นโยบาย เรื่อง การคุ้มครองข้อมูลส่วนบุคคล
กลุ่มธุรกิจการเงินเกียรตินาคินภัทร

กรรมการ ผู้บริหาร และพนักงานของบริษัทในกลุ่มธุรกิจการเงินเกียรตินาคินภัทร ให้ความสำคัญในการปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล รวมถึงแนวทางการดำเนินการ หรือแนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่ออกโดยหน่วยงานกำกับดูแล สมาคม หรือองค์กรที่เกี่ยวข้อง ("กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล") จึงได้มีการจัดทำนโยบายฉบับนี้เพื่อใช้เป็นนโยบายหลักของบริษัทในกลุ่มธุรกิจฯ โดยผ่านการอนุมัติจากคณะกรรมการสูงสุดขององค์กร สำหรับใช้เป็นแนวทางในการปฏิบัติงานที่เป็นมาตรฐานเดียวกัน โดยมีวัตถุประสงค์ในการจัดทำนโยบาย ดังนี้

- เพื่อเป็นนโยบายในการกำกับดูแลการปฏิบัติงานด้านการคุ้มครองข้อมูลส่วนบุคคลให้สอดคล้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล โดยกลุ่มธุรกิจฯ และบริษัทในกลุ่มธุรกิจฯ มีหน้าที่ต้องปฏิบัติตามอย่างเคร่งครัด
- เพื่อให้การดำเนินธุรกิจของธนาคารและบริษัทในกลุ่มธุรกิจการเงินเกียรตินาคินภัทร สอดคล้องกับข้อกำหนดของกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลและสอดคล้องตามหลักมาตรฐานสากลว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
- เพื่อให้การดำเนินธุรกิจของธนาคารและบริษัทในกลุ่มธุรกิจการเงินเกียรตินาคินภัทร สอดคล้องกับจรรยาบรรณในการดำเนินธุรกิจ และหลักการกำกับดูแลกิจการที่ดี

นโยบายการคุ้มครองข้อมูลส่วนบุคคล กลุ่มธุรกิจการเงินเกียรตินาคินภัทร มีองค์ประกอบของนโยบายที่ใช้ในการกำกับดูแล แบ่งเป็น 12 หมวด ดังนี้

<u>หมวดที่ 1 หน้าที่และความรับผิดชอบในการปฏิบัติตามนโยบาย</u>

หน่วยงานทุกหน่วยงาน ทั้งของธนาคารและบริษัทในกลุ่มธุรกิจฯ มีหน้าที่ ดังนี้

1. ให้ความสำคัญ ปฏิบัติตาม และพิจารณาจัดทำนโยบาย หลักเกณฑ์ ระเบียบ คำสั่ง ประกาศ แนวปฏิบัติ หรือคู่มือการปฏิบัติงานของกลุ่มธุรกิจฯ ("นโยบายภายในของกลุ่มธุรกิจฯ") เพื่อใช้ในการกำกับดูแล สื่อสารให้พนักงานในกลุ่มธุรกิจฯ มีความรู้ความเข้าใจและสามารถปฏิบัติงานได้อย่างถูกต้อง และสอดคล้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัด
2. กำหนดกระบวนการปฏิบัติงานภายใน รวมถึงจัดให้มีระบบงานเทคโนโลยีสารสนเทศที่ใช้สนับสนุนกระบวนการปฏิบัติงานทางด้านการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม เพียงพอ และสอดคล้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลและ นโยบายภายในของกลุ่มธุรกิจฯ

พนักงานทุกคน ทั้งของธนาคารและบริษัทในกลุ่มธุรกิจฯ มีหน้าที่ ดังนี้

1. ให้ความสำคัญ ปฏิบัติตาม และให้ความร่วมมือในการเข้าอบรมความรู้เกี่ยวกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และนโยบายภายในของกลุ่มธุรกิจฯ อย่างเคร่งครัด
2. รายงานกรณีพบเหตุละเมิดข้อมูลส่วนบุคคลโดยมิชอบด้วยกฎหมาย ให้หัวหน้าหน่วยงานรับทราบเพื่อร่วมกันตรวจสอบข้อเท็จจริงของธุรกรรมดังกล่าว และแจ้งข้อมูลให้หน่วยงานกำกับดูแลการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA Team) ทราบทันทีเมื่อพบเหตุ
3. ไม่กระทำการเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาอันเนื่องจากการปฏิบัติงานให้แก่บุคคลอื่น เว้นแต่กฎหมายกำหนดข้อยกเว้นเป็นอย่างอื่น

