นโยบายการจัดการในกรณีที่มีการละเมิดข้อมูลส่วนบุคคลและแนวทางปฏิบัติที่เกี่ยวข้อง
ของธนาคารอาคารสงเคราะห์

วันที่มีผลใช้บังคับ: 1 กรกฎาคม 2564

1. วัตถุประสงค์

นโยบายการจัดการในกรณีที่มีการละเมิดข้อมูลส่วนบุคคลและแนวทางปฏิบัติที่เกี่ยวข้องของธนาคารอาคารสงเคราะห์ ("**แนวทาง**") ฉบับนี้ จัดทำขึ้นเพื่อแสดงถึงขั้นตอนที่ธนาคารอาคารสงเคราะห์ ("**ธนาคาร**") จะปฏิบัติเมื่อเกิดเหตุการณ์รั่วไหลของข้อมูล (ตามคำนิยามด้านล่าง) ทั้งที่เกิดขึ้นจริง มีความเป็นไปได้ว่าจะเกิดขึ้น หรือสงสัยว่าจะเกิดขึ้น ซึ่งอาจนำไปสู่การละเมิดข้อมูลส่วนบุคคล

2. ขอบเขต

แนวทางนี้ใช้บังคับกับพนักงาน ผู้รับจ้าง ตัวแทน ตลอดจนบุคคลากรอื่น ๆ ของธนาคาร นอกจากนี้ ธนาคารยังกำหนดให้พันธมิตรทางธุรกิจและผู้ให้บริการภายนอก ซึ่งรวมถึง พนักงาน ผู้รับจ้าง ตัวแทน และบุคคลากรอื่น ๆ ของพันธมิตรทางธุรกิจและผู้ให้บริการภายนอกดังกล่าว ที่ต้องเก็บรวบรวม เข้าถึง จัดเก็บ หรือจัดการข้อมูลส่วนบุคคลในนามของธนาคาร (ต่อจากนี้ไปจะเรียกรวมกันว่า "**พนักงาน / ผู้รับจ้าง**") ต้องทำสัญญาเพื่อปฏิบัติตามแนวทางนี้ ทั้งนี้ แนวทางฉบับนี้จะไม่ก่อให้เกิดสิทธิใด ๆ แก่พนักงาน / ผู้รับจ้าง หรือสิทธิใด ๆ นอกเหนือหน้าที่ของธนาคารภายใต้กฎหมายที่ใช้บังคับ แนวทางนี้เป็นเป็นเอกสารภายในของธนาคาร และมิได้ก่อสิทธิหรือสิทธิพิเศษใด ๆ สำหรับบุคคลภายนอก

ผู้ใดฝ่าฝืนแนวทางฉบับนี้ อาจได้รับโทษทางวินัย ซึ่งรวมถึงการเลิกจ้าง หรืออาจส่งผลให้มีการบอกเลิกสัญญากับพันธมิตรทางธุรกิจ หรือผู้ให้บริการได้

ธนาคารอาจแก้ไขเพิ่มเติมแนวทางนี้เป็นครั้งคราว โดยธนาคารจะแจ้งให้พนักงาน / ผู้รับจ้าง ทราบตามความเหมาะสม

3. ข้อกำหนดในการรายงานเหตุการณ์รั่วไหลของข้อมูล

3.1 การติดต่อฝ่ายงานจัดการสถานการณ์

หากพนักงาน / ผู้รับจ้างใดพบ สงสัย หรือทราบถึงเหตุการณ์รั่วไหลของข้อมูลที่เกิดขึ้นจริง มีความเป็นไปได้ว่าจะเกิดขึ้น หรือสงสัยว่าจะเกิดขึ้น จะต้อง**รายงาน**ประเด็นดังกล่าวให้ฝ่ายงานจัดการสถานการณ์ทราบโดย**ทันที** (ข้อมูลการติดต่อฝ่ายงานจัดการสถานการณ์อยู่ใน**ข้อ** 3.4 ของแนวทางฉบับนี้) โดยใช้แบบฟอร์มรายงานเหตุการณ์รั่วไหลของข้อมูลต่อฝ่ายงานจัดการสถานการณ์ใน**ภาคผนวก** 1

3.2 เหตุการณ์รั่วไหลของข้อมูล

เหตุการณ์รั่วไหลของข้อมูล คือ เหตุการณ์ที่เกิดขึ้นจริง มีความเป็นไปได้ว่าจะเกิดขึ้น หรือสงสัยว่าจะเกิดขึ้น หรือการกระทำ ความขัดข้อง หรือเหตุการณ์อื่นที่ก่อให้เกิดการทำลาย การสูญหาย การเปลี่ยนแปลงของข้อมูลที่ธนาคารเป็นเจ้าของ ควบคุม หรือเก็บรักษาไว้ ไม่ว่าจะโดยตรงหรือโดยอ้อม (เช่น ข้อมูลที่อยู่ภายใต้การดูแลของพันธมิตรทางธุรกิจหรือผู้ให้บริการภายนอกอื่นที่ให้บริการแก่ธนาคาร) ไม่ว่าจะโดยอุบัติเหตุ โดยเจตนา หรือโดยมิชอบด้วยกฎหมาย หรือก่อให้เกิดการได้รับ การเปิดเผย หรือการเข้าถึงเอกสารกระดาษหรือข้อมูลทางอิเล็กทรอนิกส์โดยไม่ได้รับอนุญาต ไม่ว่าจะเป็นข้อมูลส่วนบุคคลหรือข้อมูลที่เป็นความลับหรือไม่ก็ตาม ซึ่งข้อมูลดังกล่าวอาจอยู่ในแฟ้มเอกสารกระดาษ อีเมล ตารางบันทึกบุคลากร บันทึกบัญชีเงินเดือน เครื่องแม่ข่าย (เซิร์ฟเวอร์) อุปกรณ์จัดเก็บข้อมูลแบบพกพา (เช่น คอมพิวเตอร์แล็ปท็อป หรือโทรศัพท์สมาร์ตโฟน) และฐานข้อมูลไอที เป็นต้น

ตัวอย่างเหตุการณ์บางส่วนที่มีลักษณะต้องรายงาน เช่น

- การโจรกรรมหรือการสูญหายของคอมพิวเตอร์ คอมพิวเตอร์แล็ปท็อป โทรศัพท์สมาร์ตโฟน อุปกรณ์บันทึกข้อมูลแบบธัมบ์ไดรฟ์ หรืออุปกรณ์บันทึกข้อมูลอื่นที่เป็นของธนาคาร หรือของพนักงาน / ผู้รับจ้างที่ใช้อุปกรณ์ดังกล่าวบันทึกข้อมูลที่เกี่ยวข้องกับธนาคาร
- การบุกรุกหรือการโจรกรรมสถานที่ทำงานของธนาคาร
- ผู้โจมตีก่อให้เกิดความเสี่ยงต่อระบบของธนาคาร เช่น ฐานข้อมูล คอมพิวเตอร์ เครื่องข่าย การสื่อสารของธนาคาร
- พนักงาน / ผู้รับจ้างทำการตรวจสอบ เข้าถึง หรือเปิดเผยข้อมูล แฟ้มข้อมูล หรือฐานข้อมูลนอกขอบเขตหน้าที่ที่ได้รับมอบหมาย
- บุคคลภายนอกกระทำผิดสัญญาการไม่เปิดเผยข้อมูลหรือสัญญาการรักษาความลับ
- เหตุการณ์ใดที่กล่าวมาข้างต้นซึ่งเกี่ยวเนื่องกับพันธมิตรทางธุรกิจหรือผู้ให้บริการภายนอกของธนาคาร

