สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

สัมมนารับฟังการชี้แจง

แนวปฏิบัติของภาคธุรกิจประกันวินาศภัย ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (ปรับปรุงแก้ไขครั้งที่ 1)

วันศุกร์ที่ 28 เมษายน 2566

เวลา 09.00-12.00 น. รูปแบบ Hybrid

ณ ห้องสัมมนา 501 ชั้น 5 สมาคมประกันวินาศภัยไทย

และ zoom

Current Status of the PDPA

PDPA published in the Government Gazette

27 May 2019

PDPA came into full effect

1 June 2022

Sub-regulations issued

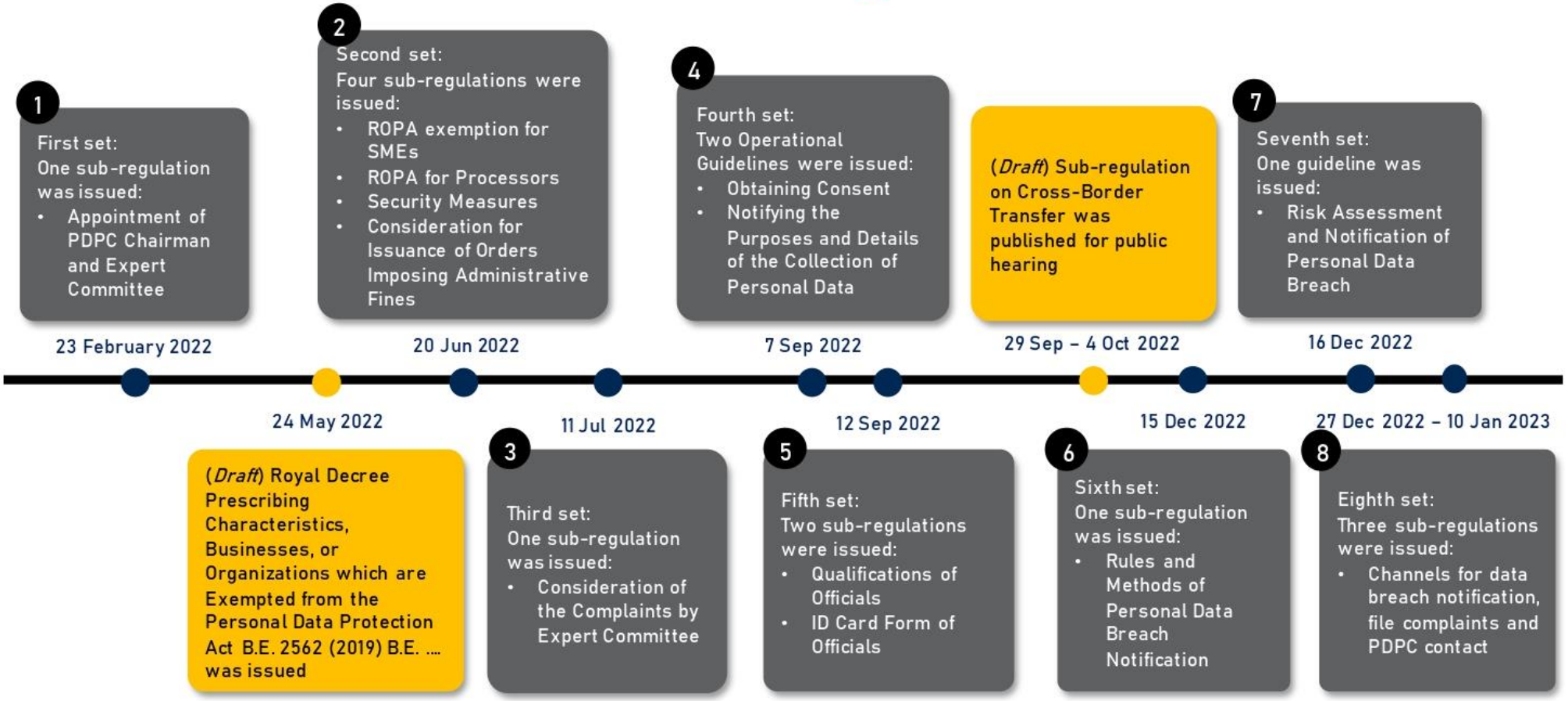
18 January 2022

The Personal Data Protection Committee (PDPC) was officially appointed.

1 October 2022

Secretary-General of the PDPC was appointed.