หมวดที่ 2 การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

1. ดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเท่าที่จำเป็นและเหมาะสม ภายใต้ขอบเขตวัตถุประสงค์ตามที่ได้แจ้งแก่เจ้าของข้อมูลส่วนบุคคลเท่านั้น โดยการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล จะต้องสามารถอ้างอิงฐานทางกฎหมาย (Lawful Basis) อย่างน้อยฐานใดฐานหนึ่งได้
2. กำหนดบทบาทหน้าที่ความรับผิดชอบและแนวทางปฏิบัติงานระหว่างกลุ่มธุรกิจฯ กับคู่ค้า ผู้ให้บริการภายนอก และพันธมิตรทางธุรกิจ อย่างชัดเจน ไม่ว่าในฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล เพื่อให้แน่ใจได้ว่าบุคคลดังกล่าวสามารถปฏิบัติงานได้อย่างถูกต้อง สอดคล้องตามหน้าที่ความรับผิดชอบที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนด

หมวดที่ 3 การขอความยินยอมและการถอนความยินยอม

1. เมื่อมีความจำเป็นต้องขอความยินยอม กลุ่มธุรกิจฯ ต้องดำเนินการขอความยินยอมพร้อมแจ้งวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลกับเจ้าของข้อมูลส่วนบุคคล ก่อนหรือขณะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ให้เป็นไปตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนดอย่างเคร่งครัด ทั้งนี้ กลุ่มธุรกิจฯ ได้มีการจัดเตรียมช่องทางและวิธีการในการแจ้งความประสงค์ในกรณีที่เจ้าของข้อมูลส่วนบุคคลประสงค์จะขอถอนความยินยอมที่ได้ให้ไว้กลับกลุ่มธุรกิจฯ รวมถึงแจ้งผลกระทบอันอาจเกิดจากการขอถอนความยินยอมดังกล่าวให้เจ้าของข้อมูลส่วนบุคคลทราบ ตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนดเช่นเดียวกัน
2. หากเจ้าของข้อมูลส่วนบุคคลประสงค์จะขอถอนความยินยอม กลุ่มธุรกิจฯ จะตรวจสอบความถูกต้องและดำเนินการตามความประสงค์ของเจ้าของข้อมูลส่วนบุคคลอย่างไม่ชักช้า เว้นแต่มีข้อจำกัดสิทธิในการถอนความยินยอมโดยกฎหมาย ทั้งนี้ การถอนความยินยอมย่อมไม่ส่งผลกระทบต่อ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมไปโดยชอบแล้ว
3. การขอความยินยอมหรือการขอถอนความยินยอมอาจทำเป็นหนังสือ ทางโทรศัพท์ หรือดำเนินการผ่านช่องทางอิเล็กทรอนิกส์ โดยต้องมีหลักฐานหรือบันทึกในรูปแบบอิเล็กทรอนิกส์เพื่อยืนยันความถูกต้อง (Verification) และจัดเก็บไว้ตลอดเวลาที่ยังมีการประมวลผลข้อมูลตามวัตถุประสงค์ของการให้ความยินยอมนั้น

Kiatnakin Phatra Bank Public Company Limited
209 KKP Tower, Sukhumvit 21 (Asoke)
Khlong Toey Nua, Wattana, Bangkok 10110
Tel. +662 165 5555
Registration No. 0107536000986

ธนาคารเกียรตินาคินภัทร จำกัด (มหาชน)
209 อาคารเคเคพี ทาวเวอร์ ถนนสุขุมวิท 21 (อโศก)
แขวงคลองเตยเหนือ เขตวัฒนา กรุงเทพมหานคร 10110
โทรศัพท์ +662 165 5555
ทะเบียนเลขที่ 0107536000986

หมวดที่ 4 ประกาศความเป็นส่วนตัว (Privacy Notice)

