมพันธ์กับท่านในฐานะผู้ติดต่อ หรือ การประสานงาน หรือตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อเหตุอื่นตามนโยบายและข้อกำหนดภายในของหน่วยงาน หรือ บริษัท

ในกรณีที่ไม่สามารถระบุระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคลได้ชัดเจน หน่วยงาน หรือ บริษัท จะเก็บรักษาข้อมูลไว้ตามระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม (เช่น อายุความตามกฎหมายทั่วไปสูงสุด 10 ปี)

6. การรักษาความมั่นคงปลอดภัย

หน่วยงาน หรือ บริษัท กำหนดให้มีมาตรการที่เหมาะสม และเข้มงวดในการรักษาความมั่นคงปลอดภัย ตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของหน่วยงาน หรือ บริษัท เพื่อป้องกันการสูญหาย การเข้าถึง ทำลาย ใช้ แปลง แก้ไขหรือมิให้มีการนำข้อมูลส่วนบุคคลไปใช้โดยไม่มีสิทธิหรือไม่ชอบด้วยกฎหมาย

7. สิทธิของท่านในฐานะเจ้าของข้อมูลส่วนบุคคล

ในฐานะที่เป็นเจ้าของข้อมูลส่วนบุคคลท่านมีสิทธิตามที่กำหนดไว้โดยพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รวมถึงสิทธิต่าง ๆ ดังนี้

- **7.1 สิทธิในการเพิกถอนความยินยอม**
  ท่านมีสิทธิในการเพิกถอนความยินยอมในการประมวลผลข้อมูลส่วนบุคคลที่ท่านได้ให้ความยินยอมกับหน่วยงาน หรือ บริษัทได้ เว้นแต่การเพิกถอนความยินยอมจะมีข้อจำกัดโดยกฎหมายหรือสัญญาที่ให้ประโยชน์แก่ท่าน ในฐานะที่ท่านเป็นเจ้าของข้อมูล

ทั้งนี้ การเพิกถอนความยินยอมจะไม่ส่งผลกระทบต่อการประมวลผลข้อมูลส่วนบุคคลที่ท่าน ได้ให้ความยินยอมไปแล้วโดยชอบด้วยกฎหมาย

- **7.2 สิทธิในการขอเข้าถึงข้อมูลส่วนบุคคล**
  ท่านมีสิทธิขอเข้าถึงและขอรับสำเนาข้อมูลของท่านซึ่งอยู่ในความรับผิดชอบของหน่วยงาน หรือ บริษัท รวมถึงขอให้หน่วยงาน หรือ บริษัท เปิดเผยการได้มาซึ่งข้อมูลดังกล่าวที่ท่านไม่ได้ให้ความยินยอมต่อหน่วยงานได้

- **7.3 สิทธิในการขอให้ส่งหรือโอนข้อมูลส่วนบุคคล**
  ท่านมีสิทธิขอให้หน่วยงาน หรือ บริษัท โอนข้อมูลส่วนบุคคลของท่านที่ท่านให้ไว้กับหน่วยงานได้ตามที่กฎหมายกำหนด

- **7.4 สิทธิในการคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล**
  ท่านมีสิทธิในการคัดค้านการประมวลผลข้อมูลที่เกี่ยวกับท่านสำหรับกรณีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับตนได้ตามที่กฎหมายกำหนด

- **7.5 สิทธิในการขอลบข้อมูลส่วนบุคคล**
  ท่านมีสิทธิขอให้หน่วยงาน หรือ บริษัท ลบหรือทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวตนได้ตามที่กฎหมายกำหนด

- **7.6 สิทธิในการขอให้ระงับการใช้ข้อมูลส่วนบุคคล**
  ท่านมีสิทธิขอให้หน่วยงาน หรือ บริษัท ระงับการใช้ข้อมูลของท่านได้ตามที่กฎหมายกำหนด

- **7.7 สิทธิในการขอแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง**
  กรณีที่ท่านเห็นว่าข้อมูลที่หน่วยงาน มีอยู่นั้นไม่ถูกต้องหรือท่านมีการเปลี่ยนแปลงข้อมูลส่วนบุคคลของท่านเอง ท่านมีสิทธิขอให้หน่วยงาน หรือ บริษัท แก้ไขข้อมูลส่วนบุคคลของท่านเพื่อให้ข้อมูลส่วนบุคคลดังกล่าวถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด

- **7.8 สิทธิในการรับทราบกรณีมีการแก้ไขเปลี่ยนแปลงแบบแจ้งเกี่ยวกับข้อมูลส่วนบุคคลของท่าน**
  หน่วยงาน หรือ บริษัท อาจมีการพิจารณาทบทวนและแก้ไขเปลี่ยนแปลงแบบแจ้งนี้ตามความเหมาะสม ในบางครั้งเพื่อให้แน่ใจว่าข้อมูลส่วนบุคคลของท่านจะได้รับความคุ้มครองอย่างเหมาะสม

- **7.9 สิทธิในการร้องเรียน**

  ท่านมีสิทธิในการร้องเรียนต่อพนักงานเจ้าหน้าที่ผู้มีอำนาจตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หากหน่วยงาน หรือ บริษัท ฝ่าฝืนหรือไม่ปฏิบัติตามพระราชบัญญัติดังกล่าวได้ ในกรณีที่เจ้าของข้อมูลส่วนบุคคลยื่นคำร้องขอใช้สิทธิภายใต้บทบัญญัติของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เมื่อหน่วยงาน หรือ บริษัท ได้รับคำร้องขอดังกล่าวแล้ว จะดำเนินการภายในระยะเวลาที่กฎหมายกำหนด อนึ่ง หน่วยงาน หรือ บริษัท สงวนสิทธิที่จะปฏิเสธหรือไม่ดำเนินการตามคำร้องขอดังกล่าวได้ในกรณีที่กฎหมายกำหนด ในกรณีที่เจ้าของข้อมูลมีข้อจำกัดโดยเลือกที่จะให้ข้อมูลส่วนบุคคลเฉพาะอย่าง อาจส่งผลให้ ไม่สามารถได้รับบริการจากหน่วยงาน หรือ บริษัท ได้อย่างเต็มที่ รวมทั้งหน่วยงาน หรือ บริษัท อาจจะไม่สามารถทำงานร่วมกับเจ้าของข้อมูลส่วนบุคคลหรือให้บริการใด ๆ ได้ หากเจ้าของข้อมูลส่วนบุคคลไม่ยินยอมให้ข้อมูลที่หน่วยงาน หรือ บริษัท ต้องการ