Current Status of the Sub-Regulations under PDPA



สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

สรุปสาระสำคัญของแนวปฏิบัติของภาคธุรกิจประกันวินาศภัย ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่ได้ปรับปรุงแก้ไขครั้งที่ 1

28 เมษายน พ.ศ. 2566

สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

กฎหมายลำดับรองที่เกี่ยวข้องกับธุรกิจประกันวินาศภัย

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565	ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565
• ประกาศฯ วันที่ 20 มิถุนายน 2565 • มีผลบังคับใช้วันที่ 21 มิถุนายน 2565 • เพิ่มเติมในบทที่ 2 ของแนวปฏิบัติฯ	• ประกาศฯ วันที่ 15 ธันวาคม 2565 • มีผลบังคับใช้วันที่ 16 ธันวาคม 2565 • เพิ่มเติมในบทที่ 8 ของแนวปฏิบัติฯ

สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565

มีมาตรการรักษาความปลอดภัยที่ครอบคลุม การเก็บ รวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล	มีมาตรการเชิงองค์กร มาตรการเชิงเทคนิค และมาตรการทางกายภาพ ที่เหมาะสม	มีกระบวนการเพื่อบริหารความเสี่ยง	มีการควบคุมการเข้าถึงข้อมูล (Access Control)
มีการป้องกันทั้งทางกายภาพ และทางเทคนิค	มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน	มีการทบทวนมาตรรักษาความปลอดภัย	สร้างเสริมการตระหนักรู้ (Privacy & Security Awareness)

กรณีมีกฎหมายอื่นกำหนดเรื่องมาตรฐานความปลอดภัยสำหรับผู้ควบคุมเอาไว้ ให้ดำเนินการตามกฎหมายนั้น โดยอย่างน้อยต้องเป็นไปตามมาตรฐานขั้นต่ำ

ประกาศ คปภ. เรื่อง หลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันชีวิต / ประกันวินาศภัย พ.ศ. 2563 (ประกาศ IT Risk Management)

1. การกำกับดูแลด้านเทคโนโลยีสารสนเทศ IT Governance
2. การบริหารโครงการด้านเทคโนโลยีสารสนเทศ IT Project Management
3. การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ IT Security
4. การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ IT Risk Management
5. การปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ IT Compliance
6. การตรวจสอบด้านเทคโนโลยีสารสนเทศ IT Audit
7. การกำกับดูแลและบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ Cybersecurity
8. การรายงานเหตุการณ์ภัยคุกคามทางไซเบอร์หรือภัยคุกคามที่มีต่อระบบเทคโนโลยีสารสนเทศ Reporting

- แนวปฏิบัติ เรื่อง หลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันชีวิต / ประกันวินาศภัย พ.ศ. 2564
- แนวปฏิบัติ เรื่อง หลักเกณฑ์การกำกับดูแลการใช้บริการจากผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ พ.ศ. 2564
- คู่มือการตอบสนองภัยคุกคามทางไซเบอร์สำหรับบริษัทประกันภัย (Cyber Incident Response Plan Handbook) พ.ศ. 2564
- แนวปฏิบัติ เรื่อง การกำกับดูแลข้อมูล (Data Governance Guideline) พ.ศ. 2565

สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

ความมั่งคงปลอดภัยทางสารสนเทศ (Information Security) 3 ประการหลัก

การควบคุมการเข้าถึงข้อมูล (Confidentiality)

- เข้าถึงข้อมูลได้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น ไม่ให้เกิดการรั่วไหลของข้อมูลโดยไม่ได้รับอนุญาต
- จัดให้มีนโยบายกำหนดขั้นข้อมูล (classification policy) เพื่อกำหนดประเภทของข้อมูลและประเภทของบุคคลที่จะเข้าถึงข้อมูลประเภทต่างๆ ได้

การควบคุมการแก้ไขข้อมูล (Integrity)

- เปลี่ยนแปลงแก้ไขข้อมูลเฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น
- จัดให้มีนโยบายแบ่งแยกหน้าที่ (separation of duty) ให้มีผู้ปฏิบัติงานถ่วงดุลตรวจสอบกันในการทำงาน

การควบคุมการหยุดชะงักของระบบ (Availability)

- ควบคุมการทำงานของระบบให้บุคคลสามารถใช้งานได้อย่างต่อเนื่อง ไม่ให้เกิดการหยุดชะงักของระบบโดยไม่ทราบล่วงหน้า
- จัดให้มีแผนฉุกเฉิน (contingency planning) ที่จะประเมินความเสี่ยงและเตรียมความพร้อมเพื่อที่จะรับมือและแก้ไขสถานการณ์ฉุกเฉิกที่อาจเกิดขึ้น

สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

มาตรการการรักษาความปลอดภัย

Organizational Measures

Technical Measures

Physical Measures

- คำนึงถึงระดับความเสี่ยง โอกาสเกิด และผลกระทบจากเหตุการละเมิดข้อมูลส่วนบุคคล
- ต้องมีการทบทวนมาตรการรักษาความปลอดภัย
- กรณีมีกฎหมายอื่นบัญญัติไว้ให้ดำเนินการตามนั้น โดยอย่างน้อยต้องเป็นไปตามมาตรฐานขั้นต่ำ

สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

มาตรการการรักษาความปลอดภัยที่ยอมรับ

ผู้ควบคุมข้อมูลส่วนบุคคลต้องมีมาตรฐานในการรักษาความปลอดภัยที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในลักษณะเดียวกันหรือใกล้เคียงกัน

ISO 27001 Information Security Management

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
ISO 27701:2019
Privacy Information Management

สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

มาตรการการรักษาความปลอดภัยขั้นต่ำ

การควบคุมการเข้าถึงข้อมูลส่วนบุคคล (Access Control)	การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)	การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)	การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลัง (Audit Trails)
• มีการพิสูจน์และยืนยันตัวตน (Identify Proofing & Authentication) • มีการอนุญาตหรือกำหนดสิทธิในการเข้าถึงและใช้งานที่เหมาะสม โดยคำนึงถึงหลักการให้สิทธิเท่าที่จำเป็น (need to know basis)	• การลงทะเบียนและการถอนสิทธิใช้งาน (User Registration and De-Registration) • การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (User Access Provisioning) • การบริหารจัดการสิทธิการเข้าถึงตามสิทธิ(Management of Privileged Access Rights)	• ป้องกันการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ • ป้องกันการกระทำนอกเหนือบทบาทหน้าที่ที่ได้รับมอบหมาย ตลอดจนการลักลอบ ทำสำเนาข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และการลักขโมยอุปกรณ์จัดเก็บ หรือประมวลผลข้อมูลส่วนบุคคล	• จัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับเข้าถึง เปลี่ยนแปลง แก้ไข หรือลบ

การทบทวนมาตรการการรักษาความปลอดภัย

เมื่อมีความจำเป็น
(Important)

เมื่อเทคโนโลยีเปลี่ยนแปลง
(Change of Technology)

เมื่อมีเหตุละเมิดข้อมูลส่วนบุคคล
(Personal Data Breach)

สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565

การละเมิดข้อมูลส่วนบุคคล (Personal Data Breach)

คือ การละเมิดมาตรการรักษาความมั่นคงปลอดภัย ที่ทำให้เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ ไม่ว่าจะเกิดจากเจตนา ความจงใจ ความประมาทเลินเล่อ การกระทำโดยปราศจากอำนาจหรือโดยมิชอบ การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ภัยคุกคามทางไซเบอร์ ข้อผิดพลาดบกพร่องหรืออุบัติเหตุ หรือเหตุอื่นใด

ตัวอย่างเหตุการณ์ที่อาจถือว่าเป็นการละเมิดข้อมูลส่วนบุคคล

- การที่บุคคลที่สามเข้าถึงข้อมูลส่วนบุคคลโดยไม่มีอำนาจ
- การส่งข้อมูลส่วนบุคคลไปยังผู้รับผิดคน
- การเปลี่ยนแปลงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต
- การสูญเสียความสามารถในการใช้ข้อมูลส่วนบุคคล (Ransomware)
- เกิดการเจาะระบบ (Hack) ที่บริษัทใช้งาน

สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

เหตุการละเมิดข้อมูลส่วนบุคคล

การละเมิดความลับของข้อมูลส่วนบุคคล
(Confidentiality Breach)

การละเมิดความถูกต้องครบถ้วนของข้อมูลส่วนบุคคล
(Integrity Breach)

การละเมิดความพร้อมใช้งานของข้อมูลส่วนบุคคล
(Availability Breach)

สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

การจัดการเหตุการละเมิดข้อมูลส่วนบุคคล

ได้รับแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล

- เจ้าของข้อมูลส่วนบุคคล
- Controller
- Processor (ต้องระบุหน้าที่การแจ้งเหตุการละเมิดภายใน 72 ชั่วโมงในสัญญา)

ตรวจสอบว่าเป็นเหตุการละเมิดข้อมูลส่วนบุคคลหรือไม่

- ตรวจสอบมาตรการรักษาความมั่นคงปลอดภัยตามข้อเท็จจริงที่เกิดขึ้น
- ทำการประเมินความเสี่ยงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคล

ทำการประเมินความเสี่ยงเหตุการละเมิดข้อมูลส่วนบุคคลตามแนวทางของ PDPC

- แนวทางการประเมินความเสี่ยงสำหรับการละเมิดข้อมูลส่วนบุคคล ตามประกาศ PDPC ข้อ 12

หากพบว่า

- มีความเสี่ยงสูง
- มีความเสี่ยง
- ไม่มีความเสี่ยง

แจ้งต่อ PDPC และ OIC ภายใน 72 ชั่วโมง ในกรณีที่พบว่า มีความเสี่ยงที่จะมีผลกระทบต่อสิทธเสรีภาพของบุคคล

