



สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

รู้ทัน เข้าใจ ปรับใช้ “กฎหมาย PDPA” กับการประกันภัยอุบัติเหตุและสุขภาพ

วันพฤหัสบดีที่ 22 กันยายน 2565

เวลา 09.00-12.00 น.

ผ่านระบบวิดีโอทัศนทางไกล (Zoom Meeting)





PDPA พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล เรื่องใกล้ตัวที่ทุกคนต้องรู้

PDPA (Personal Data Protection Act, B.E. 2562 (2019)) คือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยวันที่ 1 มิถุนายน 2565 เป็นวันที่ พ.ร.บ. PDPA นี้มีผลบังคับใช้ตามกฎหมายทั้งฉบับ

เหตุผลในการประกาศใช้ PDPA

เนื่องจากเทคโนโลยีก้าวหน้าขึ้น ช่องทางสื่อสารต่างๆ มีหลากหลายขึ้น ทำให้การละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลทำได้ง่ายขึ้น และหลายครั้งก็นำมาซึ่งความเดือดร้อนรำคาญหรือสร้างความเสียหายให้แก่เจ้าของข้อมูล ตลอดจนสามารถส่งผลกระทบต่อเศรษฐกิจโดยรวมของประเทศได้ด้วย จึงต้องมีกฎหมาย PDPA ว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลขึ้นเพื่อกำหนดหลักเกณฑ์ กติกา หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่รวมถึงการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลขึ้น



กฎหมาย / ประกาศที่เกี่ยวข้อง ที่ควรรู้

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- ประกาศ คำสั่ง ที่ออกภายใต้กรอบอำนาจ ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- ประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมธุรกิจประกันภัย เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล ของลูกค้าสำหรับธุรกิจประกันวินาศภัย พ.ศ. 2564



การคุ้มครองข้อมูลส่วนบุคคล





ส่วนที่ 1 บททั่วไป (หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล)

ส่วนที่ 2 การเก็บรวบรวมข้อมูลส่วนบุคคล

ส่วนที่ 3 การใช้หรือเปิดเผยข้อมูลส่วนบุคคล



ส่วนที่ 1 บททั่วไป : หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)



1. การเก็บรวบรวม
2. การใช้
3. การเปิดเผยข้อมูล

Data Controller

บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล (Personal Data)

ข้อมูลเกี่ยวกับบุคคล
ซึ่งทำให้สามารถระบุตัว
บุคคลนั้นได้ไม่ว่า “**ทางตรง**
หรือ ทางอ้อม” แต่ไม่รวมถึง
ข้อมูลของผู้ถึงแก่กรรม
โดยเฉพาะ และไม่รวมข้อมูล
ของนิติบุคคล

ชื่อ – นามสกุล

เลขประจำตัวประชาชน

ที่อยู่, เบอร์โทรศัพท์

วันเกิด, อีเมล,

การศึกษา, เพศ, อาชีพ,

รูปถ่าย, ข้อมูลทางการเงิน





ข้อมูลส่วนบุคคลที่มี **ความละเอียดอ่อน** (Sensitive Personal Data)

ต้องระมัดระวังเป็นพิเศษ !!!



ข้อมูลทางการแพทย์
หรือสุขภาพ



ข้อมูลทางพันธุกรรม
และไบโอเมตริกซ์



เชื้อชาติ
ความคิดเห็นทางการเมือง



ความเชื่อทางศาสนา
หรือปรัชญา



พฤติกรรมทางเพศ



ประวัติอาชญากรรม



ข้อมูลสภาพแรงงาน



บุคคลที่เกี่ยวข้องกับข้อมูลส่วนบุคคล



เจ้าของข้อมูลส่วนบุคคล

(Data Subject)

- คือ บุคคลที่ข้อมูลระบุไปถึง



ผู้ควบคุมข้อมูลส่วนบุคคล

(Data Controller)

- คือ บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ “ตัดสินใจ” เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล



ผู้ประมวลผลข้อมูลส่วนบุคคล

(Data Processor)

- คือ บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล “ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล” ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าว ต้องไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล



ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล

★ “ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจ เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

บริษัทฯ ถือเป็นผู้ควบคุมข้อมูลส่วนบุคคล หากมีลักษณะการประมวลผลข้อมูลส่วนบุคคลดังต่อไปนี้

