SME Development Bank
ธนาคารพัฒนาวิสาหกิจขนาดกลางและขนาดย่อมแห่งประเทศไทย
310 อาคาร SME Bank Tower ถนนพหลโยธิน แขวงสามเสนใน เขตพญาไท
กรุงเทพฯ 10400 โทร.0-2265-3000 โทรสาร 0-2265-4000
Small and Medium Enterprise Development Bank of Thailand
310 SME Bank Tower, Phahonyothin Road, Samsen-Nai, Phayathai,
Bangkok 10400 www.smebank.co.th SWIFT : SMEBTHBK Call Center1357

คำสั่ง

ธนาคารพัฒนาวิสาหกิจขนาดกลางและขนาดย่อมแห่งประเทศไทย

ที่ 51 /2565

เรื่อง นโยบายคุ้มครองข้อมูลส่วนบุคคล

ตามมติที่ประชุมคณะกรรมการกำกับความเสี่ยง ครั้งที่ 5/2565 เมื่อวันที่ 17 พฤษภาคม 2565 อนุมัติทบทวนนโยบายคุ้มครองข้อมูลส่วนบุคคล ปี 2565 เพื่อให้ธนาคารมีการปฏิบัติเป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นการยกระดับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าธนาคารให้เป็นไปตามที่กฎหมายกำหนด ในการการเก็บรวบรวมข้อมูล การใช้ข้อมูล การประมวลผลข้อมูลตลอดจนการเปิดเผยข้อมูลส่วนบุคคลต่อบุคคลภายนอก รวมทั้งการเข้าถึงข้อมูลส่วนบุคคล และการรักษาความปลอดภัยของข้อมูลส่วนบุคคล เพื่อให้ข้อมูลส่วนบุคคลที่ธนาคารเก็บรักษาไว้ นำไปใช้ตรงตามความต้องการของเจ้าของข้อมูลส่วนบุคคลและถูกต้องตามกฎหมาย

ทั้งนี้ ให้พนักงาน หน่วยงาน และคณะกรรมการชุดต่างๆ ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ถือปฏิบัติตามนโยบายคุ้มครองข้อมูลส่วนบุคคล ที่แนบมาท้ายคำสั่งฉบับนี้อย่างเคร่งครัด และให้ยกเลิกคำสั่งคณะกรรมการธนาคารที่ 33/2564 สั่ง ณ วันที่ 15 กันยายน 2564 เรื่อง นโยบายคุ้มครองข้อมูลส่วนบุคคล

ให้คำสั่งฉบับนี้มีผลใช้บังคับตั้งแต่วันที่ 1 มิถุนายน 2565 เป็นต้นไป

สั่ง ณ วันที่ 31 พฤษภาคม 2565

(นางสาวนารถนารี รัฐปัตย์)
กรรมการผู้จัดการ

ฝ่ายกำกับการปฏิบัติงานและคุ้มครองข้อมูลส่วนบุคคล
โทร. 02-265-3000 ต่อ 3834 ธัญนันท์

หน่วยงานเจ้าของเรื่อง : ฝ่ายกำกับการปฏิบัติงานและคุ้มครองข้อมูลส่วนบุคคล โทร. 086-3939289, 3840

นโยบายคุ้มครองข้อมูลส่วนบุคคล
ปี 2565

สารบัญ

ส่วนที่ 1 : บทนำ

1.1 เหตุผลและความจำเป็น

เพื่อให้ธนาคารพัฒนาวิสาหกิจขนาดกลางและขนาดย่อมแห่งประเทศไทย (ธนาคาร) มีการปฏิบัติเป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล) ธนาคารจึงได้กำหนดนโยบายคุ้มครองข้อมูลส่วนบุคคลขึ้น เพื่อยกระดับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลให้เป็นไปตามที่กฎหมายกำหนด ในการเก็บรวบรวมข้อมูล ใช้ข้อมูล และประมวลผลข้อมูล ตลอดจนการเปิดเผยข้อมูลส่วนบุคคลต่อบุคคลภายนอก รวมทั้งการเข้าถึงข้อมูลส่วนบุคคล และการรักษาความปลอดภัยของข้อมูลส่วนบุคคล เพื่อให้ข้อมูลส่วนบุคคลที่ธนาคารเก็บรักษาไว้นำไปใช้ตรงตามความต้องการของเจ้าของข้อมูลส่วนบุคคล และถูกต้องตามกฎหมาย

1.2 วัตถุประสงค์ของนโยบาย

เพื่อให้มั่นใจว่าธนาคารได้ตระหนัก และเข้าใจถึงการคุ้มครองข้อมูลส่วนบุคคล และเพื่อเป็นแนวทางในการนำ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ไปถือปฏิบัติโดยให้เป็นตามมาตรฐานเหมาะสม และสอดคล้องกับความเสี่ยง และวิธีการดำเนินธุรกิจของธนาคาร และเพื่อใช้เป็นแนวทางในการพัฒนาแนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล และการบริหารจัดการข้อมูลได้อย่างเหมาะสม รวมถึงกฎหมายอื่นที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

1.3 หลักการและเนื้อหา

ธนาคารต้องจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลเป็นลายลักษณ์อักษร และดำเนินการทบทวนเป็นประจำอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ รวมถึงต้องจัดให้มีการสื่อสารนโยบายคุ้มครองข้อมูลส่วนบุคคลให้กับพนักงาน และผู้ที่มีส่วนเกี่ยวข้องต่างๆ ของธนาคารได้ทราบถึงเนื้อหาของนโยบาย ตลอดจนต้องมีการกำหนดขั้นตอนการปฏิบัติงานของธนาคารที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลให้สอดคล้องกับนโยบาย

1.4 คำนิยาม

1.4.1 ข้อมูลส่วนบุคคล (Personal Data) หมายความว่า ข้อมูลเกี่ยวกับบุคคลธรรมดาซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรม

1.4.2 ข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal Data) หมายความว่า ข้อมูลส่วนบุคคลที่เป็นเรื่องเกี่ยวกับเรื่องส่วนตัวโดยแท้ของบุคคล ซึ่งมีความละเอียดอ่อน และสุ่มเสี่ยงต่อการเลือกปฏิบัติอย่างไม่เป็นธรรม หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด เช่น ข้อมูลที่เกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนา หรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสุขภาพจิต ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ อาทิ ข้อมูลอัตลักษณ์เสียง ข้อมูลจำลองใบหน้า ข้อมูลจำลองม่านตา ข้อมูลจำลองลายนิ้วมือ

1.4.3 ผู้ควบคุม.../2

1.4.3 ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) หมายความว่า บุคคล หรือนิติบุคคล หรือหน่วยงานรัฐใดซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวมข้อมูล ใช้ข้อมูล หรือเปิดเผยข้อมูลส่วนบุคคล

1.4.4 บุคคล หมายความว่า บุคคลธรรมดา

1.4.5 ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) หมายความว่า บุคคล หรือนิติบุคคล ซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวมข้อมูล ใช้ข้อมูล หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่ง หรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ทั้งนี้ บุคคล หรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

1.4.6 เจ้าของข้อมูลส่วนบุคคล (Data Subject) หมายความว่า บุคคลใดๆ ที่ข้อมูลใดๆ สามารถระบุตัวตนได้ ไม่ว่าทางตรงหรือทางอ้อม

1.4.7 เจ้าของข้อมูล (Data Owner) หมายความว่า ผู้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นรั่วไหล หรือเกิดสูญหาย

1.4.8 การประมวลผลข้อมูลส่วนบุคคล (Processing of Personal Data) หมายความว่า การดำเนินการ หรือชุดการดำเนินการใดๆ กับข้อมูลส่วนบุคคล เช่น การจัดเก็บ รวบรวม การบันทึก การจัดระบบจัดโครงสร้าง การปรับปรุง หรือการแก้ไข การดึงข้อมูล การใช้ การเปิดเผย การส่งต่อการเผยแพร่ หรือการกระทำใดๆ เพื่อให้พร้อมใช้งาน การใช้ การรวบรวม การลบ หรือการทำลายข้อมูล