3.3 ความช่วยเหลือ

พนักงาน / ผู้รับจ้างจะต้องให้ความช่วยเหลือธนาคารและฝ่ายงานจัดการสถานการณ์ในการตรวจสอบเหตุการณ์รั่วไหลของข้อมูลอย่างเต็มความสามารถ

3.4 ฝ่ายงานจัดการสถานการณ์

ฝ่ายงานจัดการสถานการณ์	
ข้อมูลติดต่อ	อีเมล: DataPrivacyOfficer@ghb.co.th โทรศัพท์: 0 2645 9000 ต่อ 6670
สมาชิก	
ผู้จัดการเหตุการณ์ลำดับแรก	**เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล**

กลุ่มงานเทคโนโลยีสารสนเทศ	**รองกรรมการผู้จัดการ กลุ่มงานเทคโนโลยีสารสนเทศ**
สายงานกฎหมาย **ศูนย์ป้องกันการทุจริต**	**ผู้ช่วยกรรมการผู้จัดการ สายงานกฎหมาย** **ผู้อำนวยการศูนย์ป้องกันการทุจริต**
ที่ปรึกษานอกองค์กร	

3.5 ความพร้อมของฝ่ายงานจัดการสถานการณ์

ฝ่ายงานจัดการสถานการณ์จะต้องจัดให้มีการเฝ้าสังเกตการณ์โดยสามารถติดต่อได้ที่ อีเมล: DataPrivacyOfficer@ghbcoth โทรศัพท์: 0 2645 9000 ต่อ 6670 ของฝ่ายงานจัดการสถานการณ์ตลอด 24 ชั่วโมง โดยไม่มีวันหยุด เพื่อให้ผู้จัดการเหตุการณ์ลำดับแรกสามารถรับรายงานได้โดยทันที

4. ขั้นตอนการจัดการเหตุการณ์รั่วไหลของข้อมูล

ระยะที่ 1: การรายงานภายในและการยืนยันเหตุการณ์รั่วไหลของข้อมูล

วัตถุประสงค์ของระยะที่ 1 คือ เพื่อระบุและยืนยันได้อย่างทันท่วงทีว่ามีเหตุการณ์รั่วไหลของข้อมูลเกิดขึ้นจริงหรือไม่ เพื่อรายงานต่อไปยังฝ่ายงานจัดการสถานการณ์

4.1 การตรวจสอบเบื้องต้น

ฝ่ายงานจัดการสถานการณ์จะมอบหมายให้สมาชิกหรือผู้ที่ได้รับมอบหมายทำการตรวจสอบในเบื้องต้นสำหรับรายงานเหตุการณ์แต่ละรายการ (“**ผู้จัดการเหตุการณ์ลำดับแรก**”)

4.1.1 ผู้จัดการเหตุการณ์ลำดับแรกจะต้องตอบกลับพนักงาน / ผู้รับจ้างที่รายงานเหตุการณ์ และขอข้อมูลเกี่ยวกับเหตุการณ์รั่วไหลของข้อมูลดังกล่าวให้ได้มากที่สุดเท่าที่มีอยู่ในเวลานั้น

4.1.2 หากเหตุการณ์รั่วไหลของข้อมูลที่เกิดขึ้นเกี่ยวข้องกับเทคโนโลยีสารสนเทศ (ไอที) หรือประเด็นอื่นเกี่ยวกับความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ ผู้จัดการเหตุการณ์ลำดับแรกจะต้องประสานงานกับสมาชิกกลุ่มงานเทคโนโลยีสารสนเทศ

4.1.3 ผู้จัดการเหตุการณ์ลำดับแรกจะต้องพิจารณาเบื้องต้น**โดยเร็วที่สุดหรือภายใน 24 ชั่วโมงแรก**ว่า จากข้อมูลที่มีอยู่นั้นมีมูลฐานอันสมเหตุสมผลหรือน่าเชื่อถือที่ทำให้เชื่อได้ว่าเหตุการณ์ดังกล่าวเกิดขึ้นจริงหรือไม่

4.1.4 หากไม่มีมูลฐานอันสมเหตุสมผลหรือโดยชอบตามกฎหมาย ผู้จัดการเหตุการณ์ลำดับแรกจะต้องจัดทำรายงานเป็นการภายในโดยระบุข้อมูลต่อไปนี้

- ระบุตัวพนักงาน / ผู้รับจ้างที่รายงานเหตุการณ์
- คำอธิบายสถานการณ์แวดล้อมของเหตุการณ์รั่วไหลของข้อมูลที่มีการรายงาน
- คำอธิบายเหตุผลที่ผู้จัดการเหตุการณ์ลำดับแรกพิจารณาว่าไม่มีมูลฐานอันสมเหตุสมผลหรือน่าเชื่อถือที่ทำให้เชื่อได้ว่าเหตุการณ์ดังกล่าวอาจเกิดขึ้นได้หรือเกิดขึ้นแล้ว

ผู้จัดการเหตุการณ์ลำดับแรกจะต้องจัดทำรายงานเป็นลายลักษณ์อักษรไปยังสมาชิกรายอื่น ๆ ของฝ่ายงานจัดการสถานการณ์

4.2 การยืนยันเหตุการณ์รั่วไหลของข้อมูล

หากผู้จัดการเหตุการณ์ลำดับแรกพิจารณาแล้วเห็นว่า มีมูลฐานอันสมเหตุสมผลหรือน่าเชื่อถือที่ทำให้เชื่อได้ว่าเหตุการณ์รั่วไหลของข้อมูลดังกล่าวเกิดขึ้นจริงแล้วนั้น ผู้จัดการเหตุการณ์ลำดับแรกจะต้องแจ้งให้สมาชิกรายอื่น ๆ ของฝ่ายงานจัดการสถานการณ์ของตนทราบโดย**ทันที เพื่อดำเนินการระยะที่** 2

ระยะที่ 2: **การจัดการเหตุการณ์รั่วไหลของข้อมูล**

วัตถุประสงค์ของระยะที่ 2 คือเพื่อจัดการเหตุการณ์รั่วไหลของข้อมูลทั้งในระดับภายในและภายนอกองค์กร ในระยะนี้จะต้องมีการประเมินเหตุการณ์รั่วไหลของข้อมูลโดยมิชักช้าและโดยเร็วที่สุดเท่าที่จะทำได้ เพื่อให้ธนาคารสามารถทำการแจ้งเตือนที่จำเป็นได้ทันเวลา หากฝ่ายงานจัดการสถานการณ์เห็นว่า จะต้องรายงานเหตุการณ์รั่วไหลของข้อมูลนั้นให้หน่วยงานรัฐบาล บุคคล หรือผู้ใดทราบตามที่กฎหมายกำหนด

ในขณะเดียวกัน จะต้องมีการดำเนินมาตรการอื่นที่จำเป็นไปพร้อม ๆ กันเพื่อควบคุมเหตุการณ์และลดความเสี่ยงและความเสียหายลงให้ได้มากที่สุด

