โทษปรับฐานละเมิด และไม่ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลกำลังเป็นเรื่องใหญ่สำหรับองค์กรธุรกิจทั่วโลกนับตั้งแต่ปี 2561 เป็นต้นมา ภายหลังการบังคับใช้ General Data Protection Regulation (GDPR) ซึ่งเป็นกฎหมายของสหภาพยุโรปว่าด้วยมาตรการคุ้มครองความเป็นส่วนตัวของข้อมูลส่วนบุคคล และเป็นต้นแบบของกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่ทั่วโลกนำไปประยุกต์ใช้ ทำให้ธุรกิจหลายแห่งถูกปรับ หรือต้องจ่ายค่าสินไหมทดแทน กรณีละเมิดหรือฝ่าฝืนกฎหมายคุ้มครองข้อมูลส่วนบุคคล

ค่าปรับ และค่าสินไหมละเมิดตามกฎหมาย PDPA ต้องจ่ายเท่าไหร่?

ก่อนอื่นต้องทราบก่อนว่า ผู้ที่มีอำนาจพิจารณาวินิจฉัยเรื่องค่าปรับ และการกำหนดโทษ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล โดยอาศัยอำนาจของ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ในการที่จะพิจารณาบทลงโทษใน 3 ลักษณะ คือ **ความรับผิดทางแพ่ง โทษอาญา และโทษทางปกครอง** โดยในกฎหมาย PDPA มีการระบุไว้อย่างชัดเจน ดังนี้ :

ความรับผิดทางแพ่ง

บุคคลหรือนิติบุคคลที่มีสถานะเป็นผู้ควบคุมข้อมูล (Data Controller) และผู้ประมวลผลข้อมูล (Data Processor) หากมีการฝ่าฝืน หรือไม่ปฏิบัติตามกฎหมาย PDPA จนทำให้เกิด ความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ไม่ว่าจะจงใจหรือประมาทเลินเล่อ ต้องชดใช้ค่าสินไหมทดแทนแก่เจ้าของข้อมูลส่วนบุคคลตามความเสียหายที่เกิดขึ้น หรือคณะกรรมการคุ้มครองข้อมูลฯ อาจพิจารณาเพิ่มโทษเป็น 2 เท่าจากความเสียงหายจริงที่เกิดขึ้น **คำนวณง่าย ๆ ก็คือ ค่าปรับจริง + 2 เท่าของค่าปรับ = เงินค่าสินไหมทดแทนที่ต้องจ่าย**

โทษทางอาญา

กฎหมาย PDPA กำหนดโทษอาญาไว้ 2 ลักษณะ คือ ปรับเงิน กับ จำคุก หรืออาจจะโดนทั้งคู่! ดังนี้ :

- เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เก็บข้อมูลส่วนบุคคลอ่อนไหว ส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล มีโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 5 แสนบาท หรือทั้งจำทั้งปรับ
- เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เก็บข้อมูลส่วนบุคคลอ่อนไหว ส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล **เพื่อแสวงหาประโยชน์** มีโทษจำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 1 ล้านบาท หรือทั้งจำทั้งปรับ
- กรณีผู้ปฏิบัติหน้าที่ตามกฎหมาย นำข้อมูลส่วนบุคคลที่ทราบจากหน้าที่ไปเปิดเผย มีโทษจำคุกไม่เกิน 6 เดือน ปรับไม่เกิน 5 แสนบาทหรือทั้งจำทั้งปรับ

ทั้งนี้ ในกรณีผู้กระทำผิดเป็น **‘นิติบุคคล’** ซึ่งเกิดจากการสั่งการของกรรมการ ผู้จัดการ หรือผู้รับผิดชอบในงานนั้น หรือละเว้นที่จะสั่งการเป็นเหตุให้เกิดการทำผิดกฎหมาย PDPA บุคคลดังกล่าวจะต้องรับโทษ ตามบทลงโทษที่กฎหมายบัญญัติไว้ในความผิดนั้นด้วย

อย่างไรก็ตาม การกำหนดโทษจะดูจากพฤติการณ์ต่างๆ เช่น ความร้ายแรงของความเสียหาย ผลประโยชน์ที่ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลได้รับ ตลอดจนสถานะทางการเงิน การบรรเทาในส่วนที่เกิดความเสียหาย หรือกล่าวให้ง่ายกว่านั้นคือขึ้นอยู่ที่ดุลยพินิจของคณะกรรมการคุ้มครองข้อมูลฯ ซึ่งบทลงโทษอาจรวมทั้ง ความรับผิดทางแพ่ง โทษอาญา และโทษทางปกครองร่วมด้วย หมายความว่า หากละเมิดอาจโดนโทษถึง 3 เด้ง!!!