- สาระสำคัญในการแจ้งตามประกาศ PDPC ข้อ 6

วิธีการแจ้ง

1. เป็นลายลักษณ์อักษรผ่านช่องทางอิเล็กทรอนิกส์ หรือ
2. ช่องทางที่ PDPC กำหนด

- มีข้อยกเว้นแจ้งล่าช้าตามประกาศ PDPC ข้อ 7 แต่ไม่เกิน 15 วัน

แจ้งต่อเจ้าของข้อมูลส่วนบุคคลด้วย ในกรณีที่มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลโดยไม่ชักช้า

- สาระสำคัญตามประกาศ PDPC ข้อ 10

วิธีการแจ้ง

1. แจ้งเป็นรายบุคคลเป็นหนังสือหรือโดยวิธีการอิเล็กทรอนิกส์
2. แจ้งเป็นกลุ่ม ผ่านสื่อสาธารณะ โดยให้เจ้าของข้อมูลส่วนบุคคลเข้าถึงได้

ทบทวนมาตรการรักษาความมั่นคงปลอดภัยเพื่อป้องกันการเกิดเหตุละเมิดในอนาคต

สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

ปัจจัยการประเมินความเสี่ยงสำหรับการละเมิดข้อมูลส่วนบุคคล และการแจ้งต่อ PDPC และ OIC*

*ข้อ 12 ของประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องหลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565 -> ประเมินความเสี่ยง

*ข้อ 6 ของประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องหลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565 -> ข้อมูลที่ต้องแจ้งต่อ PDPC และ OIC

ปัจจัยการประเมิน	รายละเอียด
ข้อ 12 (1) ลักษณะและประเภทของการละเมิดข้อมูลส่วนบุคค	• ประเภทการละเมิดความลับ / ความถูกต้อง / ความพร้อมใช้งาน • เหตุการละเมิดเกิดจาก ความผิดพลาดในการดำเนินการ / จากภัยคุกคามไซเบอร์** • เหตุการละเมิดโดย Controller หรือ Processor
ข้อ 12 (2) ลักษณะหรือประเภทของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด	• ข้อมูลส่วนบุคคลทั่วไป เช่น ข้อมูลการพิสูจน์ตัวตน ข้อมูลทางการเงิน -> เสี่ยงสูง • ข้อมูลส่วนบุคคลที่มีความอ่อนไหว -> เสี่ยงสูง
ข้อ 12 (3) ปริมาณของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด ซึ่งอาจพิจารณาจาก - จำนวนเจ้าของข้อมูลส่วนบุคคล หรือ - จำนวนรายการ (records) ของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด	• จำนวนมาก -> เสี่ยงสูง • จำนวนเจ้าของไม่มาก แต่จำนวนข้อมูลส่วนบุคคลมาก เช่น ข้อมูลทั้งหมดของเจ้าของข้อมูล -> เสี่ยงสูง
ข้อ 12 (4) ลักษณะ ประเภท หรือสถานะของเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ รวมถึงข้อเท็จจริงว่าเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ ประกอบด้วยผู้เยาว์ ผู้พิการ ผู้ไร้ความสามารถผู้เสมือนไร้ความสามารถ หรือบุคคลเปราะบาง (vulnerable persons) ที่ขาดความสามารถในการปกป้องสิทธิและประโยชน์ของตนเนื่องจากข้อจำกัดต่าง ๆ ด้วยหรือไม่ เพียงใด	• หากมีเจ้าของข้อมูลส่วนบุคคลเป็นบุคคลผู้หย่อนความสามารถ -> เสี่ยงสูง

**ต้องพิจารณาการปฏิบัติตามประกาศ OIC ที่เกี่ยวข้องเพิ่มเติม เช่น ประกาศเกี่ยวกับ IT Risk Management ประกาศ BCM/BCP

สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

ปัจจัยการประเมินความเสี่ยงสำหรับการละเมิดข้อมูลส่วนบุคคล และการแจ้งต่อ PDPC และ OIC*

ปัจจัยการประเมิน	รายละเอียด
ข้อ 12 (5) ความร้ายแรงของผลกระทบและความเสียหายที่เกิดขึ้นหรืออาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคลจากการละเมิดข้อมูลส่วนบุคคล และประสิทธิผลของมาตรการที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือจะใช้เพื่อป้องกัน ระงับ หรือแก้ไขเหตุการละเมิดข้อมูลส่วนบุคคล หรือเยียวยาความเสียหายต่อการบรรเทาผลกระทบและความเสียหายที่เกิดขึ้นหรืออาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคล	• หากข้อมูลนั้นมีผลกระทบต่อชีวิต หรือทำให้ถูกเกลียดชัง / เปิดเผยต่อสาธารณะ -> เสี่ยงสูง • ให้แจ้งวิธีการเยียวยาที่ได้ดำเนินการแล้วเบื้องต้น
ข้อ 12 (6) ผลกระทบในวงกว้างต่อธุรกิจ หรือการดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคล หรือต่อสาธารณะจากเหตุการละเมิดข้อมูลส่วนบุคคล	• หากเป็นการเปิดเผยต่อสาธารณะ -> เสี่ยงสูง
ข้อ 12 (7) ลักษณะของระบบการจัดเก็บข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิดและมาตรการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ทั้งที่เป็นมาตรการเชิงองค์กร (organizational measures) และมาตรการเชิงเทคนิค (technical measures) รวมถึงมาตรการทางกายภาพ (physical measures)	• พิจารณาว่ามาตรการรักษาความมั่นคงปลอดภัยนั้นมีความเหมาะสมหรือไม่ หากไม่เหมาะสม -> เสี่ยงสูง • ทำการทบกวนมาตรการรักษาความมั่นคง
ข้อ 12 (8) สถานะทางกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลว่าเป็นบุคคลธรรมดาหรือนิติบุคคล รวมทั้งขนาดและลักษณะของกิจการของผู้ควบคุมข้อมูลส่วนบุคคล	
ข้อ 6 (2) ชื่อ สถานที่ติดต่อ และวิธีการติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (ถ้ามี) หรือ บุคคลที่ทำหน้าที่ประสานงาน	

สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

หน้าที่ในแจ้งเหตุละเมิดข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด

ผู้มีหน้าที่แจ้ง	แจ้งใคร	เงื่อนไขในการแจ้ง
ผู้ควบคุมข้อมูลส่วนบุคคล	สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส) และสำนักงาน คปภ.	• กรณีมีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล • ภายใน 72 ชั่วโมงนับแต่ทราบเหตุ • ต้องทบทวนมาตรการรักษาความมั่นคงปลอดภัย
	เจ้าของข้อมูลส่วนบุคคล	• กรณีมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล • โดยไม่ชักช้า พร้อมกับแนวทางเยียวยา • ต้องทบทวนมาตรการรักษาความมั่นคงปลอดภัย
ผู้ประมวลผลข้อมูลส่วนบุคคล	ผู้ควบคุมข้อมูลส่วนบุคคล	ตามเงื่อนไขที่กำหนดในสัญญาประมวลผลข้อมูลส่วนบุคคล หรือข้อตกลงเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล

กรณีแจ้งล่าช้าเกินกว่า 72 ชั่วโมง ผู้ควบคุมข้อมูลส่วนบุคคลอาจขอให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล พิจารณายกเว้นความผิดจากการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลล่าช้าได้ โดยชี้แจงเหตุผลความจำเป็นและรายละเอียดที่เกี่ยวข้องโดยเร็ว ทั้งนี้ ต้องไม่เกิน 15 วันนับแต่ทราบเหตุ

สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

สาระสำคัญในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

ข้อมูลโดยสังเขปเท่าที่จะสามารถระบุได้เกี่ยวกับลักษณะและประเภทของการละเมิดข้อมูลส่วนบุคคล โดยอาจบรรยายถึงลักษณะและจำนวนเจ้าของข้อมูลส่วนบุคคล หรือลักษณะและจำนวนรายการ (records) ของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด

ชื่อ สถานที่ติดต่อ และวิธีการติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลมอบหมายให้ทำหน้าที่ประสานงานและให้ข้อมูลเพิ่มเติม

ข้อมูลเกี่ยวกับผลกระทบที่อาจเกิดขึ้นจากเหตุการละเมิดข้อมูลส่วนบุคคล

ข้อมูลเกี่ยวกับมาตรการที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือจะใช้เพื่อป้องกัน ระงับ หรือแก้ไขเหตุการละเมิดข้อมูลส่วนบุคคล หรือเยียวยาความเสียหาย โดยอาจใช้มาตรการทางบุคลากรกระบวนการ หรือเทคโนโลยี หรือมาตรการอื่นใดที่จำเป็นและเหมาะสม

ในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบทราบ หากโดยสภาพไม่สามารถดำเนินการแจ้งเป็นรายบุคคลได้ เนื่องจากไม่มีวิธีการติดต่อ หรือโดยเหตุจำเป็นอื่นใด ผู้ควบคุมข้อมูลส่วนบุคคลอาจแจ้งเหตุการละเมิดแก่เจ้าของข้อมูลส่วนบุคคลเป็นกลุ่ม หรือแจ้งเป็นการทั่วไปผ่านสื่อสาธารณะ สื่อสังคมออนไลน์ หรือโดยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใดได้ ทั้งนี้ ต้องจะต้องไม่ก่อให้เกิดความเสียหายหรือผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล

สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

ข้อยกเว้นการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

- ✓ไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล
- ✓ข้อมูลส่วนบุคคลตามเหตุการละเมิดข้อมูลส่วนบุคคลนั้น เป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้
- ✓ ข้อมูลส่วนบุคคลนั้นไม่อยู่ในสภาพที่ใช้งานได้เนื่องจากมีมาตรการทางเทคโนโลยีที่เพียงพอ
- ✓เหตุอื่นใดที่เชื่อถือได้