- ✓ บริษัทฯ เป็นผู้ที่มีอำนาจตัดสินใจว่าจะเก็บรวบรวมข้อมูลส่วนบุคคลประเภทใด
- ✓ บริษัทฯ เป็นผู้ที่มีอำนาจตัดสินใจว่าข้อมูลส่วนบุคคลนั้นนำมาใช้เพื่อวัตถุประสงค์ใด
- ✓ บริษัทฯ เป็นผู้ที่มีอำนาจตัดสินใจว่าจะเก็บข้อมูลส่วนบุคคลของบุคคลใด
- ✓ บริษัทฯ เป็นผู้ที่มีอำนาจตัดสินใจว่าจะกำหนดให้ผลของการประมวลผลข้อมูลนั้นเป็นอย่างไร
- ✓ บริษัทฯ ไม่ได้ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลตามคำสั่ง หรือในนามของบุคคลอื่น หรือเป็นผู้แทนของบุคคลอื่น หรือองค์กรอื่น



ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล

- ★ “ผู้ประมวลผลข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่ง หรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล
- ★ บุคคลธรรมดาและนิติบุคคลสามารถมีฐานะเป็นผู้ประมวลผลข้อมูลส่วนบุคคลได้ หากบุคคลธรรมดาหรือนิติบุคคลนั้น ดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่ง หรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล



การเก็บรวบรวม ใช้ หรือเปิดเผย ข้อมูลส่วนบุคคล สามารถทำได้โดยอาศัยฐานทางกฎหมายดังต่อไปนี้

ฐานสัญญา

ฐานความยินยอม

ฐานประโยชน์ที่สำคัญต่อชีวิต

ฐานหน้าที่ตามกฎหมาย

ฐานภารกิจของรัฐ

ฐานประโยชน์อันชอบธรรม

ฐานจดหมายเหตุ/ วิจัย/ สถิติ



การเก็บรวบรวม ใช้ หรือเปิดเผย ข้อมูลส่วนบุคคลที่มีความอ่อนไหว สามารถทำได้ โดยอาศัยฐานทางกฎหมาย ดังต่อไปนี้

ฐานความยินยอม (โดยชัดแจ้ง)

ฐานประโยชน์ที่สำคัญต่อชีวิต

ฐานเพื่อการดำเนินการของมูลนิธิ สมาคม หรือองค์กรไม่แสวงกำไร

ฐานข้อมูลที่เปิดเผยโดยสาธารณะโดยความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล

ฐานความจำเป็นเพื่อดำเนินการเกี่ยวกับสิทธิเรียกร้อง

ฐานความจำเป็นในการปฏิบัติตามกฎหมายเกี่ยวกับลูกจ้าง สังคม ความคุ้มครองทางสังคม

ฐานความจำเป็นในการปฏิบัติตามกฎหมายเกี่ยวกับเวชศาสตร์ป้องกัน หรือ อาชีวศาสตร์

ฐานความจำเป็นในการปฏิบัติตามกฎหมายเพื่อประโยชน์สาธารณะด้านสาธารณสุข

ฐานความจำเป็นในการปฏิบัติตามกฎหมายเพื่อการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ สถิติ

ฐานความจำเป็นในการปฏิบัติตามกฎหมายเพื่อประโยชน์สาธารณะที่สำคัญ



สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject)

- ✓ สิทธิได้รับการแจ้งให้ทราบ (Right to be informed)
- ✓ สิทธิขอเข้าถึงข้อมูลส่วนบุคคล (Right of access)
- ✓ สิทธิในการขอให้โอนข้อมูลส่วนบุคคล (Right to data portability)
- ✓ สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (Right to object)
- ✓ สิทธิขอให้ลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคล
- ✓ สิทธิขอให้ระงับการใช้ข้อมูล (Right to restrict processing)
- ✓ สิทธิในการขอให้แก้ไขข้อมูลส่วนบุคคล (Right of rectification)



หลัก ห้ามเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง **เว้นแต่**



*** เว้นแต่กรณีเข้าข้อยกเว้นที่ไม่ต้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26**



การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ (Cross-border Personal Data Transfer)



ประเทศปลายทางหรือองค์กรระหว่างประเทศ ที่รับข้อมูลส่วนบุคคลต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล (PDPA: พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล) ที่เพียงพอ เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูล หรือเป็นการปฏิบัติตามกฎหมาย/สัญญา หรือเพื่อประโยชน์สาธารณะเป็นสำคัญเท่านั้น



