Tilleke & Gibbins

สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

สรุปสาระสำคัญเกี่ยวกับการปฏิบัติตามกฎหมายลำดับรองภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act)

11 มีนาคม 2567

สวพร สัตตบุศย์ ที่ปรึกษาคณะกรรมการกฎหมายและกฎระเบียบ

อธิษฐา จิตรานุเคราะห์ ที่ปรึกษาคณะกรรมการกฎหมายและกฎระเบียบ

PDPA คืออะไร
ประชาชนจะได้ประโยชน์อะไร

PDPA คือ

Personal Data Protection Act
พ.ร.บ. คุ้มครองข้อมูลส่วนตัว
คือการเก็บ ใช้ เปิดเผย และ
ถ่ายโอนข้อมูลส่วนบุคคลต้อง
ได้รับความยินยอมจากเจ้าของข้อมูล
โดยข้อยกเว้นจะมีเหตุอื่นที่ได้รับ
อนุญาตตามกฎหมาย
บังคับใช้ตั้งแต่ 1 มิ.ย. 2565

สำหรับประชาชนอย่างเรา พ.ร.บ. นี้ทำให้ข้อมูลของเราปลอดภัยมากขึ้น ทุกคนจะใส่ใจข้อมูลส่วนบุคคลมากขึ้น

สิทธิที่ประชาชนจะได้รับ

- มีสิทธิรู้ว่าข้อมูลที่ถูกเก็บไป มีอะไรบ้าง
- ขอโอนข้อมูลตัวเองให้บริษัทอื่นได้
- ขอเข้าถึงสำเนาข้อมูลของตัวเองได้
- ขอหยุดแชร์ข้อมูลและลบเมื่อไรก็ได้

ขอขอบคุณที่มา สำนักงานคณะ กรรมการคุ้มครองข้อมูลส่วนบุคคล, ธปท. (26 พ.ค. 65)

สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

รายชื่อกฎหมายลำดับรองภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล)

ชื่อประกาศ	วันที่ประกาศ	วันที่มีผลใช้บังคับ
ประกาศเรื่อง การจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา 41(2) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2566	14 กันยายน 2566	13 ธันวาคม 2566 (มีผลบังคับใช้แล้ว)
ประกาศเรื่อง หลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศตามมาตรา 28 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2566	25 ธันวาคม 2566	24 มีนาคม 2567
ประกาศเรื่อง หลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศตามมาตรา 29 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2566	25 ธันวาคม 2566	24 มีนาคม 2567
ประกาศเรื่อง มาตรการที่เหมาะสมสำหรับการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการศึกษาวิจัยหรือสถิติตามมาตรา 24 (1) และการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติหรือประโยชน์สาธารณะอื่นตามมาตรา 26 (5) (ง) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2566	8 มกราคม 2567	7 เมษายน 2567
ประกาศเรื่อง หลักเกณฑ์เกี่ยวกับมาตรการคุ้มครองสำหรับการเก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรมที่มิได้กระทำภายใต้การควบคุมของหน่วยงานที่มีอำนาจหน้าที่ตามกฎหมาย พ.ศ. 2566	8 มกราคม 2567	7 เมษายน 2567

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา 41(2) (1/2)

- **ข้อกำหนด:** การดำเนินกิจกรรมซึ่งเป็นส่วนหนึ่งของกิจกรรมหลัก (core activities) นั้นมีความจำเป็นต้องตรวจสอบข้อมูลส่วนบุคคล หรือระบบอย่างสม่ำเสมอ + มีข้อมูลส่วนบุคคลเป็นจำนวนมาก (on a large scale) จะต้องจัดให้มี**เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล** (DPO)

- **กิจกรรมหลัก** (core activities)
  - กิจกรรมที่จำเป็นและมีความสำคัญเพื่อบรรลุวัตถุประสงค์ทางหลักของผู้ควบคุมข้อมูลส่วนบุคคล
  - เช่น การเก็บข้อมูลส่วนบุคคลของลูกค้าเพื่อการให้บริการลูกค้า
  - ไม่รวม กิจกรรมเสริมที่เป็นการสนับสนุนการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคล เช่น การดำเนินงานด้าน IT

- **การดำเนินกิจกรรมที่มีความจำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ** = ที่มีการการติดตาม (track) เฝ้าสังเกต (monitor) วิเคราะห์หรือทำนายพฤติกรรม (profile) ซึ่งเป็นระบบ (systematic) และเกิดขึ้นเป็นประจำ (regular)
  - บัตรสมาชิก, บัตรโดยสารสาธารณะ บัตรอิเล็กทรอนิกส์
  - การพิจารณาเบี้ยประกัน การป้องกันการโกงหรือฉ้อฉล การให้คะแนนเครดิต
  - การโฆษณาตามพฤติกรรม
  - TPA?

