



นโยบายการคุ้มครองข้อมูลส่วนบุคคล

ธนาคารตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล จึงได้กำหนดนโยบาย ระเบียบปฏิบัติที่เกี่ยวข้อง เพื่อให้การปฏิบัติงานของธนาคารดำเนินไปอย่างถูกต้องตามกฎหมาย และกฎระเบียบของหน่วยงานทางการที่เกี่ยวข้อง ในเรื่องต่อไปนี้

- 1. การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล :** ธนาคารกำหนดให้มีการขอความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่สอดคล้องตามข้อกำหนดของกฎหมาย โดยแจ้งให้ทราบถึงวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยคำนึงอย่างที่สุดในความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคลในการให้ความยินยอม
- 2. การเก็บรวบรวมข้อมูลส่วนบุคคลและการลบหรือทำลายข้อมูลส่วนบุคคล :** ธนาคารกำหนดให้การเก็บรวบรวมข้อมูลส่วนบุคคลต้องเป็นไปโดยชอบด้วยกฎหมาย โดยแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียดต่างๆ รวมถึงการจัดทำและเก็บรักษาบันทึกการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด และกำหนดให้มีการลบ ทำลายข้อมูลส่วนบุคคลหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ เมื่อพ้นกำหนดระยะเวลาการเก็บรักษาหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลตามหลักเกณฑ์และเงื่อนไขที่กฎหมายกำหนด
- 3. การเข้าถึงและการใช้ข้อมูลส่วนบุคคล :** ธนาคารกำหนดให้พนักงานสามารถเข้าถึงหรือใช้ข้อมูลส่วนบุคคลได้เท่าที่จำเป็นเพื่อการปฏิบัติงานและเป็นไปตามสิทธิในการเข้าถึงข้อมูลส่วนบุคคลที่ธนาคารกำหนด
- 4. การเปิดเผยและการรับข้อมูลส่วนบุคคล:** ธนาคารกำหนดให้การเปิดเผยข้อมูลส่วนบุคคลต่อบุคคลภายนอก รวมถึงการรับข้อมูลส่วนบุคคลจากบุคคลภายนอกต้องอยู่ภายใต้การได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือมีฐานที่ชอบด้วยกฎหมายรองรับ ทั้งนี้ต้องเป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง

ในกรณีที่ธนาคารมีความจำเป็นต้องเปิดเผยข้อมูลส่วนบุคคลแก่บุคคลภายนอกซึ่งได้รับการว่าจ้างให้ปฏิบัติหน้าที่ในฐานะ **ผู้ประมวลผลข้อมูลส่วนบุคคล** เช่น ผู้ให้บริการ ผู้จำหน่าย หรือผู้รับจ้าง ซึ่งดำเนินการในนามของธนาคารหรือภายใต้คำสั่งของธนาคาร ธนาคารจะดำเนินการกำกับดูแลการประมวลผลข้อมูลของบุคคลภายนอกเหล่านั้นอย่างเข้มงวด เพื่อให้เป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลและนโยบายภายในของธนาคาร โดยกำหนดไว้ภายใต้ **สัญญาการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement)** ซึ่งมีสาระสำคัญ ดังนี้:

- ประมวลผลข้อมูลส่วนบุคคลต้องกระทำภายใต้วัตถุประสงค์ที่ธนาคารกำหนดไว้เท่านั้น
- รักษาความลับของข้อมูลส่วนบุคคลอย่างเคร่งครัด
- จำกัดการเข้าถึงข้อมูลเฉพาะเจ้าหน้าที่ที่ได้รับอนุญาตเท่านั้น
- ดำเนินมาตรการด้านความมั่นคงปลอดภัยตามที่ธนาคารกำหนด
- ลบหรือทำลายข้อมูลส่วนบุคคล หรือส่งคืนให้แก่ธนาคาร พร้อมจัดส่งหลักฐานแสดงการดำเนินการดังกล่าวเมื่อสิ้นสุดสัญญา
- รายงานเหตุการณ์การละเมิดข้อมูลส่วนบุคคลให้ธนาคารทราบภายในระยะเวลาที่กำหนด และให้ความร่วมมืออย่างเต็มที่ในการสอบสวนและวิเคราะห์สาเหตุของเหตุการณ์การละเมิดข้อมูล

นอกจากนี้ ในกรณีที่ธนาคารเปิดเผยข้อมูลส่วนบุคคลให้แก่ **พันธมิตรทางธุรกิจ** หรือ **บริษัทในเครือภายใต้กลุ่มธุรกิจทางการเงินของธนาคาร** ธนาคารจะกำกับดูแลการประมวลผลข้อมูลของหน่วยงานเหล่านั้นผ่าน **สัญญาแลกเปลี่ยนข้อมูลส่วนบุคคล (Data Sharing Agreement)** ซึ่งกำหนดให้ผู้รับข้อมูลต้องประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ตกลงร่วมกันเท่านั้นและต้องปฏิบัติตามกฎหมายและข้อกำหนดที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัด



5. **การส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศ :** ธนาคารกำหนดให้การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศสามารถดำเนินการได้ในกรณีที่ประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอและสามารถบังคับตามสิทธิของเจ้าของข้อมูลส่วนบุคคลได้ หรือเป็นการส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ในต่างประเทศที่อยู่ในกลุ่มธุรกิจทางการเงินของธนาคารที่ดำเนินการตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลเพื่อการส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ในต่างประเทศและอยู่ในเครือกิจการหรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือธุรกิจร่วมกัน (binding corporate rules) ที่ได้รับการตรวจสอบและรับรองจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล หรือเป็นการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศภายใต้ข้อยกเว้นของกฎหมายหรือกฎเกณฑ์ทางการที่เกี่ยวข้อง หรือเป็นการส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลในต่างประเทศที่ได้จัดให้มีมาตรการคุ้มครองที่เหมาะสม (appropriate safeguards) ซึ่งสามารถบังคับตามสิทธิของเจ้าของข้อมูลส่วนบุคคลได้ และมีมาตรการเยียวยาทางกฎหมายที่มีประสิทธิภาพตามรูปแบบและหลักเกณฑ์ที่กฎหมายกำหนด
6. **การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล :** ธนาคารกำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมและเป็นไปตามมาตรฐานที่กฎหมายกำหนด ข้อมูลส่วนบุคคลต้องได้รับการรักษาความมั่นคงปลอดภัยด้วยมาตรการที่เหมาะสมตามที่ธนาคารกำหนด และกำหนดให้มีการทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มาตรการรักษาความมั่นคงปลอดภัยของธนาคารมีประสิทธิภาพอย่างต่อเนื่อง
7. **สิทธิของเจ้าของข้อมูลส่วนบุคคล :** ธนาคารกำหนดให้เจ้าของข้อมูลส่วนบุคคลสามารถใช้สิทธิต่างๆ ของตนตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลผ่านช่องทางที่ธนาคารได้แจ้งไว้ในประกาศแจ้งนโยบายการคุ้มครองข้อมูลส่วนบุคคลสำหรับลูกค้า
8. **หน้าที่ของธนาคารในฐานะผู้ควบคุมข้อมูลส่วนบุคคล :** ธนาคารกำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมและไม่น้อยกว่ามาตรฐานขั้นต่ำที่กฎหมายกำหนด และมีการทบทวนมาตรการดังกล่าวเมื่อจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป กรณีธนาคารต้องให้ข้อมูลส่วนบุคคลแก่บุคคลอื่น ธนาคารจะดำเนินการเพื่อป้องกันมิให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่มีอำนาจหรือโดยมิชอบ รวมถึงกำหนดให้มีระบบตรวจสอบเพื่อลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นระยะเวลาการเก็บรักษา หรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บข้อมูลส่วนบุคคลนั้น และกำหนดให้มีการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลตามหลักเกณฑ์และวิธีการที่กฎหมายกำหนด
9. **หน้าที่ของธนาคารในฐานะผู้ประมวลผลข้อมูลส่วนบุคคล :** ธนาคารกำหนดให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลต้องเป็นไปตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น โดยจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม มีการแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น และกำหนดให้มีการจัดทำและเก็บรักษาบันทึกการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลตามหลักเกณฑ์ที่กฎหมายกำหนด
10. **เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล :** ธนาคารกำหนดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลที่มีหน้าที่และความรับผิดชอบตามที่กฎหมายกำหนด
11. **การละเมิดข้อมูลส่วนบุคคล :** ธนาคารกำหนดให้การละเมิดข้อมูลส่วนบุคคลต้องมีการรายงานต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้าภายใน 72 ชั่วโมงนับแต่ทราบเหตุ และในกรณีการละเมิดมีแนวโน้มที่จะส่งผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ธนาคารจะดำเนินการแจ้งเหตุละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมแนวทางการเยียวยา
12. **การฝึกอบรม :** ธนาคารกำหนดให้พนักงานทุกคนต้องได้รับการอบรมเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลอย่างเพียงพอเพื่อให้ตระหนักถึงความสำคัญในเรื่องดังกล่าว และสามารถปฏิบัติงานได้อย่างถูกต้องตามกฎหมายและกฎเกณฑ์ทางการที่เกี่ยวข้อง