บทลงโทษหากไม่ปฏิบัติตาม PDPA

เพื่อให้ข้อมูลส่วนบุคคล หรือ (PDPA พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล) ถูกนำไปใช้ในทางที่เหมาะสมและเป็นประโยชน์มากกว่าโทษ การให้ข้อมูลแต่ละครั้งจึงต้องพิจารณาอย่างรอบคอบก่อนให้ข้อมูล เช่นการให้ข้อมูลเพื่อจัดส่งสินค้า หากมีการขอข้อมูลที่ไม่เกี่ยวกับการจัดส่ง เจ้าของข้อมูลก็มีสิทธิปฏิเสธการให้ข้อมูลนั้น และในส่วนของผู้เก็บข้อมูลก็ต้องรู้ขอบเขตในการเข้าถึงข้อมูลส่วนบุคคล มีระบบในการควบคุม/ยืนยันตัวตนในการเข้าถึงข้อมูล และจำเป็นต้องมีการกำหนดนโยบายองค์กรเพื่อให้บุคคลที่เกี่ยวข้องปฏิบัติตาม เพราะหากไม่ทำตาม PDPA อาจได้รับโทษ



บทลงโทษ



ความรับผิด ทางแพ่ง

- ตามความเสียหายที่เกิดขึ้นจริง และอาจต้องชดใช้ค่าสินไหมทดแทนเพิ่มขึ้นอีก โดยสูงสุดไม่เกิน 2 เท่าของค่าเสียหายที่แท้จริง

โทษ ทางอาญา

- จำคุกสูงสุดไม่เกิน 1 ปี หรือปรับไม่เกิน 1 ล้านบาท หรือทั้งจำทั้งปรับ

โทษ ทางปกครอง

- ปรับสูงสุดไม่เกิน 5 ล้านบาท



การเลือกใช้ฐานในการประมวลผลข้อมูลส่วนบุคคล



- ★ ในการดำเนินธุรกิจประกันวินาศภัยส่วนใหญ่ บริษัทฯ สามารถอ้างอิงฐานในการประมวลผลข้อมูลส่วนบุคคลฐานอื่นนอกจากฐานความยินยอมเป็นหลัก (ความยินยอมจะต้องไม่ใช่ฐานที่บริษัทฯ ใช้เป็นหลักในการประกอบธุรกิจ) เช่น ฐานสัญญา ฐานประโยชน์อันชอบธรรม หรือ ฐานหน้าที่ตามกฎหมาย เป็นต้น
- ★ การดำเนินการสำหรับบางวัตถุประสงค์ เช่น การประมวลผลข้อมูลส่วนบุคคลเพื่อการดำเนินกิจกรรมส่งเสริมการขาย หรือการตลาดบางประเภทที่มีลักษณะเกินความคาดหมาย บริษัทฯ อาจต้องอ้างอิงฐานความยินยอมในการประมวลผลข้อมูลส่วนบุคคลเพื่อให้บรรลุวัตถุประสงค์
- ★ แนวปฏิบัติฉบับนี้แนะนำให้บริษัทฯ กำหนดและแยกส่วนที่เป็นการขอความยินยอมสำหรับวัตถุประสงค์เพื่อการดำเนินกิจกรรมส่งเสริมการขาย หรือการตลาดที่มีลักษณะเกินความคาดหมายออกจากส่วนอื่น เพื่อให้ลูกค้าได้รับแจ้งวัตถุประสงค์ดังกล่าวอย่างชัดเจน



การเลือกใช้ฐานในการประมวลผลข้อมูลส่วนบุคคล



- ★ ประกันภัยส่วนบุคคลบางประเภท เช่น ประกันภัยสุขภาพ จำเป็นต้องอาศัยการประมวลผลข้อมูลส่วนบุคคลทั่วไปและข้อมูลส่วนบุคคลที่มีความอ่อนไหวจำนวนมาก เช่น ข้อมูลสุขภาพ ประวัติการรักษาพยาบาล ข้อมูลการตอบคำถามสุขภาพ เพื่อการพิจารณารับประกันภัย การจัดการค่าสินไหมทดแทน และการป้องกันการฉ้อฉลประกันภัย
- ★ หากข้อมูลส่วนบุคคลใด จำเป็นต่อการประมวลผลเพื่อการเข้าทำสัญญาประกันภัย การปฏิบัติตามสัญญาประกันภัย การชดเชยค่าสินไหมทดแทน และการบริหารจัดการการฉ้อฉลประกันภัย บริษัทฯ ควรดำเนินการตามแนวทางดังต่อไปนี้
 - ✓ บริษัทฯ ไม่ต้องขอความยินยอมในการประมวลผลข้อมูลส่วนบุคคล โดยอ้างอิงข้อยกเว้นตามมาตรา 24 (3) การเข้าทำสัญญาประกันภัยและการปฏิบัติตามสัญญาประกันภัย
 - ✓ บริษัทฯ ไม่ต้องขอความยินยอมในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว โดยอ้างอิงฐานการปฏิบัติตามสัญญาประกันภัย ตามมาตรา 24 (3) และอ้างอิงการก่อตั้งสิทธิเรียกร้องตามมาตรา 26 (4) หรือประโยชน์สาธารณะที่สำคัญตามมาตรา 26 (5) (จ)