1.4.9 การรั่วไหลของข้อมูลส่วนบุคคล (Personal Data Breach) หมายความว่า การรั่วไหล หรือละเมิดมาตรการความมั่นคงปลอดภัยต่อข้อมูลส่วนบุคคลทำให้เกิดความเสียหาย สูญหาย เปลี่ยนแปลง เปิดเผยโดยไม่ได้รับอนุญาต หรือการเข้าถึงข้อมูลส่วนบุคคลที่ใช้งาน

1.4.10 ผลิตภัณฑ์ (Product) หมายความว่า สินเชื่อ บริการอื่นๆ และหมายความรวมถึงมาตรการที่ธนาคารให้ความช่วยเหลือแก่ลูกค้า

1.4.11 ลูกค้า (Customer) หมายความว่า นิติบุคคล หรือบุคคลที่มีการตกลงกันทางกฎหมายซึ่งมีความสัมพันธ์ทางธุรกิจ หรือทำธุรกรรมกับธนาคาร

1.4.12 คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Committee) หมายความว่า คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1.4.13 การลบข้อมูล (Data Deletion) หมายความว่า การทำให้ข้อมูลส่วนบุคคลนั้นถูกลบออกจากระบบ และไม่อาจกู้คืนได้โดยตัวเจ้าของข้อมูลส่วนบุคคล (Data Subject) ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) หรือผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

1.4.14 การทำ.../3

1.4.14 การทำข้อมูลนิรนาม (Data Anonymization) หมายความว่า กระบวนการในการทำให้ข้อมูลส่วนบุคคลไม่สามารถระบุตัวบุคคลได้ เพื่อแสดงถึงการที่จะทำให้ไม่สามารถนำกลับมาระบุตัวบุคคลได้อีกครั้ง

1.4.15 ข้อมูลนิรนาม (Anonymized Data) หมายความว่า ข้อมูลที่ไม่สามารถใช้เพื่อระบุตัวตนของบุคคลใดบุคคลหนึ่งได้

1.4.16 โปรไฟลิ่ง (Profiling) หมายความว่า รูปแบบการประมวลผลข้อมูลส่วนบุคคลใดๆ ซึ่งมีการใช้ข้อมูลส่วนบุคคลในการประเมินลักษณะเกี่ยวกับบุคคลบางประการ โดยเฉพาะอย่างยิ่ง เพื่อวิเคราะห์หรือคาดการณ์เกี่ยวกับบุคคลในเรื่องประสิทธิภาพในการทำงาน สถานะทางเศรษฐกิจ สุขภาพของบุคคล ความชื่นชอบส่วนบุคคล พฤติกรรมบุคคล ความน่าเชื่อถือ ตำแหน่งทางภูมิศาสตร์ หรือความเคลื่อนไหวของบุคคล

1.4.17 เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO) หมายความว่า เจ้าหน้าที่ของธนาคารที่มาดูแลข้อมูลส่วนบุคคลภายในธนาคาร หรือบุคคลอื่นภายนอกธนาคารที่ทำสัญญาให้บริการกับธนาคารที่ทำหน้าที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1.4.18 คุกกี้ (Cookies) หมายความว่า ไฟล์คอมพิวเตอร์ขนาดเล็ก ซึ่งถูกบันทึกไว้ในอุปกรณ์คอมพิวเตอร์ หรือเครื่องมือสื่อสารของเจ้าของข้อมูลส่วนบุคคล เช่น สมาร์ตโฟน แท็บเล็ต หรือผ่านทางเว็บเบราว์เซอร์ในขณะที่เจ้าของข้อมูลส่วนบุคคลเข้าใช้งานระบบเว็บไซต์

ส่วนที่ 2.../4

ส่วนที่ 2 : นโยบายคุ้มครองข้อมูลส่วนบุคคล

หมวดที่ 1 หลักการสำคัญในการคุ้มครองข้อมูลส่วนบุคคล

1.1 การระบุข้อมูลส่วนบุคคลมีหลักในการพิจารณา 3 ลักษณะ ดังนี้

1.1.1 การแยกแยะ หมายความว่า การที่ข้อมูลมีความสามารถในการระบุแยกตัวบุคคลออกจากกันได้ เช่น หมายเลขประจำตัวประชาชน หมายเลขหนังสือเดินทาง หรือข้อมูลทางชีวภาพ เช่น รูปภาพใบหน้า ลายนิ้วมือ ฟิล์มเอกซเรย์ ข้อมูลสแกนม่านตา ข้อมูลอัตลักษณ์เสียง ข้อมูลพันธุกรรม

1.1.2 การติดตาม หมายความว่า การที่สามารถใช้ข้อมูลในการติดตาม เพื่อระบุลักษณะจำเพาะของบุคคลนั้น เช่น พฤติกรรม หรือกิจกรรมที่บุคคลนั้นกระทำ

1.1.3 การเชื่อมโยง หมายความว่า การที่ข้อมูลมีคุณสมบัติในการเชื่อมโยงกัน และระบุไปยังตัวบุคคลได้ เช่น วันเกิด สถานที่เกิด น้ำหนัก ส่วนสูง ข้อมูลตำแหน่งทางภูมิศาสตร์

1.2 การเก็บรวบรวมข้อมูล การนำไปใช้ และประมวลผลข้อมูลส่วนบุคคล

ในการประมวลผลข้อมูลส่วนบุคคลธนาคารจะดำเนินการโดยชอบด้วยกฎหมาย มีความโปร่งใส และเป็นธรรม โดยข้อมูลส่วนบุคคลจะถูกนำไปใช้เพื่อวัตถุประสงค์ในการดำเนินงานของธนาคารอย่างถูกต้องตามกฎหมาย เช่น การนำข้อมูลลูกค้า และพฤติกรรมการใช้บริการไปใช้ในการวิเคราะห์เพื่อการออกแบบผลิตภัณฑ์และบริการของธนาคาร รวมถึงการนำเสนอข้อเสนอพิเศษต่างๆ ที่ดีขึ้นกว่าเดิม เพื่อให้เป็นไปตามความต้องการของลูกค้าและการให้บริการที่ดีที่สุดของธนาคาร ทั้งนี้ ธนาคารจะเก็บรวบรวมข้อมูลส่วนบุคคลของลูกค้าเท่าที่จำเป็นและเกี่ยวข้อง และนำไปใช้ให้เป็นไปตามวัตถุประสงค์ของลูกค้าเท่านั้น โดยข้อมูลส่วนบุคคลที่ธนาคารเก็บรวบรวม มีความถูกต้อง เป็นปัจจุบัน และระยะเวลาในการเก็บรักษาข้อมูลเป็นไปโดยเหมาะสมกับวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล หรือตามระยะเวลาที่กฎหมายกำหนด และมีมาตรการในการรักษาข้อมูลเหล่านั้นไว้เป็นความลับ ตามเกณฑ์มาตรฐานความปลอดภัยชั้นสูงของธนาคาร ตลอดจนจะป้องกันมิให้มีการนำข้อมูลไปใช้โดยมิได้รับอนุญาตจากเจ้าของข้อมูลส่วนบุคคลก่อน

1.3 การใช้ข้อมูลส่วนบุคคล

เพื่อเป็นการรักษาสิทธิในความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคล (Data Subject) ที่ธนาคารเก็บรวบรวมไว้ ธนาคารจะไม่อนุญาตให้มีการเปิดเผยข้อมูลใดๆ นอกจากเจ้าหน้าที่ผู้ที่ได้รับอนุญาตจากธนาคาร และบุคคลที่สามตามที่ได้รับอนุญาตจากเจ้าของข้อมูล (Data Owner) ให้เข้าถึงข้อมูลตลอดจนมีการดำเนินการป้องกันมิให้มีการนำข้อมูลดังกล่าวไปใช้โดยมิได้รับอนุญาตจากเจ้าของข้อมูลส่วนบุคคล (Data Subject) ก่อน โดยธนาคารจะทำการกำหนดมาตรการการเข้าถึง และใช้ข้อมูลในแต่ละประเภทตามเหตุการณ์ หรือสถานการณ์เฉพาะ หรือตำแหน่งของบุคคลที่เกี่ยวข้อง เพื่อป้องกันไม่ให้เกิดความเสียหายหรือละเมิดต่อสิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject)