4.3 การควบคุมภัยคุกคาม

หากเหตุการณ์รั่วไหลของข้อมูลนั้นเป็นภัยคุกคามถาวร หรือเกิดภัยคุกคามอย่างต่อเนื่อง (เช่น แฮกเกอร์หรือไวรัสในระบบสารสนเทศของธนาคาร) ฝ่ายงานจัดการสถานการณ์จะต้องดำเนินการให้บุคลากรในกลุ่มงานเทคโนโลยีสารสนเทศกำหนดมาตรการที่เหมาะสมเพื่อรักษาความปลอดภัยและแยกภัยคุกคามออกไปไม่ให้สร้างความเสียหายต่อสภาพแวดล้อมทางเทคนิคของธนาคารต่อไปได้

4.4 การจัดเก็บบันทึกเอกสารที่เกี่ยวข้องกับการจัดการเหตุการณ์

ฝ่ายงานจัดการสถานการณ์ต้องจัดเก็บบันทึกเอกสารต่าง ๆ ที่เกี่ยวข้องในช่วงขั้นตอนที่ดำเนินการ ตั้งแต่พบเหตุการณ์ไปจนถึงการแจ้งให้ทราบและการแก้ไข

4.5 การเก็บหลักฐาน

ในการตรวจสอบ ฝ่ายงานจัดการสถานการณ์จะต้องจัดให้มีมาตรการที่เหมาะสมในการเก็บรักษาข้อมูลและหลักฐานที่เกี่ยวข้อง ซึ่งรวมถึง

- ระงับการลบหรือทำลายข้อมูล (รวมทั้งแฟ้มบันทึกข้อมูลอัตโนมัติ การเขียนทับลงบนเทปสำรองข้อมูล หรือการรีไซเคิล)
- สั่งให้พนักงาน / ผู้รับจ้าง ตัวแทน หรือผู้แทนที่สามารถเข้าถึงระบบได้ใช้ความระมัดระวังไม่ให้ลบ แก้ไข หรือทำให้ข้อมูลและหลักฐานที่เกี่ยวข้องได้รับความเสียหาย
- เก็บรักษารหัสหรือมัลแวร์ที่ต้องสงสัย และ
- ดำเนินการตามกฎหมายที่เกี่ยวข้องตามนโยบายของธนาคาร (ในกรณีที่เกี่ยวข้อง)

4.6 ผู้ตรวจสอบทางนิติวิทยาศาสตร์

ฝ่ายงานจัดการสถานการณ์จะพิจารณาเป็นรายกรณีว่าจำเป็นต้องให้ผู้ตรวจสอบ / บริษัทตรวจสอบทางนิติวิทยาศาสตร์เข้ามาบันทึกภาพอุปกรณ์ที่ได้รับผลกระทบ ตรวจสอบนิติวิทยาศาสตร์กับคอมพิวเตอร์ หรือบริการอื่น ๆ หรือไม่ การตรวจสอบทางนิติวิทยาศาสตร์จะควบคุมการดำเนินการโดยสายงานกฎหมายหรือที่ปรึกษาทางกฎหมายจากภายนอกเพื่อให้คำปรึกษาและคำแนะนำทางกฎหมายแก่ธนาคาร หากคาดว่าจะต้องมีการดำเนินคดี การไต่สวนทางกฎหมาย หรือการตรวจสอบภายในองค์กร

4.7 การรักษาความลับ

ฝ่ายงานจัดการสถานการณ์จะประสานงานร่วมกับฝ่ายอื่น ๆ เพื่อให้แน่ใจว่าเหตุการณ์รั่วไหลของข้อมูลจะถูกปิดเป็นความลับจนกว่าจะมีการตัดสินใจเกี่ยวกับการแจ้งให้ทราบหรือเปิดเผย นอกจากนี้จะต้องจำกัดจำนวนพนักงาน / ผู้รับจ้างที่ทราบเหตุการณ์รั่วไหลของข้อมูลให้น้อยที่สุดเท่าที่จะทำได้

4.8 การตรวจสอบขอบเขตของเหตุการณ์รั่วไหลของข้อมูล

ฝ่ายงานจัดการสถานการณ์จะตรวจสอบและรวบรวมข้อมูลเกี่ยวกับขอบเขตของเหตุการณ์รั่วไหลของข้อมูล ซึ่งรวมถึงข้อมูลต่อไปนี้ (ในกรณีที่เกี่ยวข้อง)

- เวลาและลักษณะการเกิดเหตุการณ์รั่วไหลของข้อมูล และเวลาที่พบ
- ประเภทของข้อมูล (เช่น ประเภทของข้อมูลส่วนบุคคล) ที่อาจเสี่ยงต่อการได้รับผลกระทบ
- ความเสี่ยงว่าจะเกิดความเสียหายหรือการใช้งานในทางที่ผิด และ
- ผู้ทราบเหตุการณ์รั่วไหลของข้อมูลดังกล่าว ไม่ว่าจะเป็นบุคลากรภายในหรือนอกธนาคาร

รายการตรวจสอบเกี่ยวกับเหตุการณ์รั่วไหลของข้อมูลที่ฝ่ายงานจัดการสถานการณ์อาจนำมาใช้ในการตรวจสอบมีดังนี้

- ลักษณะของเหตุการณ์รั่วไหลของข้อมูลที่ทราบ (การแฮก การสูญหายของอุปกรณ์ การโจรกรรมโดยบุคคลภายใน หรืออื่น ๆ ที่คล้ายกัน) และฝ่ายงานจัดการสถานการณ์ทราบเหตุได้อย่างไร
- ลักษณะของข้อมูลที่ได้รับผลกระทบเป็นอย่างไร ขอบข่ายของข้อมูลที่ได้รับผลกระทบมีข้อมูลที่อาจก่อให้เกิดการกระทำผิดหน้าที่ในการแจ้งเตือนหรือหน้าที่อื่นตามบังคับของกฎหมายหรือสัญญาหรือไม่
- ประเภทของบุคคลที่อาจได้รับผลกระทบ (เช่น ลูกค้า พนักงาน หรืออื่น ๆ)
- ที่อยู่ของผู้ที่อาจได้รับผลกระทบดังกล่าว (เช่น ในประเทศไทยเท่านั้นหรือประเทศอื่นด้วย)
- เราสามารถประเมินประเภทและจำนวนโดยประมาณของบันทึกข้อมูลส่วนบุคคลที่ได้รับผลกระทบได้หรือไม่
- ขอบเขตของเหตุการณ์รั่วไหลของข้อมูลที่ทราบ หากเหตุการณ์ดังกล่าวอาจเกี่ยวข้องกับการบุกรุกระบบสารสนเทศโดยไม่ได้รับอนุญาตแล้วนั้น เครื่องคอมพิวเตอร์โฮสต์ใดที่อาจถูกเข้าถึงและข้อมูลใดที่อยู่ในเครื่องเหล่านั้น รวมถึงวิธีการที่ผู้บุกรุกใช้ในการเข้าถึง
- มีการรายงานเหตุการณ์ดังกล่าวตามสื่อต่าง ๆ แล้วหรือไม่

