

คำสั่งคณะกรรมการธนาคารอาคารสงเคราะห์
ที่ 19/2569
เรื่อง นโยบายคุ้มครองข้อมูลส่วนบุคคล

โดยที่คณะกรรมการธนาคารอาคารสงเคราะห์มีหน้าที่และอำนาจ ในการกำกับ ควบคุม และอำนวยความสะดวกของธนาคาร ให้เป็นไปตามวัตถุประสงค์ของธนาคาร อาศัยอำนาจตามความในมาตรา 17 แห่งพระราชบัญญัติธนาคารอาคารสงเคราะห์ พ.ศ. 2496 และที่แก้ไขเพิ่มเติม ประกอบกับคณะกรรมการธนาคารอาคารสงเคราะห์ในการประชุมครั้งที่ 10/2569 วันที่ 26 สิงหาคม 2569 มีมติอนุมัตินโยบายคุ้มครองข้อมูลส่วนบุคคล ซึ่งได้มีการทบทวนตามที่ฝ่ายจัดการเสนอ จึงให้ยกเลิกคำสั่งคณะกรรมการธนาคารอาคารสงเคราะห์ ที่ 37/2567 เรื่อง นโยบายคุ้มครองข้อมูลส่วนบุคคลธนาคารอาคารสงเคราะห์ ลงวันที่ 29 พฤศจิกายน 2567 และให้ใช้นโยบายคุ้มครองข้อมูลส่วนบุคคลฉบับนี้แทน เพื่อให้การบริหารจัดการด้านการคุ้มครองข้อมูลส่วนบุคคลของธนาคารมีทิศทางและกรอบการบริหารจัดการที่ชัดเจนสำหรับทุกหน่วยงานภายในธนาคารได้ถือปฏิบัติ และให้คณะกรรมการธนาคาร ผู้บริหาร และพนักงานถือเป็นแนวทางปฏิบัติโดยเคร่งครัด จึงจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคล โดยมีรายละเอียดดังนี้

1. หลักการและเหตุผล / บทนำ

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล และสิทธิของเจ้าของข้อมูลส่วนบุคคล ต้องเป็นไปตามกฎหมายธนาคารในฐานะผู้ควบคุมข้อมูลส่วนบุคคล ต้องปฏิบัติตามกฎหมายโดยเคร่งครัด ดังนั้น จึงได้กำหนดนโยบายเกี่ยวกับการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล เพื่อใช้เป็นแนวทางในการปฏิบัติให้เป็นมาตรฐานเดียวกันทั่วทั้งองค์กร

2. วัตถุประสงค์ของนโยบาย

2.1 เพื่อให้กรรมการ กรรมการผู้จัดการ ผู้บริหาร และผู้ปฏิบัติงาน ตระหนักและให้ความสำคัญในการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

2.2 เพื่อกำหนดแนวทางปฏิบัติของธนาคารให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

2.3 เพื่อให้ธนาคารปฏิบัติ กำกับดูแล ควบคุมการบริหารจัดการและรักษาความมั่นคงปลอดภัยด้านข้อมูลส่วนบุคคลอย่างเหมาะสม และมีแนวทางในการคุ้มครองข้อมูลส่วนบุคคลอย่างมีประสิทธิภาพ

3. ขอบเขตนโยบาย / ขอบเขตการบังคับใช้

นโยบายฉบับนี้ใช้บังคับกับกรรมการ กรรมการผู้จัดการ ผู้บริหาร และผู้ปฏิบัติงานที่มีส่วนเกี่ยวข้องในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

/4. คำจำกัดความ...

- 2 -

4. คำจำกัดความ / คำนิยาม

“ธนาคาร” หมายความว่า ธนาคารอาคารสงเคราะห์

“คณะกรรมการธนาคาร” หมายความว่า คณะกรรมการธนาคารอาคารสงเคราะห์

“กรรมการ” หมายความว่า กรรมการธนาคารอาคารสงเคราะห์

“กรรมการผู้จัดการ” หมายความว่า กรรมการผู้จัดการธนาคารอาคารสงเคราะห์

“ผู้บริหาร” หมายความว่า พนักงานที่มีตำแหน่งตั้งแต่ระดับผู้อำนวยการฝ่าย / สำนัก / ภาค หรือเทียบเท่าขึ้นไป หรือผู้บริหารตามสัญญาจ้างที่มีตำแหน่งเทียบเท่าผู้อำนวยการฝ่าย / สำนัก / ภาคขึ้นไป หรือผู้อำนวยการศูนย์ ทั้งนี้ ไม่รวมถึงพนักงานตำแหน่งผู้อำนวยการศูนย์ ที่อยู่ภายใต้สังกัดฝ่าย / ภาค