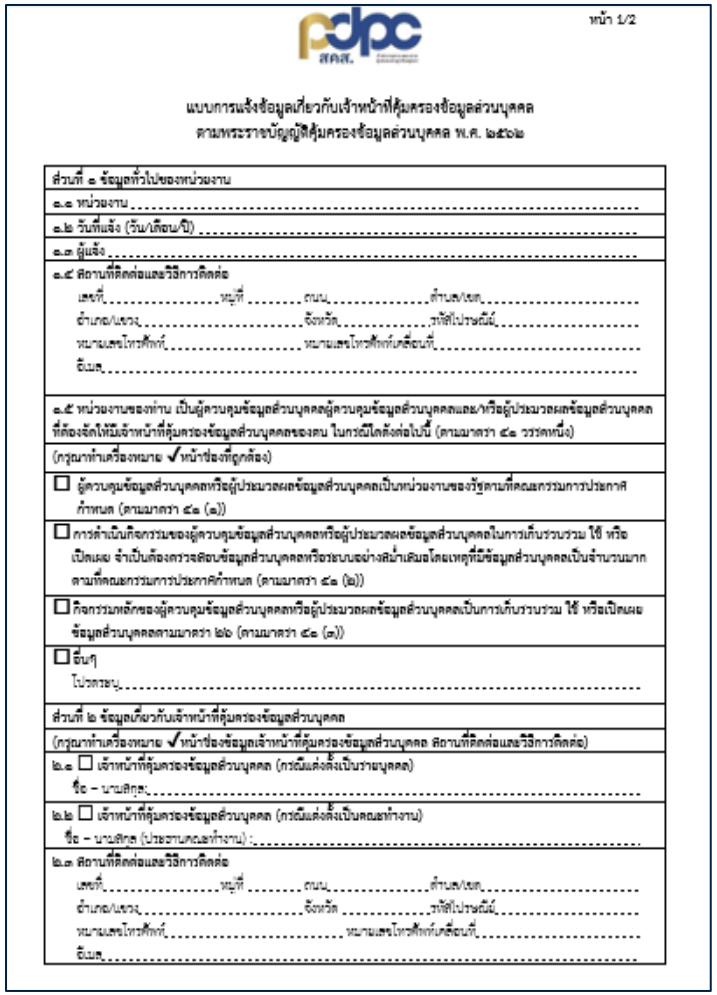
สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา 41(2) (2/2)

- กรณีที่มีข้อมูลส่วนบุคคลเป็นจำนวนมาก
  - มีจำนวนเจ้าของข้อมูลส่วนบุคคล 100,000 คน ขึ้นไป
  - การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของลูกค้าหรือผู้รับบริการตามการดำเนินงานปกติโดยบริษัทตาม**กฎหมายว่าด้วยประกันชีวิต บริษัทตามกฎหมายว่าด้วยประกันวินาศภัย ผู้ประกอบธุรกิจสถาบันการเงิน**ตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน และ **ผู้รับใบอนุญาตประกอบกิจการโทรคมนาคมแบบที่สาม**
- หลักเกณฑ์คุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
  - **ยังไม่มีข้อกำหนดในเรื่องสัญชาติหรือสถานที่ หรือสถานะของบุคคล**
  - “การสวมหมวกสองใบ” (double hatting) สามารถทำได้ – **แต่**การปฏิบัติหน้าที่หรือภารกิจดังกล่าวต้องไม่ขัดหรือแย้งต่อการปฏิบัติหน้าที่ตามพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (ในพรบ. หลัก)
  - เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะต้องสามารถเข้าถึงได้โดยง่าย และควรสามารถสื่อสารภาษาไทยได้ (*อาจมีการประกาศคุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเพิ่มเติมในอนาคต*)

สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

แบบการแจ้งข้อมูลเกี่ยวกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒



หน้า 1/2

แบบการแจ้งข้อมูลเกี่ยวกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

ส่วนที่ ๑ ข้อมูลทั่วไปของหน่วยงาน

๑.๑ หน่วยงาน .....

๑.๒ วันที่แจ้ง (วัน/เดือน/ปี) .....

๑.๓ ผู้แจ้ง .....

๑.๔ สถานที่ติดต่อและวิธีการติดต่อ

เลขที่ ..... หมู่ที่ ..... ถนน ..... ตำบล/แขวง .....
อำเภอ/เขต ..... จังหวัด ..... รหัสไปรษณีย์ .....
หมายเลขโทรศัพท์ ..... หมายเลขโทรศัพท์เคลื่อนที่ .....
อีเมล .....

๑.๕ หน่วยงานของท่าน เป็นผู้ควบคุมข้อมูลส่วนบุคคลผู้ควบคุมข้อมูลส่วนบุคคลและ/หรือผู้ประมวลผลข้อมูลส่วนบุคคล ที่ต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของตน ในกรณีใดกรณีหนึ่งต่อไปนี้ (ตามมาตรา ๔๑ วรรคหนึ่ง)

(กรุณาทำเครื่องหมาย ✓หน้าข้อที่ถูกต้อง)

☐ ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นหน่วยงานของรัฐตามที่คณะกรรมการประกาศกำหนด (ตามมาตรา ๔๑ (๑))

☐ การดำเนินกิจกรรมของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลในการเก็บรวบรวม ใช้ หรือเปิดเผย จำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอโดยเหตุที่มีข้อมูลส่วนบุคคลเป็นจำนวนมาก ตามที่คณะกรรมการประกาศกำหนด (ตามมาตรา ๔๑ (๒))

☐ กิจกรรมหลักของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นการเก็บรวบรวม ใช้ หรือเปิดเผย ข้อมูลส่วนบุคคลตามมาตรา ๒๖ (ตามมาตรา ๔๑ (๓))

☐ อื่นๆ
โปรดระบุ .....