บทบาทของบริษัทประกันวินาศภัย

ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

- ✓ แจ้งนโยบายคุ้มครองข้อมูลส่วนบุคคล ให้เจ้าของข้อมูลทราบ
- ✓ มีมาตรการดูแล Security ที่เหมาะสม และทบทวนสม่ำเสมอ
- ✓ ลบ ทำลายข้อมูล เมื่อพ้นระยะเวลาเก็บรักษา
- ✓ แจ้งเหตุละเมิด ภายใน 72 ชั่วโมงนับแต่ทราบเหตุ
- ✓ แต่งตั้ง DPO
- ✓ จัดทำ + เก็บรักษาบันทึกการงาน





การรักษาความปลอดภัยของข้อมูลส่วนบุคคล



- ★ ผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ต้อง**จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม** เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ
- ★ ผู้ควบคุมข้อมูลส่วนบุคคลยังต้อง**คอบทวนมาตรการ**ดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสมด้วย
- ★ มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสมขึ้นอยู่กับ**การดำเนินการ**ของแต่ละบริษัทฯ และมาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และ/หรือ คณะกรรมการกำหนด



การกำหนดระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล



- ★ กฎหมายไม่ได้มีการกำหนดระยะเวลาที่ชัดเจนสำหรับการเก็บรักษาข้อมูลส่วนบุคคลในแต่ละประเภท เพียงแต่กำหนดไว้ว่าการเก็บรวบรวมข้อมูลส่วนบุคคล ให้เก็บรวบรวมได้เท่าที่จำเป็น ภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล
- ★ ผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถเก็บรักษาข้อมูลส่วนบุคคลไว้ได้ตลอดไป และต้องกำหนดระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคลดังกล่าวและให้เจ้าของข้อมูลทราบ
- ★ ในกรณีที่ไม่สามารถกำหนดระยะเวลาในการเก็บรวบรวมได้ชัดเจน ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม ภายใต้วัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลแต่ละเรื่องเท่านั้น



การแจ้งนโยบายคุ้มครองข้อมูลส่วนบุคคล

เนื่องจาก **PDPA** กำหนดให้ผู้ควบคุมข้อมูลต้องแจ้งรายละเอียดในนโยบายการคุ้มครองข้อมูลส่วนบุคคลต่อเจ้าของข้อมูลส่วนบุคคล ก่อน หรือ ในขณะที่ ที่ทำการเก็บรวบรวม

ดังนั้น ในระหว่างขั้นตอนการเก็บรวบรวมข้อมูลส่วนบุคคลไม่ว่าจะเป็นข้อมูลส่วนบุคคลทั่วไปหรือข้อมูลส่วนบุคคลละเอียดอ่อน และไม่ว่าจะเป็นการเก็บรวบรวมข้อมูลส่วนบุคคลนั้นๆโดยช่องทางใด จะต้องแจ้งที่อยู่ของนโยบายฯ หรือแจ้งเนื้อหาสำคัญที่ระบุอยู่ในนโยบายฯ หรือให้สำเนานโยบายฯ แก่เจ้าของข้อมูลส่วนบุคคลรับทราบ เช่น

- ให้ระบุที่อยู่ในเว็บไซต์ของนโยบายฯ หรือจัดทำเป็น **QR Code** เพิ่มเติมในกรณีที่เหมาะสม
- แจ้งเนื้อหาสำคัญของนโยบายฯ เมื่อติดต่อเจ้าของข้อมูลทางโทรศัพท์ หรือจัดทำเป็นกระดาษเมื่อมีการติดต่อเจ้าของข้อมูลส่วนบุคคลที่ได้พบต่อหน้า
- มอบสำเนานโยบายฯ ให้แก่เจ้าของข้อมูลส่วนบุคคลได้ทันทีเมื่อมีการร้องขอ



ขอบคุณครับ
Thanks You