ผู้ควบคุมข้อมูลส่วนบุคคล ควรบันทึกเหตุที่ควรได้รับการยกเว้นและเก็บเอกสารหลักฐานที่เกี่ยวข้อง เนื่องจากมีหน้าที่ตามกฎหมายที่ต้องให้ข้อมูลหรือส่งเอกสารหรือหลักฐานเกี่ยวกับเหตุที่ควรได้รับการยกเว้น ซึ่งรวมถึงรายละเอียดเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลหรือข้อมูลอื่นใด ให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย และหน่วยงานกำกับอื่นๆ ที่เกี่ยวข้อง พิจารณา เมื่อมีการร้องขอ

สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

บทลงโทษกรณีไม่แจ้งเหตุละเมิดข้อมูลส่วนบุคคล

หากบริษัทไม่แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด บริษัทอาจถูก **โทษปรับทางปกครองไม่เกิน 3 ล้านบาท** ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มาตรา 83

ทั้งนี้ ในกรณีที่บริษัทไม่เห็นด้วยกับการลงโทษทางปกครองข้างต้น บริษัทสามารถอุทธรณ์โต้แย้งได้ตามกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครอง และกฎหมายว่าด้วยวิธีพิจารณาความของศาลปกครอง

สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

ตัวอย่างการประเมินความเสี่ยงเหตุละเมิดข้อมูลส่วนบุคคล

สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

การนับระยะเวลา 72 ชั่วโมง

การแจ้งการละเมิดข้อมูลส่วนบุคคลต่อสำนักงานฯ จะต้องดำเนินการภายใน 72 ชั่วโมงนับแต่ทราบเหตุ โดยที่การดำเนินการตรวจสอบข้อเท็จจริงเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลนั้นจะต้องดำเนินการภายใน 72 ชั่วโมงด้วยเช่นกัน ซึ่งการกำหนดระยะเวลาการแจ้งการละเมิดข้อมูลส่วนบุคคลดังกล่าวนั้น มีความแตกต่างจากหลักการเกี่ยวกับการแจ้งการละเมิดข้อมูลส่วนบุคคลตาม GDPR โดย GDPR กำหนดว่าช่วงระยะเวลาที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้ในการตรวจสอบข้อเท็จจริงเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลนั้นจะไม่ถือว่าผู้ควบคุมข้อมูลส่วนบุคคล ‘รับทราบ’ การละเมิดข้อมูลส่วนบุคคล ดังนั้น ในช่วงระยะเวลาการตรวจสอบข้อเท็จจริงดังกล่าวจึงยังไม่เริ่มนับระยะเวลาที่ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งการละเมิดข้อมูลส่วนบุคคลต่อหน่วยงานรัฐ Guidelines 9/2022 on personal data breach notification under GDPR

สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

ตัวอย่างการประเมินความเสี่ยง

ตัวอย่าง	แจ้งเหตุแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล	แจ้งเหตุแก่เจ้าของข้อมูลส่วนบุคคล	เหตุผล
1. ผู้ควบคุมข้อมูลส่วนบุคคลจัดเก็บข้อมูลส่วนบุคคลสำรองไว้ใน USB Drive โดยมีการเข้ารหัสด้วยเทคโนโลยีที่น่าเชื่อถือ ต่อมา USB Drive ดังกล่าวสูญหายไป	✘	✘	เนื่องจากเมื่อมีการเข้ารหัสด้วยมาตรการทางเทคโนโลยีที่น่าเชื่อถือแล้วข้อมูลดังกล่าวไม่สามารถเปิดใช้งานได้ การที่ USB Driveสูญหายไป จึงไม่มีความเสี่ยงกับเจ้าของข้อมูลส่วนบุคคล
2. ผู้ควบคุมข้อมูลส่วนบุคคลให้บริการจัดเก็บข้อมูลส่วนบุคคลในระบบออนไลน์ ต่อมาเกิดภัยคุกคามทางไซเบอร์ ส่งผลให้ข้อมูลส่วนบุคคลที่ระบุตัวบุคคลได้โดยตรงรั่วไหลจากระบบคอมพิวเตอร์ของผู้ควบคุมข้อมูลส่วนบุคคล	✓	✓	เนื่องจากข้อมูลส่วนบุคคลดังกล่าวอยู่ในสภาพที่ใช้งานได้และสามารถระบุตัวบุคคลได้ การที่เกิดภัยคุกคามทางไซเบอร์อาจจะก่อให้เกิดปัญหาและผลกระทบซึ่งเกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคลจำนวนมาก (ความเสี่ยงสูง)

สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

ตัวอย่างการประเมินความเสี่ยง (ต่อ)

