แนวทางการคุ้มครองข้อมูลส่วนบุคคล
บมจ. ธนาคารกสิกรไทย

บมจ. ธนาคารกสิกรไทย (“ธนาคาร”) ตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล และให้ความสำคัญกับการปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลและกฎเกณฑ์ทางการอื่นๆ ที่เกี่ยวข้องภายใต้แนวทางการคุ้มครองข้อมูลส่วนบุคคลดังต่อไปนี้

1. ข้อมูลส่วนบุคคลจะต้องถูกประมวลผลโดยชอบด้วยกฎหมาย มีความเป็นธรรมและโปร่งใส
2. การเก็บรวบรวมข้อมูลส่วนบุคคล จะต้องเก็บเฉพาะที่เกี่ยวข้องและจำเป็น เพื่อการประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ชอบด้วยกฎหมาย โดยไม่นำข้อมูลส่วนบุคคลไปประมวลผลต่อในลักษณะที่ไม่สอดคล้องกับวัตถุประสงค์
3. ในการประมวลผลข้อมูลส่วนบุคคล ตั้งแต่กระบวนการเก็บรวบรวม ใช้ หรือเปิดเผย จะดำเนินการเท่าที่เกี่ยวข้อง จำเป็นและจำกัดตามวัตถุประสงค์ในการประมวลผลข้อมูล โดยมีการแจ้งวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยให้เจ้าของข้อมูลส่วนบุคคลทราบ
4. ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม ใช้ หรือเปิดเผย ต้องมีความถูกต้อง สมบูรณ์และเป็นปัจจุบัน
5. ไม่เก็บข้อมูลส่วนบุคคลเกินความจำเป็นตามระยะเวลาที่เหมาะสมเพื่อบรรลุวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลหรือเก็บตามระยะเวลาที่กฎหมายกำหนด และจัดให้มีกระบวนการตรวจสอบเพื่อลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นระยะเวลาการเก็บรักษา
6. มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ทั้งมาตรการเชิงองค์กร (organizational measures) และมาตรการเชิงเทคนิค (technical measures) ที่เหมาะสม ซึ่งอาจรวมถึงมาตรการทางกายภาพ (physical measures) ที่จำเป็น เพื่อป้องกันการประมวลผลข้อมูลส่วนบุคคลอันมิชอบด้วยกฎหมาย