ทั้งนี้.../5

ทั้งนี้ ในกรณีที่ธนาคารมีการทำความตกลงกับบุคคลภายนอกที่เป็นคู่สัญญาบุคคลที่มีอำนาจหน้าที่ตามที่ธนาคารหรือตามที่กฎหมายกำหนดพันธมิตรทางธุรกิจหรือตัวแทนที่เป็นผู้จำหน่าย ผู้ให้บริการ หรือผู้รับจ้างของธนาคาร เพื่อพัฒนาระบบงาน อุปกรณ์ หรือปรับปรุงผลิตภัณฑ์ และกระบวนการในการให้บริการของธนาคารเพื่อเพิ่มประสิทธิภาพในการดำเนินธุรกิจของธนาคาร บุคคลภายนอกดังกล่าวจะต้องตกลงที่จะรักษาข้อมูลลูกค้าของธนาคารไว้เป็นความลับตามมาตรฐานการรักษาข้อมูลส่วนบุคคลของธนาคาร และต้องผูกพันรับผิดชอบตามกฎหมายที่มีผลใช้บังคับด้วย

1.4 การให้ความยินยอม

หลักการในการขอความยินยอม (Consent) จากเจ้าของข้อมูลส่วนบุคคล (Data Subject) ธนาคารจะพิจารณา ดังนี้

1.4.1 ต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล (Data Subject) ก่อนจึงจะเก็บข้อมูลรวบรวมข้อมูลใช้ข้อมูล เปิดเผยข้อมูลนั้นๆ ได้

1.4.2 เจ้าของข้อมูลส่วนบุคคล (Data Subject) สามารถถอนความยินยอมเมื่อใดก็ได้ โดยจะต้องถอนความยินยอมได้ง่ายเช่นเดียวกับการให้ความยินยอม เว้นแต่มีข้อจำกัดสิทธิในการถอนความยินยอมโดยกฎหมาย หรือสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคล (Data Subject)

1.4.3 ในการขอความยินยอมนั้นจะต้องคำนึงถึงอิสระของเจ้าของข้อมูลส่วนบุคคล (Data Subject) และให้สิทธิเจ้าของข้อมูลส่วนบุคคล (Data Subject) สามารถปฏิเสธไม่ให้ความยินยอมได้

1.4.4 การขอความยินยอมจะต้องกระทำอย่างชัดเจนไม่คลุมเครือ การออกแบบแบบฟอร์มการขอความยินยอมนั้น เจ้าของข้อมูลส่วนบุคคล (Data Subject) สามารถเห็นได้อย่างชัดเจนว่าธนาคารขอความยินยอมในการประมวลผลข้อมูลเพื่อวัตถุประสงค์ใดบ้าง เช่น การทำ Check Box ให้เจ้าของข้อมูลส่วนบุคคล (Data Subject) ระบุได้ หรือกรณีการขอความยินยอมในรูปแบบวาจา (Verbal Consent) ต้องมีการบันทึกในรูปแบบเสียง และธนาคารต้องมีกระบวนการพิสูจน์ และยืนยันตัวตนของลูกค้าก่อนการขอความยินยอมเพื่อให้มั่นใจว่าคู่สนทนาเป็นลูกค้าของธนาคารจริง

1.4.5 การขอความยินยอมจะทำในรูปแบบเป็นหนังสือ หรือทำโดยผ่านระบบอิเล็กทรอนิกส์ก็ได้

1.4.6 การขอความยินยอมจากผู้เยาว์ ต้องใช้ภาษาที่ง่าย และมีความเหมาะสมกับระดับความเข้าใจของผู้เยาว์ มีความชัดเจน ไม่ก่อให้เกิดความเข้าใจผิด และมีความสอดคล้องกับประมวลกฎหมายแพ่งและพาณิชย์

1.5 การถอนความยินยอม

เจ้าของข้อมูลส่วนบุคคล (Data Subject) มีสิทธิที่จะขอเพิกถอนความยินยอม (Right to Withdraw of Consent) ที่ให้ไว้ ธนาคารต้องหยุดประมวลผลข้อมูลที่เจ้าของข้อมูลส่วนบุคคล (Data Subject) เคยให้ความยินยอมไว้ และหากธนาคารไม่มีหน้าที่ในการปฏิบัติตามกฎหมายอื่นที่จะต้องเก็บรักษาข้อมูลส่วนบุคคลต่อไป ธนาคารต้องดำเนินการลบข้อมูลทันที โดยธนาคารต้องจัดให้มีช่องทางที่เจ้าของข้อมูลส่วนบุคคล (Data Subject) สามารถใช้สิทธิถอนความยินยอมได้ง่าย และเมื่อใดก็ได้เช่นเดียวกับการให้ความยินยอม เว้นแต่มีข้อจำกัดสิทธิในการถอนความยินยอมโดยกฎหมาย หรือสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคล (Data Subject)

1.6 แนวทาง.../6

1.6 แนวทางในการเก็บรวบรวมข้อมูลส่วนบุคคล และฐานในการประมวลผล

ห้ามธนาคารเก็บข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว หากไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล (Data Subject) เว้นแต่ในกรณีที่ได้รับการยกเว้นตามกฎหมาย

ในกรณีที่มีความจำเป็นเพื่อปฏิบัติตามกฎหมาย หากเจ้าของข้อมูลส่วนบุคคล (Data Subject) ไม่เปิดเผยข้อมูลดังกล่าวอาจส่งผลให้เจ้าของข้อมูลส่วนบุคคล (Data Subject) ละเมิดต่อกฎหมายได้ หรือไม่สามารถทำธุรกรรม หรือได้รับสิทธิประโยชน์ตามที่กฎหมายกำหนดไว้ นอกจากนี้ การที่เจ้าของข้อมูลส่วนบุคคล (Data Subject) ไม่ให้ข้อมูลส่วนบุคคลในกรณีที่มีความจำเป็นเพื่อเข้าทำสัญญา หรือเพื่อปฏิบัติตามสัญญากับธนาคาร ย่อมส่งผลให้ถูกปฏิเสธการเข้าทำสัญญา หรือรับชำระหนี้ตามสัญญาที่ได้ทำไว้กับธนาคาร

ธนาคารจะทำการขอความยินยอมโดยชัดแจ้งเป็นหนังสือหรือผ่านระบบอิเล็กทรอนิกส์ เว้นแต่ไม่สามารถขอความยินยอมด้วยวิธีการเช่นว่านั้นได้ พร้อมทั้งแจ้งวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลก่อนหรือในขณะที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล (Data Subject) ในการนี้เจ้าของข้อมูลส่วนบุคคล (Data Subject) มีสิทธิในการปฏิเสธการให้ความยินยอมได้โดยอิสระ และไม่อยู่ภายใต้บังคับของธนาคาร อย่างไรก็ดี ภายใต้ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ธนาคารอาจเก็บรวบรวมข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล (Data Subject) โดยไม่ต้องได้รับความยินยอมภายใต้ฐานทางกฎหมาย ดังต่อไปนี้

1.6.1 ฐานสัญญา : เป็นการจำเป็นเพื่อปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคล (Data Subject) เป็นคู่สัญญา หรือเพื่อดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคล (Data Subject) ก่อนเข้าทำสัญญา

1.6.2 ฐานการปฏิบัติตามกฎหมาย : เพื่อปฏิบัติตามกฎหมายของธนาคาร

1.6.3 ฐานประโยชน์อันชอบธรรม : เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของธนาคาร หรือของบุคคล หรือนิติบุคคลอื่น เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล (Data Subject)