- มาตรการที่อยู่ระหว่างดำเนินการเพื่อรักษาความปลอดภัยของระบบ และในขณะเดียวกันก็ต้องไม่ทำลายหลักฐานทางอิเล็กทรอนิกส์ที่สำคัญ (เช่น การตัดการเชื่อมต่อเครื่องแม่ข่ายที่มีข้อมูลส่วนบุคคลออกจากอินเทอร์เน็ต หรืออื่น ๆ ที่คล้ายกัน หรือมีการบันทึกภาพอุปกรณ์ที่อาจได้รับผลกระทบแล้วหรือไม่)
- ใครเป็นผู้ทำหน้าที่จัดการด้านเทคนิคและความมั่นคงปลอดภัยของเหตุการณ์รั่วไหลของข้อมูล ธนาคารได้ว่าจ้างให้บริษัทไอที / นิติวิทยาศาสตร์ที่มีชื่อเสียงเพื่อดำเนินการดังกล่าวแล้วหรือไม่
- มีบุคลากรอื่นใดในธนาคารที่ควรทราบเหตุการณ์ดังกล่าวหรือไม่ (เช่น ผู้บริหาร สายงานสื่อสารและภาพลักษณ์องค์กร ฯลฯ)
- หน่วยงานบังคับใช้กฎหมายได้รับการติดต่อแล้วหรือไม่ หากติดต่อแล้ว ได้ติดต่อหน่วยงานใด และใครเป็นผู้ติดต่อ

4.9 การรายงานต่อหน่วยงานบังคับใช้กฎหมาย

ในฐานะส่วนหนึ่งของการตรวจสอบ ฝ่ายงานจัดการสถานการณ์จะต้องพิจารณาว่าจำเป็นหรือสมควรต้องรายงานต่อหน่วยงานบังคับใช้กฎหมายหรือไม่ ในกรณีที่มีการเข้าถึงข้อมูลหรือระบบสารสนเทศของธนาคารโดยไม่ได้รับอนุญาต

4.10 การพิจารณาข้อกำหนดทางกฎหมายที่ใช้บังคับ

สายงานกฎหมาย และ/หรือ ที่ปรึกษาทางกฎหมายจากภายนอกจะใช้แนวทางการวิเคราะห์ใน**ภาคผนวก 4** เพื่อให้คำแนะนำแก่ฝ่ายงานจัดการสถานการณ์เกี่ยวกับกฎหมายว่าด้วยการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่จะนำมาใช้บังคับกับเหตุการณ์รั่วไหลของข้อมูล (“**กฎหมายว่าด้วยการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล**”) (**ดูภาคผนวก 4**) และให้คำแนะนำว่าเหตุการณ์รั่วไหลของข้อมูลดังกล่าวถือว่าเป็นการละเมิดความมั่นคงปลอดภัยของข้อมูลที่ต้องแจ้งหน่วยงานรัฐบาล / หน่วยงานกำกับดูแลด้านการคุ้มครองข้อมูล หรืออื่น ๆ หรือไม่ หรือต้องมีการแจ้งเตือนไปยังเจ้าของข้อมูลส่วนบุคคลผู้ที่ได้รับผลกระทบโดยตรงหรือไม่

ฝ่ายงานจัดการสถานการณ์จะต้องให้ข้อมูลตามความเป็นจริงตามที่สายงานกฎหมาย และ/หรือ ที่ปรึกษาทางกฎหมายจากภายนอกร้องขอ เพื่อให้สายงานกฎหมาย และ/หรือ ที่ปรึกษาทางกฎหมายจากภายนอกทำการประเมินทางกฎหมายที่จำเป็นได้

4.11 การพิจารณาข้อกำหนดอื่น ๆ

นอกจากนี้ สายงานกฎหมาย และ/หรือ ที่ปรึกษาทางกฎหมายจากภายนอกจะให้คำแนะนำแก่ฝ่ายงานจัดการสถานการณ์เกี่ยวกับข้อกำหนดอื่นที่นอกเหนือจากกฎหมายว่าด้วยการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่อาจกำหนดให้ต้องมีการรายงานเหตุการณ์รั่วไหลของข้อมูล ซึ่งรวมถึงข้อกำหนดดังนี้

- ระเบียบเฉพาะรายอุตสาหกรรมที่อาจนำมาใช้บังคับต่อเหตุการณ์รั่วไหลของข้อมูล
- ภาระผูกพันตามสัญญาที่มีต่อพันธมิตรทางธุรกิจหรืออื่น ๆ
- นโยบายคุ้มครองข้อมูลส่วนบุคคลหรือแถลงการณ์อื่น ๆ ในเอกสารเกี่ยวกับการแจ้งเตือนทั้งของภายในและนอกองค์กร
- คำสัญญาที่ไม่ได้มีผลผูกพันหรือนโยบายธนาคารที่มีการเผยแพร่ต่อสาธารณะ

4.12 การรายงานต่อหน่วยงานรัฐบาล หรือบุคคลอื่น ๆ

(ก) **เนื้อหาในรายงานและบทพูดสำหรับตอบคำถาม**

ฝ่ายงานจัดการสถานการณ์ควรประสานงานกับสายงานกฎหมาย และ/หรือ ที่ปรึกษาทางกฎหมายจากภายนอกเพื่อกำหนดถ้อยคำและวิธีการเผยแพร่รายงานดังกล่าวให้เป็นไปตามข้อกำหนด

หากฝ่ายงานจัดการสถานการณ์ตัดสินใจใช้บุคลากรของธนาคาร หรือให้บุคคลภายนอกที่ได้รับมอบหมายใดเป็นผู้ตอบคำถามจากผู้ที่ได้รับผลกระทบที่อาจมีข้อสงสัยเกี่ยวกับเหตุการณ์รั่วไหลของข้อมูลนั้น หรือเรื่องอื่นที่เกี่ยวข้อง ฝ่ายงานจัดการสถานการณ์จะต้องจัดทำบทพูดให้กับบุคลากรของธนาคาร หรือให้บุคคลภายนอกที่ได้รับมอบหมายและมีความพร้อมในการรับโทรศัพท์จากผู้ที่ได้รับผลกระทบ ในการแจ้งเตือนไปยังผู้ที่ได้รับผลกระทบให้ทราบนั้นควรระบุข้อมูลสำหรับติดต่อหรือข้อมูลอื่นตามกำหนด

(ข) **รูปแบบการแจ้งเตือน**

หากกฎหมายที่ใช้บังคับไม่ได้ระบุรูปแบบการแจ้งเตือนอื่นเป็นการเฉพาะ ในการบอกกล่าวไปยังผู้ที่ได้รับผลกระทบ (ที่ได้ให้ที่อยู่อีเมลไว้ให้แก่ธนาคาร) จะต้องส่งทางอีเมล์ไปยังผู้ที่ได้รับผลกระทบทุกราย พร้อมขอให้มีการตอบรับ สำหรับผู้ที่ให้ที่อยู่ไปรษณีย์ไว้ให้แก่ธนาคาร โดยไม่มีที่อยู่อีเมล์ จะต้องแจ้งให้ทราบทางไปรษณีย์ลงทะเบียน

ฝ่ายงานจัดการสถานการณ์จะต้องประสานงานกับสายงานกฎหมายและ/หรือ ที่ปรึกษาทางกฎหมายจากภายนอกเพื่อกำหนดรูปแบบที่เหมาะสมในการส่งการแจ้งเตือน โดยพิจารณาจากกฎหมายที่ใช้บังคับและต้นทุน อย่างไรก็ตามนโยบายนี้ไม่ได้กำหนดให้ต้องแจ้งให้ทราบผ่านช่องทางสาธารณะ (เช่น ทางเว็บไซต์หรือสื่อมวลชนระดับประเทศ) แต่อาจมีข้อกำหนดของกฎหมายว่าด้วยการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล หรืออาจพิจารณาแล้วว่าจะเป็นประโยชน์ในด้านลูกค้าสัมพันธ์หรือวัตถุประสงค์อื่นในบางสถานการณ์