ส่วนที่ ๒ ข้อมูลเกี่ยวกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

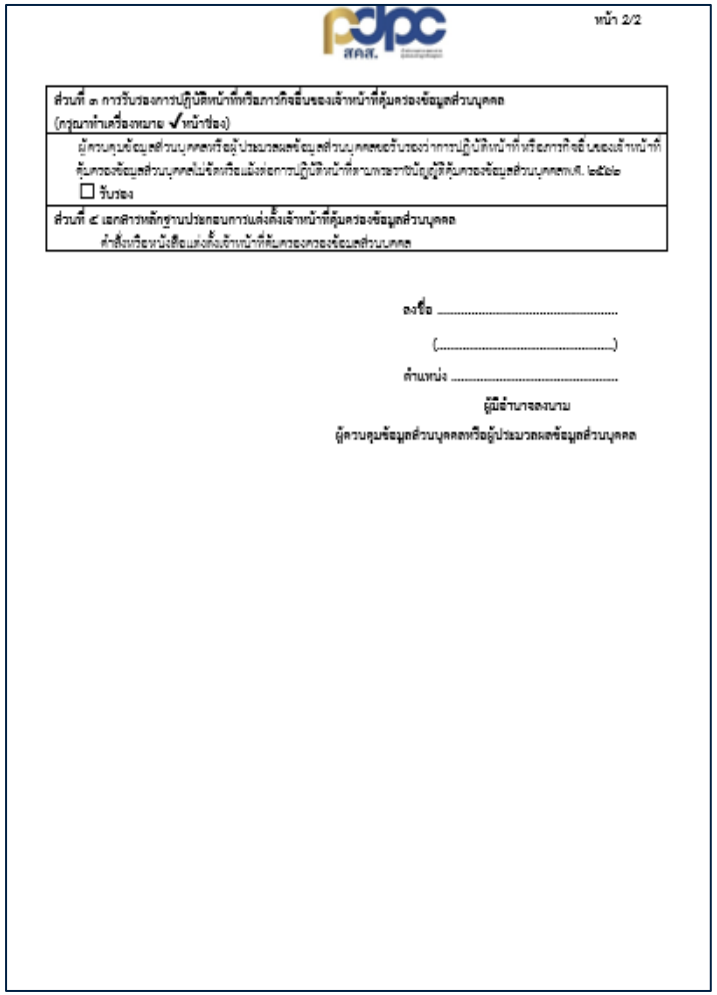
(กรุณาทำเครื่องหมาย ✓หน้าข้อข้อมูลเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล สถานที่ติดต่อและวิธีการติดต่อ)

๒.๑ ☐ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (กรณีแต่งตั้งเป็นรายบุคคล)
ชื่อ – นามสกุล .....

๒.๒ ☐ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (กรณีแต่งตั้งเป็นคณะทำงาน)
ชื่อ – นามสกุล (ประธานคณะทำงาน) .....

๒.๓ สถานที่ติดต่อและวิธีการติดต่อ

เลขที่ ..... หมู่ที่ ..... ถนน ..... ตำบล/แขวง .....
อำเภอ/เขต ..... จังหวัด ..... รหัสไปรษณีย์ .....
หมายเลขโทรศัพท์ ..... หมายเลขโทรศัพท์เคลื่อนที่ .....
อีเมล .....



หน้า 2/2

ส่วนที่ ๓ การรับรองการปฏิบัติหน้าที่หรือภารกิจอื่นของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
(กรุณาทำเครื่องหมาย ✓หน้าช่อง)

ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลขอรับรองว่าการปฏิบัติหน้าที่หรือภารกิจอื่นของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลไม่ขัดหรือแย้งต่อการปฏิบัติหน้าที่ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

☐ รับรอง

ส่วนที่ ๔ เอกสารหลักฐานประกอบการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

คำสั่งหรือหนังสือแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

ลงชื่อ .....

(.....)

ตำแหน่ง .....

ผู้มีอำนาจลงนาม

ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล

สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

หลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ

สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

ประกาศฯ เรื่อง หลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ ตามมาตรา 28

- การบังคับใช้ข้อกำหนดตามมาตรา 28 ของ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล
- นิยาม ***ส่งหรือโอนข้อมูลส่วนบุคคล*** (ไม่รวมถึง การเป็นเพียงสื่อกลาง (intermediary) / การส่งผ่านข้อมูล (data transit) / การเก็บพักข้อมูล (data storage))
- ประเทศปลายทาง/องค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ (“whitelisted countries”)
  - สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล **หรือ เมื่อผู้ควบคุมข้อมูลส่วนบุคคลเสนอ**ให้มีการวินิจฉัย มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอของประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคล ตามมาตรา 28 ได้
- การทบทวนคำวินิจฉัยมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอโดยคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
- หลักเกณฑ์ในการพิจารณามาตรฐานคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ
  - มาตรการหรือกลไกทางกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล
  - หน่วยงานหรือองค์กรที่มีหน้าที่และอำนาจในการบังคับใช้กฎหมายและกฎระเบียบ(อย่างเพียงพอ)

THE PRIVACY ADVISOR

European Commission upholds 11 adequacy decisions

The European Commission released a report 15 Jan. highlighting its review and subsequent reaffirmation of 11 data protection adequacy agreements under the EU General Data Protection Regulation. The Commission found data protection standards of adequacy partners largely remained equivalent to the GDPR or countries moved even closer to EU standards. IAPP News Editor Joe Duball reports on the Commission's findings and what it might mean to the broader EU data transfer landscape in 2024.

สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ ตามมาตรา 29 (1/2)

- นิยาม ***นโยบายในการคุ้มครองข้อมูลส่วนบุคคลในเครือกิจการหรือธุรกิจเดียวกัน*** (binding corporate rules (BCRs))
- BCRs
  - **BCRs ต้องได้รับการตรวจสอบและรับรองโดยสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล**
    - ภาษาที่ควรใช้ในเอกสาร BCRs → ภาษาไทย
    - ใช้ BCRs เมื่อไหร่ และกับข้อมูลแบบไหน?
  - **เนื้อหาที่กำหนด**
    - การมีผลและสภาพบังคับในทางกฎหมายในเครือกิจการ/ ธุรกิจเดียวกัน
    - มีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลและมาตรการรักษาความมั่นคงปลอดภัย ที่สอดคล้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
    - ข้อกำหนดที่รับรองการคุ้มครองข้อมูลส่วนบุคคล สิทธิของเจ้าของข้อมูลส่วนบุคคล และการร้องเรียน สำหรับข้อมูลส่วนบุคคลที่ถูกส่งหรือโอนไปยังต่างประเทศ

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ ตามมาตรา 29 (2/2)

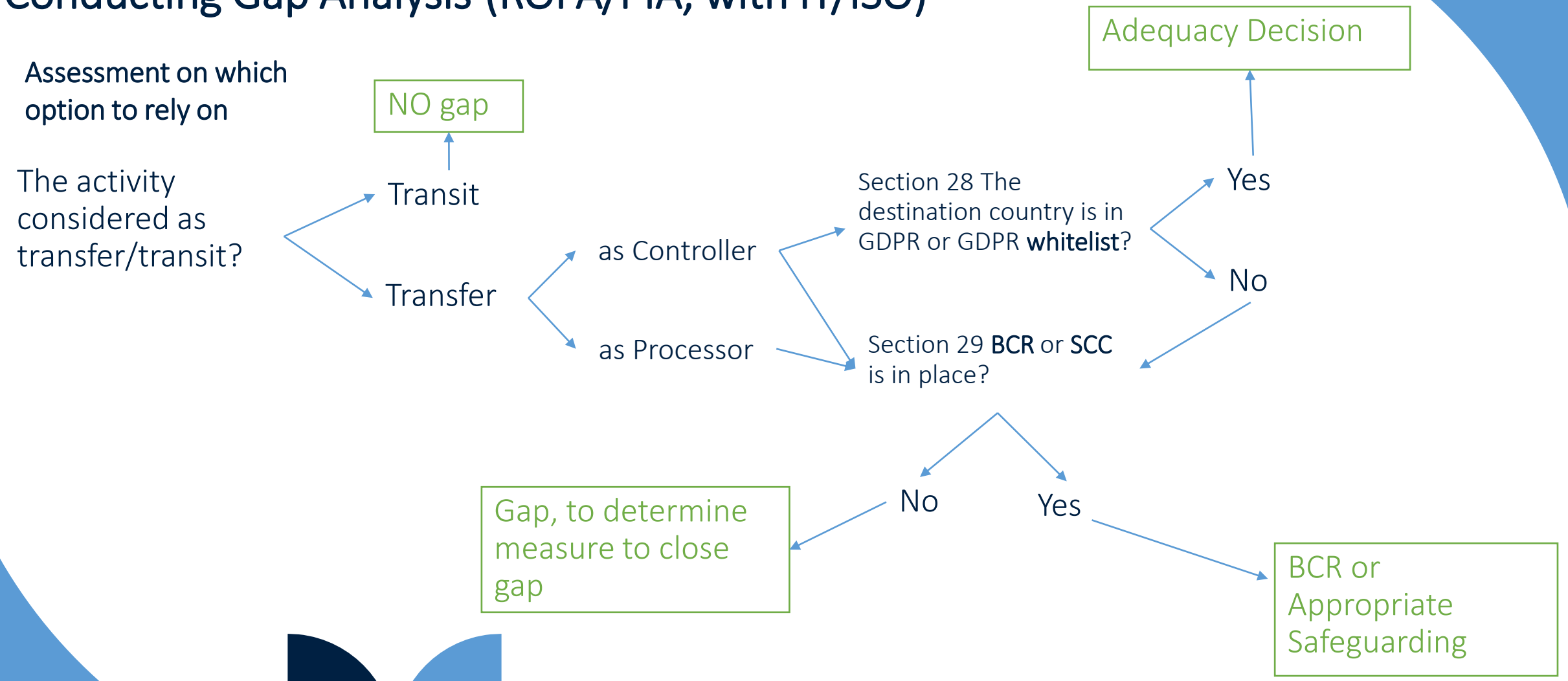
- **มาตรการคุ้มครองที่เหมาะสม (“Appropriate Safeguards”)**
  - กรณียังไม่มีคำวินิจฉัยจากคณะกรรมการฯ เรื่อง ประเทศปลายทาง/องค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ (whitelist)
  - สัญญาในการส่งหรือโอนข้อมูลส่วนบุคคล (Data Transfer Agreement) / Standard Contractual Clauses (SCCs)
    - **ข้อสัญญาที่คู่สัญญาจัดทำขึ้น** จะต้องมีเนื้อหาและข้อกำหนดตามที่ประกาศกำหนด

      (ข้อกำหนดเพิ่มเติม กรณี **ผู้ประมวลผลข้อมูลส่วนบุคคล**เป็นผู้รับข้อมูลส่วนบุคคล/ **ผู้ควบคุมข้อมูลส่วนบุคคล**เป็นผู้รับข้อมูลส่วนบุคคล)
    - **ข้อสัญญาที่จัดทำขึ้นตามกฎหมายต่างประเทศ**

      (GDPR/ASEAN Model clauses + เนื้อหาเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลตามประกาศกำหนด)
  - การรับรอง (Certification) (from other ICOs or privacy regulators)
  - ข้อกำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคลในตราสารหรือข้อตกลงที่มีผลผูกพันทางกฎหมายและสามารถใช้บังคับได้ระหว่างหน่วยงานของรัฐของประเทศไทยกับหน่วยงานของรัฐของประเทศอื่น
  - โทษของผู้ประมวลผลข้อมูล?

สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

Conducting Gap Analysis (ROPA/PIA, with IT/ISO)



สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์เกี่ยวกับมาตรการคุ้มครองสำหรับการเก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรมที่มิได้กระทำภายใต้การควบคุมของหน่วยงานที่มีอำนาจหน้าที่ตามกฎหมาย พ.ศ. 2566

- เว้นแต่กรณีมี**กฎหมายกำหนดไว้** การเก็บรวบรวมประวัติอาชญากรรมจะต้องได้รับความยินยอมโดยชัดแจ้งและเพื่อวัตถุประสงค์ดังต่อไปนี้
  - **การพิจารณารับบุคคลเข้าทำงาน**
  - **ตรวจสอบคุณสมบัติ หรือลักษณะต้องห้าม**
- แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงผลกระทบของการไม่ให้ความยินยอมหรือการถอนความยินยอม
- ระยะเวลาในการเก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรม
  - เก็บรวบรวม**ไว้ได้ไม่เกิน 6 เดือน**นับแต่วันที่ได้ดำเนินการเสร็จสิ้น (เว้นแต่ได้รับความยินยอมโดยชัดแจ้งแล้ว)
- การลบหรือทำลาย หรือทำให้เป็นข้อมูลไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ด้วยวิธีการที่เหมาะสม เมื่อสิ้นสุดระยะเวลาในการเก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรม (in practice, how?)

สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

Conducting Gap Analysis (ROPA/PIA)

ทบทวนกิจกรรมการประมวลผลข้อมูลส่วนบุคคลขององค์กรว่ามีกิจกรรมใดบ้างที่เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรม ตรวจสอบวัตถุประสงค์ในการเก็บรวบรวมให้เป็นไปตามหลักเกณฑ์ของประกาศฯ และปรับปรุง ROPA ให้ครบถ้วนถูกต้องตามประกาศฯ ฝ่ายงานที่เกี่ยวข้อง เช่น

- ฝ่ายบุคคล: การพิจารณาคัดเลือกบุคคลเข้าทำงาน การตรวจสอบคุณสมบัติในระหว่างเป็นพนักงาน เช่น หากทำความผิดอาญาเกี่ยวกับทรัพย์อาจเป็นเหตุในการเลิกจ้างตามข้อบังคับการทำงาน
- ฝ่ายบริหารตัวแทนนายหน้า: การพิจารณาคัดเลือกตัวแทน นายหน้า
- ฝ่ายเลขานุการบริษัท/ฝ่ายกำกับการปฏิบัติตามกฎหมาย/ฝ่ายกฎหมาย: การขออนุมัติแต่งตั้งกรรมการ การจดทะเบียนเปลี่ยนแปลงกรรมการ

หากข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรมมีความจำเป็นต่อการดำเนินการ ต้อง**แจ้งความจำเป็นในการเก็บรวบรวมตั้งแต่ขั้นตอนการประกาศหรือรับสมัคร**

หากต้องขอความยินยอม ต้อง**ตรวจสอบแบบคำขอความยินยอม**ในการเก็บรวบรวม ให้มีการแจ้งผลกระทบของการไม่ให้ความยินยอมหรือถอนความยินยอมเป็นไปตามกฎหมาย

ต้องจัดให้มี**มาตรการเชิงองค์กร มาตรการเชิงเทคนิค รวมถึงมาตรการทางกายภาพ**ที่จำเป็น เช่น

- มาตรการเชิงองค์กร: ทบทวนหรือจัดทำนโยบาย/ระเบียบปฏิบัติ/กระบวนการพิจารณาอนุมัติเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรมให้ชัดเจนและเป็นไปตามประกาศฯ
- มาตรการเชิงเทคนิค: มีรายงานการเข้าถึงข้อมูล การควบคุมการเข้าถึง การยืนยันตัวตนก่อนเข้าถึง การแฝงข้อมูลหรือการเข้ารหัสข้อมูล
- มาตรการเชิงกายภาพ: ไม่จัดเก็บเป็นเอกสาร หากจำเป็นต้องจัดเก็บให้จัดเก็บในห้องหรือตู้ที่มีกุญแจแน่นหนา

เก็บรวบรวมข้อมูลไว้ได้เพียงไม่เกิน 6 เดือนนับจากดำเนินการเสร็จสิ้น เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลหรือมีกฎหมายกำหนดไว้เป็นอย่างอื่น (หากมีกฎหมายอื่นกำหนดไว้ให้เก็บได้นานกว่า 6 เดือนก็สามารถเก็บได้ เช่น เก็บตามอายุความฟ้องร้องคดี)

มีระบบควบคุมและตรวจสอบ เมื่อครบระยะเวลาหรือหมดความจำเป็น ต้องลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลดังกล่าวเป็นข้อมูลที่ไม่สามารถระบุตัวเจ้าของข้อมูลส่วนบุคคลได้

ประกาศเรื่อง มาตรการที่เหมาะสมสำหรับการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการศึกษาวิจัยหรือสถิติตามมาตรา 24 (1) และการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติหรือประโยชน์สาธารณะอื่นตามมาตรา 26 (5) (ง)