1.6.4 ฐานประโยชน์สำคัญต่อชีวิต : เพื่อป้องกัน หรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

1.6.5 ฐานจดหมายเหตุ/วิจัย/สถิติ : เพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์ หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัย หรือสถิติ โดยธนาคารจะจัดให้มีมาตรการป้องกันเหมาะสม เพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล (Data Subject)

1.6.6 ฐานภารกิจของรัฐ : เป็นการจำเป็นเพื่อปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะ หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบหมายให้แก่ธนาคาร

นอกจากนี้.../7

นอกจากนี้ ธนาคารจะเก็บรวบรวมข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล (Data Subject) ต่อเมื่อธนาคารได้ข้อมูลจากเจ้าของข้อมูลส่วนบุคคล (Data Subject) โดยตรง กรณีที่ธนาคารได้รับข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล (Data Subject) จากแหล่งอื่น ธนาคารจะแจ้งให้เจ้าของข้อมูลส่วนบุคคล (Data Subject) ทราบถึงการเก็บรวบรวมนั้นภายใน 30 วัน นับแต่วันที่ทำการเก็บรวบรวม และหากเป็นการเก็บรวบรวมเพื่อทำการติดต่อถึงเจ้าของข้อมูลส่วนบุคคล (Data Subject) ธนาคารจะทำการแจ้งต่อเจ้าของข้อมูลส่วนบุคคล (Data Subject) ในครั้งแรกที่ทำการติดต่อไป หรือหากเป็นการเปิดเผยข้อมูลธนาคารจะทำการแจ้งไปยังเจ้าของข้อมูลส่วนบุคคล (Data Subject) ก่อนทำการเปิดเผยข้อมูลนั้นๆ ทั้งนี้ เว้นแต่มีข้อยกเว้นตามกฎหมายกำหนดให้ไม่ต้องดำเนินการเช่นว่านั้น

1.7 การประกาศความเป็นส่วนตัว

ประกาศความเป็นส่วนตัวเป็นข้อความ หรือรายละเอียดที่ธนาคารต้องแสดงกับเจ้าของข้อมูลส่วนบุคคล (Data Subject) เพื่ออธิบายเกี่ยวกับรายละเอียดในการประมวลผลข้อมูล เพื่อเพิ่มความโปร่งใสตามหลักการประมวลผลข้อมูลส่วนบุคคลโดยชอบด้วยกฎหมาย และเพื่อความเชื่อมั่นแก่เจ้าของข้อมูลส่วนบุคคล (Data Subject) ว่าข้อมูลที่ตนได้ให้ไว้กับธนาคาร หรือที่ธนาคารได้มาจากแหล่งอื่นนั้น จะไม่ถูกนำไปประมวลผลนอกเหนือจากรายละเอียดตามที่ระบุไว้ในประกาศความเป็นส่วนตัว นอกจากนี้ธนาคารจะต้องแจ้งประกาศความเป็นส่วนตัวแก่ลูกค้าด้วยวิธีการ หรือช่องทางที่ลูกค้าเข้าถึงง่ายอาจทำในรูปแบบเป็นหนังสือหรือผ่านระบบอิเล็กทรอนิกส์

หมวดที่ 2 การเปิดเผยข้อมูลส่วนบุคคลต่อบุคคลที่สาม

ธนาคารจะใช้และเปิดเผยข้อมูลส่วนบุคคลภายใต้วัตถุประสงค์ที่ได้ระบุไว้ในประกาศความเป็นส่วนตัว นอกจากนี้ธนาคารจะไม่เปิดเผยข้อมูลส่วนบุคคลหรือข้อมูลอื่นใด ที่สามารถบ่งชี้ได้ว่าเป็นของลูกค้าหรือผู้เกี่ยวข้องกับธนาคารให้แก่บุคคลใดๆ และป้องกันมิให้มีการนำข้อมูลของเจ้าของข้อมูลส่วนบุคคล (Data Subject) ไปใช้ เว้นแต่

2.1 ธนาคารได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล (Data Subject) หรือเป็นการดำเนินการโดยได้รับยกเว้นไม่ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล (Data Subject) ก่อนในข้อ 1.6

2.2 การใช้และประมวลผลข้อมูลส่วนบุคคลจำเป็นต่อการให้บริการตามสัญญา หรือบรรลุวัตถุประสงค์ตามคำขอของเจ้าของข้อมูลส่วนบุคคล (Data Subject)

2.3 การให้ข้อมูลแก่บริษัท ข้อมูลเครดิตแห่งชาติ จำกัด (Credit Bureau) หรือหน่วยงานอื่นใดที่เป็นการรายงานข้อมูลในลักษณะเดียวกัน

2.4 การเปิดเผยข้อมูลตามกฎหมาย เพื่อประโยชน์ในการสอบสวน หรือการพิจารณาคดี

2.5 การเปิดเผยกรณีจำเป็นต่อการตรวจสอบ หรือการป้องกันการปฏิบัติที่ฝ่าฝืนกฎหมาย เช่น การฉ้อโกง หลอกลวง การฟอกเงิน หรือการก่อการร้ายซึ่งกระทบต่อความมั่นคงของประเทศ เป็นต้น

2.6 การเปิดเผย.../8

2.6 การเปิดเผยข้อมูลตามคำสั่งของหน่วยงานของรัฐที่เกี่ยวข้องที่มีอำนาจตามกฎหมาย

โดยทั่วไปแล้ว ข้อมูลส่วนบุคคลที่อยู่ภายใต้การควบคุมของธนาคารจะถูกประมวลผลภายในประเทศไทยเท่านั้น อย่างไรก็ตาม หากมีความจำเป็นธนาคารจะทำการเปิดเผย โอน หรือส่งต่อข้อมูลไปยังบุคคล หรือหน่วยงานตามที่ระบุไว้ในข้อ 2.1 – 2.6 ซึ่งตั้งอยู่ในต่างประเทศ ทั้งนี้ ภายใต้กรอบที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลได้กำหนดไว้ และเพื่อให้บรรลุวัตถุประสงค์ตามที่กล่าวในนโยบายฯ ฉบับนี้

ในกรณีที่ธนาคารอาจมีความจำเป็นจะต้องส่ง หรือโอนข้อมูลส่วนบุคคลไปยังบุคคล หรือหน่วยงานต่างประเทศ หรือองค์กรระหว่างประเทศซึ่งมีสัญญากับธนาคาร ทั้งนี้ธนาคารจะกำหนดให้ประเทศที่รับข้อมูลส่วนบุคคลมีมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ และเป็นไปตามประกาศกำหนด

หลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ เว้นแต่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล (Data Subject) ก่อน หรือดำเนินการให้เป็นไปตามข้อยกเว้นที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลระบุให้สามารถกระทำได้ โดยไม่ต้องพิจารณามาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของประเทศนั้น เช่น การดำเนินการเพื่อปฏิบัติตามกฎหมาย เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคล (Data Subject) เพื่อดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคล (Data Subject) ก่อนเข้าทำสัญญา หรือเพื่อปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคล (Data Subject) เป็นคู่สัญญา เพื่อการทำสัญญาระหว่างธนาคารกับบุคคลหรือนิติบุคคลอื่นเพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคล (Data Subject) หรือเพื่อดำเนินภารกิจอันเกี่ยวกับประโยชน์สาธารณะที่สำคัญ

ข้อมูลส่วนบุคคลที่ถูกเปิดเผย หรือโอนไปยังต่างประเทศจะดำเนินการภายใต้มาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม โดยเจ้าของข้อมูลส่วนบุคคล (Data Subject) สามารถบังคับตามสิทธิที่เจ้าของข้อมูลส่วนบุคคล (Data Subject) มีอยู่ตามมาตรการนั้นได้ รวมถึงมีสิทธิได้รับการเยียวยาตามกฎหมาย ซึ่งธนาคารจะดำเนินการดังกล่าวข้างต้นให้เป็นไปตามประกาศหลักเกณฑ์ และวิธีการที่กำหนดโดยคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและกฎหมายที่เกี่ยวข้อง

ธนาคารมีการประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล (Data Subject) บนระบบ และกฎหมายของประเทศไทย อย่างไรก็ตาม การโอนข้อมูลดังกล่าวเพื่อการประมวลผลในบางกรณีอาจเป็นการดำเนินการข้ามประเทศ ธนาคารจะมีการตรวจสอบอย่างสม่ำเสมอ เพื่อให้เจ้าของข้อมูลส่วนบุคคล (Data Subject) มั่นใจได้ว่าการโอนข้อมูลจะเป็นไปโดยปลอดภัย และผู้รับโอนที่อยู่ต่างประเทศมีมาตรการป้องกันและคุ้มครองข้อมูลตามมาตรฐานที่กฎหมายกำหนด หรือขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล (Data Subject) กรณีเป็นประเทศที่มีมาตรการคุ้มครองข้อมูลส่วนบุคคลไม่เพียงพอ รวมทั้งมีการจัดทำสัญญากับบุคคลที่สามที่เข้ามาเกี่ยวข้องในการประมวลผลข้อมูลส่วนบุคคล เพื่อให้เป็นไปตามมาตรการที่ธนาคารกำหนด

หมวดที่ 3.../9

หมวดที่ 3 ระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล

ธนาคารสามารถเก็บข้อมูลส่วนบุคคล ตามระยะเวลาในการเก็บรักษาเฉพาะเท่าที่จำเป็นตามวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล หรือตามที่เจ้าของข้อมูลส่วนบุคคล (Data Subject) ร้องขอ หรือเก็บตามข้อกำหนดของกฎหมายที่ธนาคารจำเป็นต้องปฏิบัติ เมื่อสิ้นสุดระยะเวลาในการเก็บรักษาแล้วให้ธนาคารดำเนินการลบ หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคล (Data Subject) ด้วยวิธีการที่เหมาะสม โดยการพิจารณาวิธีการลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวตนได้นั้น เป็นสิทธิของธนาคารในการเลือกวิธีการที่เหมาะสม

ทั้งนี้ ระยะเวลาการจัดเก็บข้อมูลส่วนบุคคลอาจมีความแตกต่างกันตามประเภทของกิจกรรมและบริการ โดยมีระยะเวลาในการจัดเก็บ ดังต่อไปนี้

- กรณีที่มีกฎหมายกำหนดระยะเวลาในการจัดเก็บไว้โดยเฉพาะ ธนาคารจะทำการเก็บรักษาข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล (Data Subject) ตามกรอบระยะเวลาดังกล่าว
- กรณีที่กฎหมายไม่ได้กำหนดระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคลไว้โดยเฉพาะ ธนาคารจะกำหนดระยะเวลาในการเก็บรักษาตามความจำเป็นที่เหมาะสมในการปฏิบัติงานวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลนั้น (ปฏิบัติตามคำสั่งธนาคารที่ 145/2552 เรื่อง การจัดเก็บเอกสาร หรือที่จะมีการเปลี่ยนแปลงในอนาคต)
- กรณีที่มีเหตุการณ์ที่ฝ่าฝืนกฎหมาย หรือเกิดข้อพิพาท และจำเป็นต้องมีการสืบสวนสอบสวน ตลอดจนการรวบรวมพยานหลักฐานเพื่อดำเนินคดีตามกฎหมาย ธนาคารจะจัดเก็บข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล (Data Subject) ตามระยะเวลาเท่าที่จำเป็นจนกว่ากระบวนการนั้นจะเสร็จสิ้นหรือตามที่ระยะเวลาที่กฎหมายในเรื่องนั้นกำหนด
- ในบางกรณี ธนาคารอาจจำเป็นต้องจัดเก็บข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล (Data Subject) เกินระยะเวลาที่กำหนดข้างต้น ในกรณีการดำเนินการอย่างใดๆ เพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติ หรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย ธนาคารอาจทำการเก็บรักษาข้อมูลส่วนบุคคลในระยะเวลายาวนานกว่ากรณีทั่วไป

หมวดที่ 4 การลบหรือทำลายข้อมูลส่วนบุคคล

ธนาคารต้องลบทำลายข้อมูลส่วนบุคคล หรือทำให้ข้อมูลส่วนบุคคลอยู่ในลักษณะที่ไม่สามารถระบุตัวบุคคลของเจ้าของข้อมูลส่วนบุคคล (Data Subject) ได้ เมื่อพ้นกำหนดระยะเวลาในการเก็บรักษาหรือไม่มีความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคล หรือเมื่อเจ้าของข้อมูลส่วนบุคคล (Data Subject) ร้องขอใช้สิทธิในการลบข้อมูลส่วนบุคคล หรือถอนความยินยอม เว้นแต่เป็นกรณีที่ได้รับยกเว้นตามกฎหมาย

4.1 กรณี.../10

4.1 กรณีข้อมูลอยู่ในรูปแบบของเอกสาร Hard Copy การลบ หรือทำลายอาจต้องใช้เครื่องทำลายเอกสาร หรือจัดจ้างผู้ให้บริการเพื่อทำลายเอกสาร โดยธนาคารต้องมั่นใจว่าผู้ให้บริการมีมาตรการในการรักษาความปลอดภัยทุกขั้นตอน เพื่อป้องกันการเข้าถึง หรือเปิดเผยข้อมูลส่วนบุคคลแก่ผู้ที่ไม่ได้รับอนุญาต

4.2 กรณีข้อมูลอยู่ในรูปแบบ Soft File หรือการจัดเก็บข้อมูลในระบบของธนาคาร ธนาคารต้องลบทำลายข้อมูลส่วนบุคคล หรือทำให้ข้อมูลส่วนบุคคลอยู่ในลักษณะที่ไม่สามารถระบุตัวบุคคลของเจ้าของข้อมูลส่วนบุคคล (Data Subject) ได้

หมวดที่ 5 สถานที่จัดเก็บข้อมูลส่วนบุคคลและการกำหนดสิทธิการเข้าถึงข้อมูลส่วนบุคคล

ธนาคารได้กำหนดแนวทางและวิธีการจัดเก็บข้อมูลส่วนบุคคลไว้อย่างเหมาะสม เพื่อป้องกันความเสียหายที่อาจเกิดจากการรั่วไหลของข้อมูลส่วนบุคคล การเข้าถึง การลบ การทำลาย การส่งต่อ หรือการเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากเจ้าของข้อมูลส่วนบุคคล (Data Subject) หรือจากธนาคาร ทั้งนี้ เฉพาะผู้ที่มีอำนาจตามที่ธนาคาร หรือตามที่กฎหมายกำหนดไว้เท่านั้นที่จะมีสิทธิเข้าถึงข้อมูลส่วนบุคคล หรือเข้าถึงสถานที่ในการจัดเก็บข้อมูลส่วนบุคคลนั้นได้

สำหรับสถานที่ในการจัดเก็บข้อมูลส่วนบุคคล ธนาคารอาจว่าจ้างหน่วยงาน หรือบุคคลภายนอกให้ดำเนินการประมวลผลข้อมูลส่วนบุคคลในนามของธนาคาร และภายใต้วัตถุประสงค์ที่ทางธนาคารได้กำหนดไว้ ในการนี้ ธนาคารจะกำหนดให้หน่วยงาน หรือบุคคลภายนอกดังกล่าว เก็บรักษาข้อมูลส่วนบุคคลไว้เป็นความลับ และรักษาความปลอดภัยของข้อมูลส่วนบุคคลดังกล่าว รวมถึงป้องกันมิให้นำข้อมูลส่วนบุคคลไปประมวลผลเพื่อการอื่นใดที่เกินกว่าขอบเขตการว่าจ้าง หรือการใดที่ขัดต่อกฎหมาย