8. การเปิดเผยข้อมูลส่วนบุคคลกับบุคคลอื่นหรือหน่วยงานอื่น

หน่วยงาน หรือ บริษัท อาจมีความจำเป็นในการเปิดเผยข้อมูลส่วนบุคคลให้แก่หน่วยงาน หรือ บริษัท ในกลุ่ม หรือบุคคลหรือหน่วยงานอื่นที่เป็นพันธมิตรซึ่งทำงานร่วมกับหน่วยงาน หรือ บริษัท ในการให้บริการในรูปแบบต่าง ๆ หรือตามความจำเป็นตามสมควรในการบังคับใช้ข้อกำหนดและเงื่อนไขของหน่วยงาน หรือ บริษัท หรือกรณีที่มีการปรับโครงสร้างองค์กร การควบรวมหน่วยงาน หรือ บริษัท และอาจมีการเปิดเผยข้อมูลส่วนบุคคลให้กับหน่วยงานราชการหรือหน่วยงานภาครัฐตามข้อบังคับของกฎหมายหรือตามคำสั่งศาลหรือตามคำสั่งเจ้าหน้าที่ผู้มีอำนาจ โดยข้อมูลส่วนบุคคลจะได้รับการเก็บรักษาเป็นความลับ ทั้งในรูปเอกสารและข้อมูลอิเล็กทรอนิกส์ รวมทั้งในระหว่างการส่งผ่านข้อมูลทุกขั้นตอน

9. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

หน่วยงาน หรือ บริษัท ได้มีการดำเนินการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยมีเจ้าหน้าที่เพื่อตรวจสอบการดำเนินการของบริษัทที่เกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รวมถึงกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

10. วิธีการติดต่อ

ในกรณีที่มีข้อสงสัยหรือต้องการสอบถามรายละเอียดเพิ่มเติมเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของท่าน โปรดติดต่อหน่วยงาน หรือ บริษัท ได้ตามช่องทางดังต่อไปนี้

ชื่อหน่วยงาน

สถานที่ติดต่อ: ...

เบอร์โทรศัพท์: ...

11. การเปลี่ยนแปลงนโยบายและแนวปฏิบัติคุ้มครองข้อมูลส่วนบุคคล

หน่วยงาน หรือ บริษัท จะทำการพิจารณาทบทวนเงื่อนไขนโยบายหน่วยงาน หรือ บริษัท ฉบับนี้เป็นครั้งคราว เพื่อให้สอดคล้องกับแนวปฏิบัติ และกฎหมายที่เกี่ยวข้อง หากมีการแก้ไขเปลี่ยนแปลงหน่วยงาน หรือ บริษัท จะแจ้งให้ทราบด้วยการเผยแพร่ผ่านการประกาศที่เหมาะสมของหน่วยงาน หรือ บริษัท (Personal Data Protection Policy)

ที่มาhttps://www.cbo.moph.go.th/cbonew/index.php/%E0%B9%81%E0%B8%9A%E0%B8%9A%E0%B9%80%E0%B8%99%E0%B8%B7%E0%B9%89%E0%B8%AD%E0%B8%AB%E0%B8%B2-2/5

รู้จัก กฎหมาย PDPA พรบ.คุ้มครองข้อมูลที่องค์กรควรรู้

ในยุคที่คนส่วนใหญ่ เริ่มหันมาให้ความสำคัญกับข้อมูลส่วนตัวมากขึ้น ทำให้องค์กรต่าง ๆ ต้องเข้มงวดกับการคุ้มครองข้อมูลพนักงาน เพราะเป็นสิ่งที่สะท้อนถึงความรับผิดชอบขององค์กร ในบทความนี้ Cloud-TA จะพาทุกคนไปทำความรู้จัก กฎหมาย PDPA กฎหมายสำคัญ ที่คอยปกป้องข้อมูลส่วนบุคคลของแรงงาน เพื่อจัดการข้อมูลให้ปลอดภัย และหลีกเลี่ยงการทำผิดกฎหมาย หากพร้อมแล้ว เราไปดูกัน

ทำความรู้จัก กฎหมาย PDPA คืออะไร?

กฎหมาย PDPA หรือพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นกฎหมายที่ปกป้องข้อมูลส่วนบุคคลของแรงงาน โดยกำหนดให้นายจ้าง ต้องขอความยินยอมในการเก็บ ใช้ หรือเปิดเผยข้อมูลจากพนักงาน พร้อมกับจัดการข้อมูลอย่างปลอดภัย

ซึ่งจุดประสงค์หลักของ PDPA คือ การป้องกันไม่ให้องค์กร นำข้อมูลส่วนตัวของพนักงานไปใช้ในกิจกรรมอื่น โดยที่เจ้าของข้อมูลไม่ยินยอม หรือทำข้อมูลหลุดออกไป รวมถึงมีการเยียวยา และบทลงโทษทางกฎหมาย หากเกิดเหตุละเมิด เช่น ปรับสูงสุดไม่เกิน 5 ล้านบาท โดยข้อมูลที่ควรระมัดระวัง มีดังนี้

- **ข้อมูลส่วนบุคคล**

ข้อมูลส่วนบุคคล หรือข้อมูลทั่วไป (Personal Data) คือ ข้อมูลที่สามารถระบุตัวบุคคลนั้นได้ ทั้งในทางตรง และทางอ้อม แต่จะไม่รวมถึงข้อมูลของผู้เสียชีวิต หรือข้อมูลของนิติบุคคล ซึ่งทางแผนก HR ของแต่ละบริษัท ต้องจัดเก็บข้อมูลส่วนบุคคลให้ดี และขอความยินยอมจากพนักงานก่อนเสมอ ไม่ว่าจะเป็น

