10 พฤศจิกายน 2568

เรียน ผู้จำหน่ายสินค้า / ผู้ให้บริการ

ธนาคารกรุงศรีอยุธยา จำกัด (มหาชน) และบริษัทในเครือธนาคารกรุงศรีอยุธยา ขอแจ้งให้ทราบว่า พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ได้กำหนดหน้าที่และความรับผิดชอบให้แก่ธนาคาร (ผู้ควบคุมข้อมูลส่วนบุคคล หรือ Data Controller) และท่าน (ผู้ประมวลผลข้อมูลส่วนบุคคล หรือ Data Processor) เพื่อให้มีการคุ้มครองข้อมูลส่วนบุคคลอย่างมีประสิทธิภาพ และเพื่อให้มีมาตรการเยียวยาเจ้าของข้อมูลส่วนบุคคลจากการถูกละเมิดสิทธิในข้อมูลส่วนบุคคล

ท่านในฐานะผู้ประมวลผลข้อมูลส่วนบุคคลที่ได้รับมอบหมายจากธนาคารให้ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งของธนาคาร จึงมีหน้าที่ต้องทำการประมวลผลข้อมูลส่วนบุคคลตามข้อตกลงต่างๆ ที่ได้ทำกับธนาคารและหน้าที่ตามกฎหมาย ดังนี้ เป็นอย่างน้อย

1. ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากธนาคารเท่านั้น
2. จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้ธนาคารทราบถึงเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น
3. จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้ตามหลักเกณฑ์และวิธีการที่ทางการกำหนด

ในกรณีที่ท่านไม่สามารถปฏิบัติตามข้อตกลงและหน้าที่ที่กล่าวมาข้างต้น ได้ และทำให้เกิดเหตุละเมิดข้อมูลส่วนบุคคล (Personal Data Breach)* ไม่ว่าจะเกิดจากการกระทำโดยจงใจหรือประมาทเลินเล่อ ธนาคารจะถือเป็นความรับผิดชอบของท่านและท่านอาจต้องจ่ายค่าปรับ ค่าสินไหมทดแทนให้แก่หรือแทนธนาคาร รวมทั้งมีความผิดตามกฎหมายดังนี้ เป็นอย่างน้อย

1. ความรับผิดทางแพ่ง เช่น จ่ายค่าสินไหมทดแทนแก่เจ้าของข้อมูลส่วนบุคคล และศาลมีอำนาจสั่งจ่ายค่าสินไหมแทนเพื่อการลงโทษเพิ่มเติม แต่ไม่เกินสองเท่าของค่าสินไหมทดแทนที่แท้จริง

2. โทษทางปกครอง (แล้วแต่กรณี ซึ่งพิจารณาตามความร้ายแรงแห่งพฤติกรรมที่กระทำผิด) เช่น ระวางโทษปรับทางปกครองสูงสุดไม่เกิน 5 ล้านบาท
3. โทษอาญา เช่น ปรับหรือจำคุก

ดังนั้น ธนาคารขอให้ท่านดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามข้อตกลงที่ทำไว้กับธนาคาร และให้ท่านปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และกฎหมายต่างๆ ที่เกี่ยวข้องอย่างเคร่งครัด

*Personal Data Breach คือการที่ข้อมูลส่วนบุคคลถูกทำลาย สูญหาย ถูกแก้ไขเปลี่ยนแปลง ถูกเปิดเผยโดยไม่ได้รับอนุญาต หรือการเข้าถึง ส่งต่อ เก็บ รักษาหรือถูกประมวลผลอย่างอื่นไม่ว่าจะเกิดจากการกระทำอันมิชอบด้วยกฎหมายหรือโดยอุบัติเหตุ โดยอาจแบ่งได้เป็น 3 ประเภท ได้แก่ (1) การละเมิดความลับของข้อมูล (Confidentiality Breach) ซึ่งหมายถึง การเข้าถึงหรือการเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตหรือโดยอุบัติเหตุ (2) การละเมิดความถูกต้องแท้จริงของข้อมูล (Integrity Breach) ซึ่งหมายถึง การแก้ไขเปลี่ยนแปลงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตหรือโดยอุบัติเหตุ และ (3) การละเมิดความพร้อมใช้งาน (Availability Breach) ซึ่งหมายถึง การทำให้เข้าถึงข้อมูลไม่ได้หรือการทำให้ข้อมูลสูญหายหรือทำลายไป ไม่ว่าโดยการกระทำโดยไม่ได้รับอนุญาตหรือโดยอุบัติเหตุ

ตัวอย่างของ Personal Data Breach

(1) อุปกรณ์ที่เก็บฐานข้อมูลของลูกค้าสูญหายหรือถูกขโมย (2) ข้อมูลถูกผู้ที่ไม่ได้รับอนุญาตลบ (3) กุญแจ (key) สำหรับการถอดรหัส (decryption) ของข้อมูลที่ได้เข้ารหัส (encrypted) ไว้ได้สูญหาย ทำให้เข้าถึงข้อมูลไม่ได้ (4) การถูกโจมตีด้วย DoS (Denial of Service Attack) ทำให้ระบบไม่สามารถเข้าถึงข้อมูลส่วนบุคคล (5) การถูกโจมตีด้วย ransomware ทำให้เข้าถึงข้อมูลไม่ได้ (6) ใบแจ้งหนี้ของธนาคารของลูกค้ารายหนึ่งได้ถูกส่งไปยังลูกค้าอีกรายหนึ่ง

ธนาคารกรุงศรีอยุธยา จำกัด (มหาชน)
และบริษัทในเครือธนาคารกรุงศรีอยุธยา

หมายเหตุ : จดหมายฉบับนี้พิมพ์จากระบบอัตโนมัติ จึงไม่มีการลงลายมือชื่อ