"การศึกษาวิจัย" หมายความว่า การดำเนินการเกี่ยวกับการศึกษาค้นคว้า การวิเคราะห์ การทดลอง การทดสอบ หรือการประเมินผลอย่างเป็นระบบ เพื่อให้ได้มาซึ่งความรู้ใหม่หรือหลักการทางวิชาการในสาขาวิชาที่เกี่ยวข้อง รวมถึงการเผยแพร่ความรู้หรือหลักการทางวิชาการนั้น ทั้งที่เป็นการดำเนินการในระดับพื้นฐาน (fundamental or basic) และระดับประยุกต์ (applied) และรวมถึงการพัฒนาเทคโนโลยีและนวัตกรรมจากความรู้หรือหลักการทางวิชาการดังกล่าวด้วย

"สถิติ" หมายความว่า การดำเนินการเกี่ยวกับการเก็บรวบรวม การสำรวจ การประมวลผล การวิเคราะห์ และการสรุปผลจากข้อมูล ตลอดจนการแสดงผลหรือเผยแพร่ผลจากการดำเนินการดังกล่าว ทั้งนี้ เพื่อการเปรียบเทียบหรืออ้างอิงในภาพรวม โดยไม่ได้มุ่งหมายที่จะนำข้อมูลหรือผลจากการดำเนินการดังกล่าวมามีผลต่อการตัดสินใจหรือดำเนินการใดเกี่ยวกับเจ้าของข้อมูลส่วนบุคคลผู้ใดผู้หนึ่ง และให้หมายความรวมถึงการดำเนินงานทางสถิติและการสำรวจตามกฎหมายว่าด้วยสถิติด้วย

สคส.

สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

ประกาศเรื่อง มาตรการที่เหมาะสมสำหรับการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการศึกษาวิจัยหรือสถิติ ตามมาตรา 24 (1) และการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติหรือประโยชน์สาธารณะอื่นตามมาตรา 26 (5) (ง)

[ข้อมูลส่วนบุคคลทั่วไป] การเก็บรวมเพื่อการศึกษาวิจัยหรือสถิติ ตามมาตรา 24 (1)

- มาตรการเชิงองค์กร และมาตรการเชิงเทคนิคที่เหมาะสม
- มาตรการรักษาความมั่นคงปลอดภัยซึ่งจะต้องเป็นไปตามมาตรฐานขั้นต่ำตามพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล
- มาตรการตามมาตรฐานทางจริยธรรมที่เกี่ยวข้อง โดยไม่ขัดต่อกฎหมาย
- อาจพิจารณาดำเนินการทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ หรือมีการแฝงข้อมูล หรือมีการเข้ารหัสข้อมูล หรือมาตรการอื่นในลักษณะเดียวกันอย่างเหมาะสมตามระดับความเสี่ยง

[ข้อมูลส่วนบุคคลที่มีความอ่อนไหว] การเก็บรวบรวมเพื่อการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่นตามมาตรา 26 (5)

- เหตุผลความจำเป็นว่าการเก็บรวบรวมข้อมูลส่วนบุคคลนั้นเป็นกรณีที่มีความจำเป็น
- มาตรการเชิงองค์กร และมาตรการเชิงเทคนิคที่เหมาะสม
- มาตรการรักษาความมั่นคงปลอดภัยซึ่งจะต้องเป็นไปตามมาตรฐานขั้นต่ำตามพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล
- มาตรการตามมาตรฐานทางจริยธรรมที่เกี่ยวข้อง โดยไม่ขัดต่อกฎหมาย

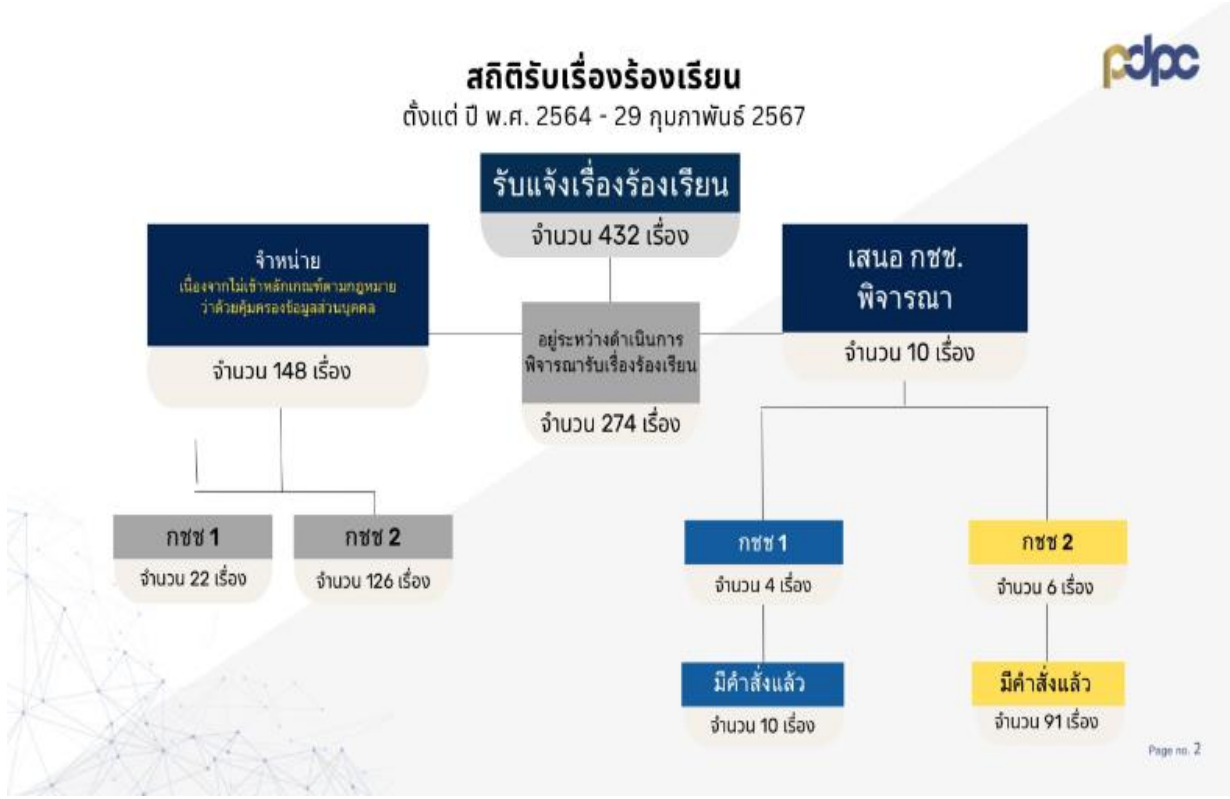
  (คณะกรรมการจริยธรรมการศึกษาวิจัยในคน → พิจารณาอนุมัติ ควบคุมและกำกับดูแลการศึกษาวิจัยหรือสถิติให้เป็นไปตามมาตรฐานทางจริยธรรม)
- อาจพิจารณาดำเนินการทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ หรือมีการแฝงข้อมูล หรือมีการเข้ารหัสข้อมูล หรือมาตรการอื่นในลักษณะเดียวกันอย่างเหมาะสมตามระดับความเสี่ยง

นอกจากมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลยังต้องจัดให้มีมาตรการเพิ่มเติมตามที่ประกาศกำหนด

สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

ข้อสังเกตเพิ่มเติม

- การบังคับใช้กฎหมายของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล, ความเข้าใจในการใช้บังคับของกฎหมาย



สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

คำสั่งคณะกรรมการผู้เชี่ยวชาญ

เรื่องร้องเรียนเกี่ยวกับประเด็นกฎหมาย คุ้มครองข้อมูลส่วนบุคคล

ประเภทธุรกิจประกันภัย

เรื่องการเสนอขายประกันโดยไม่ได้รับความยินยอม

- ผู้ถูกร้องเรียนได้รับข้อมูลส่วนบุคคลมาก่อนพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลใช้บังคับ
- ผู้ร้องเรียนได้รับการเสนอขายประกันทางโทรศัพท์ และได้มีการแจ้งระงับการติดต่อ แต่ผู้ถูกร้องเรียนยังเพิกเฉย
- คณะกรรมการผู้เชี่ยวชาญมีคำสั่งให้ ผู้ถูกร้องเรียนแจ้งการเก็บรวบรวมข้อมูลจากแหล่งอื่น/ ลบข้อมูลส่วนบุคคลของผู้ถูกร้องเรียนฯ

การให้ความร่วมมือและให้ความรู้ทางภาคธุรกิจต่อหน่วยงานที่เกี่ยวข้องมีความสำคัญ

สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

ปัญหาที่พบในภาคธุรกิจ

- การดำเนินการในลักษณะ partnership: non-insurers
  - การกำหนดเงื่อนไขตามกิจกรรมตามหน้าที่
  - ความรับผิดระหว่างกันเมื่อเกิดเหตุละเมิดข้อมูลส่วนบุคคล
- การเกิดเหตุละเมิดข้อมูลส่วนบุคคล (PDPC, OIC)
    - การเริ่มนับระยะเวลา
    - การชดใช้ค่าเสียหายจากเหตุละเมิด (data minimization, wrongful act)
- การดำเนินการของตัวแทนและนายหน้า เมื่อไหร่บริษัทฯ ต้องเข้ามามีส่วนร่วม?
  - การจัดทำสัญญา, privacy notice, การทำการอบรม
- Direct Marketing Act?

สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

พระราชกฤษฎีกาการประกอบธุรกิจบริการแพลตฟอร์มดิจิทัลที่ต้องแจ้งให้ทราบ พ.ศ. 2565

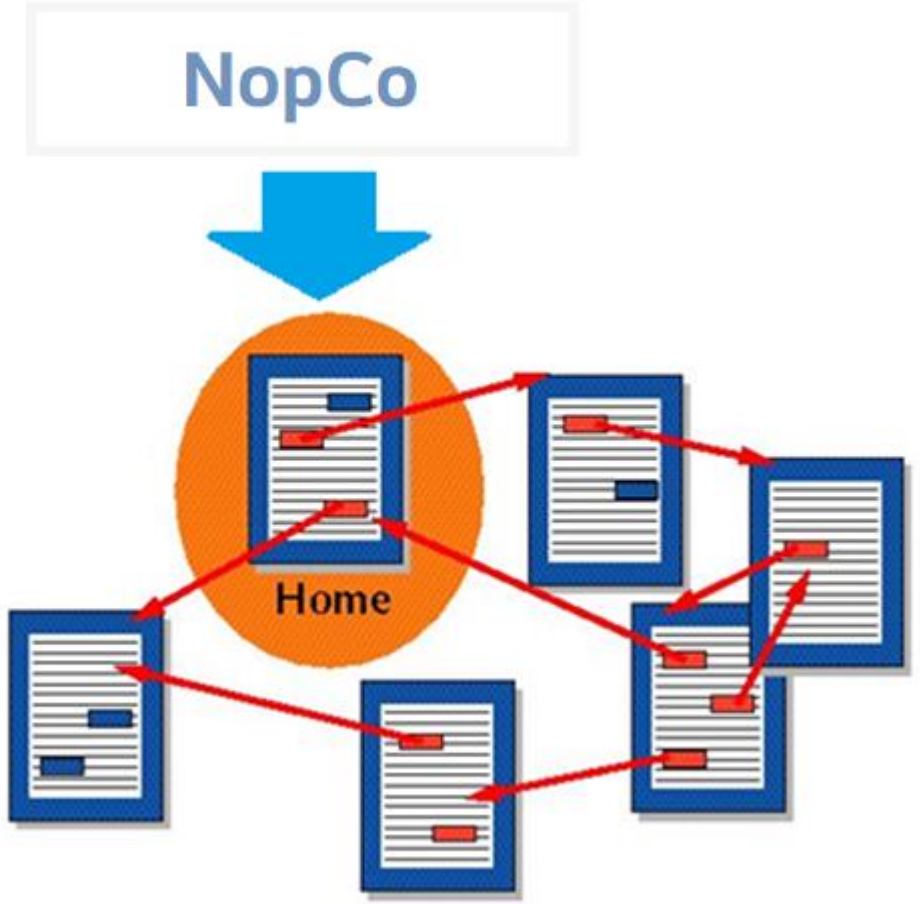
(Royal Decree on Digital Platform Services)

สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

คำจำกัดความ	ความหมาย
DPS/บริการแพลตฟอร์มดิจิทัล	การให้บริการสื่อกลางทางอิเล็กทรอนิกส์ที่มีการบริหารจัดการข้อมูลเพื่อให้เกิดการเชื่อมต่อกันโดยใช้เครือข่ายคอมพิวเตอร์ระหว่างผู้ประกอบการ ผู้บริโภค หรือผู้ใช้บริการ ***เพื่อให้เกิดธุรกรรมทางอิเล็กทรอนิกส์นี้*** (ไม่ว่าจะคิดค่าบริการหรือไม่ก็ตาม) • DPS ทีอยู่ภายใต้บังคับของพรฎ. ฉบับนี้จะต้องแจ้งและปฏิบัติตามเงื่อนไขที่พรฎ. กำหนด • DPS ที่มีไว้เพื่อเสนอสินค้าหรือบริการของผู้ประกอบธุรกิจ DPS หรือบริษัทในเครือซึ่งเป็นตัวแทนของผู้ประกอบธุรกิจ DPS ไม่ตกอยู่ภายใต้บังคับตามพรฎ. นี้ • DPS อยู่ภายใต้การกำกับดูแลของ ธปท. และ กลต. ไม่อยู่ภายใต้พรฎ. ฉบับนี้ เช่นกัน
ผู้ประกอบธุรกิจ DPS	ผู้ประกอบธุรกิจ DPS ซึ่งอาจอยู่ในประเทศไทยหรือนอกประเทศไทย **กฎหมาย DPS มีผลบังคับใช้กับผู้ประกอบธุรกิจ DPS นอกประเทศไทยด้วย หากมีการให้บริการในประเทศไทย

ReMark

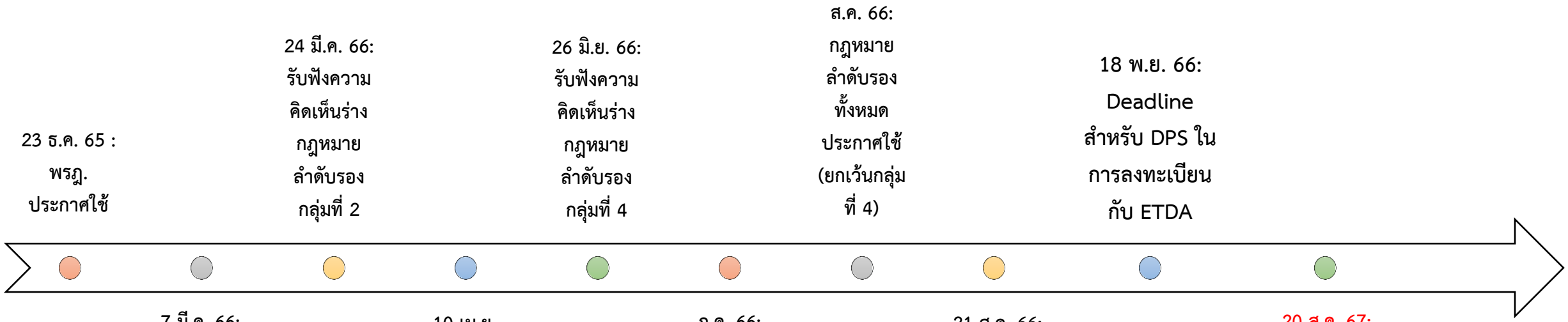
เว็บไซต์ หรือแพลตฟอร์มที่ขายสินค้า หรือบริการของผู้ประกอบธุรกิจ DPS และบริษัทในเครือ แต่มีการแปะ hyperlink หรือ banner ไปยังแพลตฟอร์มอื่น ๆ (ต้องจัดให้มีมาตรการการควบคุมเพื่อป้องกัน hyperlink/banner ที่ผิดกฎหมาย)



Hyperlink

Banner

Timeline การบังคับใช้



สมาคมประกันวินาศภัยไทย
Thai General Insurance Association

Q & A

สมาคมประกันวินาศภัยไทย
Thai General Insurance Association