หมวดที่ 6 ข้อมูลที่จัดเก็บก่อนพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล มีผลบังคับใช้

ธนาคารสามารถเก็บรวบรวมใช้ข้อมูล และประมวลผลข้อมูลส่วนบุคคลที่จัดเก็บก่อนการประกาศใช้ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้ตามวัตถุประสงค์เดิมที่เคยแจ้งต่อลูกค้า หรือตามความคาดหมายเดิมของลูกค้าโดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลแต่อย่างใด แต่จะต้องแจ้งถึงวิธีการยกเลิกความยินยอมให้ลูกค้าทราบ เพื่อให้ลูกค้าสามารถใช้สิทธิในการถอนความยินยอมได้ และหากลูกค้าถอนความยินยอมแล้ว ธนาคารจะประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ถูกถอนไปแล้วมิได้ เว้นแต่จะเข้าข้อยกเว้นตามกฎหมาย

หมวดที่ 7 การดำเนินการตามสิทธิที่ร้องขอของเจ้าของข้อมูลส่วนบุคคล (Data Subject)

ธนาคารต้องจัดให้มีหน่วยงานเพื่อรับเรื่อง หรือมี Contact Center ในการรับเรื่องจากเจ้าของข้อมูลส่วนบุคคล (Data Subject) ที่ต้องการร้องขอใช้สิทธิ โดยธนาคารต้องดำเนินการตามสิทธิของเจ้าของข้อมูลดังต่อไปนี้

7.1 สิทธิ.../11

7.1 สิทธิในการถอนความยินยอม (Right to Withdraw Consent)

เจ้าของข้อมูลส่วนบุคคล (Data Subject) มีสิทธิเพิกถอนความยินยอมที่ได้ให้ไว้แก่ธนาคารสำหรับการประมวลผลข้อมูลส่วนบุคคลเมื่อใดก็ได้ ทั้งนี้ การใช้สิทธิเพิกถอนความยินยอมอาจส่งผลต่อการดำเนินการอย่างหนึ่งอย่างใดที่อาจเกิดขึ้นภายหลังจากการเพิกถอนความยินยอมได้ อย่างไรก็ดี การเพิกถอนความยินยอมจะไม่ส่งผลกระทบต่อการประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล (Data Subject) ซึ่งเจ้าของข้อมูลส่วนบุคคล (Data Subject) ได้ให้ความยินยอมไว้ก่อนหน้านี้แล้ว

7.2 สิทธิในการเข้าถึงข้อมูลส่วนบุคคล (Right to Access)

เจ้าของข้อมูลส่วนบุคคล (Data Subject) มีสิทธิในการเข้าถึง การรับสำเนา หรือ การให้ธนาคารทำการเปิดเผยการได้มาของข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล (Data Subject) ซึ่งอยู่ในความควบคุมของธนาคาร

7.3 สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง (Right to Rectification)

ในกรณีที่เจ้าของข้อมูลส่วนบุคคล (Data Subject) เห็นว่าข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล (Data Subject) ไม่ถูกต้อง ไม่เป็นปัจจุบัน ไม่สมบูรณ์ หรืออาจก่อให้เกิดความเข้าใจผิดได้ เจ้าของข้อมูลส่วนบุคคล (Data Subject) มีสิทธิร้องขอให้ธนาคารดำเนินการแก้ไขข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล (Data Subject) ที่อยู่ในความควบคุมของธนาคารได้

7.4 สิทธิในการลบข้อมูลส่วนบุคคล (Right to be Forgotten)

หากเจ้าของข้อมูลส่วนบุคคล (Data Subject) เห็นว่าข้อมูลส่วนบุคคลดังกล่าวถูกจัดเก็บโดยไม่ชอบด้วยกฎหมาย หรือหมดความจำเป็นในการประมวลผลตามที่ได้กำหนดตามวัตถุประสงค์ หรือเจ้าของข้อมูลส่วนบุคคล (Data Subject) ได้เพิกถอนความยินยอมในการประมวลผลและธนาคารไม่มีอำนาจในการประมวลผลข้อมูลส่วนบุคคลนั้นอีกต่อไป หรือเจ้าของข้อมูลส่วนบุคคล (Data Subject) ได้ทำการคัดค้านการประมวลผลในกรณีที่ข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล (Data Subject) ถูกจัดเก็บเพื่อทำการตลาดแบบตรง หรืออาศัยฐานประโยชน์อันชอบธรรม หรือภารกิจของรัฐ เจ้าของข้อมูลส่วนบุคคล (Data Subject) มีสิทธิร้องขอให้ธนาคารทำการ ลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล (Data Subject) เป็นข้อมูลที่ไม่สามารถระบุตัวตนได้

7.5 สิทธิในการระงับการใช้ข้อมูลส่วนบุคคล (Right to Restriction)

เจ้าของข้อมูลส่วนบุคคล (Data Subject) สามารถแจ้งให้ทางธนาคารดำเนินการระงับการใช้ข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล (Data Subject) ได้ กรณีที่เจ้าของข้อมูลส่วนบุคคล (Data Subject) เห็นว่าข้อมูลดังกล่าวอยู่ในระหว่างการตรวจสอบความถูกต้องของข้อมูลส่วนบุคคล หรืออยู่ในระหว่างการตรวจสอบการใช้สิทธิคัดค้านของเจ้าของข้อมูลส่วนบุคคล (Data Subject) หรือกรณีที่ข้อมูลส่วนบุคคลนั้นต้องถูกลบ หรือทำลาย เนื่องจากการประมวลผลข้อมูลส่วนบุคคลไม่ชอบด้วยกฎหมาย หรือกรณีที่ข้อมูลส่วนบุคคลนั้นหมดความจำเป็นในการเก็บรักษาตามวัตถุประสงค์ที่ธนาคารได้กำหนดไว้ แต่เจ้าของข้อมูลส่วนบุคคล (Data Subject) เห็นว่าข้อมูลส่วนบุคคลดังกล่าวมีความจำเป็นต้องเก็บรักษา เพื่อใช้ในการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตาม การใช้สิทธิ หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

7.6 สิทธิ.../12

7.6 สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล (Right to Object)

เจ้าของข้อมูลส่วนบุคคล (Data Subject) สามารถคัดค้านการประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล (Data Subject) ที่อยู่ในความควบคุมของธนาคาร ในกรณีที่ข้อมูลส่วนบุคคลนั้นเป็นข้อมูลที่ประมวลผล เพื่อวัตถุประสงค์เกี่ยวกับการตลาดแบบตรง หรือเป็นกรณีที่ธนาคารอาศัยฐานภารกิจของรัฐ ฐานประโยชน์อันชอบธรรม หรือฐานจดหมายเหตุ/วิจัย/สถิติ

7.7 สิทธิในการให้โอนย้ายข้อมูลส่วนบุคคล (Right to Data Portability)

เจ้าของข้อมูลส่วนบุคคล (Data Subject) มีสิทธิขอรับข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล (Data Subject) ที่อยู่ในความควบคุมของธนาคาร โดยข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคล (Data Subject) ร้องขอจะต้องเป็นข้อมูลที่สามารถอ่าน หรือใช้งานได้ด้วยเครื่องมือหรืออุปกรณ์ซึ่งมีลักษณะการทำงานโดยอัตโนมัติ นอกจากนี้ เจ้าของข้อมูลส่วนบุคคล (Data Subject) สามารถร้องขอให้ธนาคารส่งหรือโอนข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล (Data Subject) ข้างต้นไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่น หรืออาจร้องขอให้ธนาคารรับโอนข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล (Data Subject) จากผู้ควบคุมส่วนบุคคลอื่น ทั้งนี้ การดำเนินการเช่นว่านั้นจะต้องสามารถกระทำได้ในทางเทคนิค