บทลงโทษทางปกครอง

หากเกิดข้อมูลรั่วไหลข้อมูลส่วนบุคคลแล้วไม่แจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ตามกฎหมายอาจได้รับโทษสูงสุดไม่เกิน 3 ล้านบาท และอาจจะถูกตรวจสอบจากหน่วยงานกำกับดูแลแล้วเข้าข่ายได้รับโทษกระทงอื่น ๆ อีก ดังนี้

1. <u>โทษปรับทางปกครองไม่เกิน 1,000,000 บาท</u>

กรณีความผิด :

-
    - มาตรา 23 กรณีผู้ควบคุมข้อมูลส่วนบุคคลไม่ได้แจ้งให้เจ้าของข้อมูลทราบก่อนหรือระหว่างเก็บรวบรวมข้อมูลส่วนบุคคลตามมาตรานี้
    - มาตรา 30 วรรคสี่ กรณีผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามคำขอเข้าถึงและขอรับสำเนา
    - มาตรา 39 วรรคหนึ่ง กรณีผู้ควบคุมข้อมูลส่วนบุคคลไม่ได้ทำบันทึกรายการ RoPA ตามมาตรานี้
    - มาตรา 41 วรรคหนึ่ง กรณีผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลไม่ได้จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ของตนในกรณีที่กฎหมายกำหนด
    - มาตรา 19 วรรคสาม ไม่ขอความยินยอมตามแบบหรือข้อความที่คณะกรรมการกำหนด และวรรคหก ไม่แจ้งผลกระทบจากการถอนความยินยอม

2. <u>โทษปรับทางปกครองไม่เกิน 3,000,000 บาท</u>

กรณีความผิด :

-
    - มาตรา 21 กรณีผู้ควบคุมข้อมูลส่วนบุคคลไม่ได้แจ้งให้เจ้าของข้อมูลทราบตามมาตรานี้

- มาตรา 22 กรณีผู้ควบคุมข้อมูลส่วนบุคคลเก็บข้อมูลโดยไม่เป็นไปตามวัตถุประสงค์และเกินจำเป็น
- มาตรา 24 กรณีผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลตามมาตรานี้ (เก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่มีฐานทางกฎหมายอื่นรองรับ)
- มาตรา 25 กรณีผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นโดยไม่ปฏิบัติสอดคล้องตามมาตรานี้
- มาตรา 27 กรณีผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยโดยไม่ได้รับความยินยอม หรือนอกขอบเขตวัตถุประสงค์
- มาตรา 28 และ 29 กรณีผู้ควบคุมข้อมูลส่วนบุคคลโอนข้อมูลไปต่างประเทศ โดยไม่ได้ปฏิบัติตามหลักเกณฑ์ที่คณะกรรมการกำหนด
- มาตรา 32 วรรคสอง กรณีเจ้าของข้อมูลได้ใช้สิทธิคัดค้านแต่ผู้ควบคุมข้อมูลส่วนบุคคลยังใช้ข้อมูลต่อไป
- มาตรา 37 ผู้ควบคุมไม่ได้ปฏิบัติหน้าที่ให้เป็นไปตามมาตรานี้ (4) แจ้งเหตุละเมิดภายใน 72 ชั่วโมงหลังทราบเหตุ หรือขอความยินยอมโดยการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดวัตถุประสงค์ หรือการส่งหรือโอนข้อมูลโดยไม่ปฏิบัติตามมาตรา 29 วรรคหนึ่งหรือวรรคสาม

3. <u>โทษปรับทางปกครองไม่เกิน 5,000,000 บาท</u>

กรณีความผิด :

-
- มาตรา 26 ผู้ควบคุมข้อมูลที่ฝ่าฝืนเก็บรวบรวมข้อมูลอ่อนไหวโดยไม่ได้รับความยินยอม
- มาตรา 27 กรณีผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยโดยไม่ได้รับความยินยอม หรือนอกขอบเขตวัตถุประสงค์
- มาตรา 28 และ 29 กรณีผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลอ่อนไหวตามมาตรา 26 ไปต่างประเทศ โดยไม่ได้ปฏิบัติตามหลักเกณฑ์ที่คณะกรรมการกำหนด

ทั้งนี้ คณะกรรมการผู้เชี่ยวชาญมีอำนาจสั่งลงโทษปรับทางปกครองตามที่กำหนดไว้ หรือสั่งให้แก้ไข หรือตักเตือนก่อนก็ได้ จากข้อมูลเรื่องค่าปรับ ค่าสินไหมทดแทน และโทษทางปกครองที่ต้องจ่ายหากบุคคลหรือนิติบุคคลมีการละเมิดกฎหมาย จะโดยจงใจหรือประมาทก็ตาม ผู้ประกอบการสามารถเตรียมความพร้อมก่อนกฎหมายบังคับใช้ หรือการแต่งตั้งเจ้าหน้าที่ DPO เพื่อให้การดำเนินการขององค์กรสามารถลดความเสี่ยงที่อาจมีการละเมิดกฎหมายได้ ซึ่งเป็นแนวทางที่ทุกองค์กรควรดำเนินการ ขณะเดียวกัน ธุรกิจขนาดเล็ก หรือ SME หากไม่ได้มีการเก็บข้อมูลส่วนบุคคลเป็นจำนวนมาก หรือมีการประมวลผลข้อมูลส่วนบุคคลเป็นครั้งคราว อาจพิจารณาแต่งตั้งเจ้าหน้าที่ประสานงานข้อมูลส่วนบุคคลที่มีความรู้ ความเข้าใจเรื่องกฎหมาย PDPA ก็จะเป็นแนวที่ที่สามารถลดความสี่ยงจากการละเมิดกฎหมายได้เช่นกัน