- ชื่อ – นามสกุล หรือชื่อเล่น
- เลขประจำตัวประชาชน, เลขหนังสือเดินทาง, เลขบัตรประกันสังคม, เลขใบอนุญาตขับขี่, เลขประจำตัวผู้เสียภาษี, เลขบัญชีธนาคาร และเลขบัตรเครดิต
- ที่อยู่, อีเมล และหมายเลขโทรศัพท์
- ข้อมูลอุปกรณ์อิเล็กทรอนิกส์ เช่น IP address, MAC Address และ Cookie ID
- ข้อมูลระบุทรัพย์สินของบุคคล
- ข้อมูลที่สามารถเชื่อมโยงไปยังข้อมูลส่วนตัว เช่น วันเดือนปีเกิด, เชื้อชาติ, สัญชาติ และข้อมูลตำแหน่งที่อยู่
- ข้อมูลหมายเลขอ้างอิง ที่เก็บไว้ในไมโครฟิล์ม
- ข้อมูลการประเมินผลการทำงาน
- ข้อมูลบันทึก ที่ใช้ติดตามตรวจสอบกิจกรรมต่าง ๆ ของบุคคล
- ข้อมูลที่สามารถใช้ในการค้นหาข้อมูลส่วนบุคคลอื่น ในอินเทอร์เน็ต

- **ข้อมูลส่วนบุคคลที่อ่อนไหว**

ในส่วนของข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Personal Data) เป็นข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนและสุ่มเสี่ยงต่อการถูกใช้ ในการเลือกปฏิบัติอย่างไม่เป็นธรรมภายในองค์กร ดังนั้น HR ต้องระมัดระวังข้อมูลในส่วนนี้เป็นพิเศษ ไม่ว่าจะเป็น

- เชื้อชาติ
- ความคิดเห็นทางการเมือง
- ความเชื่อทางศาสนา
- พฤติกรรมทางเพศ
- ประวัติอาชญากรรม
- ข้อมูลสุขภาพ ความพิการ และข้อมูลสุขภาพจิต
- ข้อมูลสหภาพแรงงาน
- ข้อมูลทางชีวมิติ (Biometric) เช่น ลายนิ้วมือ, รูปภาพใบหน้า และข้อมูลพันธุกรรม
- **ข้อมูลที่ไม่จำเป็นต้องขอความยินยอม**

แม้ว่าทางบริษัท จะต้องมีการเก็บข้อมูลส่วนตัว และต้องได้รับคำยินยอม (Consent) จากเจ้าของข้อมูลอยู่เสมอ เมื่อต้องการนำข้อมูลไปใช้ แต่ในพรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้มีการระบุข้อยกเว้น ที่ไม่จำเป็นต้องขอความยินยอมไว้ในมาตรา 24, 26 และ 27 โดยสรุปข้อยกเว้นไว้ ดังนี้

- กรณีที่ต้องป้องกัน หรือระงับเหตุอันตรายต่อชีวิต
- การดำเนินกิจกรรมโดยชอบ ด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสม
- ใช้สิทธิเรียกร้องตามกฎหมาย
- การรักษาทางการแพทย์
- การประเมินขีดความสามารถในการทำงาน

บทลงโทษใน พรบ.คุ้มครองข้อมูลส่วนบุคคล ที่ HR ต้องรู้

ในกรณีที่บริษัทเปิดเผยข้อมูลส่วนตัวของพนักงาน และเจ้าของข้อมูลส่วนบุคคลได้ร้องขอตามสิทธิ PDPA แล้ว แต่ทางบริษัท และฝ่าย HR ยังคงเพิกเฉย เจ้าของข้อมูลสามารถดำเนินตามกฎหมาย เพื่อให้ทางองค์กรได้รับบทลงโทษได้ 3 ส่วน ได้แก่ โทษทางแพ่ง โทษทางอาญา และโทษทางปกครอง โดยมีรายละเอียด ดังนี้

- **โทษทางแพ่ง**

หากบริษัททำให้พนักงานเสียหาย จากการที่ข้อมูลส่วนตัวถูกเผยแพร่ โทษทางแพ่ง ได้กำหนดให้ชดใช้ค่าสินไหมทดแทนที่เกิดขึ้นจริง ให้กับเจ้าของข้อมูลส่วนบุคคล และอาจต้องจ่ายบวกเพิ่มอีก เป็นค่าสินไหมทดแทน จากการลงโทษเพิ่มเติมสูงสุดได้อีก 2 เท่าของค่าเสียหายจริง

โดยบทลงโทษทางแพ่งของ PDPA มีอายุความ 3 ปี นับแต่วันที่ผู้เสียหาย รู้ถึงความเสียหาย และรู้ตัวผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ เว้นแต่จะพิสูจน์ได้ว่า เหตุการณ์ที่เกิดขึ้นนั้น เป็นเหตุสุดวิสัย หรือเป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ ซึ่งปฏิบัติการตามหน้าที่ และอำนาจตามกฎหมาย

- **โทษทางอาญา**

การละเมิดสิทธิ PDPA ที่เข้าข่ายผิดกฎหมายอาญา มักเป็นการใช้ข้อมูล หรือเปิดเผยข้อมูล และส่งโอนข้อมูลไปยังต่างประเทศ รวมถึงละเมิดข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Personal Data) โดยบทลงโทษ PDPA ทางอาญามีทั้งโทษจำคุก และโทษปรับ โดยมีโทษจำคุกสูงสุดไม่เกิน 1 ปี หรือปรับไม่เกิน 1 ล้านบาท หรือทั้งจำทั้งปรับ