7.8 สิทธิร้องเรียน (Right to Lodge a Complaint)

หากเจ้าของข้อมูลส่วนบุคคล (Data Subject) เห็นว่าธนาคารได้ทำการละเมิดกฎหมายคุ้มครองข้อมูลส่วนบุคคล เจ้าของข้อมูลส่วนบุคคล (Data Subject) มีสิทธิร้องเรียนไปยังคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้ทันที

ทั้งนี้ ธนาคารอาจมีสิทธิที่จะใช้เหตุแห่งการปฏิเสธคำร้องขอของเจ้าของข้อมูลส่วนบุคคล (Data Subject) ได้หากพิจารณาแล้วว่าธนาคารมีความจำเป็นที่จะต้องปฏิบัติตามกฎหมายโดยไม่อาจดำเนินการตามคำร้องขอได้ หรือพิจารณาแล้วเห็นว่าการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject) นั้นไม่สมเหตุสมผล หรือกระทบต่อสิทธิเสรีภาพของบุคคลอื่น โดยมีการกำหนดกระบวนการในการพิจารณาการขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject) อย่างเหมาะสมและเป็นไปตามที่กฎหมายกำหนด

หมวดที่ 8 หน้าที่และความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO)

ธนาคารอาจทำหน้าที่เป็นทั้งผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) และผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) ดังนั้น จึงกำหนดภาระหน้าที่ไว้ ดังนี้

8.1 ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) มีหน้าที่และความรับผิดชอบ ดังนี้

8.1.1 ควบคุม.../13

8.1.1 ควบคุมให้ธนาคารมีการดำเนินการประมวลผลข้อมูลส่วนบุคคลได้ตามวัตถุประสงค์อันชอบด้วยกฎหมาย โดยจัดให้มีมาตรการรักษาความปลอดภัยที่เหมาะสมทั้งมาตรการเชิงเทคนิค (Technical Measure) และมาตรการเชิงบริหารจัดการ (Organizational Measure) เพื่อป้องกันการสูญหาย การเข้าถึงข้อมูล ใช้ข้อมูล หรือเปลี่ยนแปลงแก้ไข หรือเปิดเผยข้อมูลโดยมิชอบและต้องทบทวนมาตรการในการรักษาความปลอดภัยของข้อมูลเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป

8.1.2 ในกรณีที่ธนาคารต้องให้ข้อมูลส่วนบุคคลแก่บุคคล หรือนิติบุคคลอื่น จะต้องดำเนินการป้องกันไม่ให้ผู้นั้นนำข้อมูลส่วนบุคคลไปใช้ หรือเปิดเผยโดยมิชอบ

8.1.3 ต้องจัดให้มีระบบในการตรวจสอบเพื่อลบ หรือทำลายข้อมูลส่วนบุคคล หรือทำให้ข้อมูลไม่สามารถระบุตัวบุคคลได้ เมื่อพ้นกำหนดระยะเวลาในการเก็บรักษา หรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคล (Data Subject) ร้องขอ หรือเจ้าของข้อมูลส่วนบุคคล (Data Subject) ได้ถอนความยินยอม เว้นแต่จะทำการเก็บรักษาไว้ภายใต้ข้อยกเว้นตามกฎหมาย หากเกิดเหตุการณ์ละเมิดขึ้นซึ่งทำให้ข้อมูลส่วนบุคคลรั่วไหล ต้องแจ้งแก่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ภายใน 72 ชั่วโมงนับแต่ทราบเหตุ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการณ์ละเมิดให้เจ้าของข้อมูลส่วนบุคคล (Data Subject) ทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้า ทั้งนี้ การแจ้งดังกล่าว และข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

8.1.4 ธนาคารต้องจัดให้มีการเก็บบันทึกข้อมูลเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพื่อให้เจ้าของข้อมูลส่วนบุคคล (Data Subject) และสำนักงานคุ้มครองข้อมูลส่วนบุคคลสามารถตรวจสอบได้โดยบันทึกเป็นหนังสือ หรือระบบอิเล็กทรอนิกส์ก็ได้

8.1.5 ธนาคารต้องดำเนินการให้เป็นไปตามสิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject) หากเจ้าของข้อมูลส่วนบุคคล (Data Subject) มีการร้องขอใช้สิทธิ

8.1.6 ธนาคารต้องเลือกผู้ประมวลผลข้อมูลส่วนบุคคลที่มีมาตรการเชิงเทคนิค และเชิงบริหารจัดการที่เหมาะสมในการประมวลผล และการรักษาความมั่นคงปลอดภัยของข้อมูล

8.1.7 ธนาคารจะต้องจัดให้มีการทำข้อตกลง (Data Processing Agreement : DPA) ระหว่างธนาคารและผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) เพื่อให้ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) ดำเนินการให้เป็นไปตามข้อตกลง

8.1.8 หากธนาคารมีการโอนข้อมูลไปยังต่างประเทศจะต้องทำโดยชอบด้วยกฎหมาย และต้องมั่นใจว่าประเทศปลายทางที่รับข้อมูลส่วนบุคคลมีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ

8.1.9 ต้องทำ.../14

8.1.9 ต้องทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment : DPIA) ในกรณีที่การประมวลผลข้อมูลมีความเสี่ยงที่จะเกิดผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล (Data Subject)

8.1.10 ธนาคารต้องให้ความร่วมมือกับหน่วยงานกำกับดูแล หรือทำหน้าที่ตามกฎหมายตามคำสั่งของหน่วยงานรัฐในการเข้าถึงข้อมูล

8.2 ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) มีหน้าที่และความรับผิดชอบ ดังนี้

8.2.1 ต้องเก็บรวบรวมข้อมูล ใช้ข้อมูล หรือเปิดเผยข้อมูลส่วนบุคคลตามที่ได้ตกลงกับผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) เท่านั้น ไม่ดำเนินการนอกเหนือจากที่ตกลงกับผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) หากไม่ได้รับอนุญาตเป็นลายลักษณ์อักษร เว้นแต่คำสั่งดังกล่าวนั้นขัดต่อกฎหมาย

8.2.2 ต้องจัดให้มีมาตรการในการรักษาความมั่นคงและปลอดภัยที่เหมาะสมมีมาตรการเชิงเทคนิค และเชิงบริหารจัดการ เพื่อรักษาความมั่นคงปลอดภัยในการประมวลผลที่เหมาะสมกับความเสี่ยง เพื่อป้องกันการสูญหาย เข้าถึงใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจ หรือโดยมิชอบ รวมทั้งแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ทราบถึงเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

8.2.3 ต้องจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้ตามหลักเกณฑ์ และวิธีการที่ธนาคารกำหนด หรือตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

8.2.4 กรณีที่ข้อมูลส่วนบุคคลเกิดการรั่วไหล (Data Breach) ต้องแจ้งเหตุดังกล่าวต่อผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) โดยไม่ชักช้าหลังจากทราบเหตุ เพื่อดำเนินการตามกระบวนการของธนาคารต่อไป

8.3 เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO)

ธนาคารต้องมีบุคลากรที่ทำหน้าที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO) เพื่อการคุ้มครองสิทธิประโยชน์ของธนาคาร และเพื่อคุ้มครองสิทธิประโยชน์ของเจ้าของข้อมูลส่วนบุคคล (Data Subject) และช่วยให้ธนาคารสามารถบริหารจัดการข้อมูลส่วนบุคคลได้อย่างมีประสิทธิภาพ และประสิทธิผลโดยมีหน้าที่และความรับผิดชอบ ดังนี้

8.3.1 ให้คำแนะนำแก่ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) หรือผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) รวมทั้งลูกจ้าง หรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) หรือผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) เกี่ยวกับการปฏิบัติตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

8.3.2 ตรวจสอบ.../15

8.3.2 ตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) หรือผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) รวมทั้งลูกจ้าง หรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) หรือผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล

8.3.3 ประสานงานและให้ความร่วมมือกับสำนักงานคุ้มครองข้อมูลส่วนบุคคลในกรณีที่มีปัญหาเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) หรือผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

8.3.4 รักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้ หรือได้มาเนื่องจากการปฏิบัติหน้าที่ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

8.3.5 เป็นศูนย์กลางรับเรื่องในกรณีที่เจ้าของข้อมูลส่วนบุคคล (Data Subject) ต้องการติดต่อ หรือมีข้อสงสัย หรือต้องการสอบถามข้อมูลเกี่ยวกับรายละเอียดการเก็บรวบรวมข้อมูล ใช้ข้อมูล หรือเปิดเผยข้อมูลส่วนบุคคลของตน รวมถึงสิทธิต่างๆ ของเจ้าของข้อมูลส่วนบุคคล (Data Subject) ตามนโยบายฉบับนี้ โดยแจ้งช่องทางต่างๆ ในการติดต่อให้เจ้าของข้อมูลส่วนบุคคล (Data Subject) ทราบอย่างชัดเจน

ทั้งนี้ ธนาคารต้องสนับสนุนการปฏิบัติงานของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) โดยจัดหาเครื่องมือ หรืออุปกรณ์อย่างเพียงพอ รวมทั้งอำนวยความสะดวกในการเข้าถึงข้อมูลส่วนบุคคล เพื่อการปฏิบัติหน้าที่ และให้อำนาจหน้าที่ และมีความเป็นอิสระในการทำงาน โดยมีสายการรายงานที่ตรงไปยังผู้บริหารสูงสุดของธนาคาร

หมวดที่ 9 การแบ่งแยกหน้าที่สำหรับการบริหารจัดการข้อมูลและการบริหารความเสี่ยงที่เกี่ยวข้องกับข้อมูลส่วนบุคคล (Three Lines of Defense)

ธนาคารต้องจัดให้มีการแบ่งแยกหน้าที่สำหรับการบริหารจัดการการรักษาความปลอดภัย และการบริหารความเสี่ยงที่เกี่ยวข้องกับข้อมูลส่วนบุคคลอย่างชัดเจน เพื่อให้แน่ใจว่าพนักงานทุกคนทราบ และตระหนักถึงหน้าที่และความรับผิดชอบของตนได้อย่างเหมาะสมโดยโครงสร้างการจัดแบ่งหน้าที่ มีดังนี้

9.1 First Line of Defense ได้แก่ หน่วยงานทางธุรกิจ หรือหน่วยงานปฏิบัติงานทำหน้าที่กำหนดวัตถุประสงค์ และวิธีการในการดำเนินการเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล เป็นผู้เก็บรวบรวมข้อมูลจากเจ้าของข้อมูลส่วนบุคคล (Data Subject) บันทึกข้อมูลลงในระบบฐานข้อมูลของธนาคาร และรับผิดชอบในการตรวจสอบคุณภาพของข้อมูลที่เก็บรวบรวม

9.2 Second.../16

9.2 Second Line of Defense ได้แก่ หน่วยงานบริหารความเสี่ยง หน่วยงานกำกับหน่วยงานบัญชีและการเงิน หน่วยงานด้านสารสนเทศ หน่วยงานบริหารทรัพยากรบุคคล หน่วยงานวางแผนงบประมาณ หน่วยงานด้านกระบวนการ หน่วยงานบริหารอาคารสถานที่ รวมถึงเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ทำหน้าที่ควบคุม กำกับดูแลธนาคารในภาพรวม เช่น ทำหน้าที่กำกับดูแลการปฏิบัติงานวางแนวทาง กรอบแนวคิดเงื่อนไข และขั้นตอนปฏิบัติงานให้กับ First Line of Defense คอยสอดส่องตรวจหาช่องว่างในการปฏิบัติงานในส่วนที่ไม่ชัดเจน เพื่อหาแนวทางป้องกันและแก้ไข และเพื่อกำหนดแนวทางในการจัดการกับความเสี่ยงที่อาจเกิดขึ้น

9.3 Third Line of Defense ได้แก่ ฝ่ายตรวจสอบภายในที่ทำหน้าที่ในการตรวจสอบว่าธนาคารมีการปฏิบัติงานที่เกี่ยวข้องกับการบริหารจัดการข้อมูลและการบริหารความเสี่ยงเป็นไปตามข้อกำหนดของกฎหมายและนโยบายที่เกี่ยวข้องกับการบริหารจัดการข้อมูลของธนาคาร และมีนโยบายที่เพียงพอและเหมาะสม โดยธนาคารควรกำหนดให้หน่วยงานตรวจสอบภายในสามารถรายงานตรงต่อคณะกรรมการตรวจสอบได้

หมวดที่ 10 เหตุการณ์การรั่วไหลของข้อมูลส่วนบุคคล (Personal Data Breach)

ในกรณีที่มีการรั่วไหลของข้อมูลส่วนบุคคลเกิดขึ้นภายในธนาคาร ผู้ที่ทราบเหตุต้องแจ้งไปยังเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) โดยเร็วที่สุด เพื่อดำเนินการตรวจสอบถึงสาเหตุที่มาและระบุจุดต้นเหตุของการรั่วไหล และประเมินผลกระทบที่เกิดขึ้น โดยพิจารณาถึงผลกระทบต่อสิทธิและเสรีภาพขั้นพื้นฐาน ผลกระทบต่อชีวิตและทรัพย์สินของเจ้าของข้อมูลส่วนบุคคล (Data Subject) ดังนี้

10.1 หากผลการประเมินแสดงให้เห็นว่าไม่มีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล (Data Subject) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) สามารถทำการจดบันทึกไว้ และอาจไม่จำเป็นต้องแจ้งเจ้าของข้อมูลส่วนบุคคล (Data Subject) หรือแจ้งต่อสำนักงานคุ้มครองข้อมูลส่วนบุคคลถึงเหตุการณ์การรั่วไหลที่เกิดขึ้น

10.2 หากผลการประเมินแสดงให้เห็นว่าการรั่วไหลของข้อมูลเป็นความเสี่ยงสูง ซึ่งมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล (Data Subject) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ต้องแจ้งแก่เจ้าของข้อมูลส่วนบุคคล (Data Subject) รวมทั้งแนวทางในการเยียวยา และแจ้งเหตุละเมิดของข้อมูลส่วนบุคคลแก่สำนักงานคุ้มครองข้อมูลส่วนบุคคลโดยไม่ล่าช้าภายในระยะเวลา 72 ชั่วโมง นับจากทราบเหตุการณ์การรั่วไหลของข้อมูลส่วนบุคคล

หมวดที่ 11.../17

หมวดที่ 11 บทลงโทษผู้ฝ่าฝืนนโยบายฯ และ/หรือละเมิดสิทธิส่วนบุคคล

ผู้ใดกระทำการใดโดยจงใจ หรือประมาทเลินเล่อ หรืองดเว้นไม่ปฏิบัติตามนโยบายนี้ ถือว่าผู้นั้นกระทำผิดวินัย และต้องรับผิดชอบชดใช้ความเสียหายแก่ธนาคาร หรือผู้ที่ได้รับผลกระทบจากการกระทำดังกล่าว ตลอดจนรับผิดในทางแพ่ง โทษอาญา หรือโทษทางปกครองตามกฎหมายต่อไปด้วย

หมวดที่ 12 การทบทวนนโยบายการคุ้มครองข้อมูลส่วนบุคคล

ฝ่ายกำกับการปฏิบัติงานและคุ้มครองข้อมูลส่วนบุคคล ควรทบทวนนโยบายคุ้มครองข้อมูลส่วนบุคคลทุกปี เพื่อให้มั่นใจว่านโยบายดังกล่าวยังคงสอดคล้องกับกฎหมาย โดยนำเสนอคณะกรรมการกำกับความเสี่ยงพิจารณาอนุมัติ และรายงานคณะกรรมการธนาคารเพื่อทราบ