ตัวอย่าง	แจ้งเหตุแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล	แจ้งเหตุแก่เจ้าของข้อมูลส่วนบุคคล	เหตุผล
3. ระบบไฟฟ้าใน call center ของผู้ควบคุมข้อมูลส่วนบุคคลขัดข้อง โดยไฟดับชั่วคราว ส่งผลให้ระบบคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ของผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถให้บริการได้ชั่วคราว	✗	✗	เนื่องจากข้อมูลส่วนบุคคลดังกล่าวไม่อยู่ในสภาพพร้อมใช้งานเนื่องจากปัญหาด้านเทคโนโลยี เมื่อระบบไฟฟ้ากลับมาเหมือนเดิม ข้อมูลส่วนบุคคลดังกล่าวก็สามารถใช้งานได้ จึงไม่ถือว่าเป็นกรณีละเมิดข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล
4. ผู้ควบคุมข้อมูลส่วนบุคคลถูกภัยคุกคามทางไซเบอร์ โดยถูกโจมตีจากมัลแวร์เรียกค่าไถ่ (Ransomware) เพื่อควบคุมข้อมูลส่วนบุคคลทั้งหมด และผู้ควบคุมข้อมูลส่วนบุคคลไม่มีข้อมูลสำรอง จึงไม่สามารถที่จะเข้าถึงและใช้งานข้อมูลดังกล่าวได้	✓	✓	เนื่องจากข้อมูลส่วนบุคคลดังกล่าวอยู่ในสภาพที่สามารถระบุตัวบุคคลได้ การถูกโจมตีจากมัลแวร์เรียกค่าไถ่ทำให้ข้อมูลดังกล่าวไม่อยู่ในสภาพที่พร้อมใช้งาน และข้อมูลสำรองที่มีอยู่ไม่สมบูรณ์เพียงพอที่จะให้บริการ หรือไม่สามารถเรียกใช้งานข้อมูลสำรองได้ภายในระยะเวลาที่กำหนดของแต่ละบริษัท

สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

ตัวอย่างการประเมินความเสี่ยง (ต่อ)

ตัวอย่าง	แจ้งเหตุแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล	แจ้งเหตุแก่เจ้าของข้อมูลส่วนบุคคล	เหตุผล
5. บริษัทได้รับการติดต่อจากลูกค้า 10 ราย ว่าได้รับใบแจ้งหนี้เรียกเก็บเงินของบุคคลที่ไม่รู้จัก และทำการตรวจสอบแล้วภายใน 24 ชั่วโมง พบว่ามีการรั่วไหลของข้อมูลส่วนบุคคล จำนวน 10 ราย	✓	✓	เนื่องจากข้อมูลดังกล่าวเป็นข้อมูลที่รั่วไหลออกไปจริงในเบื้องต้นมีผลกระทบเฉพาะผู้ที่ถูกเรียกเก็บเงินตามใบแจ้งหนี้ อย่างไรก็ตาม บริษัทในฐานะผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการตรวจสอบเพิ่มเติมว่ามีบุคคลอื่นใดที่ข้อมูลรั่วไหลออกไปภายนอกหรือไม่ หากพบจะต้องแจ้งเพิ่มเติม และอาจปรับระดับความเสี่ยงเป็นสูงได้
6. บริษัทถูกภัยคุกคามทางไซเบอร์ โดยการโจมตีระบบจาก Hacker ทำให้ประวัติข้อมูลสุขภาพบางส่วนรั่วไหล	✓	✓	จำเป็นต้องแจ้งเหตุ หากเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหวและสามารถระบุตัวตนของผู้เอาประกันภัยหรือบุคคลอื่นที่เกี่ยวข้องได้

สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

ตัวอย่างการประเมินความเสี่ยง (ต่อ)

ตัวอย่าง	แจ้งเหตุแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล	แจ้งเหตุแก่เจ้าของข้อมูลส่วนบุคคล	เหตุผล
7. บริษัทให้บริการแบบออนไลน์ ซึ่งจำเป็นต้องมีการลงทะเบียนข้อมูลผู้ใช้บริการและกำหนดรหัสผ่าน เช่น การเรียกร้องค่าสินไหมทดแทน การตรวจสอบกรมธรรม์ประกันภัย เป็นต้น ต่อมาถูกโจมตีจากภัยคุกคามทางไซเบอร์ โดยข้อมูลผู้ใช้บริการและรหัสผ่านถูกเข้าถึง และถูกนำไปโพสต์บนอินเทอร์เน็ต	✓	✓	เนื่องจากข้อมูลที่มีการรั่วไหลบนอินเทอร์เน็ต ซึ่งถูกโจมตี เป็นการกระทำความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ข้อมูลที่รั่วไหลประกอบด้วยรายชื่อและข้อมูลสำคัญของผู้ใช้บริการ จึงจำเป็นต้องแจ้งเหตุแก่เจ้าของข้อมูลส่วนบุคคลเพราะมีความเสี่ยงสูงที่ข้อมูลดังกล่าวจะถูกนำไปทำธุรกรรมที่ผิดกฎหมาย
8. ระบบผู้ให้บริการประมวลผลข้อมูลส่วนบุคคลของบริษัทเกิดปัญหา และไม่สามารถแก้ไขให้กลับมาพร้อมใช้งานภายใน Service Level Agreement ที่กำหนด เป็นเหตุให้ผู้ใช้บริการไม่สามารถเข้าใช้บริการได้	✓	✗	ผู้ให้บริการประมวลผลข้อมูลส่วนบุคคลต้องตรวจสอบข้อเท็จจริงเพิ่มเติม หากพบว่าระบบถูกโจมตีจากภัยคุกคามทางไซเบอร์ ต้องแจ้งบริษัทตามที่ระบุไว้ในสัญญาหรือข้อตกลงที่เกี่ยวข้อง บริษัทต้องแจ้งทั้งสำนักงานฯ และเจ้าของข้อมูลส่วนบุคคลพร้อมปรับระดับเป็นความเสี่ยงสูง

สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

ตัวอย่างการประเมินความเสี่ยง (ต่อ)

ตัวอย่าง	แจ้งเหตุแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล	แจ้งเหตุแก่เจ้าของข้อมูลส่วนบุคคล	เหตุผล
9. บริษัททำการตลาดแบบตรง โดยต้องการส่งข้อมูลส่วนบุคคลไปยังผู้รับข้อมูลแต่ละราย แต่เกิดความผิดพลาด จึงทำให้มีการส่งอีเมลไปยังผู้รับข้อมูลทั้งหมดจำนวน 100 คน พร้อมกัน	✓	✓	การพิจารณาว่าจะต้องแจ้งเหตุแก่เจ้าของข้อมูลหรือไม่ ขึ้นอยู่กับการเข้าถึงข้อมูล หากมีการเข้ารหัสข้อมูลดังกล่าวทั้งหมด จึงไม่จำเป็นต้องแจ้งเหตุ
10. บริษัทใส่อีเมลผู้รับจำนวน 100 คน เข้าไปในช่อง To หรือ CC แทนที่จะระบุไว้ในช่อง BCC ทำให้ผู้รับเห็นรายชื่ออีเมลของบุคคลอื่นที่ไม่เกี่ยวข้อง	✓	✓	การพิจารณาว่าจะต้องแจ้งเหตุแก่เจ้าของข้อมูลหรือไม่ ขึ้นอยู่กับปริมาณของข้อมูลส่วนบุคคลที่ส่งออกไปและลักษณะของข้อมูลด้วย

สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

1. Data Protection Legislation

- Personal Data Protection Act B.E. 2562 (2019) (PDPA)

2. Subordinate Regulations under the PDPA

Effective

10 Key Subordinate Regulations under the PDPA have been issued

1) Notification of the PDPC re: Rules and Methods of Personal Data Breach Notification B.E. 2565 (2022)
2) Notification of the PDPC re: Rules on Qualifications of Competent Officials under the PDPA B.E. 2565 (2022)
3) Notification of the PDPC re: Specifying Form of the Identification Card of the Competent Officials under the PDPA B.E. 2565 (2022)
4) Notification of the PDPC re: the Qualifications and Prohibitions, Term of Office, Vacation from Office, and Other Operations of the Expert Committee B.E. 2565 (2022)
5) Notification of the PDPC re: Exemption from Maintenance of Records Obligation of the Data Controller Which is a Small Organization B.E. 2565 (2022)
6) Notification of the PDPC re: Rules and Methods for Preparation and Maintenance of Records of Personal Data Processing Activities for the Data Processor B.E. 2565 (2022)
7) Notification of the PDPC re: Security Measures of the Data Controller B.E. 2565 (2022)
8) Notification of the PDPC re: Rules on Consideration for Issuance of Orders Imposing Administrative Fines by the Expert Committee B.E. 2565 (2022)
9) Notification of the PDPC re: Rules and Methods for recruiting a Chairperson and the Honorary Director in a commission supervising the Office of the PDPC B.E. 2565 (2022)
10) Rules of the PDPC re: the Filing, Refusal of Acceptance, Dismissal, Consideration, and Timeframe for the Consideration of the Complaints B.E. 2565 (2022)

3 guidelines under the PDPA have been issued

1) Operational Guideline re: Obtaining Consent from Data Subjects under the PDPA
2) Operational Guideline re: the Notification of the Purposes and Details of Collection of Personal Data from the Data Subjects under PDPA
3) Guideline re: Risk Assessment and Notification of Personal Data Breach

Draft

2 Draft Subordinate Regulations were Published for Public Hearings

- (*Draft*) Royal Decree Prescribing Characteristics, Businesses, or Organizations which are Exempted from the Personal Data Protection Act B.E. 2562 (2019) B.E. ....
- (*Draft*) Notification of the PDPC re: Criteria and Policies on the Protection of Personal Data that is Sent or Transferred Overseas B.E. ....

สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

Q & A