หากไม่สามารถแจ้งเตือนได้ตามข้อนี้ ฝ่ายงานจัดการสถานการณ์ควรปรึกษาสายงานกฎหมายและ/หรือที่ปรึกษาทางกฎหมายจากภายนอกโดยทันที เพื่อพิจารณาใช้วิธีการที่เหมาะสมในการแจ้งเตือนอื่น ฝ่ายงานจัดการสถานการณ์อาจชะลอการส่งการแจ้งเตือนหากหน่วยงานบังคับใช้กฎหมายเห็นว่าการแจ้งเตือนไปยังผู้ที่ได้รับผลกระทบนั้นอาจเป็นอุปสรรคต่อการสืบสวนทางอาญา

4.13 การตอบคำถาม

ฝ่ายงานจัดการสถานการณ์จะต้องวางแผนวิธีการสำหรับตัวแทนของธนาคารในการตอบข้อซักถามของสื่อมวลชน รัฐบาล หรือผู้อื่น ในกรณีส่วนใหญ่ ข้อซักถามนั้นควรส่งไปยังสายงานกฎหมาย หรือสายงานสื่อสารและภาพลักษณ์องค์กรโดยตรงเพื่อการวิเคราะห์และจัดเตรียมแนวทางคำตอบ

ระยะที่ 3: มาตรการหลังเกิดเหตุการณ์

4.14 ข้อกำหนดเรื่องการจัดทำบันทึกเอกสาร

ไม่ว่าจะมีการพิจารณานำกฎหมายว่าด้วยการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลมาใช้บังคับต่อเหตุการณ์รั่วไหลของข้อมูลหรือไม่ก็ตามนั้น ฝ่ายงานจัดการสถานการณ์จะต้องจัดทำเอกสารบันทึกเหตุการณ์รั่วไหลของข้อมูลให้เพียงพอ

โดยเฉพาะอย่างยิ่งการประเมินทางกฎหมายที่ไม่ได้นำกฎหมายว่าด้วยการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลมาใช้บังคับ ทั้งนี้ ให้ใช้แบบฟอร์มบันทึกเหตุการณ์รั่วไหลของข้อมูลใน**ภาคผนวก** 2 เพื่อการบันทึกรายละเอียดที่เกี่ยวข้อง

4.15 มาตรการแก้ไข

ฝ่ายงานจัดการสถานการณ์จะต้องประสานงานกับสายงานกฎหมาย และกลุ่มงานเทคโนโลยีสารสนเทศ เพื่อกำหนดมาตรการทางเทคนิคและทางองค์กรที่จำเป็นในการป้องกันไม่ให้เกิดเหตุการณ์รั่วไหลของข้อมูลที่คล้ายกันอีกในอนาคต ซึ่งรวมถึงแนวทาง การฝึกอบรมเพื่อสร้างความเข้าใจ กระบวนการสำหรับพนักงาน / ผู้รับจ้าง ฝ่ายงานจัดการสถานการณ์ควรประเมินความสัมพันธ์กับบุคคลภายนอกที่อาจเกี่ยวข้องกับเหตุการณ์รั่วไหลของข้อมูล พร้อมดำเนินมาตรการที่เหมาะสม เช่น การแก้ไขสัญญา การแก้ไขกระบวนการต่าง ๆ และ/หรือ การฝึกอบรม การปรับปรุงมาตรการความปลอดภัย การเลือกผู้ให้บริการรายใหม่ เป็นต้น ขณะเดียวกันบุคคลภายนอกมีหน้าที่ตามสัญญาที่จะต้องแจ้งให้ธนาคารทราบโดยทันทีหากเกิดเหตุการณ์รั่วไหลของข้อมูล ไม่ว่าที่เกิดขึ้นจริงหรือสงสัยว่าจะเกิดขึ้นก็ตาม ทั้งนี้ คู่สัญญาบุคคลภายนอกดังกล่าวนั้นจะดำเนินการให้คำแนะนำแก่สายงานกฎหมายและ และกลุ่มงานเทคโนโลยีสารสนเทศหากต้องมีการปรับเปลี่ยนกระบวนการใดๆที่เกี่ยวข้องกับการจัดการเหตุการณ์รั่วไหลของข้อมูลนั้น

4.16 การทบทวนภาระผูกพันตามกรมธรรม์ประกันภัย

ฝ่ายงานจัดการสถานการณ์จะต้องทบทวนกรมธรรม์ประกันภัยของธนาคาร ที่ใช้บังคับ เพื่อพิจารณาว่า ควรแจ้งให้ทราบตามข้อกำหนดในกรมธรรม์ประกันภัยที่ยังคงมีผลบังคับหรือไม่ ซึ่งรวมถึงเวลา เนื้อหา และรูปแบบการแจ้งเตือน

ภาคผนวก 1

แบบฟอร์มรายงานเหตุการณ์รั่วไหลของข้อมูลต่อฝ่ายงานจัดการสถานการณ์

กรุณากรอกรายละเอียดด้านล่าง และส่งอีเมลไปยังที่อยู่อีเมลสำหรับติดต่อฝ่ายงานจัดการสถานการณ์ที่ E-mail : DataPrivacyOfficer@ghb.co.th

คำอธิบายเหตุการณ์รั่วไหลของข้อมูล	
วันและเวลาที่พบเหตุการณ์รั่วไหลของข้อมูล	
ผู้ที่ระบุเหตุการณ์รั่วไหลของข้อมูล	ชื่อ: ตำแหน่ง: ฝ่าย: [ประเทศ:] อีเมล: หมายเลขโทรศัพท์:
พนักงาน / ผู้รับจ้างที่รายงาน:	☐ เป็นบุคคลเดียวกับผู้ที่ระบุเหตุการณ์รั่วไหลของข้อมูล ชื่อ: ตำแหน่ง: ฝ่าย: [ประเทศ:] อีเมล: หมายเลขโทรศัพท์:
ระบบที่อาจหรือได้รับผลกระทบ	
ประเภทบุคคลที่อาจหรือได้รับผลกระทบ (เช่น ลูกค้า พันธมิตรทางธุรกิจ พนักงาน / ผู้รับจ้าง ผู้ติดต่อในกรณีฉุกเฉินสำหรับพนักงาน / ผู้รับจ้าง ผู้เยาว์ ผู้พิการ)	

ประเภทของข้อมูลที่อาจหรือได้รับผลกระทบ	
ผู้ใดรับทราบถึงเหตุการณ์รั่วไหลของข้อมูลบ้าง	

ภาคผนวก 2

แบบฟอร์มบันทึกเหตุการณ์รั่วไหลของข้อมูล

โปรดอธิบายรายละเอียดเหตุการณ์รั่วไหลของข้อมูล โดยละเอียด

.....

.....

.....

วันและเวลาที่พบเหตุการณ์รั่วไหลของข้อมูล

.....

มีการพบเหตุการณ์รั่วไหลได้อย่างไร (เช่น รายละเอียดผู้ที่ระบุเหตุการณ์รั่วไหลของข้อมูล และ/หรือ พนักงาน / ผู้รับจ้างที่รายงาน)

.....

ประเภทของเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ (เลือกทุกข้อที่มีความเกี่ยวข้อง)

☐ ลูกค้า
☐ พนักงาน
☐ พันธมิตรทางธุรกิจ
☐ ไม่ทราบแน่ชัด
☐ ผู้เยาว์ / ผู้พิการ
☐ อื่น ๆ (โปรดระบุ) .....

ประเภทของข้อมูลที่เกิดการรั่วไหลหรือได้รับผลกระทบ (เลือกทุกข้อที่มีความเกี่ยวข้อง)

☐ ข้อมูลทั่วไป เช่น ชื่อ ข้อมูลติดต่อ
☐ เอกสารทางราชการ เช่น บัตรประจำตัวประชาชน
☐ Usernames, Passwords
☐ ข้อมูลด้านการเงิน เช่น เลขบัตรเครดิต
☐ ข้อมูล GPS Location
☐ ข้อมูลเรื่องสุขภาพหรือความพิการ
☐ ข้อมูลด้านความคิดเห็นทางการเมือง
☐ ข้อมูลประวัติอาชญากรรม
☐ ข้อมูลทางชีวภาพ
☐ ข้อมูลสหภาพแรงงาน
☐ อื่น ๆ (โปรดระบุ) .....

ปริมาณโดยคร่าวของข้อมูลที่รั่วไหลหรือได้รับผลกระทบ

.....

ปริมาณโดยคร่าวของเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ

.....

โปรดอธิบายอย่างละเอียดถึงผลกระทบที่น่าจะเกิดหรือเกิดจากการรั่วไหล

.....

ความน่าจะเป็นที่การรั่วไหลของข้อมูลส่วนบุคคลจะส่งผลกระทบที่เป็นการคุกคามต่อเจ้าของข้อมูลส่วนบุคคล

☐ เป็นไปได้สูง ☐ เป็นไปได้

☐ เป็นกลาง ☐ เป็นไปได้ต่ำ

☐ เป็นไปไม่ได้ ☐ ไม่ทราบแน่ชัด

โปรดอธิบายอย่างละเอียดถึงผลกระทบที่อาจจะเกิด หรือ เกิดไปแล้วต่อเจ้าของข้อมูลส่วนบุคคล

.....

.....

หากมีการล่าช้าในการแจ้งเหตุการณ์รั่วไหลของข้อมูลเกิดขึ้น โปรดระบุรายละเอียดและเหตุผลประกอบ

.....

.....

จงอธิบายมาตรการที่ได้บังคับใช้ในการควบคุมการรั่วไหลที่เกิดขึ้น

.....

.....

ได้มีการแจ้งเจ้าของข้อมูลส่วนบุคคลถึงเหตุการณ์รั่วไหลของข้อมูลหรือไม่

☐ มีการแจ้งเจ้าของข้อมูลส่วนบุคคลเรียบร้อยแล้ว ☐ อยู่ในระหว่างการดำเนินการแจ้งเจ้าของข้อมูลส่วนบุคคล

☐ มีการตัดสินใจที่จะไม่แจ้งเจ้าของข้อมูลส่วนบุคคล ☐ อยู่ในระหว่างการตัดสินใจของธนาคาร

☐ อื่น ๆ (โปรดระบุ) .....

หากตอบว่ามีการแจ้ง โปรดชี้แจงรายละเอียด

.....

.....

ได้มีการแจ้งหน่วยงานบังคับใช้กฎหมายถึงเหตุการณ์รั่วไหลของข้อมูลหรือไม่

☐ มีการแจ้ง ☐ ไม่มีการแจ้ง

☐ ยังไม่ทราบแน่ชัด

☐ อื่น ๆ (โปรดระบุ) .....

หากตอบว่ามีการแจ้ง โปรดชี้แจงรายละเอียด

.....

.....

ภาคผนวก 3

แผนภาพการดำเนินการแจ้งเหตุการณ์รั่วไหลของข้อมูล

พนักงาน / ผู้รับจ้างกรอกแบบฟอร์มรายงานเหตุการณ์รั่วไหลของข้อมูล และนำส่งแก่ฝ่ายงานจัดการสถานการณ์

- ฝ่ายงานจัดการสถานการณ์ได้รับเรื่องแจ้งจากพนักงาน / ผู้รับจ้าง
- แต่งตั้ง **ผู้จัดการเหตุการณ์ลำดับแรก** เพื่อพิจารณาความเป็นไปได้ของเหตุการณ์รั่วไหลของข้อมูล**ภายใน 24 ชั่วโมง**

มีมูลฐาน | ไม่มีมูลฐาน

ดำเนินการดังต่อไปนี้

ดำเนินการจัดทำรายงานภายในโดยระบุรายละเอียดดังต่อไปนี้

- ระบุตัวพนักงาน / ผู้รับจ้างที่รายงานเหตุการณ์
- คำอธิบายสถานการณ์แวดล้อมของเหตุการณ์รั่วไหลของข้อมูลที่มีการรายงาน
- คำอธิบายเหตุที่ผู้จัดการเหตุการณ์ลำดับแรกพิจารณาว่าไม่มีมูลฐานอันสมเหตุสมผลหรือไม่น่าเชื่อถือ

1. **ควบคุมภัยคุกคาม**

2. **จัดเก็บบันทึกเอกสารที่เกี่ยวข้องกับการจัดการเหตุการณ์ตั้งแต่พบเหตุการณ์จนถึงขั้นตอนการแก้ไข**

3. **เก็บหลักฐาน**
   - ระงับการลบ หรือทำลายข้อมูล
   - สั่งให้พนักงาน / ผู้รับจ้างหรือบุคคลอื่นใดที่เข้าระบบได้ ให้ใช้ความระมัดระวังไม่ทำให้หลักฐานหรือข้อมูลที่เกี่ยวข้องได้รับความเสียหายหรือถูกแก้ไขเปลี่ยนแปลง หรือ ลบ
   - เก็บรักษารหัสหรือมัลแวร์ที่ต้องสงสัยไว้
   - ดำเนินการตามกฎหมายหรือระเบียบของธนาคารที่เกี่ยวข้อง

4. **ผู้ตรวจสอบทางนิติวิทยาศาสตร์**
   ให้งานจัดการสถานการณ์ ร่วมด้วย สายงานกฎหมาย หรือที่ปรึกษาด้านกฎหมายพิจารณาถึงความจำเป็นในการมอบหมายให้ผู้ตรวจสอบทางนิติวิทยาศาสตร์เพื่อช่วยในการบันทึกรายละเอียดผลกระทบ ตรวจสอบคอมพิวเตอร์ หรือส่วนอื่น ๆ ที่เกี่ยวข้อง

5. **การรักษาความลับ**

6. **ตรวจสอบขอบเขตของเหตุการณ์รั่วไหลของข้อมูล**
   - เวลาและลักษณะการเกิดเหตุการณ์รั่วไหลของข้อมูล และเวลาที่พบเหตุการณ์
   - ประเภทข้อมูล (เช่น ประเภทข้อมูลส่วนบุคคล) ที่อาจเสี่ยงต่อการได้รับผลกระทบ
   - ความเสี่ยงว่าจะเกิดความเสียหายหรือการใช้งานในทางที่ผิด
   - ผู้ทราบเหตุการณ์รั่วไหลของข้อมูลดังกล่าวไม่ว่าจะเป็นบุคคลากรภายในหรือภายนอกธนาคาร

7. **พิจารณาและประเมินข้อกำหนดทางกฎหมายและข้อกำหนดอื่น ๆ**

8. **รายงานต่อหน่วยงานภาครัฐ หรือ เจ้าของข้อมูลส่วนบุคคลผู้ได้รับผลกระทบ (หากจำเป็น)**
   - **เนื้อหา**: กำหนดถ้อยคำและวิธีการเผยแพร่
   - **รูปแบบการแจ้ง**: ถ้ากฎหมายมิได้กำหนดไว้เป็นอื่น ให้ดำเนินการแจ้งผ่านอีเมล / ไปรษณีย์ไปยังผู้ที่ได้รับผลกระทบ และขอให้มีการตอบรับ

หลังเกิดเหตุ
(ไม่ว่าจะเป็นกรณีมีมูลฐานหรือไม่มีมูลฐาน)

- จัดทำเอกสารบันทึกเหตุการณ์รั่วไหลของข้อมูล โดยเฉพาะการประเมินทางกฎหมายที่ไม่ได้นำกฎหมายว่าด้วยการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลมาใช้บังคับ
- กำหนดมาตรการทางเทคนิคและทางองค์กรที่จำเป็นในการป้องกันไม่ให้เกิดเหตุการณ์รั่วไหลของข้อมูลที่คล้ายกันอีกในอนาคต รวมถึงประเมินความสัมพันธ์กับบุคคลภายนอกที่อาจเกี่ยวข้องกับเหตุการณ์รั่วไหลของข้อมูล พร้อมดำเนินมาตรการที่เหมาะสม

ภาคผนวก 4

สรุปสาระสำคัญของกฎหมายว่าด้วยการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล – ประเทศไทย

<table>
<tr><th>ลำดับที่</th><th>กฎหมายว่าด้วยการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล</th><th>รายละเอียด</th></tr>
<tr><td>1.</td><td>พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (“พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล”)</td><td>
ข้อกำหนดว่าด้วยการแจ้งเตือนตามพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลมีอยู่ 2 ประเภทด้วยกัน
<table>
<tr><th>1. หน้าที่ในการแจ้งต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล</th><th>2. หน้าที่ในการแจ้งให้เจ้าของข้อมูลทราบ</th></tr>
<tr><td>โดยไม่ชักช้าภายใน 72 ชั่วโมง นับตั้งแต่ผู้จัดการเหตุการณ์ลำดับแรกทราบเหตุการณ์</td><td>โดยไม่ชักช้า</td></tr>
<tr><td>แจ้งการเกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคล</td><td>แจ้งให้ทราบเรื่องการเกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคล<u>และ</u>มาตรการแก้ไขเยียวยา</td></tr>
<tr><td>มีแนวโน้มก่อให้เกิดความเสี่ยงที่จะกระทบต่อสิทธิและเสรีภาพของบุคคล</td><td>มีแนวโน้มก่อให้เกิดความเสี่ยง<u>สูง</u>ที่จะกระทบต่อสิทธิและเสรีภาพของบุคคล</td></tr>
<tr><td>ข้อยกเว้นไม่ต้องแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลและวิธีการแจ้งเหตุการณ์จะมีกำหนดไว้ในกฎหมายลำดับรองต่อไป</td><td>ข้อยกเว้นไม่ต้องแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลและวิธีการแจ้งเหตุการณ์จะมีกำหนดไว้ในกฎหมายลำดับรองต่อไป</td></tr>
</table>
</td></tr>
</table>

		• *"ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ดังต่อไปนี้:* *...(4)* ***แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมงนับแต่ทราบเหตุ*** *เท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล* ***ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย*** *ทั้งนี้การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด" (มาตรา 37)* • *"ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามมาตรา 21 มาตรา 22 มาตรา 24 มาตรา 25 วรรคหนึ่ง มาตรา 27 วรรคหนึ่งหรือวรรคสอง มาตรา 28 มาตรา 32 วรรคสอง หรือมาตรา 37 หรือขอความยินยอมโดยการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ หรือไม่ปฏิบัติตามมาตรา 21 ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา 25 วรรคสอง หรือส่งหรือโอนข้อมูลส่วนบุคคลโดยไม่เป็นไปตามมาตรา 29 วรรคหนึ่งหรือวรรคสามต้องระวางโทษปรับทางปกครองไม่เกินสามล้านบาท" (มาตรา 83)* • *"ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้:* *...(2) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น" (มาตรา 40)* • *"ผู้ประมวลผลข้อมูลส่วนบุคคลผู้ใดไม่ปฏิบัติตามมาตรา 40 โดยไม่มีเหตุอันควร หรือส่งหรือโอนข้อมูลส่วนบุคคลโดยไม่เป็นไปตามมาตรา 29 วรรคหนึ่งหรือวรรคสาม หรือไม่ปฏิบัติตามมาตรา 37 (5) ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา 38 วรรคสอง ต้องระวางโทษปรับทางปกครองไม่เกินสามล้านบาท" (มาตรา 86)*

2.	พระราชบัญญัติการรักษาความปลอดภัยมั่นคงไซเบอร์ พ.ศ. 2562 (“**พ.ร.บ. การรักษาความปลอดภัยมั่นคงไซเบอร์**”)	• พ.ร.บ. การรักษาความปลอดภัยมั่นคงไซเบอร์กำหนดให้มีการรายงานต่อหน่วยงานที่มีอำนาจ โดยเป็นข้อกำหนดที่นำมาใช้บังคับกับองค์กรที่มี “โครงสร้างพื้นฐานสำคัญทางสารสนเทศ” ตามกฎหมายลำดับรองที่ออกตามมาตรา 49 ของพระราชบัญญัตินี้ และสำหรับภัยคุกคามไซเบอร์ที่มีผลกระทบสำคัญ • *“เมื่อมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศรายงานต่อสำนักงานและหน่วยงานควบคุมหรือกำกับดูแล และปฏิบัติการรับมือกับภัยคุกคามทางไซเบอร์ตามที่กำหนดในส่วนที่ 4 ทั้งนี้ คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) อาจกำหนดหลักเกณฑ์และวิธีการการรายงานด้วยก็ได้” (มาตรา 57)* • *“หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใดไม่รายงานเหตุภัยคุกคามทางไซเบอร์ตามมาตรา 57 โดยไม่มีเหตุอันสมควร ต้องระวางโทษปรับไม่เกินสองแสนบาท” (มาตรา 73)*

ภาคผนวก 5

แนวทางกฎหมายว่าด้วยการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

1. **แนวทางในการพิจารณากำหนด – พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล**

ฝ่ายงานจัดการสถานการณ์จะต้องวิเคราะห์ลักษณะ ขอบข่าย และความรุนแรงของเหตุการณ์รั่วไหลของข้อมูลตามทิศทางและแนวทางของ[สายงานกฎหมาย] หรือที่ปรึกษาทางกฎหมายจากภายนอก ซึ่งควรทำเป็นรายกรณีไป โดยพิจารณาจากชุดคำถามต่อไปนี้