“ผู้ปฏิบัติงาน” หมายความว่า พนักงานที่มีตำแหน่งตั้งแต่ระดับผู้อำนวยการศูนย์ ที่อยู่ภายใต้สังกัดฝ่าย / ภาค ผู้ช่วยผู้อำนวยการฝ่าย / สำนัก / ภาค หรือเทียบเท่าลงมา รวมถึงพนักงานสัญญาจ้าง ลูกจ้างธนาคาร และลูกจ้างเหมางานธุรการ (Outsourced Staff)

“บุคคล” หมายความว่า บุคคลธรรมดา

“ข้อมูลส่วนบุคคล” (Personal Data) หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

“ข้อมูลอ่อนไหวส่วนบุคคล” (Sensitive Data) หมายความว่า ข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกัน

“เจ้าของข้อมูลส่วนบุคคล” (Data Subject) หมายความว่า บุคคลที่ข้อมูลส่วนบุคคลนั้น บ่งชี้ไปถึง

“ผู้ควบคุมข้อมูลส่วนบุคคล” (Data Controller) หมายความว่า ธนาคารซึ่งมีอำนาจหน้าที่ ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

“ผู้ประมวลผลข้อมูลส่วนบุคคล” (Data Processor) หมายความว่า บุคคลหรือนิติบุคคล ซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของธนาคาร ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

5. เนื้อหาของนโยบาย

หลักเกณฑ์การบริหารจัดการด้านการคุ้มครองข้อมูลส่วนบุคคลของธนาคาร มีดังนี้

5.1 ธนาคารดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยชอบด้วยกฎหมาย มีความเป็นธรรมและโปร่งใส

5.2 ธนาคารดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเท่าที่จำเป็น

/5.3 ธนาคาร...

5.3 ธนาคารดำเนินการแจ้งรายละเอียดเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผย ข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคล

5.4 การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลต้องเป็นไปตามวัตถุประสงค์ อันชอบด้วยกฎหมายที่ธนาคารได้แจ้งรายละเอียดไว้กับเจ้าของข้อมูลส่วนบุคคล

5.5 การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ต้องได้รับความยินยอม จากเจ้าของข้อมูลส่วนบุคคล เว้นแต่กฎหมายให้อำนาจธนาคารสามารถทำได้

5.6 การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลอ่อนไหวส่วนบุคคล (Sensitive Data) ต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่กฎหมายให้อำนาจธนาคารสามารถทำได้

5.7 การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของธนาคารมีความถูกต้องสมบูรณ์ และเป็นปัจจุบัน

5.8 ธนาคารต้องกำหนดกระบวนการและวิธีปฏิบัติ รวมถึงจัดให้มีระบบด้านเทคโนโลยีสารสนเทศ ในการขอความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคล

5.9 ธนาคารต้องกำหนดกระบวนการและวิธีปฏิบัติ รวมถึงจัดให้มีระบบด้านเทคโนโลยีสารสนเทศ กรณีเจ้าของข้อมูลส่วนบุคคลขอใช้สิทธิตามกฎหมาย ได้แก่

- (1) การเพิกถอนความยินยอม
- (2) การเข้าถึงข้อมูลส่วนบุคคล
- (3) การแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง
- (4) การลบข้อมูลส่วนบุคคล
- (5) การระงับการใช้ข้อมูลส่วนบุคคล
- (6) การขอรับข้อมูลส่วนบุคคลเกี่ยวกับตน / ขอให้โอนย้ายข้อมูลส่วนบุคคล

ด้วยวิธีการอัตโนมัติ

- (7) การคัดค้านการประมวลผลข้อมูลส่วนบุคคล

5.10 ธนาคารต้องกำหนดกระบวนการและวิธีปฏิบัติในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล รวมถึงแนวทางการประเมินความเสี่ยงกรณีเกิดเหตุการละเมิดข้อมูลส่วนบุคคล พร้อมแนวทางการเยียวยา เจ้าของข้อมูลส่วนบุคคล

5.11 ธนาคารต้องกำหนดกระบวนการและวิธีปฏิบัติในการจัดเก็บ การลบ การทำลาย ข้อมูลส่วนบุคคล

5.12 ธนาคารในฐานะผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ต้องดำเนินการจัดให้มี ข้อตกลงในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล กับผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) ของธนาคาร

/5.13 ธนาคาร...