พิจารณา ปรับปรุง และแก้ไขเพิ่มเติมเกี่ยวกับรายละเอียดของประกาศความเป็นส่วนตัว (Privacy Notice) ของกลุ่มธุรกิจฯ ให้สอดคล้องกับข้อเท็จจริงเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของกลุ่มธุรกิจฯ ให้เป็นปัจจุบัน โดยคำนึงถึงความเป็นธรรม (Fairness) การจำกัดวัตถุประสงค์และรายละเอียดในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (Purpose Limitation) ความยินยอม (Consent) และการอ้างผลประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interest) และต้องมีการเก็บบันทึกการปรับปรุงหรือแก้ไขเพิ่มเติมประกาศความเป็นส่วนตัว (Privacy Notice) ทุกครั้ง เพื่อเป็นหลักฐานประกอบการพิจารณาตรวจสอบในภายหลัง

ทั้งนี้ สามารถศึกษารายละเอียดเพิ่มเติมได้ที่ประกาศความเป็นส่วนตัว (Privacy Notice) กลุ่มธุรกิจการเงินเกียรตินาคินภัทร https://www.kkpfg.com/th/dataprotection

หมวดที่ 5 มาตรการรองรับการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

1. จัดให้มีช่องทาง มาตรการ และกระบวนการพิจารณาในการรองรับเมื่อมีการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลให้สอดคล้องและเป็นไปตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนด โดยกลุ่มธุรกิจฯ จะดำเนินการพิจารณา ตรวจสอบ และดำเนินการให้เจ้าของข้อมูลส่วนบุคคลใช้สิทธิได้โดยไม่ชักช้า
2. จัดให้มีการบันทึกการจัดการข้อมูลส่วนบุคคล เพื่อใช้เป็นหลักฐานเมื่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลหรือเจ้าของข้อมูลส่วนบุคคลร้องขอ

หมวดที่ 6 ระยะเวลาการเก็บรักษาและการลบทำลายข้อมูลส่วนบุคคล

1. กลุ่มธุรกิจฯ ต้องเก็บรักษาข้อมูลส่วนบุคคลเท่าที่จำเป็นภายใต้วัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลดังกล่าว จนกว่าเจ้าของข้อมูลส่วนบุคคลจะปิดบัญชีหรือยุติความสัมพันธ์กับกลุ่มธุรกิจฯ

   ทั้งนี้ กลุ่มธุรกิจฯ อาจมีความจำเป็นต้องเก็บรักษาข้อมูลส่วนบุคคลต่อไปตามระยะเวลาที่กฎหมายกำหนดหรือตามระยะเวลาที่นโยบายหรือระเบียบปฏิบัติงานภายในของกลุ่มธุรกิจฯ กำหนดเพื่อวัตถุประสงค์อย่างใดอย่างหนึ่งเป็นการเฉพาะ
2. กลุ่มธุรกิจฯ จะดำเนินการลบหรือทำลายข้อมูลส่วนบุคคล เมื่อสิ้นสุดความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล หรือสิ้นสุดระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล หรือเข้าเหตุกรณีอื่นใดที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนด

หมวดที่ 7 มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

กลุ่มธุรกิจฯ จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล (Data Security) ที่มีประสิทธิภาพ มีความเหมาะสมและสอดคล้องตามหลักเกณฑ์ที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนดและเป็นไปตามหลักการกำกับดูแลข้อมูลที่ดี (Data Governance) ทั้งที่อยู่ในระบบเทคโนโลยีสารสนเทศหรือที่อยู่นอกระบบเทคโนโลยีสารสนเทศ เพื่อมิให้ข้อมูลส่วนบุคคลเกิดการสูญหาย เสียหาย หรือมีการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือถูกเปิดเผย โดยปราศจากอำนาจหรือโดยมิชอบด้วยกฎหมาย

ทั้งนี้ กลุ่มธุรกิจฯ มีการทบทวนมาตรการดังกล่าวเมื่อมีการปรับปรุง เปลี่ยนแปลง แก้ไข กระบวนการปฏิบัติงานภายในกลุ่มธุรกิจฯ หรือเมื่อใดก็ตามที่ข้อกำหนดของกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลหรือกฎหมายอื่นใดที่เกี่ยวข้องมีการประกาศใช้บังคับใหม่ หรือมีการปรับปรุง เปลี่ยนแปลง แก้ไข เพื่อให้แน่ใจได้ว่ากลุ่มธุรกิจฯ มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสมและเพียงพอ

หมวดที่ 8 การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

กลุ่มธุกิจฯ มีการกำหนดกระบวนการและช่องทางการรับแจ้งเหตุละเมิดข้อมูลส่วนบุคคลรวมถึงการรั่วไหลของข้อมูลส่วนบุคคล โดยหากพิจารณาแล้วพบว่าเหตุละเมิดข้อมูลส่วนบุคคลฯ มีความเสี่ยงที่จะกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะดำเนินการแจ้งเหตุละเมิดดังกล่าวตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนดโดยไม่ชักช้า

หมวดที่ 9 การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

กลุ่มธุรกิจฯ ได้แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เพื่อกำกับดูแลการปฏิบัติงานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของกลุ่มธุรกิจฯ โดยบุคคลดังกล่าวต้องมีความรู้ความเข้าใจเกี่ยวกับกฎหมายและมาตรฐานสากลเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและมีความเป็นอิสระในการปฏิบัติงาน โดยสามารถรายงานไปยังผู้บริหารสูงสุดของกลุ่มธุรกิจฯ ได้โดยตรง และมีหน้าที่ต้องรักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่ของตน

หมวดที่ 10 การบริหารความเสี่ยงและการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล

กลุ่มธุรกิจฯ ได้จัดให้มีกระบวนการบริหารความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคลสำหรับผลิตภัณฑ์ บริการ ช่องทางการให้บริการ รวมทั้งกระบวนการปฏิบัติงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคล เพื่อให้ทราบว่าแต่ละผลิตภัณฑ์ บริการ ช่องทางการให้บริการ หรือกระบวนการปฏิบัติงานนั้น มีความเสี่ยงต่อการละเมิดข้อมูลส่วนบุคคลมากน้อยเพียงไร เพื่อพิจารณากำหนดแนวทางในการลดหรือบรรเทาความเสี่ยงที่อาจเกิดขึ้น ก่อนเริ่มให้บริการ รวมถึงจะมีการทบทวนความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคลสำหรับผลิตภัณฑ์ บริการ ช่องทางการให้บริการ หรือกระบวนการปฏิบัติงานอย่างสม่ำเสมอ และ กลุ่มธุรกิจฯ อาจจัดให้มีการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment หรือ DPIA) ตามหลักเกณฑ์การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลของกลุ่มธุรกิจฯ ที่เห็นสมควร

หมวดที่ 11 การตรวจสอบภายในเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

กลุ่มธุรกิจฯ กำหนดให้หน่วยงานตรวจสอบภายในทำหน้าที่ประเมินผลประสิทธิภาพในการปฏิบัติงานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลภายในองค์กรทั้งกระบวนการปฏิบัติงานโดยพนักงาน และระบบเทคโนโลยีสารสนเทศที่ใช้สนับสนุนในการปฏิบัติงาน อย่างน้อยปีละ 1 ครั้ง โดยให้รายงานตรงต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลและ/หรือคณะผู้บริหารระดับสูง

หมวดที่ 12 การฝึกอบรมความรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

กลุ่มธุรกิจฯ ให้ความสำคัญกับการฝึกอบรมและพัฒนาบุคลากรให้มีความรู้ความเข้าใจและวิธีปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล เพื่อป้องกันมิให้เกิดการละเมิดข้อมูลส่วนบุคคล หรือการรั่วไหลของข้อมูลส่วนบุคคล หรือเหตุการณ์ใดๆ ที่ไม่สอดคล้องตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยพนักงานใหม่ทุกคนต้องได้รับการอบรมความรู้พื้นฐานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ก่อนประเมินผลรับเป็นพนักงาน หรือในเวลาใดก็ตามที่มั่นใจได้ว่าพนักงานใหม่ที่คัดเลือกเข้ามาต้องผ่านการอบรมความรู้พื้นฐานดังกล่าว โดยมีการทดสอบหลังการอบรมเพื่อประเมินผลความรู้และมีการเก็บบันทึกประวัติการอบรมในหัวข้อดังกล่าวไว้เป็นหลักฐาน รวมถึงได้รับการอบรมทบทวนความรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง