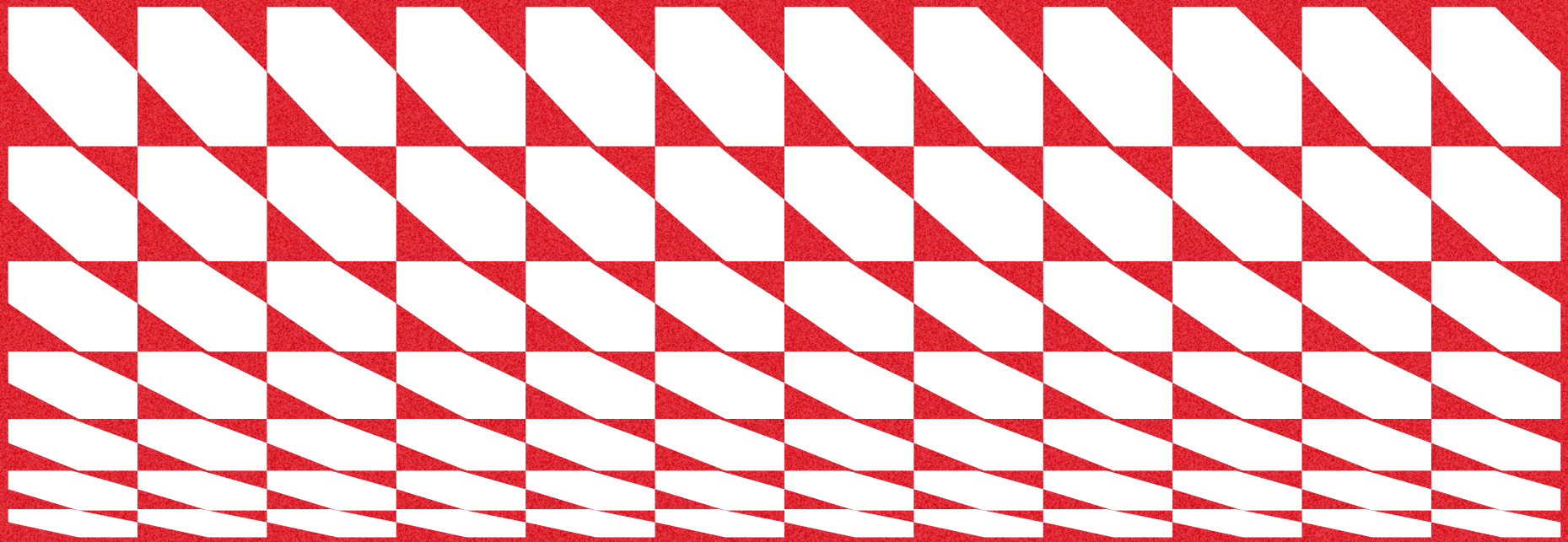
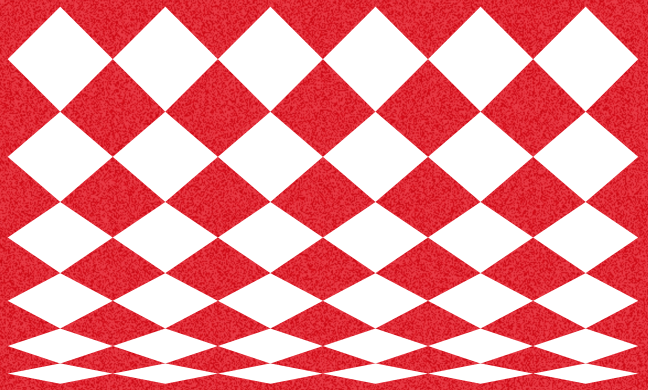


กฎหมายคุ้มครองข้อมูลส่วนบุคคล

นุรัตน์ ปวนคำมา • สำนักวิชานิติศาสตร์ มหาวิทยาลัยแม่ฟ้าหลวง • nurat.pua@mfu.ac.th

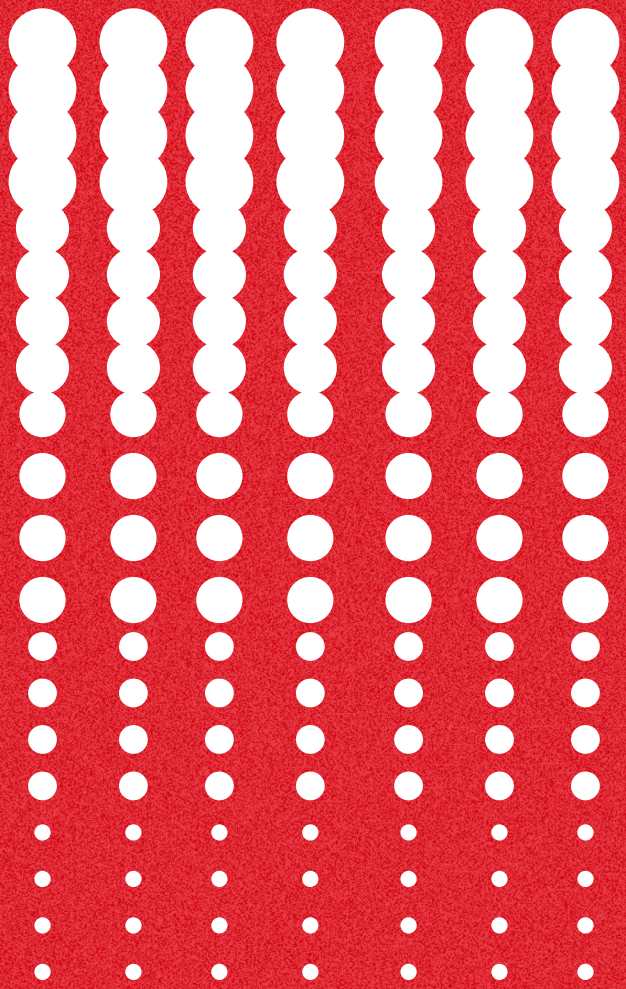
TABLE OF **CONTENTS**



01. บททั่วไปว่าด้วยข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล คืออะไร ?

“ข้อมูลเกี่ยวกับบุคคล ซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ”



คำสำคัญ:

- ข้อมูลของบุคคล + ระบุตัวตนได้
- เป็นข้อมูลของคนที่ยังมีชีวิตอยู่

ข้อมูลส่วนบุคคล มีกี่ประเภท ?

ข้อมูลส่วนบุคคลทั่วไป

ข้อมูลส่วนบุคคลละเอียดอ่อน/
ข้อมูลส่วนบุคคลอ่อนไหว

ข้อมูลส่วนบุคคลทั่วไป

-ชื่อ นามสกุล
-ชื่อเล่น
-วันเกิด
-น้ำหนัก
-ส่วนสูง

-เลขประจำตัวประชาชน
-หนังสือเดินทาง
-เลขบัตรประกันสังคม
-เลขใบอนุญาตขับขี่
-เลขประจำตัวผู้เสียภาษี

-ที่อยู่
-E-mail ส่วนตัว
-หมายเลขโทรศัพท์

-IP address
-Cookie ID
-รหัสเข้าโทรศัพท์/Ipad/โน๊ตบุ๊ค

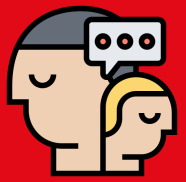
-ทะเบียนรถยนต์
-โฉนดที่ดิน
-เลขบัญชีธนาคาร
-เลขบัตรเครดิต

Facebook/IG/Line

ข้อมูลส่วนบุคคลละเอียดอ่อน

ข้อมูลส่วนบุคคลที่เกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนา หรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด

เชื้อชาติ/เผ่าพันธุ์



ข้อมูลความเชื่อ
ลัทธิ ศาสนา ปรัชญา

ข้อมูลสุขภาพ/
ความพิการ

-กรุ๊ปเลือด
-ผลการตรวจสุขภาพ
-ประวัติการรักษาพยาบาล

ข้อมูลพันธุกรรม/
ข้อมูลชีวภาพ

-ข้อมูลภาพจำลองใบหน้า
-ข้อมูลภาพจำลองม่านตา
-ข้อมูลลายนิ้วมือ
-ข้อมูลพันธุกรรม
-ข้อมูลอัตลักษณ์เสียง

ข้อมูลอื่น ๆ

-ข้อมูลสหภาพแรงงาน
-ความคิดเห็นทางการเมือง
-ประวัติอาชญากรรม
-พฤติกรรมทางเพศ

ขอบเขตการบังคับใช้ ?

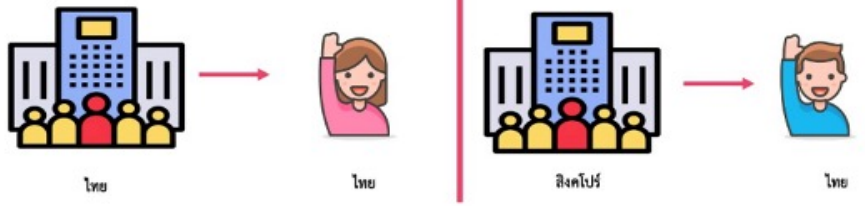
หลักการ: กฎหมายนี้ ใช้บังคับกับกิจกรรมที่มีการนำข้อมูลส่วนบุคคลไปประมวลผล

มีข้อมูลส่วนบุคคล + อยู่ในไทย

เป็นหน่วยงาน/องค์กรที่อยู่ในไทย ไม่ว่าจะเก็บรวบรวม-ใช้-เปิดเผยข้อมูลส่วนบุคคลนั้นใน/นอกไทยก็ตาม

มีข้อมูลส่วนบุคคล + อยู่ต่างประเทศ

เป็นหน่วยงาน/องค์กรที่อยู่ต่างประเทศ แต่มีการเสนอสินค้า/บริการให้เจ้าของข้อมูลในไทย หรือมีการเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลที่เกิดขึ้นในไทย



ขอบเขตการบังคับใช้ ?

หลักการ: กฎหมายนี้ ใช้บังคับกับกิจกรรมที่มีการนำข้อมูลส่วนบุคคลไปประมวลผล

เว้นแต่: 1. เพื่อประโยชน์ส่วนตัว/เพื่อกิจกรรมในครอบครัวของบุคคลนั้น

2. การดำเนินงานของหน่วยงานรัฐ เพื่อประโยชน์ด้านความมั่นคง การรักษาความปลอดภัย การป้องกันปราบปรามการฟองเงิน นิติวิทยาศาสตร์ การรักษาความมั่นคงปลอดภัยไซเบอร์

3. เพื่อกิจการของสื่อมวลชน งานศิลปกรรมหรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพ/เพื่อประโยชน์สาธารณะเท่านั้น

ขอบเขตการบังคับใช้ ?

หลักการ: กฎหมายนี้ ใช้บังคับกับกิจกรรมที่มีการนำข้อมูลส่วนบุคคลไปประมวลผล

เว้นแต่: 4. การประชุมสภา

5. การพิจารณาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการยุติธรรม

6. การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

บุคคลที่เกี่ยวข้องในการคุ้มครองข้อมูลส่วนบุคคล ?

ผู้ประมวลผลข้อมูลส่วนบุคคล

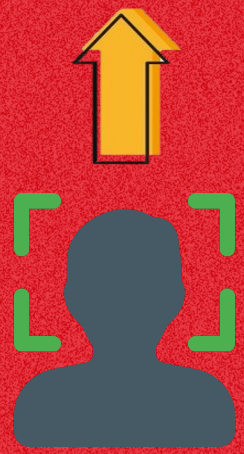
บุคคล/นิติบุคคล ซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคล

บุคคล/นิติบุคคล ซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

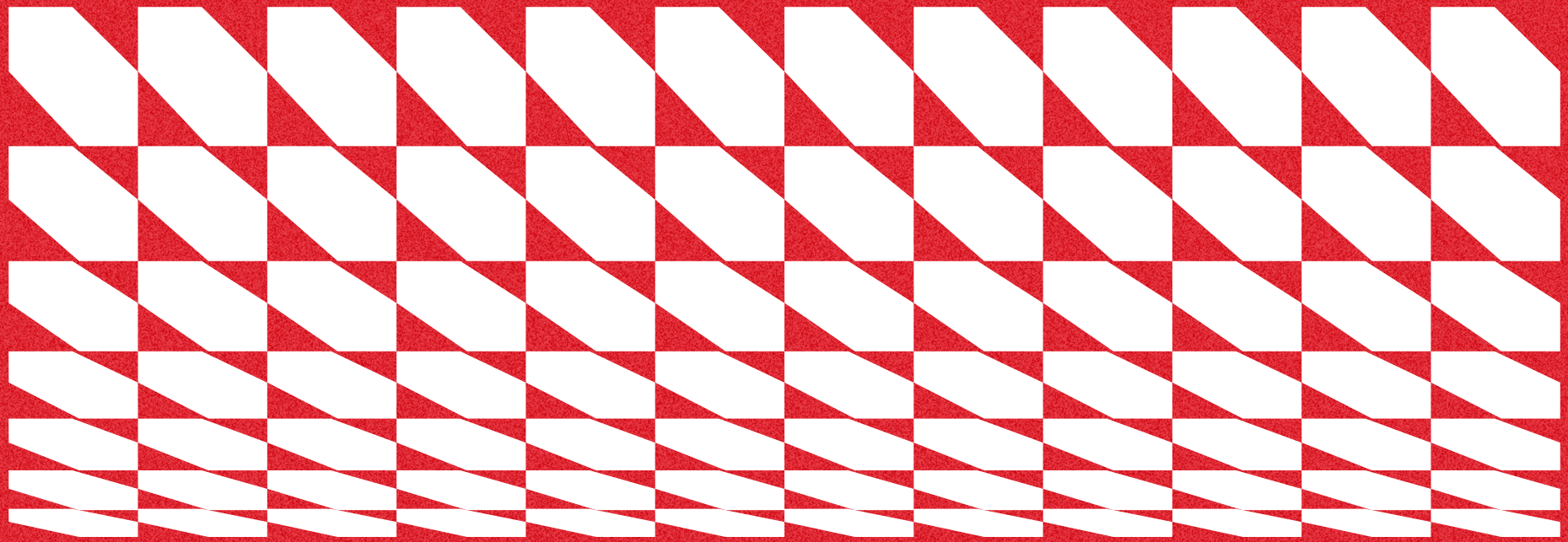
ผู้มีหน้าที่ในการให้คำแนะนำและตรวจสอบการดำเนินงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคล



เจ้าของข้อมูลส่วนบุคคล

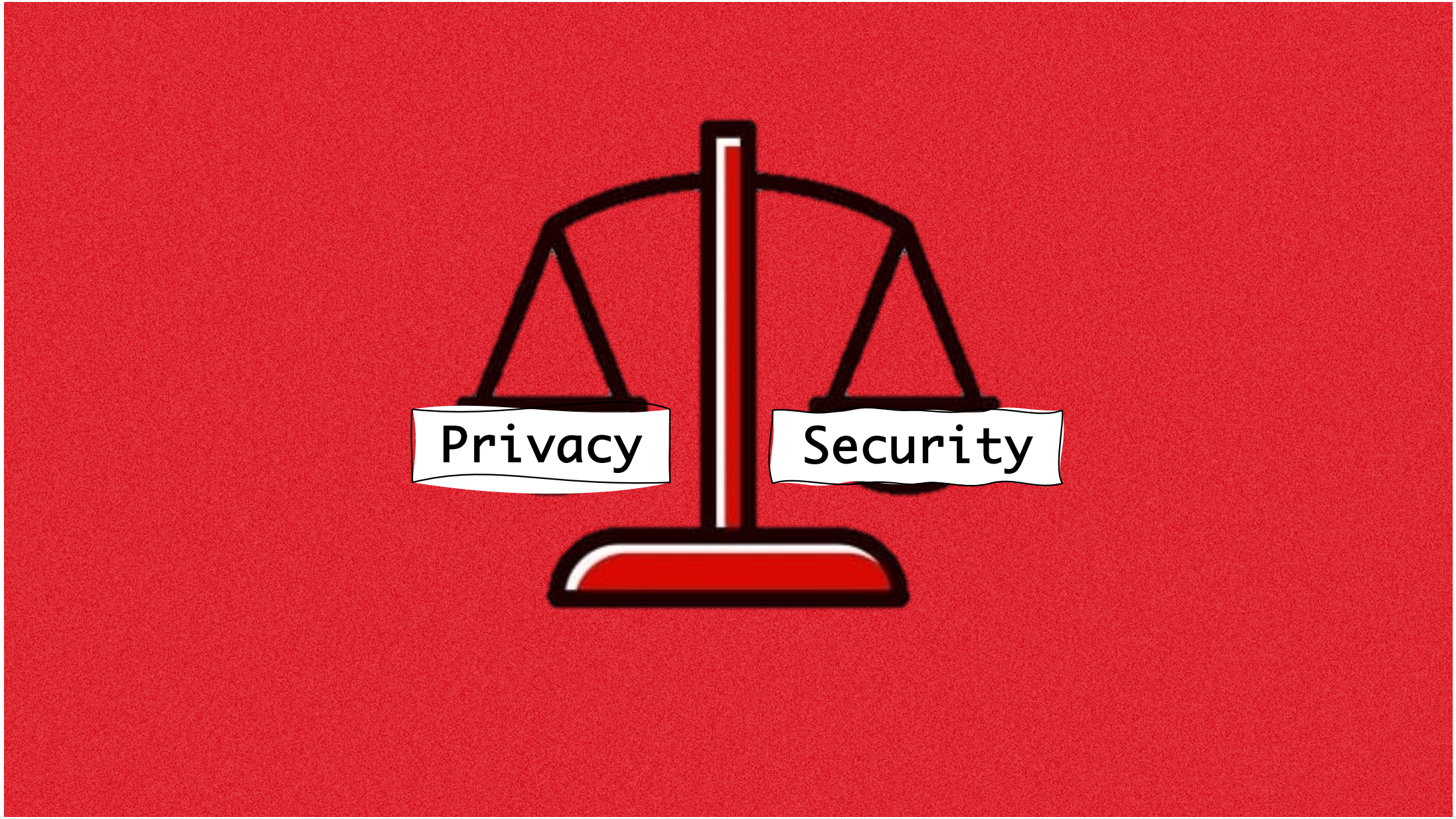
บุคคลที่ข้อมูลส่วนบุคคลระบุไปถึง

02. หลักการคุ้มครองข้อมูลส่วนบุคคล



แนวคิดพื้นฐานในการคุ้มครองข้อมูลส่วนบุคคล

ความยินยอม

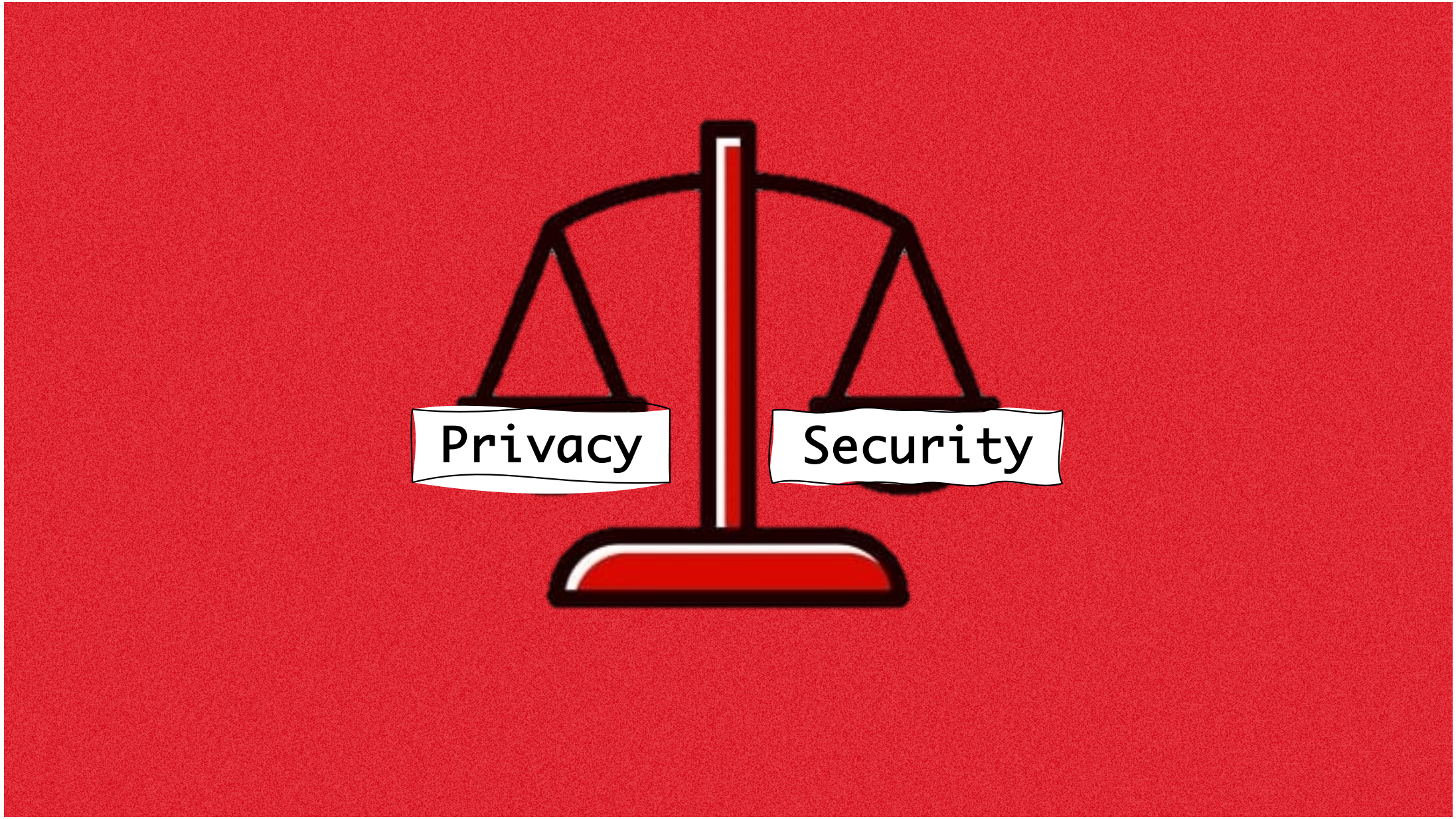

Privacy
Security

หลักการคุ้มครองข้อมูลส่วนบุคคล

: ผู้ควบคุมข้อมูลส่วนบุคคล

เก็บรวบรวม	ใช้	เปิดเผย	เก็บรักษา	ทำลาย
✓ ได้รับความยินยอม ✓ เก็บเท่าที่จำเป็น ✓ แจ้งวัตถุประสงค์	✓ ใช้ /เปิดเผย ต้องเป็นข้อมูลที่เก็บโดยชอบ ✓ ใช้/เปิดเผย ต้องทำตามวัตถุประสงค์ที่แจ้งไว้ ✓ หากโอนข้อมูลไปต่างประเทศ ประเทศปลายทางต้องมีมาตรฐานเพียงพอ	✓ มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล ✓ แจ้งเหตุละเมิดข้อมูลส่วนบุคคล	✓ มีระบบตรวจสอบเพื่อดำเนินการลบ/ทำลาย	

Privacy & Security


Privacy
Security

เจ้าของข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล

หลัก:ต้องเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งไว้ก่อน/ขณะที่เก็บรวบรวม
ม. 21

เก็บรวบรวม

ฐานความยินยอม
ม. 19-20

ข้อมูลส่วนบุคคลทั่วไป
ม. 24

หลัก ต้อง**ขอความยินยอม**จากเจ้าของข้อมูลส่วนบุคคล
เว้นแต่ สัญญา, ระงับอันตรายต่อชีวิต ร่างกาย สุขภาพ, ปฏิบัติหน้าที่ตามกฎหมาย, ภารกิจสาธารณะ/อำนาจรัฐ, ประโยชน์โดยชอบด้วยกฎหมาย, เอกสารประวัติศาสตร์ จดหมายเหตุ วิจัย สถิติ

ข้อมูลส่วนบุคคลละเอียดอ่อน
ม. 26

หลัก ต้อง**ขอความยินยอมโดยชัดแจ้ง**จากเจ้าของข้อมูลส่วนบุคคล
เว้นแต่ เพื่อป้องกัน/ระงับอันตรายต่อชีวิต ร่างกายหรือสุขภาพของเจ้าของข้อมูลส่วนบุคคล + เจ้าของข้อมูลส่วนบุคคลไม่อาจให้ความยินยอมได้, เป็นกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมขององค์กรที่ไม่แสวงหากำไร, เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล, เป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย, เป็นการจำเป็นเพื่อวัตถุประสงค์เกี่ยวกับเวชศาสตร์ป้องกัน/อาชีวเวชศาสตร์ สาธารณสุข แรงงาน การวิจัย หรือประโยชน์สาธารณะสำคัญ

ฐานความจำเป็น
ม. 22

เก็บได้**เท่าที่จำเป็นตามวัตถุประสงค์**ที่ชอบด้วยกฎหมาย

ฐานแจ้งวัตถุประสงค์
ม. 23

ต้องแจ้งให้ทราบ**ก่อน/ขณะ** เก็บรวบรวมข้อมูล; วัตถุประสงค์,แจ้งหน้าที่ต้องให้ข้อมูลเพื่อปฏิบัติตามกฎหมาย/สัญญา/ความจำเป็นในการทำสัญญา, ประเภทข้อมูล+ระยะเวลาการเก็บ, ประเภทของบุคคล/หน่วยงานที่อาจถูกเปิดเผย, ข้อมูลการติดต่อผู้ควบคุมข้อมูล, สิทธิของเจ้าของข้อมูล

ใช้

เปิดเผย

•ใช้/เปิดเผย ต้องเป็นข้อมูลที่เก็บรวบรวมมาโดยชอบ
-ข้อมูลส่วนบุคคลทั่วไป ใช้มาตรา 24*
-ข้อมูลส่วนบุคคลละเอียดอ่อน ใช้มาตรา 26*
*หากเป็นข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอม เมื่อจะใช้/เปิดเผยต้องทำบันทึกการใช้/เปิดเผยในรายการตามมาตรา 39 ด้วย
•ใช้/เปิดเผยต้องทำตามวัตถุประสงค์ที่ได้แจ้งไว้
•หากจะโอนข้อมูลไปต่างประเทศ **ประเทศปลายทางต้องมีมาตรฐานเพียงพอ**

เก็บรักษา

- มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล
- แจ้งเหตุละเมิดข้อมูลส่วนบุคคล

iCloud

Drive

Google

รูปแบบการเก็บรักษา

มาตรการรักษาความมั่นคงปลอดภัยของข้อมูล

เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจ/โดยไม่ชอบ

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
เรื่อง มาตรการรักษาความมั่นคงปลอดภัย
ของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565

ฝ่าฝืน มีความผิดตามมาตรา 83 โทษปรับทางปกครองไม่เกิน 3 ล้านบาท

องค์กร

-**<u>ออกกฎ ระเบียบ วิธีปฏิบัติ</u>** สำหรับควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคล

-**<u>สร้างการตระหนักรู้</u>**แก่ผู้บริหารและผู้ปฏิบัติงาน

เทคนิค

-**<u>จัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลัง</u>**เกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลฯ ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้ หรือเปิดเผย

-**<u>จัดให้มีระบบสำรองและกู้คืนข้อมูล</u>** เพื่อให้ระบบยังสามารถดำเนินการได้อย่างต่อเนื่อง

-**<u>จัดเตรียมเทคโนโลยีเพื่อป้องกันความเสี่ยง</u>**ที่อาจเกิดขึ้นในอนาคต

กายภาพ

-**<u>มีการควบคุมการเข้าถึง</u>**ข้อมูลฯและอุปกรณ์ในการจัดเก็บ โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

-**<u>กำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน</u>**

การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

หน้าที่ในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคล

ไม่มีความ**เสี่ยง**ต่อสิทธิของเจ้าของข้อมูลส่วนบุคคล → **ไม่ต้องแจ้ง แต่ให้บันทึกเหตุ**ไว้เป็นข้อมูลอ้างอิง

มีความ**เสี่ยง**ต่อสิทธิของเจ้าของข้อมูลส่วนบุคคล → **แจ้ง**ให้ สคส. ทราบภายใน **72 ชั่วโมง**นับแต่ทราบเหตุเท่าที่จะสามารถทำได้

มีความ**เสี่ยงสูง**ต่อสิทธิของเจ้าของข้อมูลส่วนบุคคล → **แจ้ง**ให้ สคส. ทราบภายใน **72 ชั่วโมง** นับแต่ทราบเหตุเท่าที่จะสามารถทำได้

แจ้งเหตุให้เจ้าของข้อมูลทราบพร้อมแนวทางการเยียวยาโดยไม่ชักช้า

มาตรา 37(4)

สาเหตุการละเมิดข้อมูลส่วนบุคคล

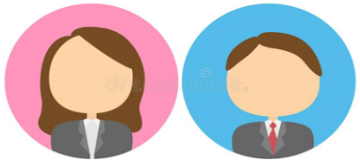
1. เกิดจากบุคคลภายนอก (Outsider)

การแฮกข้อมูล

การ Scamming ที่ทำให้องค์กรปล่อยข้อมูลส่วนบุคคลออกมา

การขโมย Lap-top/ Hard Disk/ USB/เอกสารต่าง ๆ

2. เกิดจากบุคคลภายใน (Insider)



การทำ Lap-top/ เอกสารหาย

การส่งข้อมูลไปยังผู้อื่นที่ไม่ใช่เจ้าของข้อมูลส่วนบุคคล

การเข้าถึง หรือเปิดเผยข้อมูลโดยบุคคลที่ไม่มีอำนาจ

การกำจัด/ทำลายวัตถุ/เอกสารที่มีข้อมูลส่วนบุคคลไม่ถูกวิธี

3. เกิดจาก Computer hardware หรือระบบ Software เกิดข้อผิดพลาด

กรณีตัวอย่างการละเมิดข้อมูลส่วนบุคคล

กรณีที่ 1: เครื่องคอมพิวเตอร์แบบพกพาถูกขโมย

ข้อเท็จจริง: เครื่องคอมพิวเตอร์แบบพกพาถูกขโมย ทำให้ข้อมูลส่วนบุคคลสูญหายไป ซึ่งข้อมูลส่วนบุคคลที่เก็บไว้ประกอบด้วย รายงานการศึกษาทางการแพทย์ แฟ้มข้อมูลการสัมภาษณ์บุคคล และไฟล์ข้อมูลเหล่านั้นไม่มีการเข้ารหัส (Encrypted)

ผลทางกฎหมาย: เกิดการละเมิดข้อมูลส่วนบุคคลขึ้นแล้ว
เหตุผล: ไม่มีมาตรการรักษาความปลอดภัยที่เหมาะสม และไฟล์ดังกล่าวมีข้อมูลส่วนบุคคลอยู่ ทั้งที่ข้อมูลดังกล่าวควรเป็นความลับและไม่สมควรถูกเข้าถึงโดยง่าย การละเลยดังกล่าวจึงขัดต่อหน้าที่และหลักความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล
แนวทางป้องกัน: ควรมีการเข้ารหัส (Encryption) การกำหนดรหัสแทนชื่อบุคคล การกำหนดรหัสผ่าน (Password) สำหรับไฟล์ที่เชื่อมโยงกับรหัสแทนชื่อบุคคล นอกจากนั้นควรมีระเบียบภายในองค์กรเกี่ยวกับขั้นตอนการอนุมัติ

กรณีตัวอย่างการละเมิดข้อมูลส่วนบุคคล

กรณีที่ 2: ส่งอีเมล์ผิด

ข้อเท็จจริง: ฝ่ายจัดหางานแห่งหนึ่งส่งอีเมล์ผิดเกี่ยวกับการอบรมที่จะเกิดขึ้นให้กับบุคคลที่ลงทะเบียนในระบบผู้หางาน โดยส่งไปยังผู้อื่นที่ไม่ใช่ผู้ลงทะเบียน ทำให้มีเอกสารของผู้หางานทั้งหมดถูกแนบไปกับอีเมล์นั้น อันได้แก่ ชื่อ อีเมล์ ที่อยู่ หมายเลขบัตรประกันสังคม ข้อมูลดังกล่าวกระทบต่อผู้หางานกว่า 60,000 คน และบริษัทนี้ก็ได้ติดต่อไปยังผู้ที่รับอีเมล์นั้นให้ลบข้อมูลทั้งหมดและห้ามใช้ข้อมูลเหล่านี้

ผลทางกฎหมาย: เกิดการละเมิดข้อมูลส่วนบุคคลแล้ว
เหตุผล: เพราะมีการเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตหรือนอกวัตถุประสงค์ของเจ้าของข้อมูลส่วนบุคคล ทำให้เกิดการสูญเสียความลับของข้อมูลส่วนบุคคล
แนวทางป้องกัน: สร้างการตระหนักรู้ให้กับพนักงาน

กรณีตัวอย่างการละเมิดข้อมูลส่วนบุคคล

กรณีที่ 3: ถูกโจมตีโดย Ransomware

ข้อเท็จจริง: โรงพยาบาล ถูกโจมตีโดย Ransomware ทำให้ผู้ใช้งานไม่สามารถใช้งานคอมพิวเตอร์และไม่สามารถเข้าถึงข้อมูลผู้ป่วยได้ เนื่องจากมีการเข้ารหัสไฟล์ (Encrypting file) และผู้กระทำเรียกร้องเงินจากโรงพยาบาลเพื่อแลกกับการปลดการเข้ารหัสเพื่อให้ใช้ข้อมูลได้

ผลทางกฎหมาย: เกิดการละเมิดข้อมูลส่วนบุคคลแล้ว

เหตุผล: เพราะข้อมูลส่วนบุคคลถูกเข้าถึงโดยผู้ไม่มีอำนาจ สะท้อนให้เห็นว่า **มาตรการรักษาความปลอดภัยข้อมูลส่วนบุคคลของโรงพยาบาล ที่นำมาใช้ไม่มีประสิทธิภาพ**

แนวทางป้องกัน:

-ควรมีนโยบาย/ขั้นตอนปฏิบัติในการสำรอง (Backup) ข้อมูลอย่างเพียงพอ

-ควรมีนโยบาย/เอกสารขั้นตอนปฏิบัติเพื่อรับมือ Ransomware หรือ Virus อื่น

-สร้างการตระหนักรู้ให้กับพนักงาน เกี่ยวกับการเปิดไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ซึ่งไม่ทราบว่าผู้ส่งเป็นใคร

ทำลาย

มีระบบตรวจสอบเพื่อดำเนินการลบ/ทำลาย

(1) เมื่อพ้นกำหนดระยะเวลาการเก็บรักษา

(2) เป็นข้อมูลส่วนบุคคลที่ไม่เกี่ยวข้อง

(3) เป็นข้อมูลส่วนบุคคลที่เกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวม

(4) เมื่อเจ้าของข้อมูลร้องขอ/ขอถอนความยินยอม

รูปแบบการทำลาย

03.
การเตรียมความพร้อมในทางปฏิบัติ

Check-list การคุ้มครองข้อมูลส่วนบุคคล (ภาคปฏิบัติ)

เจ้าของข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล

ด้าน Privacy

+ หน้าที่ของผู้ควบคุมข้อมูล

- ✓ เก็บรวบรวม
- ✓ ใช้
- ✓ เปิดเผย

ถูกต้องตามกฎหมาย

ข้อมูลส่วนบุคคล

1.แบบฟอร์มการขอความยินยอม (Consent Form)
2. ประกาศความเป็นส่วนตัว (Privacy Notice)

ด้าน Security

- ✓มีมาตรการรักษาความมั่นคงปลอดภัย
- ✓ มีระบบป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ชอบ
- ✓ มีระบบตรวจสอบเพื่อลบ/ทำลาย
- ✓ มีการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

1. แนวปฏิบัติเกี่ยวกับการเข้าถึงข้อมูลส่วนบุคคลในหน่วยงาน
2. ระบบการลบ/ทำลายข้อมูลส่วนบุคคล
3. บันทึกการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activity: ROPA)
4. สัญญาประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement)

Check-list การคุ้มครองข้อมูลส่วนบุคคล (ภาคปฏิบัติ)

ข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคล

ด้าน Privacy

+ หน้าที่ของผู้ควบคุมข้อมูล

- ✓ เก็บรวบรวม
- ✓ ใช้
- ✓ เปิดเผย

} ถูกต้องตามกฎหมาย

1.แบบฟอร์มการขอความยินยอม (Consent Form)

2. ประกาศความเป็นส่วนตัว (Privacy Notice)

ตัวอย่างแบบฟอร์มขอความยินยอม

เอกสารแสดงความยินยอม (Consent Form)

วันที่_____

ในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของท่าน อปท. มีวัตถุประสงค์ดังต่อไปนี้

1. เพื่อ.....
2. เพื่อ.....
3. เพื่อ.....

ซึ่งประเภทข้อมูลส่วนบุคคลที่อปท. ใช้ในการเก็บรวบรวม ใช้หรือเปิดเผย (“ประมวลผล”) ได้แก่

.....

.....

ก่อนการแสดงเจตนาข้าพเจ้าได้อ่านรายละเอียดจากเอกสารชี้แจงข้อมูลหรือได้รับคำอธิบายจากอปท. ถึง**วัตถุประสงค์**ในการเก็บรวบรวม ใช้และเปิดเผยข้อมูลส่วนบุคคล และมีความเข้าใจดีแล้ว

ข้าพเจ้าให้ความยินยอมหรือปฏิเสธไม่ให้ความยินยอมในเอกสารนี้ด้วยความสมัครใจ ปราศจากการบังคับหรือชักจูง และข้าพเจ้าทราบว่าข้าพเจ้าสามารถถอนความยินยอมนี้เสียเมื่อใดก็ได้ โดยผ่านช่องทาง.....

เมื่อได้อ่านข้อความครบถ้วนแล้ว ข้าพเจ้า

❒ “ให้” ความยินยอม ❒ “ไม่ให้” ความยินยอม

ลงชื่อ.....เจ้าของข้อมูลส่วนบุคคล

(..... ชื่อ-นามสกุล ตัวบรรจง .....)

ทั้งนี้ ท่านสามารถอ่านรายละเอียดในประกาศความเป็นส่วนตัว (Privacy Notice) ของอปท. ได้ ทาง .....

QR Code

ตัวอย่างประกาศความเป็นส่วนตัว

ประกาศเกี่ยวกับความเป็นส่วนตัวของ อปท. (Privacy Notice)

****

อปท. ตระหนักและให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการ โดยถือปฏิบัติอย่างเคร่งครัดในเรื่องการเคารพสิทธิความเป็นส่วนตัวเป็นสำคัญ

คำประกาศเกี่ยวกับความเป็นส่วนตัวฉบับนี้ จึงถูกจัดทำขึ้นเพื่อให้ท่านในฐานะเจ้าของข้อมูลส่วนบุคคลได้ทราบรายละเอียดของวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผย (รวมเรียกว่า “**ประมวลผล**”) ข้อมูลส่วนบุคคล รวมทั้งสิทธิต่าง ๆ ของท่านภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ทั้งนี้ การประมวลผลข้อมูลส่วนบุคคลของท่านตามวัตถุประสงค์ในประกาศนี้ อปท.ดำเนินการในฐานะ**ผู้ควบคุมข้อมูลส่วนบุคคล** (DataController) ซึ่งหมายความว่า อปท. เป็นผู้มีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

- คำนิยาม
- ฐานกฎหมายในการประมวลผลข้อมูลส่วนบุคคล
- ประเภทของข้อมูลส่วนบุคคลที่จัดเก็บ
- วัตถุประสงค์ในการประมวลผลข้อมูล
- การใช้
- การเปิดเผย
- การรักษาความมั่นคงปลอดภัยของข้อมูล
- การเก็บรักษา
- ระยะเวลา/ทำลาย
- สิทธิและช่องทางร้องเรียนของเจ้าของข้อมูล

เว็บไซต์ของหน่วยงานมีนโยบายคุกกี้ (Cookies Policy)

หน้าแรก | เจ้าหน้าที่ | ประกาศเกี่ยวกับความเป็นส่วนตัว | ข้อมูลเผยแพร่ | การขอใช้สิทธิ์ข้อมูลส่วนบุคคล | ติดต่อเรา

นโยบายการใช้คุกกี้ (Cookies Policy)

เมื่อท่านได้เข้าสู่เว็บไซต์ของเรา ข้อมูลที่เกี่ยวข้องกับการเข้าสู่เว็บไซต์ของท่านจะถูกเก็บเอาไว้ในรูปแบบของคุกกี้ โดยนโยบายคุกกี้นี้จะอธิบายถึงความหมาย การทำงาน วัตถุประสงค์ รวมถึงการลบและการปฏิเสธการเก็บคุกกี้เพื่อความเป็นส่วนตัวของท่าน โดยการเข้าสู่เว็บไซต์นี้ ถือว่าท่านได้อนุญาตให้เราใช้คุกกี้ตามนโยบายคุกกี้ที่มีรายละเอียด ดังต่อไปนี้

คุกกี้คืออะไร

คุกกี้ คือ ไฟล์ข้อมูลขนาดเล็ก เพื่อจัดเก็บข้อมูลโดยจะบันทึกลงไปในอุปกรณ์คอมพิวเตอร์ และ/หรือ เครื่องมือสื่อสารที่เข้าใช้งานของท่าน เช่น แท็บเล็ต, สมาร์ทโฟน ผ่านทางเว็บเบราว์เซอร์ในขณะที่ท่านเข้าสู่เว็บไซต์ของเรา เว็บไซต์ของมหาวิทยาลัยอาจใช้คุกกี้ในบางกรณี

มหาวิทยาลัยแม่ฟ้าหลวง ใช้คุกกี้เฉพาะเพื่อการจัดเก็บข้อมูลที่อาจเป็นประโยชน์ต่อเจ้าของข้อมูลในครั้งถัดไปที่เจ้าของข้อมูลกลับมาเยี่ยมชมเว็บไซต์ของบริษัทฯ เมื่อเจ้าของข้อมูลเข้าใช้บริการเว็บเบราว์เซอร์ เจ้าของข้อมูลสามารถตั้งค่าเพื่อยอมรับคุกกี้ทั้งหมดหรือปฏิเสธคุกกี้ทั้งหมด หรือแจ้งเตือนให้เจ้าของข้อมูลทราบเมื่อมีการส่งคุกกี้ โดยเจ้าของข้อมูลสามารถเข้าไปตั้งค่าที่เมนู "ความช่วยเหลือ" ในเบราว์เซอร์เพื่อเรียนรู้วิธีการเปลี่ยนแปลงการใช้คุกกี้ของเจ้าของข้อมูลได้ โปรดทราบว่าการปิดการใช้งานคุกกี้อาจส่งผลต่อการใช้งานบางบริการของเจ้าของข้อมูลได้

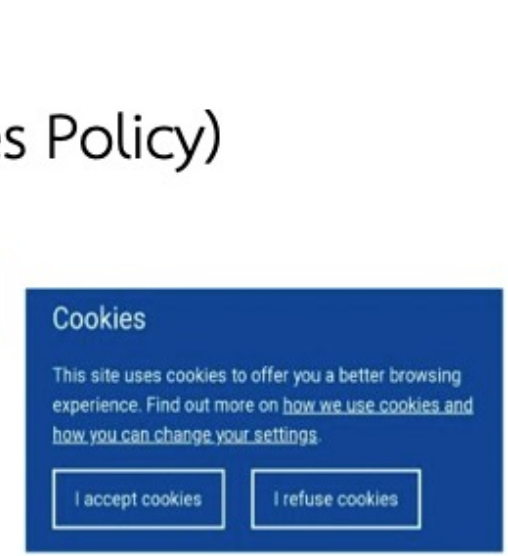
คุกกี้ใช้อย่างไร

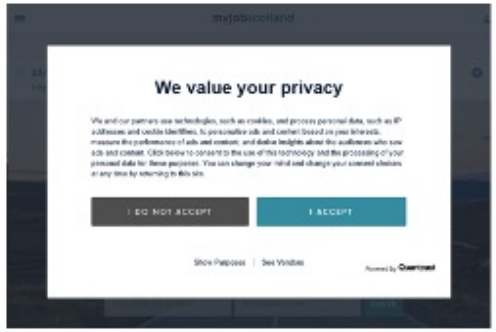
เราใช้คุกกี้เพื่อเพิ่มประสบการณ์และความพึงพอใจของท่าน โดยจะทำให้เราเข้าใจลักษณะการใช้งานเว็บไซต์ของท่านได้เร็ว และทำให้เว็บไซต์ของเราเข้าถึงได้ง่าย สะดวกยิ่งขึ้น บางกรณีเราจำเป็นต้องให้บุคคลที่สามดำเนินการ ซึ่งอาจจะต้องใช้อินเตอร์เน็ตโปรโตคอล แอดเดรส (IP Address) และคุกกี้เพื่อวิเคราะห์ทางสถิติ ตลอดจนเชื่อมโยงข้อมูลและประมวลผลตามวัตถุประสงค์ทางการตลาด

ประเภทของคุกกี้ที่ถูกใช้

ข้อมูลเผยแพร่

- พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล
- นโยบายธรรมาภิบาลข้อมูล
- นโยบายการคุ้มครองข้อมูลส่วนบุคคล
- นโยบายการใช้คุกกี้
- Template เอกสาร PDPA
- ข่าวสาร PDPA





Check-list การคุ้มครองข้อมูลส่วนบุคคล (ภาคปฏิบัติ)

ด้าน Security

✓มีมาตรการรักษาความมั่นคงปลอดภัย

✓ มีระบบป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ชอบ

✓ มีระบบตรวจสอบเพื่อลบ/ทำลาย

✓ มีการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

1. แนวปฏิบัติเกี่ยวกับการเข้าถึงข้อมูลส่วนบุคคลในหน่วยงาน
2. ระบบการลบ/ทำลายข้อมูลส่วนบุคคล
3. บันทึกการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activity: ROPA)
4. สัญญาประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement)

ตัวอย่าง แบบฟอร์มบันทึกการเข้าถึงข้อมูลส่วนบุคคล

อปท.....

ฝ่าย/แผนก/ส่วนงาน:

วัน/เดือน/ปี	ผู้ขอใช้สิทธิเข้าถึงข้อมูล (ชื่อ/ตำแหน่ง/หน่วยงาน)	กิจกรรมที่ขอเข้าถึง (เช่น ขอรายชื่อพนักงาน,การเบิกจ่ายสวัสดิการ)	รูปแบบการจัดเก็บข้อมูลส่วนบุคคล (เอกสาร/อิเล็กทรอนิกส์)	ข้อมูลส่วนบุคคลที่เกี่ยวข้อง (โปรดระบุ เช่น ชื่อ นามสกุล ที่อยู่ หมายเลขโทรศัพท์)	ประเภทข้อมูล		วัตถุประสงค์ในการเข้าถึง	ระยะเวลาการเข้าถึง	การส่ง/โอนข้อมูลไปยังหน่วยงานอื่น (ภายใน/ภายนอก อปท.)	มาตรการดูแลรักษาความปลอดภัยของข้อมูล	ผู้อนุมัติการเข้าถึง
					ข้อมูลทั่วไป	ข้อมูลอ่อนไหว					

ตัวอย่าง แบบฟอร์มบันทึกการทำลายข้อมูลส่วนบุคคล

อปท. .....

ฝ่าย/แผนก/ส่วนงาน :

วัน/เดือน/ปี	กิจกรรมที่จัดเก็บ (เช่น การบรรจุเจ้าหน้าที่/การเบิกจ่ายสวัสดิการ/การสมัครงาน)	ข้อมูลส่วนบุคคลที่เกี่ยวข้อง (โปรดระบุ เช่น ชื่อ นามสกุล ที่อยู่ หมายเลขโทรศัพท์)	ประเภทข้อมูล		รูปแบบการจัดเก็บข้อมูล (เอกสาร/อิเล็กทรอนิกส์)	ระยะเวลาการจัดเก็บ	วิธีการทำลาย	ผู้อนุมัติการทำลาย
			ข้อมูลทั่วไป	ข้อมูลอ่อนไหว				

ตัวอย่าง ROPA

ข้อมูลส่วนบุคคลที่เก็บรวบรวม	วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคล		ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล/ตัวแทน + DPO+ ช่องทางติดต่อ	ระยะเวลาการเก็บรักษาและการลบ	สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล	การใช้/เปิดเผยข้อมูลที่ได้รับยกเว้นไม่ต้องขอความยินยอม	การปฏิเสธคำขอ/การคัดค้าน	มาตรการรักษาความมั่นคงปลอดภัย
	ข้อมูลส่วนบุคคลทั่วไป	ข้อมูลส่วนบุคคลอ่อนไหว						

ตัวอย่างสัญญาประมวลผลข้อมูล

- กิจกรรมการประมวลผลข้อมูลส่วนบุคคล
- มาตรการด้านความมั่นคงปลอดภัย
- คำสั่ง/วิธีการประมวลผลข้อมูลส่วนบุคคลของผู้ควบคุมฯ
- มาตรการด้านความมั่นคงปลอดภัยพิเศษกรณีมีการประมวลผลข้อมูลอ่อนไหว
- การจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล
- การลบ/ทำลายข้อมูลส่วนบุคคลภายหลังจากประมวลผลเสร็จสิ้น
- แจ้งผู้ควบคุมกรณีมีการละเมิดข้อมูลส่วนบุคคล
- หน้าที่ความรับผิดของผู้ประมวลผลข้อมูลส่วนบุคคล

THANKS!