

“PDPA Workshop หลังบังคับใช้...อะไรที่ต้องยกระดับ”

วันศุกร์ที่ 9 ธันวาคม 2565 เวลา 09.00-12.30 น.

ณ อาคารอเนกประสงค์ ธนาคารแห่งประเทศไทย สำนักงานภาคเหนือ

กรณีศึกษา 2

เกี่ยวกับการดำเนินการรองรับเหตุละเมิด

คำถามเพื่อพิจารณา:

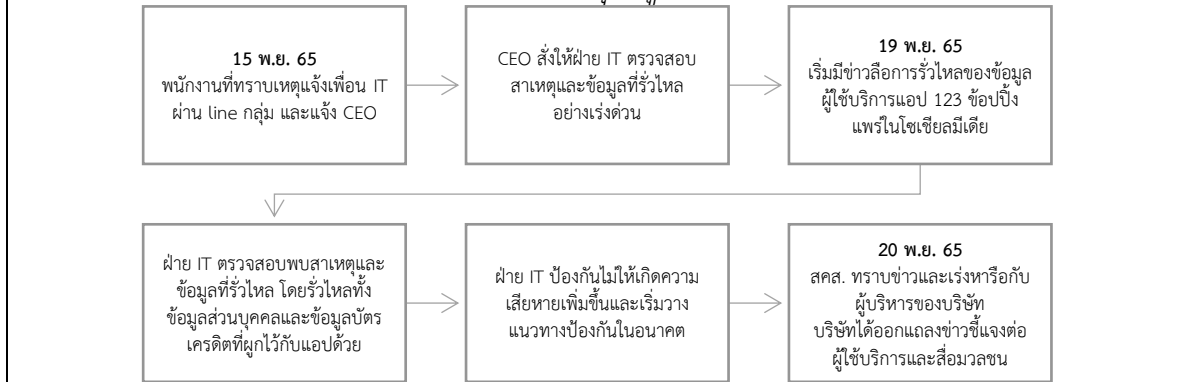
1. องค์กรจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมตามข้อกำหนดของกฎหมายแล้วหรือไม่
2. องค์กรมีลักษณะเข้าข่ายที่จะต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือไม่
3. องค์กรจัดเตรียมกระบวนการจัดการเหตุละเมิดอย่างเหมาะสมแล้วหรือไม่



นายหนึ่งเป็นลูกค้าประจำที่ชอบซื้อของผ่าน e-Commerce application ของบริษัท 123 ซ้อปปี้ง จำกัด ซึ่งเป็นบริษัทที่ได้รับความนิยมเป็นอันดับ 1 ในประเทศ มีลูกค้ากว่า 1 ล้านราย เหตุเพราะ application ของบริษัทใช้งานง่าย สามารถบันทึกข้อมูลบัตรเครดิตหรือบัญชีธนาคารไว้บน application ได้ ไม่ต้องกรอกข้อมูลซ้ำทุกครั้งที่มีซื้อสินค้า วันที่ 15 พฤศจิกายน 2565 พนักงานของบริษัท 123 ซ้อปปี้งพบธุรกรรมซื้อสินค้าผ่าน application ที่ค่อนข้างผิดปกติ มียอดชำระเงินของลูกค้าหลายรายรวมถึงนายหนึ่ง ที่ถูกตัดเงินจากบัตรเครดิตที่ผูกไว้เป็นมูลค่าเท่ากันหลายครั้งในเวลาไล่เลี่ยกัน จึง cap screen ข้อมูลส่วนบุคคลของลูกค้ารวมถึงธุรกรรมชำระเงินที่ผิดปกติส่งใน LINE กลุ่มให้เพื่อนพนักงานที่อยู่แผนก IT ช่วยตรวจสอบให้รวมถึงแจ้งไปยัง CEO ของบริษัทเพื่อรับทราบเหตุการณ์ดังกล่าว เนื่องจากบริษัทยังไม่มีแต่งตั้ง DPO ซึ่ง CEO ได้สั่งการให้ฝ่าย IT หาข้อมูลและจุดรั่วไหลของข้อมูลอย่างเร่งด่วน

จากการตรวจสอบพบว่า ระบบของบริษัทถูกโจมตีจากภัยไซเบอร์ ทำให้ข้อมูลของลูกค้าหลายรายถูกขโมยไป รวมถึงข้อมูลบัตรเครดิตที่ผูกไว้กับ application ถูกขโมยไปใช้ซื้อสินค้าด้วย ผู้บริหารจึงให้พนักงานเร่งแก้ไขปัญหาอย่างเร่งด่วน ระหว่างนั้นเริ่มมีข่าวลือใน LINE และ social media เรื่องการรั่วไหลของข้อมูลลูกค้า และข้อมูลบัตรเครดิตที่ผูกไว้กับ application ของบริษัท 123 ซ้อปปี้ง ทำให้ลูกค้าขาดความเชื่อมั่น ลบข้อมูลบัตรเครดิตที่ผูกไว้และยกเลิกการติดตั้ง application เป็นจำนวนมาก

Flow กระบวนการประสานงานของบริษัทเมื่อเกิดเหตุข้อมูลรั่วไหล



เวลาผ่านไปจนถึงวันที่ 20 พฤศจิกายน 2565 บริษัทสามารถแก้ไขและป้องกันฐานข้อมูลลูกค้าไม่ให้เกิดความเสียหายเพิ่มขึ้น และจากข่าวที่ออกไปนั้น ทำให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ทราบเหตุการณ์และเร่งหารือต่อผู้บริหารของบริษัท รวมถึงออกแถลงข่าวให้ผู้ใช้บริการ สื่อมวลชน และหน่วยงานที่เกี่ยวข้องอื่นรับทราบเหตุการณ์ดังกล่าวด้วย

จดหมายแถลงข่าวของบริษัท 123 ซ้อปปี้ง จำกัด

20 พฤศจิกายน 2565

หนังสือชี้แจง

กรณีข่าวการรั่วไหลของข้อมูลผู้ใช้บริการแอปพลิเคชัน 123 ซ้อปปี้ง

ตามที่มีการรายงานข่าวการรั่วไหลของข้อมูลผู้ใช้บริการแอปพลิเคชันของบริษัท 123 ซ้อปปี้ง จำกัด (บริษัทฯ) ส่งผลกระทบต่อผู้ใช้บริการมากกว่า 1 ล้านราย ปรากฏในข่าวสื่อโซเชียลมีเดียหลายช่องทางในช่วงหลายวันที่ผ่านมา ขอเรียนชี้แจงว่า บริษัทฯ ได้ทำการตรวจสอบสาเหตุแล้วพบว่า ข่าวการรั่วไหลข้อมูลของผู้ใช้บริการกว่า 1 ล้านรายไม่เป็นความจริง อย่างไรก็ตาม มีการรั่วไหลของข้อมูลผู้ใช้บริการเพียงบางส่วนจริงแต่ไม่เกิน 1,000 ราย ซึ่งคิดเป็น 0.1% เทียบกับฐานข้อมูลผู้ใช้บริการทั้งหมดของบริษัท ซึ่งบริษัทฯ ได้ดำเนินการแก้ไขและป้องกันไม่ให้เกิดความเสียหายมากกว่าที่ปรากฏในข่าว พร้อมทั้งประสานแจ้งหน่วยงานที่เกี่ยวข้องรับทราบเรียบร้อยแล้ว

ทั้งนี้ ขอยืนยันว่าบริษัทฯ ให้ความสำคัญในการป้องกันข้อมูลและความเป็นส่วนตัวของลูกค้าเป็นสำคัญ และจะเร่งดำเนินการวางแผนทางป้องกันที่รัดกุม เพื่อป้องกันเหตุการณ์ดังกล่าวในอนาคต เพื่อรักษาความเชื่อมั่นของการใช้บริการของบริษัทฯ ต่อไป

กรณีต้องการทราบข้อมูลเพิ่มเติม กรุณาติดต่อ

ฝ่ายประชาสัมพันธ์ บริษัท 123 ซ้อปปี้ง จำกัด

โทรศัพท์ 02-123-xxxx