“บริษัทเอกชนรายใหญ่ของประเทศ ถูกสั่งปรับ โทษทางปกครอง PDPA เป็นครั้งแรก หลังคณะกรรมการผู้เชี่ยวชาญ คณะที่ 2 สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล มีคำสั่งออกมาอย่างเป็นทางการ”

21 สิงหาคม 2567 – คณะกรรมการผู้เชี่ยวชาญ คณะที่ 2 (เรื่องร้องเรียนเกี่ยวกับเทคโนโลยีดิจิทัล และอื่น ๆ) สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล มีคำสั่งลงวันที่ 31 กรกฎาคม 2567 ให้บริษัทเอกชนปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัด โดยคำสั่งฯ ระบุ **โทษทางปกครอง PDPA และค่าปรับรวมสูงถึง 7,000,000 บาท**

เกิดอะไรขึ้นกับภาคเอกชนและข้อมูลส่วนบุคคล?

ก่อนหน้านี้มีกรณีข้อมูลส่วนบุคคลของลูกค้าบริษัทเอกชนรายใหญ่ของประเทศที่มีการซื้อขายสินค้าออนไลน์รั่วไหลจำนวนมาก ส่งผลให้มีผู้ได้รับความเสียหายผ่านการใช้ข้อมูลส่วนบุคคลโดยไม่ชอบ จนเป็นข่าวในสื่อสังคมออนไลน์ และมีการเรียกบริษัทมาชี้แจ้งเกี่ยวกับเหตุละเมิดดังกล่าวต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (PDPC) แล้ว ตรวจสอบพบว่าเป็นข้อมูลการซื้อสินค้าและข้อมูลส่วนบุคคลของลูกค้าบริษัทจริง และมีความบกพร่องในการทำตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA) ในหลายประเด็น

ทั้งนี้ สคส. ได้รวบรวมพยานหลักฐานเกี่ยวกับการกระทำผิดตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเพื่อส่งให้คณะกรรมการผู้เชี่ยวชาญพิจารณาโทษทางปกครองต่อไป

รายละเอียดโทษทางปกครองและค่าปรับ

คณะกรรมการผู้เชี่ยวชาญ คณะที่ 2 (เรื่องร้องเรียนเกี่ยวกับเทคโนโลยีดิจิทัล และอื่น ๆ) มีคำสั่งตัดสินให้บริษัทแห่งดังกล่าวรับโทษปรับทางปกครองภายใต้ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) และกฎหมายลำดับรอง ใน 3 ประเด็น ดังนี้

1. กรณีไม่แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) – 1,000,000 บาท

บริษัทเข้าข่ายเป็นกิจการขนาดใหญ่ ที่เก็บรวบรวม ใช้ หรือประมวลผลข้อมูลส่วนบุคคล “เป็นกิจกรรมหลักของผู้ควบคุมข้อมูลส่วนบุคคล” ผ่านการจัดจำหน่ายสินค้าแก่ผู้บริโภคทั่วประเทศ และมีข้อมูลส่วนบุคคลของลูกค้าจำนวนมาก (จำนวนตั้งแต่ 100,000 รายขึ้นไป) จึงเข้าข่ายจำเป็นต้องมีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ตามกฎหมาย PDPA มาตรา 41 (2)

2. กรณีไม่มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม – 3,000,000 บาท

บริษัทไม่มีมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลที่มีมาตรฐานขั้นต่ำตามที่กฎหมายกำหนดหรือไม่มีประสิทธิภาพเพียงพอ ตามกฎหมาย PDPA มาตรา 37 (1) ทำให้เกิดเหตุการละเมิดข้อมูลส่วนบุคคลอย่างต่อเนื่อง โดยนอกจากนั้นในเชิงรายละเอียดยังขาด:

1) มาตรการการควบคุมการเข้าถึงข้อมูลส่วนบุคคล (Access Control) และ

2) การกำหนดสิทธิในการเข้าถึงหรือใช้งาน (Authorization)

3. กรณีไม่แจ้งเหตุละเมิดข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด – 3,000,000 บาท

เมื่อเกิดเหตุละเมิดข้อมูลส่วนบุคคลขึ้น จะต้องแจ้งต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ภายใน 72 ชั่วโมงหลังทราบเหตุ และหากการละเมิดนั้นประเมินแล้วว่ามีผลกระทบต่อสิทธิของเจ้าของข้อมูลส่วนบุคคลจะต้องดำเนินการแจ้งต่อเจ้าของข้อมูลด้วย ตามกฎหมาย PDPA มาตรา 37 (4) ซึ่งบริษัทไม่ได้ดำเนินการตามที่กฎหมายกำหนด

นอกเหนือจากการสั่งปรับทางปกครองแล้ว ในประกาศดังกล่าวยังมีแนวทางที่คณะกรรมการผู้เชี่ยวชาญฯ มีคำสั่งออกมาให้บริษัทปฏิบัติตาม ได้แก่

- ให้ปรับปรุงมาตรการรักษาความมั่นคงปลอดภัยเพื่อป้องกันไม่ให้ข้อมูลรั่วไหล
- จัดอบรมบุคลากรที่เกี่ยวข้องกับการเข้าถึง เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
- เพิ่มเติมมาตรการรักษาความมั่นคงปลอดภัยให้ทันกับเทคโนโลยีที่เปลี่ยนแปลง
- แจ้งความคืบหน้าให้สคส.ทราบภายใน 7 วัน

โดยหากไม่ปฏิบัติตามแนวทางข้างต้นนี้ ระวางโทษปรับเพิ่มอีกสูงสุดไม่เกิน 500,000 บาท ตามกฎหมาย PDPA มาตรา 89

สรุปบทเรียนจากเคสภาคเอกชนถูกปรับทางปกครอง 7 ล้าน

หน่วยงานกำกับดูแลด้านการคุ้มครองข้อมูลส่วนบุคคลไทย สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และคณะกรรมการผู้เชี่ยวชาญ (ปัจจุบันมี 4 คณะ) การดำเนินงานและบังคับใช้กฎหมาย PDPA อย่างจริงจังมากขึ้น องค์กรหากไม่มีการ “ทำ PDPA” ดำเนินงานให้สอดคล้องตามกฎหมายอาจเสี่ยงข้อมูลรั่วไหลหรือถูกตรวจสอบ อันเป็นเหตุให้ได้รับโทษทางปกครองได้เช่นกัน ต้องปรับปรุงองค์กรให้สอดคล้องตามกฎหมาย ที่แย่ไปกว่านั้นคือเสียชื่อเสียง ความไว้วางใจจากลูกค้าที่มาใช้บริการและ Stakeholder อื่น ๆ ลดลง