- **โทษทางปกครอง**

สำหรับโทษทางปกครอง จะเป็นกรณีของการไม่ปฏิบัติตาม PDPA ในส่วนของการใช้ข้อมูล การเปิดเผยข้อมูล และส่งข้อมูลไปยังต่างประเทศ ซึ่งจะเป็นโทษที่แยกออกมา จากการชดใช้ค่าเสียหายของโทษทางแพ่ง และโทษทางอาญาอีกด้วย ซึ่งโทษปรับจะมีตั้งแต่ 1 ล้านบาท สูงสุดไม่เกิน 5 ล้านบาท

สำหรับผู้ประกอบการ หรือเจ้าของบริษัท ที่กำลังมองหาเครื่องมือในการจัดการข้อมูลส่วนตัวของพนักงาน และเอกสารสำคัญขององค์กรให้ปลอดภัย เพื่อไม่ให้ละเมิดPDPA และ**กฎหมายแรงงาน**บางส่วน ขอแนะนำ **Cloud-TA** เพราะระบบของเรา จัดเก็บข้อมูลอย่างปลอดภัย บนระบบคลาวด์ของไมโครซอฟต์ (Microsoft Azure) มั่นใจได้เลยว่าข้อมูลทั้งหมดจะถูกรักษาไว้อย่างปลอดภัยแน่นอน

เรื่องต้องรู้ ! กฎหมาย PDPA เกี่ยวข้องกับแผนกอะไรบ้าง

PDPA ไม่ได้เป็นเรื่องของ HR และพนักงานแต่ละคนเท่านั้น เนื่องจาก ภายในองค์กร มีการจัดเก็บข้อมูลส่วนบุคคลหลากหลายรูปแบบ ไม่ว่าจะเป็น ข้อมูลของลูกค้า พนักงานบริษัท บริษัทคู่ค้า และผู้สมัครงาน ด้วยเหตุนี้ พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จึงมีความเกี่ยวข้องกับหลายแผนกในองค์กร ไม่ว่าจะเป็น

- **แผนกฝ่ายบุคคล (HR)**

แผนกฝ่ายบุคคล (HR) เป็นตำแหน่งที่คอยสรรหา และคัดเลือกบุคลากร รวมถึงดูแลเรื่องเงินเดือน และสวัสดิการพนักงานในบริษัท ทำให้ HR ต้องคลุกคลีกับเอกสารข้อมูลส่วนบุคคล ทั้งของผู้สมัครงานกับบริษัท และพนักงานในองค์กร ทั้งยังมีข้อมูลสุขภาพที่เกี่ยวข้องของพนักงานแต่ละคนอีกด้วย

- **แผนกเทคโนโลยีสารสนเทศ (IT)**

อีกหนึ่งแผนกที่มีส่วนเกี่ยวข้องกับ PDPA โดยตรง คือ แผนกเทคโนโลยีสารสนเทศ (IT) เพราะต้องจัดทำระบบการจัดเก็บข้อมูล และมาตรการรักษาความปลอดภัยของข้อมูล รวมถึงออกแบบ UX/UI ของเว็บไซต์ และแอปพลิเคชันให้สอดคล้องตาม กฎหมาย PDPA

- **แผนกการตลาด และแผนกบริการลูกค้า**

สำหรับฝ่ายการตลาด และฝ่ายบริการลูกค้า ก็มีส่วนเกี่ยวข้องกับ PDPA ในส่วนของการเก็บ และใช้ข้อมูลส่วนบุคคลของลูกค้า เพื่อนำข้อมูลที่ได้ไปพัฒนาสินค้า หรือคอนเทนต์ต่าง ๆ ให้ตรงกับกลุ่มเป้าหมาย และกระตุ้นยอดขายให้เพิ่มขึ้นในทุกแคมเปญ

- **แผนกบัญชี**

แผนกบัญชี มีหน้าที่คอยรับเงิน เก็บเงิน และนำเงินฝากธนาคาร รวมถึงตรวจสอบความถูกต้อง และจัดทำรายงานทางการเงินในแต่ละเดือน ทำให้เจ้าหน้าที่บัญชีประจำองค์กร มีส่วนเกี่ยวข้องกับ PDPA ในเรื่องของการจัดเก็บข้อมูลส่วนบุคคลของลูกค้า เช่น บัญชีธนาคาร, เอกสารยืนยันตัวตน และเอกสารลับทางธุรกิจ เป็นต้น

- **แผนกกฎหมาย**

ปิดท้ายกันด้วย แผนกกฎหมาย ถือเป็นแผนกที่มีส่วนเกี่ยวข้องกับ PDPA โดยตรง เพราะต้องคอยตรวจสอบการดำเนินงานขององค์กร ให้สอดคล้องกับกฎหมาย โดยเฉพาะ**กฎหมายแรงงาน** รวมถึงดำเนินการ ด้านงานคดี ทั้งในคดีแพ่ง คดีอาญา และคดีทางปกครอง

ที่มา รู้จัก กฎหมาย PDPA พรบ.คุ้มครองข้อมูลที่องค์กรควรรู้

สรุป PDPA คืออะไร ฉบับเข้าใจง่าย พร้อมแนะแนว

PDPA คือ อะไร ?

PDPA คือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ซึ่งเป็นกฎหมายที่ถูกสร้างมาเพื่อป้องกันการละเมิดข้อมูลส่วนบุคคลของทุกคน รวมถึงการจัดเก็บข้อมูลและนำไปใช้โดยไม่ได้แจ้งให้ทราบ และไม่ได้รับความยินยอมจากเจ้าของข้อมูลเสียก่อน

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act: PDPA) คือกฎหมายใหม่ที่ออกมาเพื่อแก้ไขปัญหาการถูกล่วงละเมิดข้อมูลส่วนบุคคลที่เพิ่มมากขึ้นเรื่อย ๆ ในปัจจุบัน เช่น การซื้อขายข้อมูลเบอร์โทรศัพท์และข้อมูลส่วนตัวอื่น ๆ โดยที่เจ้าของข้อมูลไม่ยินยอม ที่มักพบได้มากในรูปแบบการโทรมาโฆษณา หรือล่อลวง

โดยกฎหมายนี้ได้เริ่มบังคับใช้อย่างเต็มรูปแบบเมื่อวันที่ 1 มิ.ย. 2565 เป็นกฎหมายที่ให้ความคุ้มครองข้อมูลส่วนบุคคล เช่น ชื่อ ที่อยู่ เบอร์โทรศัพท์ รูปถ่าย บัญชีธนาคาร อีเมล ไอดีไลน์ บัญชีผู้ใช้ของเว็บไซต์ ลายนิ้วมือ ประวัติสุขภาพ เป็นต้น ซึ่งข้อมูลเหล่านี้สามารถระบุถึงตัวเจ้าของข้อมูลนั้นได้ อาจเป็นได้ทั้งข้อมูลในรูปแบบเอกสาร กระดาษ หนังสือ หรือจัดเก็บในรูปแบบอิเล็กทรอนิกส์ก็ได้

PDPA มีความเป็นมาอย่างไร ?