<u>หมายเหตุ</u>: ในทุกกรณี [สายงานกฎหมาย] จะต้องตรวจสอบว่า หน่วยงานที่มีอำนาจได้ออกกฎหมายลำดับรองหรือแนวทางปฏิบัติเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลและการประเมินความเสี่ยงแล้วหรือไม่ หากมีการออกออกกฎหมายลำดับรองหรือแนวทางปฏิบัติแล้วจะต้องนำมาพิจารณาร่วมกับชุดคำถามต่อไปนี้

คำถามที่ 1: เหตุการณ์รั่วไหลของข้อมูลของข้อมูลนี้เกี่ยวข้องกับ “ข้อมูลส่วนบุคคล” ตามคำนิยามใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลหรือไม่

(หากใช่ กรุณาอ่านคำถามต่อไป)

คำถามที่ 2: เหตุการณ์รั่วไหลของข้อมูลเกี่ยวกับการทำลาย สูญหาย หรือแก้ไขโดยอุบัติเหตุหรือโดยมิชอบด้วยกฎหมาย หรือการเปิดเผยหรือเข้าถึงข้อมูลส่วนบุคคลที่รับส่ง จัดเก็บ หรือประมวลผล โดยการเปิดเผยหรือเข้าถึงนั้นไม่ได้รับอนุญาตใช่หรือไม่ (การ “ละเมิดข้อมูลส่วนบุคคล”)

(หากใช่ กรุณาอ่านคำถามต่อไป)

คำถามที่ 3: การละเมิดข้อมูลส่วนบุคคลดังกล่าวอาจก่อให้เกิดความเสี่ยงที่จะกระทบต่อสิทธิและเสรีภาพของบุคคลตามแนวทางดังกล่าวหรือไม่

(หมายเหตุ: การประเมินความเสี่ยงควรพิจารณาจากกฎหมายลำดับรองหรือแนวทางปฏิบัติหากมีการออกกฎหมายลำดับรองหรือแนวทางปฏิบัติแล้ว)

(หากใช่ กรุณาอ่านคำถามต่อไป)

คำถามที่ 4: มีกฎหมายลำดับรองใดที่ยกเว้นให้ไม่ต้องรายงานต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลหรือไม่ หากมี ข้อยกเว้นนั้นนำมาใช้บังคับได้หรือไม่

(หากคำตอบข้อ 4 คือไม่มี ฝ่ายงานจัดการสถานการณ์ควรพิจารณาว่า<u>จะต้องรายงานต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลหรือไม่</u>)

ฝ่ายงานจัดการสถานการณ์ดำเนินการตามคำถามข้อถัดไป

คำถามที่ 5: มีความเป็นไปได้ที่ความเสี่ยงนั้นจะพิจารณาได้ว่าเป็นความเสี่ยงสูงที่จะกระทบต่อสิทธิและเสรีภาพของบุคคลหรือไม่

แนวทางการประเมินความเสี่ยง – ในการพิจารณาว่ามีความเสี่ยงหรือความเสี่ยงสูงนั้นจะต้องพิจารณาตามรายการต่อไปนี้เป็นรายกรณีไป

- ประเภท (ความละเอียดอ่อน) ของข้อมูลส่วนบุคคลที่เกี่ยวกับเหตุการณ์รั่วไหลของข้อมูลนั้น
- ปริมาณข้อมูลส่วนบุคคลส่วนบุคคล
- จำนวนเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ
- ประเภทของการละเมิดข้อมูลส่วนบุคคล
- ความสามารถในการระบุถึงตัวตนของบุคคลได้โดยง่าย
- ลักษณะพิเศษของผู้ที่ได้รับผลกระทบ (เช่น กลุ่มที่มีความอ่อนไหว)
- ลักษณะพิเศษของผู้ควบคุมข้อมูลส่วนบุคคล

(หมายเหตุ: การประเมินความเสี่ยงควรพิจารณาจากกฎหมายลำดับรองหรือแนวทางปฏิบัติหากมีการออกกฎหมายลำดับรองหรือแนวทางปฏิบัติแล้ว)

คำถามที่ 6: มีกฎหมายลำดับรองใดที่ยกเว้นให้ไม่ต้องแจ้งต่อเจ้าของข้อมูลหรือไม่ หากมี ข้อยกเว้นนั้นนำมาใช้บังคับได้หรือไม่

(หากคำตอบข้อ 6 คือไม่มี ฝ่ายงานจัดการสถานการณ์ควรพิจารณาว่า (1) จะต้องรายงานต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลหรือไม่ และ (2) จะต้องแจ้งต่อเจ้าของข้อมูลหรือไม่

2. แนวทางในการพิจารณากำหนด – พ.ร.บ. การรักษาความปลอดภัยมั่นคงไซเบอร์

ฝ่ายงานจัดการสถานการณ์จะต้องวิเคราะห์ลักษณะ ขอบข่าย และความรุนแรงของเหตุการณ์รั่วไหลของข้อมูลตามทิศทางและแนวทางของ [สายงานกฎหมาย] หรือที่ปรึกษาทางกฎหมายจากภายนอก ซึ่งควรทำเป็นรายกรณีไป โดยพิจารณาจากชุดคำถามต่อไปนี้

หมายเหตุ: ในทุกกรณี [สายงานกฎหมาย] จะต้องตรวจสอบว่า หน่วยงานที่มีอำนาจได้ออกกฎหมายลำดับรองหรือแนวทางปฏิบัติเกี่ยวกับโครงสร้างพื้นฐานสำคัญ การละเมิดข้อมูล และการประเมินความเสี่ยงแล้วหรือไม่ หากมีการออกออกกฎหมายลำดับรองหรือแนวทางปฏิบัติแล้วจะต้องนำมาพิจารณาร่วมกับชุดคำถามต่อไปนี้

คำถามที่ 1: มีกฎหมายลำดับรองใดที่กำหนดหลักเกณฑ์ของหน่วยงานโครงสร้างพื้นฐานสำคัญหรือไม่ หากมีธนาคารเป็นไปตามหลักเกณฑ์ใด

(หากใช่ กรุณาอ่านคำถามต่อไป)

คำถามที่ 2: เหตุการณ์รั่วไหลของข้อมูลของข้อมูลถือนี้เป็น “ภัยคุกคามทางไซเบอร์” ตามคำนิยามใน พ.ร.บ. การรักษาความปลอดภัยมั่นคงไซเบอร์หรือไม่

(หากใช่ กรุณาอ่านคำถามต่อไป)

คำถามที่ 3: มีกฎหมายลำดับรองใดที่กำหนดหลักเกณฑ์ภัยคุกคามทางไซเบอร์ที่มี “นัยสำคัญ” หรือไม่ หากมี เหตุการณ์รั่วไหลของข้อมูลของข้อมูลนี้เป็นไปตามหลักเกณฑ์ใด

(หากมี ฝ่ายงานจัดการสถานการณ์จะต้องพิจารณาว่าจะต้องรายงานต่อคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) และคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) หรือไม่

[หมายเหตุ: ควรใส่แนวทางการประเมินความเสี่ยงตามกฎหมายหรือระเบียบเฉพาะส่วน (ถ้ามี) เพิ่มเติม และควรปรับปรุงแนวทางการประเมินความเสี่ยงนี้ให้เป็นข้อมูลล่าสุดเป็นครั้งคราว]