การประมวลผลข้อมูลข้อมูลส่วนบุคคล

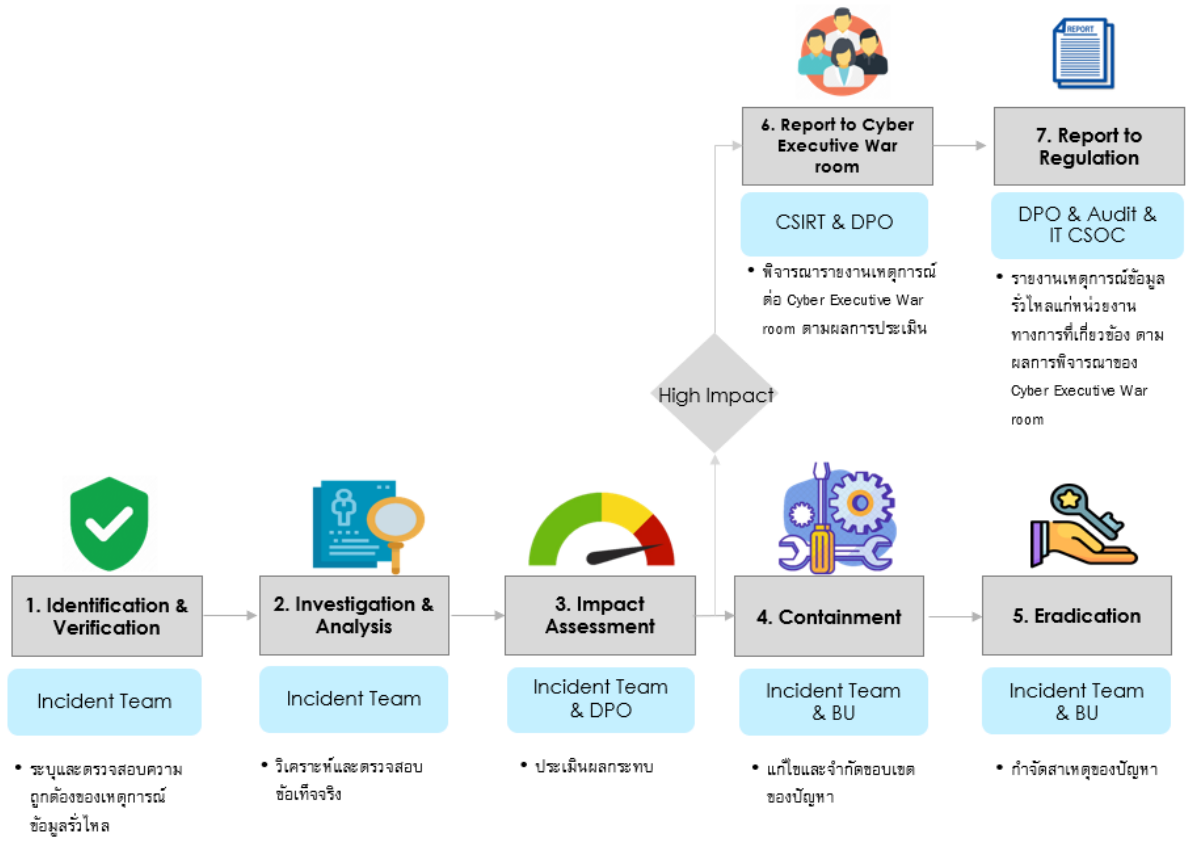
ธนาคารมีการประมวลผลข้อมูลส่วนบุคคลของลูกค้าตามวัตถุประสงค์ที่แจ้งไว้ในประกาศแจ้งนโยบายการคุ้มครองข้อมูลส่วนบุคคลของธนาคารภายใต้ฐานที่ชอบด้วยกฎหมาย ทั้งนี้ ธนาคารอาจมีการประมวลผลข้อมูลส่วนบุคคลของลูกค้าเพื่อวัตถุประสงค์อื่นที่นอกเหนือจากการส่งมอบผลิตภัณฑ์และบริการที่ลูกค้าสมัครใช้บริการ เช่น การวิเคราะห์ วิจัย และ/หรือ จัดทำข้อมูลทางสถิติ รวมถึงเพื่อการพัฒนาปรับปรุงผลิตภัณฑ์ และ/หรือบริการของธนาคาร รวมถึงการทำการตลาดภายใต้ฐานความยินยอม (Consent) และในกรณีธนาคารมีการประมวลผลข้อมูลส่วนบุคคลภายใต้ฐานประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interest) เช่น การประมวลผลข้อมูลเพื่อการบริหารความเสี่ยง กำกับ ตรวจสอบ การบริหารจัดการภายในองค์กร และการป้องกันการทุจริต รวมถึงการบริหารจัดการด้านเทคโนโลยีสารสนเทศเพื่อป้องกันรับมือและลดความเสี่ยงด้านเทคโนโลยีสารสนเทศ และภัยคุกคามไซเบอร์ เป็นต้น ธนาคารได้จัดให้มีการประเมินการใช้ฐานประโยชน์โดยชอบด้วยกฎหมาย (3 Parts Test) เพื่อพิจารณาความจำเป็นและความได้สัดส่วนก่อนการประมวลผลข้อมูลส่วนบุคคล

ในปี 2566 ธนาคารมีการใช้ข้อมูลลูกค้าเพื่อวัตถุประสงค์ทางการตลาด โดยได้รับความยินยอมจากลูกค้าเรียบร้อยแล้ว โดยมีสัดส่วนการใช้ข้อมูล คิดเป็นร้อยละ 70.80 ของจำนวนลูกค้าบุคคลทั้งหมด

แนวทางการจัดการข้อร้องเรียนเกี่ยวกับข้อมูลส่วนบุคคล (OR)

ธนาคารกำหนดกระบวนการตอบสนองและการรายงานเหตุการณ์รั่วไหลของข้อมูลซึ่งครอบคลุมการสูญหาย การเข้าถึง การใช้การเปลี่ยนแปลง การแก้ไข หรือการเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบด้วยกฎหมาย โดยกรณีที่ได้รับแจ้งหรือตรวจพบเหตุการณ์รั่วไหลของข้อมูล ธนาคารจะตรวจสอบข้อเท็จจริง วิเคราะห์และประเมินเหตุการณ์ รวมถึงประเมินความเสี่ยงและผลกระทบตามหลักเกณฑ์ภายในที่ธนาคารกำหนด เช่น จำนวนเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ ปริมาณและความอ่อนไหวของข้อมูลส่วนบุคคล เป็นต้น และรายงานเหตุการณ์และผลการประเมินความเสี่ยงต่อคณะกรรมการที่รับผิดชอบ เพื่อพิจารณากำหนดแนวทางการแก้ไขตอบสนอง เยียวยา และแจ้งเหตุการณ์ต่อหน่วยงานทางการตามข้อกำหนดของกฎหมายตามแต่กรณี

กรณีตรวจพบว่า มีการละเมิดข้อมูลส่วนบุคคล การฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลถือเป็นการฝ่าฝืนคำสั่ง และ/หรือระเบียบของธนาคาร เมื่อดำเนินการตรวจสอบอย่างครบถ้วนรอบด้านแล้วพบว่า มีการกระทำความผิดจริง ธนาคารอาจมีการดำเนินการทางวินัย ได้แก่ ว่ากล่าวตักเตือน การภาคทัณฑ์ การชดเชยค่าเสียหาย การหักค่าจ้าง การลดตำแหน่ง และ/หรือการลดเงินเดือน จนถึงการพ้นสภาพจากการเป็นพนักงาน ตามสมควรแต่กรณี



DPO: Data Protection Officer

CSOC: Cyber Security Operation Center

CSIRT: Computer Security Incident Response Team

การตรวจสอบโดยหน่วยงานภายนอก (OR)

ธนาคารยังให้ความสำคัญกับเรื่อง Check and Balance ที่เหมาะสมในกระบวนการสำคัญ มีการกำหนดความต้องการด้านความปลอดภัยไซเบอร์ในกระบวนการพัฒนาระบบทุกขั้นตอนตั้งแต่การคัดเลือกผู้ให้บริการ การออกแบบโซลูชัน การพัฒนาระบบงาน การทดสอบด้านความปลอดภัยไซเบอร์ ตลอดจนการนำระบบขึ้นใช้งานจริง ทั้งนี้ ธนาคารให้บริษัทที่ปรึกษาชั้นนำประเมินระดับความพร้อมด้านการบริหารจัดการความเสี่ยงด้านไซเบอร์ (Cyber Risk Maturity) อ้างอิงตามมาตรฐานสากล (NIST)* นอกจากนี้ ธนาคารยังได้รับการรับรองตามมาตรฐาน ISO 27001:2013 ติดต่อกันตั้งแต่ปี 2557 โดยครอบคลุมบริการและแอปพลิเคชันที่สำคัญ Data Center และศูนย์เฝ้าระวังภัยไซเบอร์ (CSOC)

NIST หรือ National Institute of Standards and Technology เป็นหน่วยงานที่กำหนดมาตรฐานและแนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศสหรัฐอเมริกา ซึ่งได้รับการยอมรับในระดับสากล และมีการนำมาใช้อ้างอิงอย่างแพร่หลาย

การตรวจสอบโดยฝ่ายตรวจสอบภายใน (IA)

ฝ่ายตรวจสอบภายในของธนาคารมีการประเมินความเสี่ยง (risk-based assessment) เพื่อจัดให้มีการตรวจสอบการปฏิบัติตามกฎหมาย และระเบียบข้อบังคับตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ซึ่งขอบเขตของการตรวจสอบครอบคลุมในด้านการกำกับดูแลของธนาคาร รวมถึงกระบวนการปฏิบัติงานของธนาคารที่เกี่ยวข้องกับวงจรชีวิตของข้อมูลและมาตรการรักษาความปลอดภัยของข้อมูล โดยมีการรายงานผลการตรวจสอบต่อคณะกรรมการตรวจสอบ