- 4 -

5.13 ธนาคารมีการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

5.14 ธนาคารต้องกำหนดกระบวนการและวิธีปฏิบัติ รวมถึงจัดให้มีระบบด้านเทคโนโลยีสารสนเทศ ในการบันทึกรายการการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities : ROPA) และ ประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment : DPIA)

5.15 ธนาคารมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

5.16 ธนาคารมีการแก้ไขปัญหาและจัดการเรื่องร้องเรียน (Problem and complaint handling)

5.17 ธนาคารจัดให้มีระบบการควบคุม กำกับ และตรวจสอบ (3 Lines of defense)

5.18 ธนาคารเก็บข้อมูลส่วนบุคคลไว้จนกว่าจะพ้นภาระผูกพันตามกฎหมาย

6. หน้าที่และอำนาจผู้ที่เกี่ยวข้องกับนโยบาย

6.1 คณะกรรมการธนาคาร

- (1) อนุมัตินโยบายคุ้มครองข้อมูลส่วนบุคคลของธนาคาร
- (2) ทบทวนและประเมินประสิทธิภาพของนโยบาย กระบวนการ และ วิธีปฏิบัติอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ
- (3) ดูแลให้ธนาคารปฏิบัติตามนโยบายและกฎหมายคุ้มครองข้อมูลส่วนบุคคล อย่างเคร่งครัด

6.2 กรรมการผู้จัดการ

- (1) กำหนดให้มีกระบวนการ และวิธีปฏิบัติ รวมทั้งมีระบบงานที่รองรับ การบริหารจัดการและรักษาความปลอดภัยด้านข้อมูลส่วนบุคคลให้สอดคล้องกับนโยบายคุ้มครองข้อมูลส่วนบุคคล อย่างเหมาะสมและมีประสิทธิภาพ
- (2) กำหนดและทบทวนหน้าที่และอำนาจของคณะกรรมการ / คณะทำงาน ชุดต่าง ๆ ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล
- (3) กำหนดให้มีการจัดทำระเบียบ คู่มือปฏิบัติงาน หรือ แนวปฏิบัติที่ดี ในการดำเนินการที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล และกำหนดให้มีการติดตามและควบคุมดูแล ภาพรวมของการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้การดำเนินธุรกิจของธนาคารเป็นไปตามกฎหมาย
- (4) กำหนดให้มีการสื่อสารให้ผู้บริหาร และผู้ปฏิบัติงาน เข้าใจถึงความสำคัญ ของนโยบายคุ้มครองข้อมูลส่วนบุคคล และการดำเนินการที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

7. การประเมินและรายงานผลการปฏิบัติงาน

เพื่อให้การนำนโยบายไปสู่การปฏิบัติได้ผลอย่างจริงจัง เป็นไปตามกฎหมาย กฎระเบียบ นโยบายและคู่มือปฏิบัติงานธนาคาร จึงได้กำหนดให้ผู้บริหาร และผู้ปฏิบัติงานที่เกี่ยวข้องทำหน้าที่ ในการประเมินและรายงานผลการปฏิบัติงานธนาคารให้เป็นไปตามนโยบายอย่างเคร่งครัด

/8. อำนาจ...

8. อำนาจอนุมัติและการทบทวนนโยบาย

คณะกรรมการธนาคารเป็นผู้อนุมัตินโยบาย โดยธนาคารต้องจัดให้มีการทบทวนและประเมินประสิทธิภาพของนโยบายเสนอคณะกรรมการธนาคารพิจารณา อย่างน้อยปีละ 1 ครั้ง หรือหากมีการเปลี่ยนแปลงซึ่งมีผลกระทบอย่างมีนัยสำคัญ ให้นำเสนอคณะกรรมการธนาคารพิจารณา เพื่อให้มั่นใจว่านโยบายดังกล่าวเหมาะสมกับสภาพแวดล้อมการดำเนินงานของธนาคาร

ทั้งนี้ ตั้งแต่วันที่ 26 สิงหาคม 2569 เป็นต้นไป

สั่ง ณ วันที่ 4 กันยายน 2569



(นายอัศรุตม์ สนธยานนท์)

ประธานกรรมการธนาคารอาคารสงเคราะห์