กฎหมาย PDPA เรียกได้ว่าถอดแบบมาจากกฎหมายต้นแบบอย่างกฎหมาย GDPR (General Data Protection Regulation) ซึ่งเป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป วัตถุประสงค์ของการเก็บรักษาข้อมูลส่วนบุคคลของกฎหมายทั้ง 2 ฉบับ ก็เพื่อป้องกันไม่ให้ผู้ไม่ประสงค์ดีทำการแฮ็กข้อมูลหรือละเมิดความเป็นส่วนตัวเพื่อข่มขู่หวังผลประโยชน์จากทั้งจากตัวเจ้าของข้อมูลเองหรือจากบุคคลที่ดูแลข้อมูล

PDPA สำคัญอย่างไร ?

ความสำคัญของ PDPA คือการทำให้เจ้าของข้อมูลมีสิทธิในข้อมูลส่วนตัวที่ถูกจัดเก็บไปแล้ว หรือกำลังจะถูกจัดเก็บมากขึ้น เพื่อสร้างความปลอดภัยและเป็นส่วนตัวให้แก่เจ้าของข้อมูล โดยมีสิทธิที่สำคัญคือ สิทธิการรับทราบและยินยอมการเก็บข้อมูลส่วนตัว และสิทธิในการขอเข้าถึงข้อมูลส่วนตัว คัดค้านและเพิกถอนการเก็บและนำข้อมูลไปใช้ และสิทธิขอให้ลบหรือทำลายข้อมูลส่วนตัว

สิทธิที่เพิ่มขึ้นของเจ้าของข้อมูล ทำให้ผู้ประกอบการขององค์กรและบริษัทต่าง ๆ ต้องปรับเปลี่ยนกระบวนการเก็บรวบรวมและนำข้อมูลส่วนตัวของเจ้าของข้อมูลไม่ว่าจะเป็นลูกค้า พนักงานในองค์กร หรือบุคคลใด ๆ ที่เกี่ยวข้องให้เป็นไปตามหลักปฏิบัติของ PDPA พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

โดยหากคุณเป็นผู้ประกอบการ หรือเป็นตัวแทนองค์กรที่ดำเนินการเรื่อง PDPA วันนี้เราจะช่วยคุณเปลี่ยนแนวทางการดำเนินงานเพื่อให้สอดคล้องกับกฎหมาย PDPA กัน

หากคุณต้องการเก็บรวบรวมข้อมูล ประมวลผลข้อมูล นำข้อมูลไปใช้ รวมถึงการเก็บรักษาและดูแลความปลอดภัยของข้อมูลส่วนบุคคลของลูกค้าและบุคคลที่เกี่ยวข้อง คุณจะต้องดำเนินการตามขั้นตอนต่อไปนี้โดยด่วน เพราะในขณะนี้ประเทศไทยได้เริ่มบังคับใช้ พ.ร.บ. PDPA แล้ว หากคุณไม่ดำเนินการตามหลักของ PDPA คุณอาจต้องรับโทษร้ายแรงทั้งทางแพ่ง อาญา และปกครอง

องค์ประกอบสำคัญของ PDPA

บุคคลที่ต้องปฏิบัติตามกฎหมาย PDPA ประกอบด้วย เจ้าของข้อมูลส่วนบุคคล (Data Subject) และผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) โดยผู้ควบคุมข้อมูลส่วนบุคคลนั้นเปรียบเสมือนผู้ดูแลระบบ เป็นฝ่ายปฏิบัติงาน มีหน้าที่เก็บรวบรวม และนำข้อมูลส่วนบุคคลที่ขอความยินยอม (Consent) จากเจ้าของข้อมูลไปใช้ ยกตัวอย่างเช่น เว็บไซต์ขายของออนไลน์ ตัวผู้จัดทำเว็บไซต์ก็จะต้องขอข้อมูลทั้งชื่อ ที่อยู่ เบอร์โทรศัพท์ ข้อมูลการจ่ายเงิน เพื่อนำไปดำเนินการสั่งซื้อและจัดส่งสินค้าไปยังที่อยู่ของเจ้าของข้อมูล ซึ่ง PDPA เมื่อได้ข้อมูลมาแล้ว ก็ต้องจัดให้มีมาตรการรักษาความปลอดภัยข้อมูลด้วย

ขั้นตอนการทำตาม PDPA ต้องทำอย่างไร ?

STEP 1 การเก็บรวบรวมข้อมูลส่วนบุคคล

1. จัดทำ Privacy Policy แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ

องค์กรหรือเจ้าของเว็บไซต์สามารถแจ้งเจ้าของข้อมูลผ่าน Privacy Policy บนเว็บไซต์หรือแอปพลิเคชัน หรือช่องทางการติดต่ออื่น ๆ เช่น การลงทะเบียนผ่านเว็บไซต์ หรือทางโซเชียลมีเดีย

- แจ้งว่าจะขอเก็บข้อมูลอะไรบ้าง เพื่อวัตถุประสงค์ใด
- แจ้งสิทธิของเจ้าของข้อมูล โดยสามารถถอนความยินยอมได้ทุกเมื่อ

- ข้อความอ่านเข้าใจง่าย ชัดเจน ใช้ภาษาไม่กำกวม ไม่มีเงื่อนไขในการยินยอม คลิก PDPA Pro เพื่อสร้าง Privacy Policy ที่ถูกต้องตาม PDPA

2. การจัดการเว็บไซต์ แอปพลิเคชัน และ Third-party

นอกจากการจัดทำ Privacy Policy ผ่านเว็บไซต์หรือแอปพลิเคชันแล้ว การขอจัดเก็บ Cookie ก็จะต้องแจ้งเพื่อขอความยินยอมให้ใช้ข้อมูลส่วนบุคคลจากผู้ใช้งานด้วย ซึ่งที่เราพบเห็นได้ทั่วไป มักแจ้งขอเก็บ Cookie เป็น Pop up เล็ก ๆ ทางด้านล่างเว็บไซต์ คลิก Cookie Wow เพื่อจัดทำ Cookie Consent Banner เพียงไม่กี่นาที ส่วน Third Party ที่เก็บข้อมูลส่วนบุคคล เช่น เว็บไซต์โฆษณาที่ทำการตลาด ก็ต้องระบุวัตถุประสงค์และขอความยินยอมการเก็บรวบรวมข้อมูลไว้ใน Privacy Policy ด้วย

3. การเก็บข้อมูลพนักงาน

สำหรับการเก็บข้อมูลส่วนบุคคลของพนักงานนั้นก็ต้องจัดทำนโยบายความเป็นส่วนตัวสำหรับพนักงานหรือ HR Privacy Policy เพื่อแจ้งวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลของพนักงานเช่นเดียวกัน แนะนำว่าสำหรับพนักงานเก่า ให้แจ้ง Privacy Policy เป็นเอกสารใหม่ ส่วนพนักงานใหม่ ให้แจ้งในใบสมัคร 1 ครั้ง และแจ้งในสัญญาจ้าง 1 ครั้ง คลิก PDPA Pro เพื่อสร้าง Privacy Policy สร้าง HR Privacy Policy ถูกต้องตาม PDPA

STEP 2 การใช้หรือประมวลผลข้อมูลส่วนบุคคล

แต่ละฝ่ายในองค์กรควรร่วมกำหนดแนวทางหรือนโยบายในการดำเนินการด้านข้อมูลส่วนบุคคล (Standard Operating Procedure) และบันทึกรายการข้อมูลส่วนบุคคลที่มีการเก็บหรือใช้ (Records of Processing Activity: ROPA) ทั้งข้อมูลที่จัดเก็บในฐานข้อมูลอิเล็กทรอนิกส์ ข้อมูลเอกสารที่จับต้องได้ ข้อมูลส่วนบุคคลทั่วไป ข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Personal Data) ซึ่งเป็นข้อมูลที่ระบุตัวบุคคลได้เฉพาะเจาะจงมากขึ้น เช่น เชื้อชาติ ความคิดเห็นทางการเมือง ศาสนา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ (face ID, ลายนิ้วมือ) รวมถึงห้ามเปิดเผยข้อมูลส่วนบุคคลให้กับบุคคลที่ไม่มีความรับผิดชอบโดยตรง

สิ่งที่ควรทำ

- แอด Line เจ้าของข้อมูลส่วนบุคคล หลังจากขออนุญาตแล้ว
- ส่ง Direct Marketing ให้ลูกค้าหลังจากที่ลูกค้ายินยอมแล้ว

- ส่งข้อมูลลูกค้าจาก Cookie ไป Target Advertising ต่อ หลังจากที่ลูกค้ายินยอมแล้ว
- ส่งข้อมูลให้ Vendor หลังจากบริษัทได้ทำความตกลงกับ Vendor ที่มีข้อกำหนดเรื่องความคุ้มครองข้อมูลส่วนบุคคลแล้ว
- การให้บริการที่ต้องวิเคราะห์ข้อมูลส่วนบุคคลจำนวนมากหรือใช้ Sensitive Personal Data เช่น การสแกนใบหน้า จะต้องขอความยินยอมก่อน
- รวบรวมสถิติลูกค้าเพื่อพัฒนาบริการ โดยไม่ใช้ข้อมูลส่วนบุคคลของลูกค้า

STEP 3 มาตรการด้านความปลอดภัยของข้อมูลส่วนบุคคล

- กำหนดแนวทางอย่างน้อยตามมาตรฐานขั้นต่ำด้านการรักษาความปลอดภัยข้อมูลส่วนบุคคล (Minimum Security Requirements) ได้แก่ การรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ซึ่งควรครอบคลุมถึงมาตรการป้องกันด้านการบริหารจัดการ (Administrative Safeguard) มาตรการป้องกันด้านเทคนิค (Technical Safeguard) และมาตรการป้องกันทางกายภาพ (Physical Safeguard) ในเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล (Access Control) ตามประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
- กำหนดนโยบายรักษาระยะเวลาการเก็บข้อมูล และการทำลายเอกสารที่มีข้อมูลส่วนบุคคล (Data Retention)
- มีกระบวนการ Breach Notification Protocol ซึ่งเป็นระบบแจ้งเตือนเพื่อปกป้องข้อมูลจากการโจมตีจากผู้ไม่หวังดี

STEP 4 การส่งหรือเปิดเผยข้อมูลส่วนบุคคล

- ทำสัญญาหรือข้อตกลงกับผู้ให้บริการภายนอก หรือทำ Data Processing Agreement เพื่อคุ้มครองข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานกฎหมาย PDPA
- ในกรณีโอนข้อมูลไปต่างประเทศ ให้ทำสัญญากับบริษัทปลายทางเพื่อคุ้มครองข้อมูลตามมาตรฐาน PDPA
- มีกระบวนการรับคำร้องจากเจ้าของข้อมูลส่วนบุคคล ควรเป็นวิธีที่ง่ายไม่ซับซ้อน และไม่กำหนดเงื่อนไข อาจผ่านการยื่นแบบฟอร์ม ส่งคำร้องผ่านช่อง Chat หรือส่งอีเมลก็ได้

STEP 5 การกำกับดูแลข้อมูลส่วนบุคคล

ในประเทศไทย มีสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ซึ่งเป็นหน่วยงานภาครัฐเป็นผู้กำกับดูแลกฎหมาย PDPA ให้แต่ละองค์กรต้องปฏิบัติตาม โดยองค์กรที่ทำการเก็บรวบรวม นำไปใช้ หรือเปิดเผยข้อมูลของเจ้าของข้อมูลส่วนบุคคลในราชอาณาจักรไทยเพื่อการขายสินค้าหรือบริการให้กับเจ้าของข้อมูล ควรมีเจ้าหน้าที่คุ้มครองข้อมูล หรือ DPO (Data Protection Officer) ซึ่งเป็นผู้มีความรู้ด้านกฎหมาย PDPA ด้านเทคโนโลยี เข้ามาดูแลและตรวจสอบนโยบายการเก็บรักษาข้อมูลส่วนบุคคลของลูกค้าให้เกิดความปลอดภัย ทั้งนี้ขึ้นอยู่กับขนาดและประเภทของธุรกิจเป็นเกณฑ์ในการพิจารณาว่าควรแต่งตั้ง DPO หรือไม่ ?

ที่มาhttps://pdpa.pro/blogs/in-summary-what-is-pdpa

PDPA คืออะไร? คุ้มครองข้อมูลอะไรบ้าง เรื่องต้องรู้ฉบับเข้าใจง่าย

PDPA (Personal Data Protection Act, B.E. 2562 (2019)) คือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยวันที่ 1 มิถุนายน 2565 เป็นวันที่ พ.ร.บ. PDPA นี้มีผลบังคับใช้ตามกฎหมายทั้งฉบับ เหตุผลในการประกาศใช้ PDPA เนื่องมาจากเทคโนโลยีก้าวหน้าขึ้น ช่องทางสื่อสารต่างๆ มีหลากหลายขึ้น ทำให้การละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลทำได้ง่ายขึ้น และหลายครั้งก็นำมาซึ่งความเดือดร้อนรำคาญหรือสร้างความเสียหายให้แก่เจ้าของข้อมูล ตลอดจนสามารถส่งผลต่อเศรษฐกิจโดยรวมของประเทศได้ด้วย จึงต้องมีกฎหมาย PDPA ว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลขึ้นเพื่อกำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่รวมถึงการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลขึ้น

ข้อมูลส่วนบุคคล

คือข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม โดยข้อมูลของผู้ถึงแก่กรรมและข้อมูลนิติบุคคล ไม่ถือเป็นข้อมูลส่วนบุคคลตาม พ.ร.บ. PDPA คุ้มครองข้อมูลส่วนบุคคลนี้

ข้อมูลส่วนบุคคล (Personal Data) ได้แก่ ชื่อ - นามสกุล, เลขประจำตัวประชาชน, ที่อยู่, เบอร์โทรศัพท์, วันเกิด, อีเมล, การศึกษา, เพศ, อาชีพ, รูปถ่าย, ข้อมูลทางการเงิน นอกจากนี้ยังรวมถึง **ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Personal Data)** ด้วย เช่น ข้อมูลทางการแพทย์หรือสุขภาพ, ข้อมูลทางพันธุกรรมและไบโอเมทริกซ์, เชื้อชาติ, ความคิดเห็นทางการเมือง, ความเชื่อทางศาสนาหรือปรัชญา, พฤติกรรมทางเพศ, ประวัติอาชญากรรม, ข้อมูลสหภาพแรงงาน เป็นต้น

สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject) ได้แก่

- สิทธิได้รับการแจ้งให้ทราบ (Right to be informed)
- สิทธิขอเข้าถึงข้อมูลส่วนบุคคล (Right of access)
- สิทธิในการขอให้โอนข้อมูลส่วนบุคคล (Right to data portability)
- สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (Right to object)
- สิทธิขอให้ลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคล (Right to erasure (also known as right to be forgotten)

- สิทธิขอให้ระงับการใช้ข้อมูล (Right to restrict processing)
- สิทธิในการขอให้แก้ไขข้อมูลส่วนบุคคล (Right of rectification)

บุคคลที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

- **เจ้าของข้อมูลส่วนบุคคล (Data Subject)** คือ บุคคลที่ข้อมูลระบุไปถึง
- **ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)** คือ บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ "ตัดสินใจ" เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
- **ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)** คือ บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล "ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล" ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าว ต้องไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

การเก็บรวบรวม ใช้ หรือเปิดเผย ข้อมูลส่วนบุคคล สามารถทำได้ในกรณีต่อไปนี้

- ได้รับความยินยอมจากเจ้าของข้อมูส่วนบุคคล
- จัดทำเอกสารประวัติศาสตร์ หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ การศึกษาวิจัยหรือการจัดทำสถิติ
- ป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล
- จำเป็นเพื่อปฏิบัติกฎหมาย หรือสัญญา
- จำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือของบุคคลอื่น
- จำเป็นเพื่อประโยชน์สาธารณะ และการปฏิบัติหน้าที่ในการใช้อำนาจรัฐ

การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ (Cross-border Personal Data Transfer)

ประเทศปลายทางหรือองค์การระหว่างประเทศ ที่รับข้อมูลส่วนบุคลต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล (PDPA พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล) ที่เพียงพอ เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูล หรือเป็นการปฏิบัติตามกฎหมาย/สัญญา หรือเพื่อประโยชน์สาธารณะเป็นสำคัญเท่านั้น

บทลงโทษหากไม่ปฏิบัติตาม PDPA

เพื่อให้ข้อมูลส่วนบุคคล หรือ (PDPA พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล) ถูกนำไปใช้ในทางที่เหมาะสมและเป็นประโยชน์มากกว่าโทษ การให้ข้อมูลแต่ละครั้งจึงต้องพิจารณาอย่างรอบคอบก่อนให้ข้อมูล เช่นการให้ข้อมูลเพื่อจัดส่งสินค้า หากมีการขอข้อมูลที่ไม่เกี่ยวกับการจัดส่ง เจ้าของข้อมูลก็มีสิทธิปฏิเสธการให้ข้อมูลนั้น และในส่วนของผู้เก็บข้อมูล ก็ต้องรู้ขอบเขตในการเข้าถึงข้อมูลส่วนบุคคล มีระบบในการควบคุม/ยืนยันตัวตนในการเข้าถึงข้อมูล และจำเป็นต้องมีการกำหนดนโยบายองค์กรเพื่อให้บุคคลที่เกี่ยวข้องปฏิบัติตาม เพราะหากไม่ทำตาม PDPA อาจได้รับโทษดังนี้

- **ความรับผิดทางแพ่ง** ตามความเสียหายที่เกิดขึ้นจริง และอาจต้องชดใช้ค่าสินไหมทดแทนเพิ่มขึ้นอีก โดยสูงสุดไม่เกิน 2 เท่าของค่าเสียหายที่แท้จริง
- **โทษทางอาญา** จำคุกสูงสุดไม่เกิน 1 ปี หรือปรับไม่เกิน 1 ล้านบาท หรือทั้งจำทั้งปรับ
- **โทษทางปกครอง** ปรับสูงสุดไม่เกิน 5 ล้านบาท

ที่มา https://www.scb.co.th/th/personal-banking/stories/tips-for-you/pdpa-about-us

บทลงโทษตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล หรือ PDPA ของไทย

PDPA มีการกำหนดบทลงโทษเอาไว้ทั้ง 3 ประเภทที่กล่าวมาทั้งหมด!! โดยมีรายละเอียดดังนี้

1. โทษทางแพ่ง มีการกำหนดให้ชดใช้ค่าสินไหมทดแทนให้กับเจ้าของข้อมูลส่วนบุคคลที่ได้รับความเสียหายจากการละเมิด **<u>บวกกับ</u>** ชดใช้ค่าสินไหมทดแทนเพื่อการลงโทษเพิ่มเติมสูงสุดเป็น 2 เท่าของค่าเสียหายจริง

   ค่าสินไหมทดแทน + (ค่าสินไหมทดแทนเพื่อการลงโทษ x 2)

เท่ากับว่า หากศาลตัดสินให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องชดใช้ค่าสินไหมทดแทนให้แก่เจ้าของข้อมูลส่วนบุคคล 10 ล้านบาท ศาลอาจจะกำหนดค่าสินไหมเพื่อการลงโทษเพิ่มอีก 20 ล้านบาท รวมเป็น 30 ล้านบาท!!!

ค่าสินไหมทดแทน + (ค่าสินไหมทดแทนเพื่อการลงโทษ x 2)

10,000,000 + (10,000,000 x 2) = 30,000,000

2. โทษทางอาญาของ PDPA มี 2 โทษคือ โทษจำคุก และ โทษปรับ ถึงตรงนี้หลายคนคงจะงงว่า หากผู้กระทำผิดเป็นบริษัท (นิติบุคคล) แล้ว บริษัทจะได้รับโทษจำคุกได้ยังไง คำตอบคือ กรรมการหรือบุคคลซึ่งรับผิดชอบในการดำเนินงานของบริษัทนั้นๆ นั่นแหละ ที่อาจจะได้รับโทษจำคุก และโทษอาญาที่สูงที่สุดของ PDPA คือ **โทษจำคุก 1 ปี หรือปรับ 1 ล้านบาท** หรือทั้งจำทั้งปรับ ซึ่งโทษสูงสุดนี้มาจากการใช้หรือเปิดเผยข้อมูล

หรือส่งโอนข้อมูลไปต่างประเทศในส่วนที่เป็นข้อมูลส่วนบุคคล sensitive ที่ไม่เป็นไปตามข้อกำหนดของ PDPA เพื่อแสวงหาผลประโยชน์ที่ไม่ควรได้โดยชอบด้วยกฎหมาย และโทษปรับนี้เป็นคนละส่วนต่างหากจากการชดใช้ค่าเสียหายทางแพ่งที่กล่าวในข้อ 1 ข้างต้น

3. โทษทางปกครองของ PDPA คือโทษปรับเป็นตัวเงิน **ซึ่งมีตั้งแต่ 1 ล้านบาทไปจนถึง 5 ล้านบาท** โดยกรณีที่จะโดนโทษปรับสูงสุด 5 ล้านบาทนี้ คือกรณีที่มีการฝ่าฝืนข้อกำหนดที่เกี่ยวกับการใช้หรือเปิดเผยข้อมูล หรือส่งโอนข้อมูลไปต่างประเทศในส่วนที่เป็นข้อมูลส่วนบุคคล sensitive และแน่นอนว่า โทษปรับนี้เป็นคนละส่วนต่างหากจากการชดใช้ค่าเสียหายทางแพ่งและโทษปรับทางอาญา

หมายความว่า หากมีการละเมิดข้อกำหนดของ PDPA อาจจะโดนบทลงโทษทั้ง 3 ประเภทนี้พร้อมกันได้

ที่มา

https://www.pdpaplus.com/Article/Detail/138066/%E0%B8%9A%E0%B8%97%E0%B8%A5%E0%B8%87%E0%B9%82%E0%B8%97%E0%B8%A9%E0%B8%95%E0%B8%B2%E0%B8%A1-%E0%B8%9E-%E0%B8%A3-%E0%B8%9A-%E0%B8%84%E0%B8%B8%E0%B9%89%E0%B8%A1%E0%B8%84%E0%B8%A3%E0%B8%AD%E0%B8%87%E0%B8%82%E0%B9%89%E0%B8%AD%E0%B8%A1%E0%B8%B9%E0%B8%A5%E0%B8%AA%E0%B9%88%E0%B8%A7%E0%B8%99%E0%B8%9A%E0%B8%B8%E0%B8%84%E0%B8%84%E0%B8%A5-%E0%B8%AB%E0%B8%A3%E0%B8%B7%E0%B8%AD-PDPA-%E0%B8%82%E0%B8%AD%E0%B8%87%E0%B9%84%E0%B8%97%E0%B8%A2